Getting the Full Benefits of the ISO 27001 to Develop an ISMS based on Organisations' InfoSec Culture

B. Shojaie[1], H. Federrath[1] and I. Saberi[2]

[1]Security in Distributed Systems, University of Hamburg, Hamburg, Germany
[2]Security in Distributed Applications, Technical University of Hamburg, Hamburg, Germany
e-mail: {shojaie,federrath}@informatik.uni-hamburg.de, iman.saberi@tuhh.de

Abstract

The ISO/IEC 27001 is an important and the most leading international information security management standard in the information security (InfoSec) world. The benefits of implementing the ISO 27001 are to provide market assurance and IT governance, based on customer demands and legal requirements. Although the ISO 27001 is a generic standard for all types of organisations and countries, there are still some countries that do not adopt the ISO 27001 largely. The main reason for this low adoption rate is the cultural barriers of implementing ISO 27001. The considerable influences of culture on the InfoSec have long been a topic of public and scientific interests. However, the relationship between InfoSec cultural behaviour and the ISO 27001 efficiency was unfounded. Understanding influential national cultural characteristics is considerably important for establishing a strong InfoSec culture, which is compatible with the ISO 27001 requirements. Based on the literature review, personal interviews and limited results of the preliminary survey, this study found three distinguished cultural behaviours the most applicable cultural characteristics to the ISO 27001 efficiency. This study reduces the cultural barriers of implementing ISO 27001 by enhancing required resources and insiders' cooperation in overarching employees' bypassing of defined rules and regulations.

Keywords

ISO 27001 Adoption, Withdrawn Certificate, Hofstede, InfoSec Cultural Behaviour

1. Introduction

The ISO 27001 is a best-known systematic approach for protecting sensitive information and establishing an Information Security Management System (ISMS) (ISO/IEC, 2005). According to the ISO 27001, organisations should consider business and national information security (InfoSec) requirements to implement the ISO 27001 as an integrated part of organisational management structure. The ISO 27001 enhances the InfoSec level of the whole system based on organisation's objectives, size, structure and processes that change over time. InfoSec requirements are considerably influenced by cultural characteristics (behaviour and mind-set), which are widely different between organisations (Ashenden, 2008) and countries (Da Veiga, 2015). It is proved (Ashenden, 2008) that several nontechnical issues influence the ISO 27001 implementation. The efficiency of the ISO 27001 is affected by internals who are involved in executing ISO 27001 rules and regulations, based on the job requirements (Shojaie et al., 2015). Cultural characteristics should be considered in early stages of establishing ISO 27001 (planning phase), as insiders are involved in using the ISO 27001 instructions. The national dominant mind-set and behaviour for protecting important asset affect the decisions of adopting and implementing the ISO 27001 as an initial step of selecting an ISMS standard (Fomin, 2008).

Although the ISO 27001 is the most adopted international ISMS standard, the number of ISO 27001 withdrawn certificates increase each year remarkably (ISO, 2014). These withdrawn certificates are significantly important, as these organisations had enough motivations to select and implement the ISO 27001 as a considerably high-resource-demanding project. However, these organisations did not maintain and update the InfoSec requirements to an acceptable level for renovating their ISO 27001 certificates. Considering cultural characteristics as a pre-phase plan (Shojaie, 2015) can help to reduce the number of ISO 27001 withdrawn certificates and additional costs of implementing the ISO 27001 noticeably. This research will address the following question: How the ISO 27001 standard can be used to develop the ISMS for organisations with different InfoSec cultural characteristics?

The remainder of the paper is organised as follows: Section 2 discusses the motivation of the paper and cultural barriers of implementing the ISO 27001. Section 3 introduces the most leading national literature and cultural dimensions, which are applicable to the ISO 27001 implementation. Section 4 as the main contribution of the paper, establishes a relationship between selected national cultural dimensions and the ISO 27001 efficiency. Afterwards, section 5 investigates the cultural barriers of implementing ISO 27001 with analysing the countries with the highest level of the ISO 27001 adoption rate and withdrawn certificates. Finally, section 6 concludes the paper based on the literature review, the IS0 27001 survey 2014, and personal talks with the ISO 27001 experts and limited results of the preliminary survey.

