Athens Institute for Education and Research
ATINER

ATINER's Conference Paper Series
COM2016-1986

The Effects of National Culture on the Implementation of ISM Standards based on the ISO 27001

Bahareh Shojaie
PhD Candidate
The University of Hamburg
Germany

Hannes Federrath
Professor
The University of Hamburg
Germany

Iman Saberi
PhD Candidate
Technical University of Hamburg
Germany

ATINER CONFERENCE PAPER SERIES No: COM2016-1986

An Introduction to ATINER's Conference Paper Series

ATINER started to publish this conference papers series in 2012. It includes only the papers submitted for publication after they were presented at one of the conferences organized by our Institute every year. This paper has been peer reviewed by at least two academic members of ATINER.

Dr. Gregory T. Papanikos
President
Athens Institute for Education and Research

This paper should be cited as follows:

Shojaie, B., Federrath, H. and Saberi, I. (2016). **"The Effects of National Culture on the Implementation of ISM Standards based on the ISO 27001",** Athens: ATINER'S Conference Paper Series, No: **COM2016-1986.**

Athens Institute for Education and Research
8 Valaoritou Street, Kolonaki, 10671 Athens, Greece
Tel: + 30 210 3634210 Fax: + 30 210 3634209 Email: info@atiner.gr URL: www.atiner.gr
URL Conference Papers Series: www.atiner.gr/papers.htm

ISSN: 2241-2891
22/09/2016

The Effects of National Culture on the Implementation of ISM Standards based on the ISO 27001

Bahareh Shojaie

Hannes Federrath

Iman Saberi

Abstract

This paper analyses the reasons for creating national security standards and laws in contrast to applying the most adopted international ISO/IEC 27001 standard. The ISO 27001 is popular among several countries and industries, because it offers market assurance and IT governance by protecting sensitive information in a structured way. Recent literature has indicated that cultural characteristics influenced the information security. This paper investigates the main differences between the studied national security standards and the ISO 27001 to investigate the reasons for the ISO 27001 low adoption rate. This paper answers the question whether national IS guidelines influence the adoption rate of the ISO 27001, with building a relationship between national cultural characteristics and the ISO 27001 performance. This paper presents the most applicable cultural dimensions with respect to the ISO 27001 to point out new ways of enhancing this standard long-term performance. Moreover, this study uncovers national and socio-economic barriers, which should be taken into account during future development of the ISO 27001 as well as when measuring its effectiveness and adoption rate. The results indicated that national characteristics and cultural barriers are important reasons for the ISO 27001 low adoption rate, which influence national security guidelines selection and performance.

Keywords: ISMS (Information Security Management Systems), ISO 27001 Annual-growth, National Culture, National Security Guidelines, ISO/IEC 27001.

Introduction

Organisations' IS (information security) characteristics and needs provide distinctive requirements and motivations for establishing an ISMS, as there are various IS standards and guidelines types to comply with. ISO 27001 is the first international ISM standard that offers a certification (ISO/IEC, 2005). Although ISO 27001 provides comprehensive ISMS specifications, requirements and a catalogue for measures (Henson 2015), there are several national IS standards and guidelines developed in different countries.

Implementing ISO 27001 provides several benefits for organisations, as they have an acceptable up to date IS level, according to the IS requirements and regular audits (ISO/IEC, 2005). Customer demand is one of the most important reasons for implementing ISO 27001 (Shojaie et al., 2014) especially for organisations handling confidential data of their customers. The ISO 27001 can help management significantly to prove an acceptable level of data protection, in case of security incidents (Fomin and Barlette, 2008).

The ISO 27001 gets the benefits of long-term experiences of former best practices, which certification is essential for organisations to meet legal or stakeholders' requirements, or generally a precondition to apply for tenders. Especially, in the case of litigation or regress claims (on the grounds of inadequate information security), the ISO 27001 certification may be significantly beneficial (ISO/IEC, 2013).

Most of the countries with a high number of ISO 27001 certificates (ISO, 2014) have a strong national economy level (such as China or Japan) and they are interested in ISM standards because of their global activities. Interestingly, the United States, which have the biggest national economy, was ranked relatively lower (ISO/IEC, 2013) compared to the top 10 countries with the highest ISO 27001 annual-growth. Cultural characteristics and barriers are possibly two of the reasons for this relatively low adoption rate.

Based on the authors' best knowledge, most of the prevailing literature focused on comparisons between one national IS guideline (or ISM standard) and the ISO 27001 (Arora, 2010; Beckers et al., 2014; Gikas, 2010). In contrast, this paper investigates the cultural influences of adopting ISO 27001 among the countries with national IS guidelines, which gets benefits of the most leading cultural literature, selected national dimensions and the ISO 27001 survey 2014 (ISO, 2014) statistics.

