Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2011

Implementation of ISO 27001 in Saudi Arabia – obstacles, motivations, outcomes, and lessons learned

Belal AbuSaad
King Saud University, Saudi Arabia

Fahad A. Saeed
King Saud University, Saudi Arabia

Khaled Alghathbar
King Saud University, Saudi Arabia

Bilal Khan
King Saud University, Saudi Arabia

Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/105

IMPLEMENTATION OF ISO 27001 IN SAUDI ARABIA–OBSTACLES, MOTIVATIONS, OUTCOMES, AND LESSONS LEARNED

Belal AbuSaad[1], Fahad A. Saeed[1], Khaled Alghathbar[1, 2], Bilal Khan[1]
[1]Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia,
[2]Information Systems Department, College of Computer and Information Sciences,
King Saud University, Saudi Arabia.
bmustafa.c@ksu.edu.sa, fneyaz@ksu.edu.sa, kalghathbar@ksu.edu.sa, bilalkhan@ksu.edu.sa

Abstract

Protecting information assets is very vital to the core survival of an organization. With the increase in cyber-attacks and viruses worldwide, it has become essential for organizations to adopt innovative and rigorous procedures to keep these vital assets out of the reach of exploiters. Although complying with an international information security standard such as ISO 27001 has been on the rise worldwide, with over 7000 registered certificates, few companies in Saudi Arabia are ISO 27001 certified. In this paper, we explore the motives, obstacles, challenges, and outcomes for a Saudi organization during their implementation of ISO 27001, with the goal of shedding some light on the reason behind the low adoption of the ISO 27001 certification standard in the region of study. While customer satisfaction and good partner relationships are essential for an organization's survival, strikingly, none of the organizations interviewed indicated that their goals included meeting consumer requirements or a partner's mandates.

Keywords
Empirical Study; Information Security Standards; ISO 27001; ISMS; PDCA; Policy

INTRODUCTION

Driven by market competition, service improvement, and work efficiency, most organizations today have moved away from a paper-based workplace to the more contemporary and convenient computer-based information technology (IT). Accordingly, protecting such information assets is very vital to the core survival of organizations. With the increase in cyber-attacks and viruses worldwide, it has become essential for organizations to adopt innovative and rigorous procedures to keep these vital assets out of the reach of exploiters.

ISO 27001/27002 (2005a; 2005b) is an international standard for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS). It is a step-by-step guideline that can be used by organizations to evaluate their valuable assets and possible risks, and then build a strategic methodology to protect these assets. ISO 27001/27002 was developed based on the British Standard BS 7799 (British Standards Institution, 1995; 1999), which was designed ten years earlier (1995) for British organizations searching for a strong and reliable management information system. At present (2011), over 7200 organizations worldwide have already certified their ISMS (ISO, n.d.). This standard is built on the concept of a PDCA (Plan-Do-Check-Act) cycle. In the *Plan* phase, emphasis is placed on listing the organization's assets, and then classifying each asset based on its relevance importance to the organization and the kinds of measures needed to protect these assets. The *Do* phase concentrates on the process of implementing these measures. The *Check* phase stresses the procedures used by the organization to evaluate the effectiveness of the measures and, finally, the *Act* phase involves the process of correcting those measure that have proven to be ineffective. The PDCA cycle is a continuous one that needs to be checked and re-evaluated at least once a year.

Our study aimed to explore the motives, obstacles, challenges, and outcomes for Saudi organizations during the implementation of ISO 27001. The data collected in a survey was evaluated to help us explore the reason behind the low adoption of the ISO 27001 standard, despite the benefit from doing so.

The rest of this paper is organized as follows. In Section 2, a representation of related work will be introduced to shed some light on what organizations experience during their implementation of such certification. Section 3 will cover the methodology adopted for our study. Then, Section 4 will present the results of a survey and a data analysis of those results. Finally, Section 5 will present the conclusion and future work of this study.

RELATED WORK

Mataracioglu et al. (2011) argued that the legislation on public information security that an organization has to obey plays a significant role in user acceptance. Their survey model was constructed based on four elements that they perceived had a substantial effect on user acceptance of ISO 27001 implementation in Turkish organizations. The four components included in this model were the perceived usefulness, attitude toward use, social norms, and performance expectancy. Their findings revealed that government legislation on information security should only come after an organization has implemented ISO 27001, otherwise the legislation will only hinder the organization's productivity.