2. Background of Study

Most of the organisations implement the ISO 27001 to get advantages of the most adopted international standard (such as customer assurance and marketing benefits). The ISO 27001 adoption is influenced by national regulations and organisational requirements, based on the most leading literature (Ifinedo, 2014). The dominant national culture influences internals, as their sensitivity to accurately executing InfoSec tasks is not the same in one organisation (who are known as main InfoSec enemies (Ashenden et al., 2013)). Furthermore, adopting ISO 27001 rules and regulations require a level of cultural change (insiders' behaviour) to preserve the organisational InfoSec requirements (Fomin, 2008). On the one hand, the cultural effects are bottom-up (Hui et al., 1985); on the other hand, the ISMS implementation is a top-down approach. As a result, it is considerably challenging to change insiders' behaviour to satisfy organisational InfoSec requirements (Ernest Chang et al,. 2007). So, organisations should consider practicability of defined rules and regulations with organisational InfoSec culture as an important step of designing the ISO 27001

(Shojaie, 2015), because insider's cooperation is an important factor for improving the efficiency of the ISO 27001 (Montesino, 2011).

Based on the personal talks, most organisations focus on the ISO 27001 technical features (infrastructure configurations) and overlook the management aspects of human resources (insiders). One of the main stages of establishing ISO 27001 is to increase insiders' InfoSec knowledge (such as training and awareness programs), which addresses insiders constantly. These types of programs are required as business, organisational and InfoSec requirements change frequently and rapidly. These programs should address updated security requirements and relevant security vulnerabilities (based on the insiders' job requirements) as well as approaches of dealing with these threats (ISO/ IEC, 2013). The effectiveness of these programs continuously influences required resources for executing influences InfoSec tasks (such as human being or time). Besides that, insiders' security sensitivity or agreeableness influences frequency, duration or required level of these programs (Ifinedo, 2014). These programs can help significantly to reduce misunderstandings, errors, and relevant security breaches (Montesino, 2011), which address all insiders (organisational personnel with different levels of InfoSec knowledge and requirements). There are different publications of modelling national culture (Hui et al., 1985). The most applicable and popular literature is Hofstede (Hofstede et al., 1991), based on the current knowledge of authors. Some literature (Freeman, 2007) focused on importance and approaches of handling InfoSec tasks in large organisations (such as maintenance and regular updates). However, the role of insiders in executing InfoSec tasks was not considered sufficiently.

3. Fundamentals

The authors' discipline for selecting literature is based on popularity, number of citations and relevance for defining the relationship between the ISO 27001 and cultural characteristics. Based on the former analysis (Shojaie, 2015) and the most applicable publications to the InfoSec tasks, Hofstede was selected for further analysis (Hofstede et al., 1991). Hofstede is the father of defining cultural dimensions, whose selected cultural dimensions are uncertainty avoidance (*UAI*), power distance (*PDI*) and individualism (*IDV*). Regulations and effective controls are described based on the *UAI* (ways of dealing with conflicts). The role differentiation is shown by the *PDI* (relation to authority). Besides, the level of insiders' *IDV* (conception of self) influences the level of compliance with organisational requirements. Co-workers with different *PDI* and *IDV* may find it difficult to communicate (Hofstede et al., 1991). Based on the further analysis and Hofstede literature, the three cultural types are determined. These distinguished cultural types can affect the efficiency of the ISO 27001 considerably, because of extensive numbers of ISO 27001 instructions and bureaucratic procedures (as the main basis and the most challenging stages of the ISO 27001 implementation).

In order to establish a relationship between cultural dimensions and the ISO 27001 efficiency in the real world, this paper get the benefits of the ISO 27001 survey 2014 (ISO, 2014). This research is limited to the narrow available literature in the field of

InfoSec and cultural dimensions, and experts were not highly interested in sharing their practical experiences with the academic world (Fomin, 2008). The aim of this research is to find the national influential cultural characteristics to improve the ISO 27001 efficiency and achievements. The combination of the Hofstede selected cultural dimensions and the ISO 27001-adoption rate is the contribution of this paper.