This paper is structured as follows: Literature Section reviews the prevailing ISMS literature; and it introduces the most leading cultural publications applicable to national IS guidelines foundation as well as the ISO 27001 adoption. Discussion and Results Section analyses the national IS guidelines development, selection and comparison as the main contribution of the paper. This section provides advices for improving the ISO 27001 adoption rate in countries with the national IS guidelines, based on the former analysis. Besides that, the last part of Discussion and Results Section demonstrates the

results of the ISO 27001 survey 2014 (ISO, 2014) analysis, and the relationship with the selected cultural dimensions. This last section provides recommendations for countries with the ISO 27001 low adoption rate. Finally, there is the Conclusions Section.

Literature

The first part discussed the national IS guidelines and the ISO 27001, and the second part analysed the most leading national cultural literature (Hofstede and Gelfand) applicable to the studied ISM standards and guidelines.

IT systems are considerably influenced by social, economic and political structures, as common national characteristics (Henson, 2015). The interaction between organisations' insiders and the IT systems (with different purposes and technical knowledge) can result in high complexity. As a result, organisations usually use standards to reduce the systems complexity (ISO/IEC, 2005). For example, developing ISM standards has several advantages, such as reducing costs, improving system compatibility and information exchange, as well as establishing a basic security level in all organisational systems and processes.

Currently, one of the most implemented standards is the ISO 27001:2013, (with more than 24000 certificates in diverse countries and economies - the Appendix "ISO 27001 worldwide annual-growth" (ISO, 2014)), which outlines comprehensive organisational requirements for developing the ISMS. However, former national guidelines and standards are mainly based on providing risk mitigation procedures for organisations and governments (Maier, 2014). National security Guidelines are mainly limited to technical aspects rather than strategic features of developing the ISMS (Gikas, 2010). Based on the authors' best knowledge (Kuligowski, 2009; Arora, 2010), Becker's publication is one of the most adopted frameworks for comparing and analysing several types of ISM standards (Beckers et al., 2014).

Former publications mainly focused on the influences of cultural characteristics on the IS tasks (Katsikas et al., 2005; Tsohou et al., 2007; Schlienger and Teufel, 2003; Schein, 2010). According to the recent literature (Torres et al., 2006; Yanus and Shin, 2007; Fomin and Barlette, 2008; Barlette and Fomin, 2010; Henson, 2015) one of the critical success factors for ISMS development is to implement the IS guidelines as a part of the organisations' culture. The other success factor is to get the management high level of support and engagement (in terms of resources such as budget, and required level of insiders' training and awareness). Internal audits and consistent updates and improvements are key features for preserving the efficiency of an ISM standard (Shojaie et al., 2015).

One of the main reasons for implementing ISO 27001 is to provide a proper interaction between insiders, processes and technologies (ISO/IEC, 2005). Building a relationship between ISM standards and national culture can

help significantly to uncover effective cultural characteristics on creating, selecting and adopting ISM standards.

Based on the authors' best knowledge, Hofstede, as the father of cultural dimensions, is the most influencing and popular literature to the IS (Hofstede et al., 1991). According to the recent literature and former analysis (Ifinedo, 2014; Shojaie et al., 2014; Shojaie et al., 2015), the most applicable Hofstede dimensions are uncertainty avoidance (UAI), power distance (PDI) and individualism (IDV). The UAI is used to describe effective rules and regulations (dealing with conflicts). The PDI demonstrates the role of differentiation (relation to authority), which is mainly based on the level of authority ranking and equality matching. The PDI and UAI together demonstrate the way organisations normally do their duties. Furthermore, the IDV (conception of self) influences people compliance level with organisational requirements.

Gelfand dimensions (tightness vs. looseness) are based on the level of enforcing and demanding rules and standards in a society (Gelfand, 2006). In tight countries, integration and uniformity is considerably important, and deviation from established rules is hardly acceptable (Shojaie et al., 2015). This paper has several limitations, as the selected cultural dimensions are not available for all studied countries. For example, the Gelfand dimensions of the studied countries were not available thoroughly (nearly half), based on the analysed literature. The number of publications is relatively limited in this interdisciplinary study, based on the relationship between cultural characteristics and the IS guidelines. According to the so far discussions, Hofstede selected dimensions were chosen for further studies.