According to Fomin et al. (2008), one reason for the low adoption of the ISO 27001 standard compared with similar standards such as ISO 9001 and ISO 14001 is the lack of scholarly interest in the standard. They discovered that the number of publications dedicated to IS 27001 is relatively low compared with those devoted to information security management systems. Furthermore, the high cost in money and time, as well as the huge amount of necessary paperwork, played a major role in the low adoption of the standard compared to Management System Standards (MSS) such as ISO 9001 and ISO 14001.

Thomas Neubauer et al. (2011) claimed that despite acknowledgements from organizations of the importance of implementing information security standards such as ISO 27001, organizations often refrain from doing so because of the higher cost of implementing such a standard, and the lack of evidence that such a standard has a positive cost/benefit ratio. In their paper, they suggested a two-phase approach that would assist company decision makers to define the best sets of countermeasures for complying with security standards such as ISO 27001. As a first step, they suggested a security ontology that would serve as an Ontological knowledge base for potential countermeasure implementations. The second step involved the implementation of a decision support system, "Antana," which would determine alternative solutions for decision makers that are both feasible for given constrains and efficient with respect to multiple objectives.

Wolfgang Boehmer et al. (Boehmer, 2008) argued that it is essential to have a tool that can measure the effectiveness and economic efficiency of implementing an information security management system (ISMS) based on ISO 27001 in an enterprise. In their paper, they introduced a Key Performance Indicators (KPI) measurement tool based on four levels of hierarchal construction, which would allow an enterprise to evaluate the effectiveness and efficiency of their implementation of an ISMS based on the ISO 27001 standard.

Hong et al. (2003) suggested an integrated system for information security management. In their paper, they proposed the integration of security policy theory, risk management theory, control and auditing theory, management system theory, and contingency theory in order to build a comprehensive theory for information security management (ISM).

Coles Kemp et al. (2006) claimed that the ownership of information security is one of the key elements that are pertinent to the success of making effective, easily-implemented, measurable decisions. Their research concentrated on two aspects of information security ownership: ownership of the asset and ownership of the risk treatment actions.

Evans et al. (2010) argued that a new approach is needed to ensure a reliable and secure engineering system. They stated that implementing either the ISO 27001 or ISO 26702 standard will not fulfill the security needs of an organization. Thus, they felt that a system that integrated both standards would be a more suitable model to ensure more reliable and secure engineering systems.

Hagen et al. (2008) conducted a survey involving Norwegian organizations to evaluate the effectiveness of implementing information security measures. Their findings indicated that technical measures such as security policies and procedures are the most commonly implemented measures, whereas awareness creation activities are less common, even through awareness creation activities are assessed as being more effective organizational measures than technical-administrative ones.

Singh et al. (2007) conducted a survey of Indian organizations to measure the impact of ISO certification on output parameters. Their findings revealed that ISO implementation enhances the output performance of firms; it has positive effects on most aspects of an organization's parameters.

In March 2006, Wander (2008) conducted a survey study in Oulu, Finland to evaluate the implementation experiences for the ISO/IEC 17799 standard. His study revealed that a lack of information about the ISO/IEC

17799 standard was the main cause of resistance among organizations' employees. However, with proactive communication and the use of internal advocates, management was able to overcome this obstacle. Moreover, all of those interviewed acknowledged that ISO/IEC 17799 fits well in their organization. Furthermore, it turned the organization into a more security aware one.

J. Stuart Broderick (Broderick, 2006) reasoned that the idea that an information security management system (ISMS) is the sole responsibility of the security department of the organization is only a myth. In reality, an ISMS must be driven by the executive management of the organization; otherwise ISMS implementation is doomed to fail.

Nabi et al. (2010) conducted a survey to evaluate the status of information security (IS) in Saudi Arabian organizations. Even though Saudi organizations in all sectors showed an interest in determining the effectiveness of their information security controls, at 78%, banks were the most serious about this issue and performed penetration tests more than once per year.

Henning (2009) studied the effectiveness of using the Project Management Body of Knowledge (PMBOK) in the implementation of ISO 27001. His conclusion indicated that higher management involvement and support, as well as project management leadership that is capable of planning, communicating, and negotiating throughout the duration cycle of the project, are key factors for the success of the ISO 27001 implementation process.