4. Results

Based on the established relationship between ISO 27001 efficiency and cultural dimensions, this study is divided into two main parts. The first part is based on the most significant national cultural characteristics and behaviours, and the second part focused on the ISO 27001-adoption rate. Understanding InfoSec culture of a local organisation is less challenging, when the national and organisational cultural is the same between insiders. Some insiders may change their InfoSec culture (behaviour and mind-set) faster to comply with organisational security requirements (Hofstede et al., 1991). However, some may not change their behaviour fast enough to comply with organisational updated guidelines and procedures.

4.1. The ISO 27001 Adoption & Cultural Behaviours

Based on the so far discussions, there are three distinguished cultural behaviours, concerning the ISO 27001 implementation requirements. These three types are referred as A, B and C in this paper. In type A, everything is permitted, even what is forbidden based on the authority's behaviour and mind-set (based on authority) (Hofstede et al., 1991). The type A country is mainly politically united, and authorities are mostly not interested in formal decision-making with workers (Hofstede et al., 1991). In the type B, everything is forbidden, except what is permitted (based on rules). The type B country is principally united and their decision-making is formal between management and workers. Besides that, type B is mostly a professional bureaucratic country. In type C, everything is permitted, except what is forbidden (based on situations). The type C country mainly resists documenting industrial rules and they are not principally united. The type C is a full bureaucratic country (Hofstede et al., 1991).

ISO 27001 implementation as a cycling approach is expressed like a machine (ISO/IEC, 2005) with definite inputs and outputs. Based on the earlier discussions, this paper defines three types of insiders' culture (A, B and C) as an input. This shapes the effectiveness and productivity of output (well-structured instructions and countermeasures compatible with dominant InfoSec organisational culture). These identified cultural types are possibly determined by a questionnaire, which can result in one type, or a mixture of types. Based on the current state of the insiders' InfoSec culture (A, B or C types), this paper provides some advice for compatibility of the ISO 27001 implementation with the determined cultural type.

The type A is described as a training-based (TB) culture. An evaluation test is required to determine the current level of insiders' InfoSec culture (behaviour and knowledge). Based on the average current level of insiders' InfoSec culture, the next desired InfoSec cultural level is adjusted (according to the ISO 27001 defined responsibilities and organisational requirements). After gaining the desired level of insiders' InfoSec knowledge, future improvements should be measured and planed as the next steps to preserve the required level of organisational InfoSec requirements. The training programs help to reach the next level of the desired InfoSec culture.

The type B is described as a rule-based (RB) culture. The first step is to clarify and document the main ISO 27001 instructions and guidelines, based on the current level of insiders' InfoSec culture (behaviour and knowledge). After defining base-line instructions, future sophisticated rules and regulations should be measured based on a scheduled time plan. This second enhancement step states possible consequences (penalties) of not obeying rules (according to the ISO 27001 defined responsibilities and organisational requirements). The training programs help to reach the next level of the desired InfoSec culture. The third step is documenting all the current and future rules and regulations, and distributing to all insiders. The aim of these documented instructions is not increase insiders' support, adoption and commitment (based on defined ISO 27001 rules and the required level of insiders' InfoSec knowledge).

The type C is described as a vaccination-based (VB) or penetration-based culture. At the first step, the current level of insiders' InfoSec culture (behaviour and knowledge) is unknown and varies between insiders. As a result, an evaluation test should be designed (called vaccination) for determining the current level of insiders' InfoSec culture. For example, after all employees leave the organisation for the day, an organised team may check the workplace to estimate the current level of insiders' InfoSec culture (such as clean desktop). This organised security team (from inside of an organisation) is structured to implement this vaccination for evaluating insiders' adoption and compatibility with the defined ISO 27001 responsibilities and requirements. Furthermore, this organised team can search for InfoSec misbehaviours (written passwords, easily guessed passwords, unlocked doors and especially access control policies) to collect evidence of compatibility of the ISO 27001 rules and regulations with the current insiders' InfoSec behaviour.