Discussion and Results

As the first step, this section identified the reasons for establishing several national IS guidelines; afterwards, this section focused on the main differences between the national IS guidelines and the ISO 27001. As a third step, this section analysed the selected national IS guidelines' characteristics and comparison with the ISO 27001. The last part of this section summarised the main differences and similarities between selected national IS guidelines and the ISO 27001. The ISO 27001 performance is possibly enhanced by these research further advices.

National IS Guidelines Development

This section analysed possible reasons and motivations for creating national ISM standards and guidelines. The first reason for creating national IS guidelines is based on the time of these guidelines establishment. For the first time, the Department of Trade and Industry (DTI) of the UK published a user's code of practice for the IS that was the foundation of the BS 7799 in 1995. Meanwhile, other standards were created in different countries. For example,

the IT baseline protection standard of Germany and the DITSCAP of the United States were both published before 1995.

The second reason is based on practical challenges of developing the ISO 27001. Because of the ISO 27001 generic content and lack of technical measures, specific IS concerns and requirements of different industries and countries are not addressed adequately. On the one hand, the ISO 27001 generic content opens space for different interpretations and flexibility for implementation. On the other hand, this generic content is a definite requirement for proposing an international standard suitable for any types of organisation. As a result, most of the national IS guidelines expand the ISO 27001 (for example the ISM Maturity Model of the Open Group (OPEN GROUP, 2011), or the German IT baseline protection catalogues), which recommends several technical measures such as cryptographic techniques.

The third reason is based on specific legislation and national requirements. For example, the United States has several security standards (DITSCAP, TCSEC and DIACAP), because of the growing requirements of the US Government agencies to meet US legislation requirements. Besides that, other IS guidelines could not comply with the US legislation requirements. In practice, both FISMA (government organisations and contractors) and the ISO 27001 (non-governmental US companies and most multi-national organisation) standards are adopted in the United States (Maier, 2014).

One of the possible concerns of implementing the ISO 27001 is a financial issue. This standard development demands a relatively high level of resources, which is not economically feasible for all types of organisations. Based on the further analysis of top 10 countries (ISO, 2014), the countries' economy power is recognised as one of the possible effective factors, such as Germany. However, Russia as one of the largest national economies was not ranked among the countries with ISO 27001 high adoption rate. Accordingly, further analysis leads this research to the fourth reason, which is based on national characteristics (history and development of countries). For example, countries such as Romania and Bulgaria have a higher level of ISO 27001-adoption rate compared to Russia. The number of ISO 27001 certificates has raised in Romania and Bulgaria, since they became members of the European Union (Maier, 2014). Because most of the EU members have large economies, they commonly have a relatively ISO 27001 high adoption rate (the UK, Italy, Romania, Spain and Germany as top 10).

Principally, countries adopt a national IS guideline to follow the main reasons, motivations and goals (national or industrial) for addressing the aimed targeted group. The countries with the national IS guidelines mostly adopt the ISO 27001 because of international trends requirements, such as customer demands, marketing edge or international regulations compatibility (Shojaie et al., 2014).

All in all, one of the possible reasons for creating national IS guidelines is based on the time of establishing the international ISM standard. The second investigated reason is focused on the ISO 27001 generality, which addresses every organisation regardless of their systems properties, IS requirements or

expertise in every country. Furthermore, cultural characteristics and international trading relationships might affect the ISO 27001 adoption rate (ISO, 2014), based on the so far discussions.

National IS Guidelines Selection

First, this section focused on the practical challenges and concerns of developing the ISO 27001. Then, this section addressed the national IS guidelines selection procedure for further analysis. It is challenging for organisations to adopt an ISM standard, as it changes the organisation's structure and processes considerably (Shojaie et al., 2015). Especially for small and medium sized organisations, the costs of implementing an ISM standard are relatively high (considering limited resources). The ISO 27001 certification is mainly recognized as a competitive advantage between competing organisations, especially in international processes (Maier, 2014).

Some of the IS guidelines are defined as recommendations and best practices; while some others are IS laws, which compliance is a requirement for corresponding organisations (Maier, 2014). Organisations mostly adopted national IS guidelines, other countries' or organisations' IS guidelines, before the ISO 27001 publication. Many organisations adopt relatively old national IS guidelines compared to the ISO 27001 latest update in 2013 (Maier, 2014). Some of the national IS guidelines (such as the German IT baseline protection standard) are compatible with the ISO standards. However, most of these national IS guidelines were not compatible with the ISO 27001, as they were published before the ISO 27001, or they have specific ISM laws (for protecting infrastructure critical systems such as federal agencies or banks). As a result, it is important to compare and identify similar and different components of these national guidelines.