METHODOLOGY

In this study, an empirical survey was designed to evaluate the implementation of ISO 27001 in Saudi Arabian organizations. Comprehensive and constructive interviews covered four different areas that organizations will be faced with during the implementation phase of the ISO 27001 certification process, including motivations, obstacles, success factors, and outcomes. The interviews were conducted by arranging personal interviews with the person responsible for implementing and supervising the ISO 27001 project. Out of the thirteen certified Saudi organizations, we were able to conduct eight interviews, which gave the survey a success rate of 61.5%.

DATA ANALYSIS AND RESULTS

The collected data showed that two thirds of the participants were relatively large organizations with more than 500 employees, with only two of the responding companies (25%) indicating 50–500 employees, as shown in figure 1 below. Out of the total respondents, five (62.5%) were governmental organizations, while the rest were telecommunication, IT, and financial services companies.

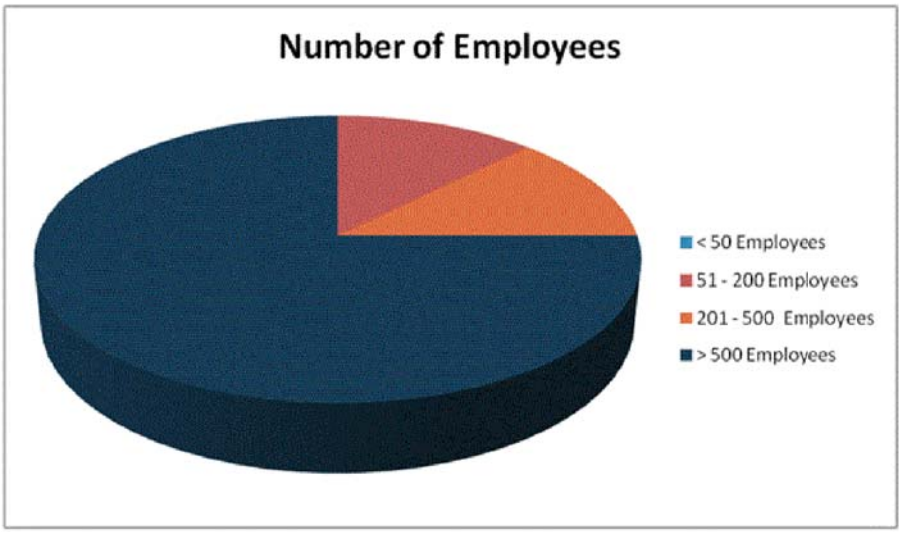

Figure 1 Respondents' distribution based on size of organization that they represented.

Although the survey was quite inclusive, for the sake of brevity, not all of the results can be mentioned here. Selected results in the relevant areas are given to represent the whole situation.

Obstacle factors

Identifying Organization's Assets

As this study revealed, identifying an organization's assets was one of the major obstacles for all of the organizations. Four of the organizations (50%) categorized identifying the organization's assets as a primary obstacle, whereas three (37.5%) stated that it was a secondary obstacle. The final results showed that identifying an organization's assets was the highest rated primary obstacle for all of the organizations. Only one organization stated that identifying assets was not applicable, and the reason behind that was the limited scope of implementation compared with the number of employees that belonged to this scope. Moreover, it should be mentioned that all of the participants in the study identified a limited scope for certification, either specific services or areas, rather than the level of the whole organization, even the one with the small size.

Weak Team Experience

Experience can make or break a project because team members with good experience can tackle challenges and use them to their advantage, while inexperienced teams see minor obstacles as unsolvable problems. When participants were asked if weak team experience was an obstacle during their implementation of ISO 27001 50% said it was a secondary obstacle, while 37.5% stated that it was in fact a primary obstacle. The remaining 12.5% did not see it as an obstacle for their implementation process because this organization is one of the biggest organizations in the IT security industry in the region of study, and their consultants practiced what they tried to preach.

Resistant To Change

When interviewees were asked whether resistance to change from employees in their organizations was a primary or a secondary obstacle during the implementation phase of the ISO 27001standard, three organizations (37.5%) indicated that it was a major obstacle, while three organizations (37.5%) stated that it was a secondary obstacle, and two organizations (25%) specified that it was not applicable.