Afterwards, this organised team randomly implements the next rounds of vaccination in different unannounced time durations for finding the strengths and weaknesses of currently defined ISO 27001 instructions. After each vaccination, further improvements should be scheduled to enhance compatibility of the insiders' InfoSec behaviour with the ISO 27001 instructions (as one of the most important factors on the ISO 27001 efficiency). Possible consequences (penalties) can be in the shape of cards (red, yellow or green cards). It is important to get insiders' confirmation with the relevant ISO 27001 rules in a written and documented form (such as signature) after each training and awareness programs (InfoSec knowledge enhancement session). Gaining remarkable grades in these programs' exams does not ensure a secured behaviour, or well-developed InfoSec culture (based on the ISO 27001 instructions). On the one hand, the fact that the type C is mostly multi-national helps to reduce InfoSec cultural biases; on the other hand, it is considerably challenging to identify a unified integrated culture. The Appendix 1 shows the graphical model of these cultural behaviours.

In order to determine an organisational cultural type, it is important to evaluate the average of insiders' InfoSec culture. There are two methods for evaluating insiders' InfoSec culture. The first evaluation method is based on theoretical training programs, which is designed after the termination of each training program, which only consists of the training programs materials. The second evaluation method is practical, which is designed as a penetration test without former announcements. Based on the results of these two theoretical and practical evaluation methods (Pass-Pass, Pass-Fail and Fail), three cultural types are determined and the average of the evaluated cultural type shows the organisational culture.

Understanding these cultural barriers provides a realistic future outlook (regarding required resources), which can improve human resource communication and the ISO 27001-adoption rate. The requirements of the ISO 27001 implementation may not be thoroughly integrated with the countries with high number of ISO 27001 withdrawn certificates. These types of countries allocate considerable investments of resources (for the ISO 27001 implementation) to get the ISO 27001 certification. After three years of implementing ISO 27001, they might not maintain and update the organisational InfoSec requirements to an acceptable level to renew the ISO 27001 certificate. These withdrawn certificates are possibly the result of this long-term project incompatibility with organisational InfoSec culture or the ISO 27001 inefficiency in providing the expected organisational InfoSec level. For better understanding of the most leading InfoSec culture in a quick and straightforward way, a questionnaire of the ISO 27001-readiness evaluation can be designed (known as pre-phase plan). The pre-phase plan should consist of both technical and cultural features (based on the Hofstede cultural dimensions) to evaluate the required resources for implementing the ISO 27001.

4.2. The ISO 27001 Adoption & Cultural Characteristics

For establishing a relationship between the Hofstede selected cultural dimensions and the ISO 27001 efficiency, this study analysed the top 50 countries with the highest average level of the ISO 27001-annual growth and the top 10 countries with the highest average level of the ISO 27001 withdrawn certificates (ISO, 2014). According to the average number of the ISO 27001-annual growth from 2006 until 2014, the top 50 countries were analysed (with the highest average number of issued certificates). The motivation was to find reasons for ISO 27001-low adoption, based on the Hofstede cultural dimensions of selected countries (The Hofstede Centre, 2016). The reason for choosing these top 50 countries (with the highest ISO 2700-annual growth) was to reduce the number of non-cultural features (such as customer demand), which influence the implementation and adoption of the ISO 27001. The first country with the highest average level of the ISO 27001-annual growth was Japan and the fiftieth country was South Africa. As cultural dimensions of Chinese Taipei and Republic of Korea were not available, Pakistan and Argentina were replaced instead for further analysis of the top fifty countries. These two countries

(Pakistan and Argentina) had the same average level of annual growth compared to South Africa.

Based on the cultural characteristics of these top fifty countries, this paper compared these countries' selected cultural dimensions (The Hofstede Centre, 2016) with the three identified cultural types. Concerning the average level of the ISO 27001-annual growth, France was ranked twenty-eighth as a representative of type A (*UAI*:3, *PDI*:2, *IDV*:2), the UK was ranked third as a representative of type B (*UAI*:1, *PDI*:1, *IDV*:3), Germany was ranked ninth as a representative of type C (*UAI*:2, *PDI*:1, *IDV*:2) these nine years (from 2006 until 2014). The main difference between these three cultural representatives was based on the *UAI* field; France had the highest level of the *UAI*, Germany was ranked moderately; while, the UK had the lowest level of the *UAI*. The UK had the highest value of the *IDV*. The other two (France and Germany) ranked moderately. Among these three cultural representatives, France had the most similar cultural characteristics to Japan (the highest adoption rate) in the *UAI* and the *PDI* fields (*UAI*:3, *PDI*:2, *IDV*:1).