Among one hundred and eighty six countries, there are some countries with one IS guideline (such as China, Germany, Russia, and Brazil), while some others have more than one IS guideline (such as United States, India, Japan, and Singapore). For example, Japan and Russia developed an IS strategy guideline for outlining governmental obligations and directions for future national IS enhancements (Maier, 2014). Australian organisations mostly adopt the AS/NZS ISO/IEC 17799, which is mainly based on the original British ISO/IEC 17799 standard with minor modifications. Based on the former analysis, the scope of the paper, the cultural characteristics availability, the Beckers comparison criteria (Beckers et al., 2014), the structure and content analysis of these IS guidelines, thirty selected countries were compared with the ISO 27001 (such as the US (FISMA), China, India (NTRO), Canada (MITS), Hong Kong (GovHK), Austria, Singapore (MAS), United Arab Emirates).

Selected IS Guidelines National Cultural Characteristics

Based on the analysis so far, national socio-economic background and culture can affect the ISO 27001 adoption rate and the main focus of the national IS guidelines. This section is based on the selected IS guidelines and their national cultural characteristics, which are expected to influence the ISO 27001 adoption (such as historical or economics background). Afterwards, these selected IS guidelines were compared with the ISO 27001.

The United States (as multicultural and diverse-ethics) and China (as large global importer/exporter) are both large counties with a high number of population in the world. Germany is known as one of the most populated, economic and political power in Europe. South Africa is recognised as an advanced-industrial (as the second largest economy in Africa) and multi-ethnic country (wide variety of cultures, languages and religions). Moreover, Hong Kong is categorised as one of the most important leading international financial centres and populated countries. The United Arab Emirates' high income is mainly based on the oil and natural gas supplies, as a business gateway for West Asia and Africa.

India is one of the most populated countries with a large and fast growing economy, because of several market economic reforms. However, India faces several challenges, such as poverty, corruption and terrorism. Pakistan is well known as a multicultural, regional and middle power country, which struggles with overpopulation, terrorism, poverty and corruption. Pakistan is a member of several international political organisations and groups such as the UN. Furthermore, Uganda is recognised as a populated landlocked country, with several conflicts and civil wars. Uganda' official language is English, and the government published the national IS strategy guideline for improving IS awareness and establishing an IS culture. In addition, Rwanda has a lower level of corruption (compared to its neighbouring countries), but restrictions of free speech (in contrary with human rights). The country's economy is generally based on agriculture and tourism. Music, dance, traditional arts and crafts shaped Rwandan culture.

Canada is considered as one of the most ethnically diverse and multicultural countries in the world, which has a sophisticated and wealthy economy with a high level of education, government transparency, civil liberties and economic freedom. Besides that, Canada is a member of several international and intergovernmental institutions. Austria as a rich country is a member of several international institutions such as the UN. Additionally, Singapore is referred to as one of the major financial centres, which is a member of several international political and trade groups (such as the Association of South East Asian Nations (ASEAN)). Latvia maintains its national identity through language and musical traditions (European Capital of Culture), which is a member of different international organisations (such as the NATO). The targeted group of Latvia's national security guideline of information systems is mainly the financial sector.

Selected IS Guidelines Comparison

This section discusses the main differences and similarities of selected national IS guidelines and the ISO 2001. The main difference between these studied guidelines was based on stakeholder description. In contrary to the ISO 27001 generic and high-level instructions, the analysed national IS guidelines mainly targeted a particular organisational type or interest groups (government sectors, financial organisations or critical infrastructures). However, a few numbers of guidelines are aimed for all types of organisations (the German IT baseline protection standard or the Austrian information security handbook).

In contrary to the ISO 27001, which leaves details of implementing instructions to organisations (general scope), some of these national IS guidelines indicate step by step advices on implementing different processes (detailed scope). The ISO 27001 is mainly based on management features of the IS and security processes (ISO/IEC, 2013). While most of the investigated IS national guidelines address IS technical features (Maier, 2014). Some of these IS national guidelines provide fast and easy implementation requirements (South Africa). However, some others focus on high-level complex security management instructions and sophisticated information systems requirements (American FISMA).

Most of the technical-advanced and economically powerful countries essentially require advanced and more detailed procedures for protecting their organisations' critical infrastructures and sophisticated information systems (United States, Canada or Germany). Nevertheless, analysed developing countries generally do not require extensive security requirements, and focus on practical and easily understandable implementation procedures (Rwanda or Uganda).