Unclear understanding of standard

Six of the respondents (75%) stated that understanding the standard was a secondary challenge when starting the process of certificate implementation, while the remainder (25%) stated that understanding the standard was not an issue.

Top Management Involvement

In the case of top management's involvement in the project, four organizations (50%) revealed that top management's involvement in the project was a secondary obstacle, while three (37.5%) indicated that it was not relevant, and only one organization (12.50%) characterized top management's involvement as a primary obstacle. Surprisingly, all of the respondents reported that information security is recognized by top management as an important issue, but it appears that they tend to concentrate on business profits rather than security.

Saudi Arabia's Culture

In general, different cultures and lifestyles could have negative or positive effects on the implementation of an international standard. In this study, we tried to measure the effect of Saudi Arabia's culture on the implementation of an international standard such as ISO 27001. When we asked whether Saudi Arabia's culture had any effect on the implementation of ISO 27001, the answers were as follows: 62.5% of the organizations said that Saudi Arabia's culture was not a factor in the implementation of the standard, another 25% of the organizations mentioned that Saudi Arabia's culture was somewhat an obstacle but not a major one, and the remaining 12.5% indicated that Saudi Arabia's culture was indeed a major obstacle during their implementation process for ISO 27001.

Figure 2 illustrates the obstacle rating factors that influenced organizations during the implementation of the ISO 27001standard in Saudi Arabia.

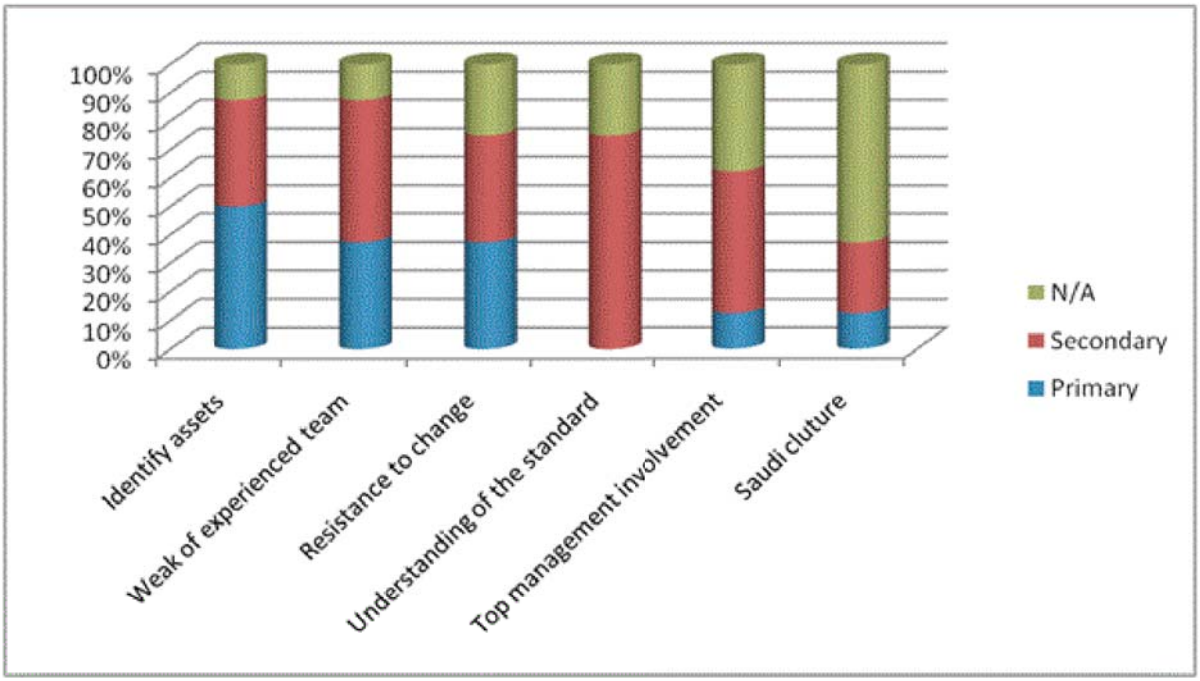

Figure 2 Obstacle factor ratings during implementation of ISO 27001 standard.

Motivation factors

Enhancing Organization's Security

Protecting an organization's assets is essential to the survival of the organization. In this study, we attempted to evaluate the motives behind adopting the ISO 27001 standard in Saudi Arabia. During the interviews, we asked the participants whether enhancing security was a motivating factor for implementing the ISO 27001 standard and all of the organizations (100%) stated that it was, in fact, the number one motivation for adopting the ISO 27001 standard.