Countries with the same cultural characteristics of type A were France, Spain, and Poland. Countries with the same cultural characteristics of type B were UK, USA, and Canada. Countries with the same cultural characteristics of type C were Germany, Switzerland, Norway, Finland, and Iceland. Countries with the same cultural characteristics as Japan were Bulgaria, Turkey, Brazil, Greece, Croatia, Slovenia, and Portugal. Japan had the most similar cultural characteristics compared to the top fifty countries (with the highest level of the ISO 27001-annual growth). These cultural similarities are the same level of the Hofstede selected dimensions of the *UAI*, *PDI* and *IDV*. The high level of cultural similarities with Japan shows that the governmental regulations are not the only reason for the highest level of the ISO 27001-annual growth in Japan. The Japanese national systematic, well-organised and disciplined behaviour possibly affect the high adoption and efficiency of the ISO 27001. The average value of the *UAI* for these top fifty countries was 2.14 (more than 50%), the average value of the *PDI* was 1.86 (more than 25%) and the *IDV* average value was 1.48 between the ranges of 0 to 4 (The Hofstede Centre, 2016).

This study benefited from the preliminary results of an online survey, which can provide an outlook for future research. The limited results of the empirical study based on the limited sample shed light on the most influential factors that are easily ignored by most organisations. The limited results demonstrate that more than half of the respondents (The ISO 27001 experts) believe spending money on computer security technology (*UAI*), centralised decision making (*PDI*), individual assessment (*IDV*) and cooperative and self-disciplined employees (insiders' InfoSec culture) are effective factors in improving the ISO 27001 efficiency.

Based on the above discussions and justifications, the ISO 27001 technical controls are mostly considered adequate by allocating enough resources. The nontechnical ISO 27001 controls (such as policies) are considerably influenced by the executers' abilities to make secure decisions based on their limited knowledge, time and available information. Based on the personal talks with the ISO 27001 experts, the main barriers of implementing ISO 27001 are bureaucratic procedures and compatibility of the ISO 27001 controls and instructions with the insiders' InfoSec culture. Based on the former analysis (shojaie et al., 2015), the *UAI* (influences the ISO 27001 rules and regulation) and the *PDI* (focuses on the communication with authorities,) are defined as important features in implementing the ISO 27001. On the one hand, the *IDV* influences the efficiency of the ISO 27001 with more attempts in improving the individual InfoSec knowledge (training and awareness programs). On the other hand, low *IDV* shows high respect to the organisations' interests and benefits (such as reputation or customer satisfaction), which influences the ISO 27001-adoption rate considerably (shojaie et al., 2015).

The top ten countries with the highest average level of withdrawn certificates mostly have a high level of the ISO 27001-annual growth (such as Japan (ranked as first) and Singapore (ranked as twenty-seventh)). The highest number of withdrawn certificates belonged to Chinese Taipei (ranked as first), and India had the lowest level of withdrawn certificate (ranked as tenth). The high number of withdrawn certificates of Chinese Taipei could be the result of a high number of ISO 27001 certificates compared to other countries. The relatively high demands for the ISO 27001 certificate at the national level can motivate organisations to establish this standard. However, high level of required resources or incompatibility with the insiders' InfoSec culture can make this long-term project inefficient. This inefficiency possibly results in inadequate maintenance phase of developing the ISO 27001, which does not an acceptable InfoSec organisational level, based on the updated InfoSec requirements.

Based on the above analysis, India was one of the perfect countries for implementing ISO 27001, as the second level of the average ISO 27001-annual growth, the tenth level of average withdrawn certificates and the cultural characteristics (*UAI*:1, *PDI*:2, *IDV*:1). The highest number of withdrawn certificates was in the year 2011 (Republic of Korea, China and Chinese Taipei), followed by the year 2009 (Chinese Taipei, the UK and Hungary). To sum up, the highest level of incompatibility belonged to Chinese Taipei (2009), the Republic of Korea and China (2011). Chinese Taipei showed the highest level of ISO 27001 incompatibility earlier than the rest of countries in 2009. The Republic of Korea had the highest level of withdrawn certificates in 2011. Most of the countries experienced a high level of withdrawn certificates (only once) in 2011, except Chinese Taipei, which experienced high number of withdrawn certificates (twice) in the years 2009 and 2011. The influences of the ISO 27001 update in 2013, and growing number of withdrawn certification in 2008 and 2009 (the approximate time period for renewing the ISO 27001:2005 certificates) are important to consider.