Most of the analysed developing countries (Uganda or Pakistan) possibly implement the ISO 27001 to provide a baseline protection level. While, developed countries (Singapore or Austria) can practice the ISO 27001 as a basis; and specify an additional security requirements guideline addressing particular IS requirements (Maier, 2014). Furthermore, the ISO 27001 could target different types of audiences or organisations more specifically. For this aim, the ISO 27001 possibly provides an additional set of requirements, recommended methodologies or security measures (as most of the analysed national IS guidelines are proposed for particular target groups).

National IS Guidelines and National Cultural Characteristics

This section focused on the selected countries' cultural characteristics (Hofstede and Gelfand), based on the 2014 survey of ISO 27001 (ISO, 2014). According to the former discussions, implementing the ISO 27001 in an organisation requires a cultural change as it changes the employees' routine and communication devices (Shojaie et al., 2015). The highest number of the ISO 27001 certificates belonged to the East Asia & pacific; Europe and Central & South Asia were on the second and third stage.

The highest average level of the ISO 27001 annual-growth was in 2009 (four years after the ISO 27001 first publication in 2005), which could be the result of governmental (such as the US government) financial help around the world to recover market. Another possible reason is that insiders caused a higher level of security breaches compared to outsiders (such as terrorists), which lead to higher global concerns and attentions to the importance of the IS management features. The least average level of the ISO 27001 annual-growth was in 2014 (one year after the ISO 27001 update in 2013), which could be the results of the global financial crisis (so called phase three of the global financial crisis). Another possible reason is that small organisations had lower level of the IS investments compared to previous years. Besides that, the main focus of cyber-attacks was in Europe in 2014.

The results of this paper indicated that there was an extensive variety between the selected countries with national IS guidelines and the ISO 27001 annual-growth (ISO, 2014). It was ranged from the average highest ISO 27001 certification numbers (Japan, India, the UK, China) until the average lowest certification numbers (Rwanda, Uganda, Malawi, Azerbaijan), which demonstrates various levels of interests from different countries in the IS guidelines (with different levels of IS concerns). Some of the analysed countries were among the top 10 countries of the ISO 27001 annual-growth (such as Japan, the UK, India, China, United States and Germany).

Based on the statistics of the ISO 27001 withdrawn certificates from 2006 until 2011 (ISO, 2014), the top three countries with the highest number of withdrawn certificates were Japan, China and the UK. While, the lowest number of the ISO 27001 withdrawn certificates belonged to United Arab Emirates, Russian Federation, South Africa and the United States. The numbers of withdrawn certificates were unknown for some countries, such as Uganda or Malawi (ISO, 2014). These withdrawn certificates are considerably important as these countries had sufficient reasons to establish such a high demanding resource project at the beginning (such as enhancing the current IS). However, they did not have adequate reasons to maintain and improve this international ISM standard (such as nonconformity of the ISO 27001 requirements with the national cultural characteristics).

The average ISO 27001 annual-growth of the countries with more than one national IS guidelines is significantly higher than the countries with one national IS guideline, which possibly demonstrates the higher level of IS concerns. When the countries have a relatively lower level of IS knowledge principally, they aimed for improving the basic national IS awareness to an advanced desired level. However, the countries' main goal with considerably higher IS knowledge was to acquire a more sophisticated national IS knowledge level (based on the specific national and organisational requirements).

Furthermore, the average level of the ISO 27001 annual-growth belonged to developed countries, compared to the studied developing countries. Most of the analysed countries have a relatively high level of the UAI and PDI dimensions (more than 50%) according to the Hofstede centre (Hofstede,

2016). On average, countries with more than one national IS guidelines are relatively ranked higher in the UAI, PDI and IDV dimensions (more than 50%), which are considered as tight countries. The highest average number of the ISO 27001 certificates, annual-growth and withdrawn certificates belonged to Japan from 2006 until 2014. The cultural characteristics of some of the studied countries were not available (such as Rwanda), which is a limitation of this research. The ISO 27001 experts are not interested in sharing their professional experiences with the academy that is considered as the other limitation of this paper.

Based on the so far analysis, adopting a national IS guideline for some countries act as a motivation to enhance the national IS level and to attract more attention to the importance of the IS field. Besides that, having a national IS guideline could lead to higher level of interests in establishing an international ISM standard. For some other countries, a national IS guideline is considered enough to satisfy their security requirements. There are some factors that influence the ISO 27001 adoption rate, such as language, the extent of international communication and trends and governmental regulations. Besides that, the national IS guidelines' aim and focus as well as generality and similarity level to the ISO 27001 affect this standard adoption rate. Developing a national IS guideline possibly presents higher levels of attention, care and concerns about the IS (both theoretical and practical levels), as one of the national characteristics. Four appendixes are inserted for improving the clarification of so far discussion.

Conclusions

This paper analyses the national IS guidelines and classifies them based on common characteristics, such as historical background, national economy and global activities. This research investigates the main differences between the studied national IS guidelines and the most adopted international ISO 27001 standard. Besides that, this paper analyses the ISO 27001 annual-growth in selected countries, based on the ISO 27001 survey 2014 (ISO, 2014). The main differences between these national IS guidelines are based on the stakeholder description, and the level of focus on technical aspects.

Recent literature indicated the importance of cultural characteristics on the IS. This paper follows up on previous works by defining the relationship between the studied national ISM standards and the selected cultural dimensions from the most popular literature. The ISO 2001 adoption rate is influenced by several cultural characteristics such as internal conflicts, historical background, governmental regulations, number of population, level of ethically diversity, and international institutions membership (EU). The results of this research indicated that cultural characteristics, international trends and national economic power should be considered for implementing ISO 27001, as the most leading national features.

The countries with national IS guidelines have several motivations and reasons for not adopting the ISO 27001 as a single point of reference (such as the ISO 27001 development time interval, language and generality). One of the important reasons for introducing a national IS guideline is to address specific national or industrial IS requirements. Based on the national and organisational IS requirements, the ISO 27001 adoption rate may be influenced by the national IS guidelines. Improving the national IS knowledge (generally or specifically based on the IS requirements) is the main motivation for establishing national IS guidelines, which are not particularly satisfied by the international ISO 27001 adoption.

References

Arora, V., 2010. Comparing different information security standards: COBIT v s. ISO 27001. Línea. Disponible en Carnegie Mellon University, Qatar: (http://qatar. cmu.edu/media/assets/CPUCIS2010-1. pdf).

Barlette, Y. and Fomin, V.V., 2008, January. Exploring the suitability of IS security management standards for SMEs. In Hawaii International Conference on System Sciences, Proceedings of the 41st Annual (pp. 308-308). IEEE.

Barlette, Y. and Fomin, V.V., 2010. The Adoption of Information Security Management Standards. Information Resources Management: Concepts, Methodologies, Tools and Applications: Concepts, Methodologies, Tools and Applications, p.69.

Beckers, K., Côté, I., Fenz, S., Hatebur, D. and Heisel, M., 2014. A structured comparison of security standards. In Engineering secure future internet services and systems (pp. 1-34). Springer International Publishing.

Dunbar, B., 2002. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment. Sans Institute, 2002, pp.1-9.

Fomin, V.V., Vries, H. and Barlette, Y., 2008, September. ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption. In EUROMOT 2008 Conference, Nice, France.

Gelfand, M.J., Nishii, L.H. and Raver, J.L., 2006. On the nature and importance of cultural tightness-looseness. Journal of Applied Psychology,91(6), p.1225.

Gikas, C., 2010. A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. Information Security Journal: A Global Perspective, 19(3), pp.132-141.

Henson, R. and Garfield, J., 2015. What Attitude Changes Are Needed to Cause SMEs to Take a Strategic Approach to Information Security?. Athens Journal of Business and Economics.

Hofstede, G., Hofstede, G. J., & Minkov, M. ,1991. Cultures and organizations: Software of the mind (Vol. 2). London: McGraw-Hill.

Hofstede, G., the Hofstede Centre http://geert-hofstede.com/countries.html (accessed 10 April 2016).

Ifinedo, P., 2014. The effects of national culture on the assessment of information security threats and controls in financial services industry. International Journal of Electronic Business Management, 12(2), p.75.

International Organization for Standardization/ International Electrotechnical Commission, 2005. ISO/IEC 27001:2005: Information technology – Security techniques – Information security management systems – Requirements.

International Organization for Standardization/ International Electrotechnical Commission, 2013. ISO/IEC 27001:2013: Information Technology – Security Techniques – Information Security Management Systems – Requirements .

International Organization for Standardization (ISO), 2014. ISO Survey 2014.

Katsikas, S.K., Lopez, J. and Pernul, G., 2005. Trust, privacy and security in digital business. COMPUTER SYSTEMS SCIENCE AND ENGINEERING, 20(6), p.391.

Kuligowski, C., 2009. Comparison of IT Security Standards. Technical report.

Maier, F., 2014, December. A comparison of national and international Information Security Standards based on cultural differences. Hamburg University.

Schein, E.H., 2010. Organizational culture and leadership (Vol. 2). John Wiley & Sons.