The highest level of withdrawn certificates could be the result of organisational resistance to the established ISO 27001 rules and responsibilities. Furthermore, inconsistency of the ISO 27001 instructions with the whole system possibly makes this project isolated (not an integrated part of the whole system). It could be the results of the incompatibility of insiders (employees with the ISO 27001 instructions), or an external motivation that does not maintain the expected ISO

27001 long-term efficiency and achievements. This external motivation (from outside of organisation, such as customer demands) may not transfer into internal motivation to maintain and improve the ISO 27001 implementation processes. Furthermore, financial problems influence the adoption rate of the ISO 27001 remarkably; for example 2008 was known as a global financial crisis, which could be one of the possible reasons for high number of ISO 27001 withdrawn certificates. The financial crisis of 2011 (Black Monday) also affected United States, Middle East, Europe and Asia, which can be the reason for high number of withdrawn certificates. The results of this study can be biased because of a lack of available literature and practical experiments that were not shared in papers about the ISO 27001. To sum up, from psychological points of view, it is the first time that an ISMS standard is combined with this discipline.

5. Discussion

Based on the analysis and justifications, the countries with an average high number of ISO 27001 withdrawn certificates and low adoption rate are the main focus of this section. This paper analysed the most popular cultural dimensions of Hofstede (*UAI*, *PDI*, and *IDV*), as a pre-phase plan. This pre-phase plan should be considered in designing the cultural section of the ISO 27001-readiness evaluation questions, which helps to identify an effective general strategy for implementing ISO 27001. Furthermore, the determined cultural characteristics should be the main focus of the ISO 27001 countermeasure and protection approaches (such as controls selection or InfoSec training programs). These cultural characteristics help to predict the cultural challenges and barriers of implementing the ISO 27001 (such as insiders' resistance to defined rules and regulations). The ISO 27001 establishment demands a considerable level of resources, which restricts insiders in performing their every day work responsibilities by defining several rules and regulations. These defined regulations can be in contradiction with insiders' perceived first priority of doing their tasks quickly. Professor Edward Humphreys (Humphreys, 2009) as the "father" of the ISO/IEC 27000 family also believes that cultural characteristics affect the efficiency of the ISO 27001. Some InfoSec scenarios can be designed for insiders based on the InfoSec requirements of their jobs to show them appropriate secure behaviours for facing real world InfoSec threats and vulnerabilities. It is necessary to estimate insiders' current level of InfoSec knowledge and their abilities to transfer the ISO 27001 instructions into daily practices and routines. These practical experiences of executing defined instructions are more effective than theoretical InfoSec training sessions. These practical experiences are possible by designing penetration tests intended to test insiders' ISO 27001 adoption with the updated InfoSec requirements (by an anonymous group inside the organisation).

According to personal talks with several ISO 27001 experts, the main challenges of the ISO 27001 implementation are based on human resource management and an adequate level of InfoSec training programs. An inadequate level of insiders' InfoSec knowledge (especially physical access control or cryptography policies) results in the ISO 27001 failure in providing an acceptable organisational InfoSec level. According to this interview, the other practical issues of establishing the ISO 27001 is to frequently update the InfoSec requirements and vulnerabilities. It is challenging for most of the organisations to monitor proper implementation of the ISO 27001, based on defined rules and regulations. Furthermore, the ISO 27001 efficiency depends considerably on the comprehensive support of management to allocate the adequate required resources (especially the budget) to implement defined policies (such as InfoSec training programs for all insiders). It is especially important to show management the graphical and visual benefits of implementing the ISO 27001 (such as the reduced level of financial losses as a result of implementing the ISO 27001 rules) to receive sufficient level of support.