Schlienger, T. and Teufel, S., 2003, September. Analyzing information security culture: increased trust by an appropriate information security culture. In Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on (pp. 405-409). IEEE.

Shojaie, B., Federrath, H., & Saberi, I., 2014, September. Evaluating the effectiveness of ISO 27001: 2013 based on Annex A. In Availability, Reliability and Security (ARES), 2014 Ninth International Conference on (pp. 259-264). IEEE.

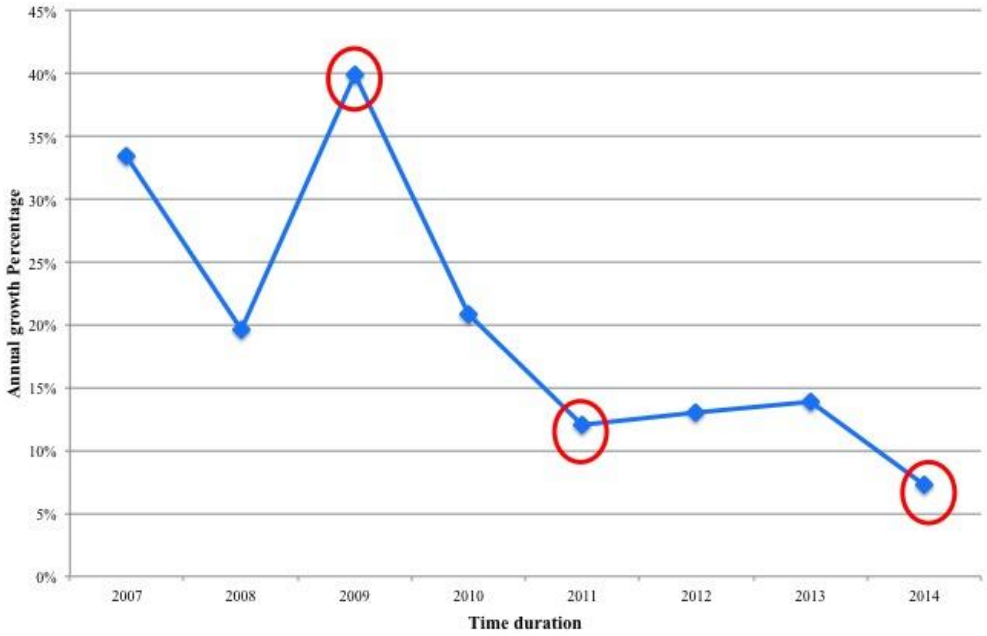
Shojaie, B., Federrath, H., & Saberi, I., 2015, August. The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001. In Availability, Reliability and Security (ARES), 2015 10th International Conference on (pp. 159-167). IEEE.

Torres, J.M., Sarriegi, J.M., Santos, J. and Serrano, N., 2006. Managing information systems security: critical success factors and indicators to measure effectiveness. In Information Security (pp. 530-545). Springer Berlin Heidelberg.

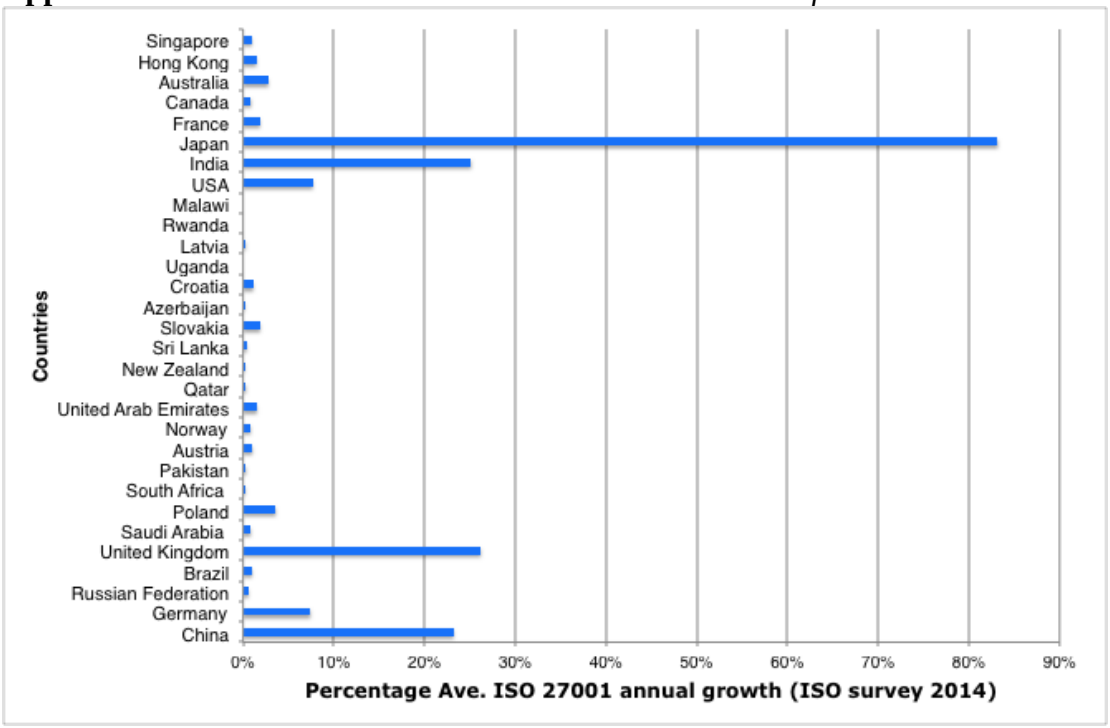
Tsohou, A., Theoharidou, M., Kokolakis, S. and Gritzalis, D., 2007. Addressing cultural dissimilarity in the information security management outsourcing relationship. In Trust, Privacy and Security in Digital Business (pp. 24-33). Springer Berlin Heidelberg.