According to the discussions with ISMS professional consultants of ISO 27001 implementation and the personal discussions, as well as the results of the limited preliminary survey, we suggest that organisational culture plays an important role in the countries (with high number of ISO 27001 withdrawn certifications and lowest level of adoption rate). One of the possible reasons could be the national culture does not fully support the rule-based basis and strict instructions of the ISO 27001. In these types of countries, the management behaviour as well as training and awareness programs play a more significant role in improving the ISO 27001 implementation. These two important factors possibly lead to more systematic behaviour according to the ISO 27001 defined guidelines, procedures and expected (visual) results. One perfect example is Japan, which has the highest level of the ISO 27001 adoption in practice.

It is important to design the ISO 27001 based on the organisational InfoSec requirements and dominant cultural characteristics for a high level of efficiency. For example, most of the countries with low ISO 27001-adoption rate do not have an extensive international communication for adopting an international ISMS standard. Besides that, they may not have adequate motivation to enhance the organisational InfoSec culture. The identified cultural characteristics are important when designing the ISO 27001 training and awareness programs. For example, the *IDV* is self-motivated in improving the InfoSec knowledge and skills. On the one hand, the *IDV* may not require physical attendance of these InfoSec training programs regularly, which influences the required frequency level and materials (such as online self-training websites). On the other hand, low *IDV* may respect and adopt the ISO 27001 rules and regulations actively to satisfy organisational InfoSec requirements. It is important for management to actively participate in the ISO 27001 training programs, as authorities' InfoSec behaviour (especially their sensitivity to the ISO 27001 instructions' compatibility) influences the InfoSec behaviour of the type A and the *PDI*. Focusing on the consequences and penalties of incompatibility with the ISO 27001 instructions can improve the *UAI* InfoSec behaviour. For the type B as a rule-based culture, it is suggested to focus more frequently on flyers and reminders (such as screen saver) to increase employees' awareness of defined ISO 27001 instructions. The type C may require higher level of resources for implementing training programs for designing penetration tests compared to the types A and B. The cultural barriers concerning different InfoSec features (such as privacy) exist in almost all countries (with different levels of execution difficulties and resistance) for adopting the ISO 27001.

Some organisations use cultural characteristics as a tool to manage different stages of the ISO 27001 implementation wisely, with adequate care and considerations. The insiders' well-developed InfoSec culture can provide higher opportunities for better adoption and proper execution of the ISO 27001 guidelines, policies and countermeasures. These successful organisations manage national characteristics in an appropriate way to adopt the organisational InfoSec requirements. However, the ISO 27001 survey 2014 statistics show that even a systematic behaviour (known as a suitable culture for adopting ISO 27001) in Japan (as the best sample with the highest average level of the ISO 27001-annual growth) can transfer the ISO 27001 into an inefficient project with inadequate management. Furthermore, this inefficiency can cause new security breaches as a result of incomplete InfoSec procedures and insiders' incompatible InfoSec culture with the organisational InfoSec requirements (result in ISO 27001 instructions ignorance). The most important part of establishing ISO 27001 concerning cultural characteristics is managing these national cultural characteristics appropriately, based on the organisational InfoSec requirements and objectives.

6. Conclusion

All types of organisations can benefit from implementing an Information Security Management System (ISMS) in accordance with the ISO 27001. The ISO 27001 instructions are mainly preventive based, and contain strict InfoSec countermeasures, which are not fully compatible with all national cultural characteristics. Therefore, it is important to evaluate organisational InfoSec culture and implement the ISO 27001 instructions accordingly to prepare an appropriate environment for guiding employees when using InfoSec. Understanding cultural characteristics helps management to be aware of possible cultural barriers and biases to enhance resources allocation and improve the ISO 27001 efficiency. The ISO 27001-adoption rate is influenced by several global and national criteria, such as financial crisis (national and global), InfoSec well-known events (disasters or privacy breaches), governmental regulation, policies, and international communications. This paper benefited from the Hofstede selected cultural dimensions, the ISO 27001 survey 2014, personal talks with several ISO 27001 experts and limited results of the preliminary survey to build a relationship between three defined cultural types and the ISO 27001 efficiency. This study can improve both ISO 27001 practical success factors and theoretical features by introducing the most influential cultural characteristics and establishing a relationship with the ISO 27001-adoption rate (in different countries). These selected national cultural dimensions can help to improve the ISO 27001 achievements by optimising applicability of the ISO 27001 guidelines and finding the main focus of the training InfoSec programs (as two main stages of implementing the ISO 27001). Based on the three cultural types (A, B and C), this paper provides some advice on how to enhance the ISO 27001 efficiency, predict possible cultural barriers, and propose possible solutions to overcome cultural difficulties.