Yanus, R. and Shin, N., 2007. Critical Success Factors for Managing an Information Security Awareness Program. In *Proceedings of the sixth Annual ISOneWorld Conference*.

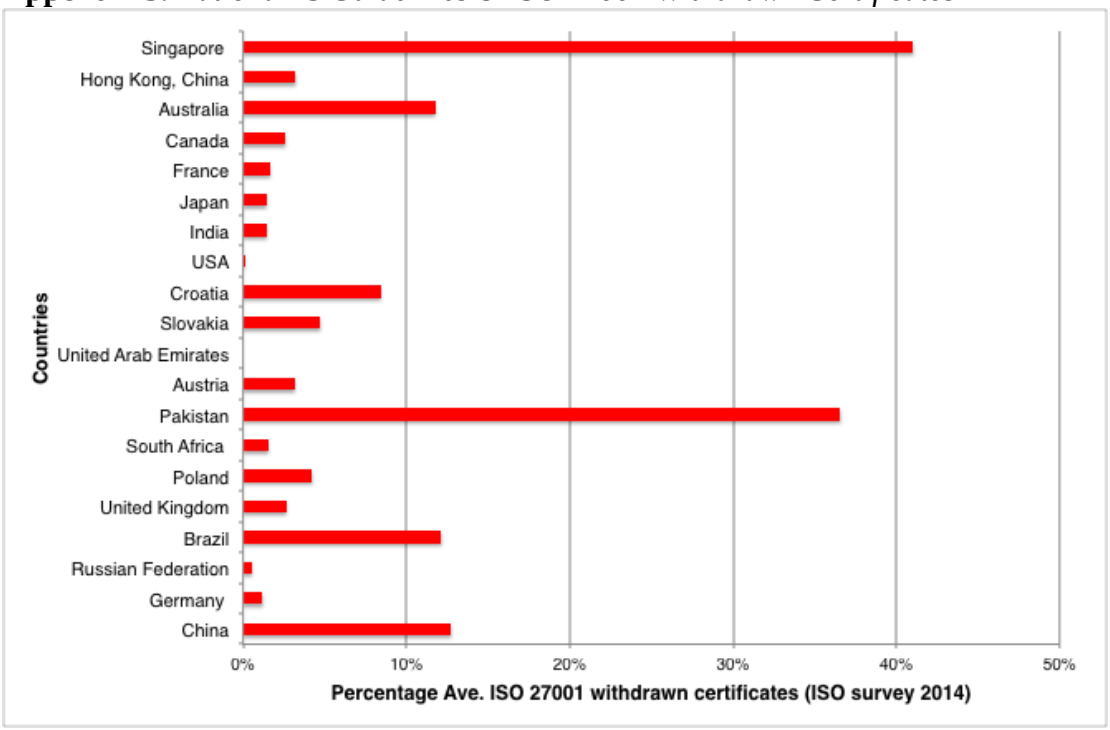
Appendix 1. *ISO 27001 Worldwide Annual-growth*



Appendix 2. *National IS Guidelines & ISO 27001 Issued Certificates*



Appendix 3. *National IS Guidelines & ISO 27001 Withdrawn Certificates*



Appendix 4. *National IS Guidelines & Cultural Characteristics*