7. Acknowledgment

We thank Mr. Eiman Khorasani Rad and Mr. Nima Nabavi (TÜV NORD Iran) for their comments and recommendations on a draft version of this paper.

8. References

Ashenden, D., 2008. Information Security management: A human challenge?. Information security technical report, 13(4), pp.195-201.

Ashenden, D. and Sasse, A., 2013. CISOs and organisational culture: Their own worst enemy?. Computers & Security, 39, pp.396-405.

Da Veiga, A., 2015. The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study. In Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015) (p. 22). Lulu. com.

Da Veiga, A., 2015. An Information Security Training and Awareness Approach (ISTAAP) to Instil an Information Security-Positive Culture. In Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015) (p. 95). Lulu. com.

Ernest Chang, S. and Lin, C.S., 2007. Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), pp.438-458.

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.

Freeman, E.H., 2007. Holistic information security: ISO 27001 and due care. Information Systems Security, 16(5), pp.291-294.

Hofstede, G., Hofstede, G.J. and 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 March 2016)

Hui, C.H. and Triandis, H.C., 1985. Measurement in cross-cultural psychology a review and comparison of strategies. Journal of cross-cultural psychology, 16(2), pp.131-152.

Humphreys, E., 2009. Are we addicted to information insecurity?. Hagenberg University.

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. ISO/IEC 2005.

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

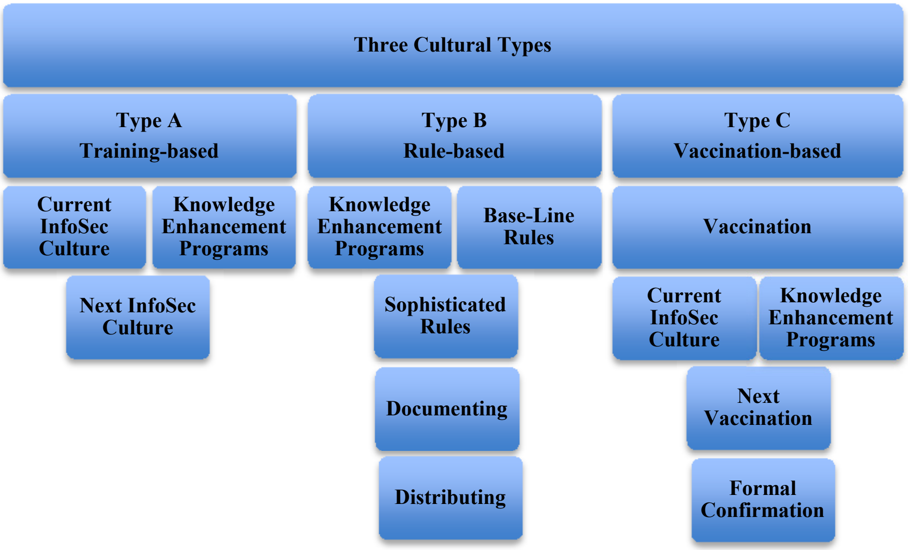
International Organization for Standardization (ISO)., 2014. ISO Survey 2014. ISO/IEC 2014.

Montesino, R. and Fenz, S., 2011, August. Information security automation: how far can we go?. In Availability, Reliability and Security (ARES), 2011 Sixth International Conference on (pp. 280-285). IEEE.

Shojaie, B., Federrath, H. and 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. and 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.

Appendix 1: Three Cultural Behaviours Modelling


Three Cultural Types
Type A
Training-based
Type B
Rule-based
Type C
Vaccination-based
Current InfoSec Culture
Knowledge Enhancement Programs
Knowledge Enhancement Programs
Base-Line Rules
Vaccination
Next InfoSec Culture
Sophisticated Rules
Current InfoSec Culture
Knowledge Enhancement Programs
Documenting
Next Vaccination
Distributing
Formal Confirmation