Getting competitive advantage

While enhancing the security of the organization was the primary reason for adopting the ISO 27001 standard, at 62.5%, competitive advantage came second in motivating organizations to adopt the ISO 27001 standard. To our surprise, none of the organizations interviewed indicated that one of their goals for obtaining ISO 27001 certification was consumer requirements or a partner's mandates. Figure 3 below illustrates the motivating factor results from the survey.

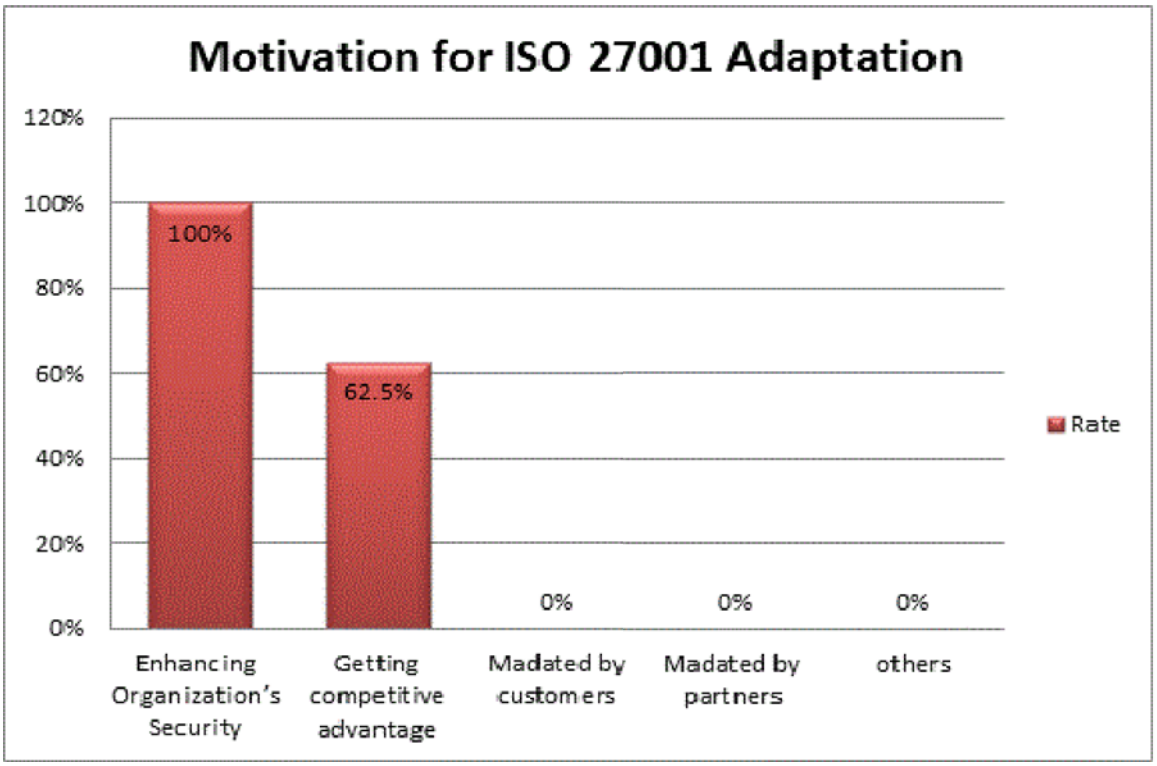

Figure 3 Motivation factors for adopting ISO 27001 standard.

Outcome

Changing Organizational Culture in Relation to Information Security

During the interviews, we asked the participants to point out some of the tangible outcomes they experienced after the implementation of the ISO27001 standard. Five responds felt that a primary outcome of implementing the ISO 27001 standard was a change in the organizational culture in relation to information security, whereas the rest of the organizations (37.5%) considered it to be a secondary outcome.

Providing Formality and Visibility to Information Security

Regarding whether the ISO 27001 implementation had provided formality and visibility to information security practices for the organizations, all of the participating organizations said that it was a primary benefit, even during the implementation processes.

Raising Organization Confidence and Validation

Another topic that was discussed in the interview was whether the ISO 27001 implementation had raised the organization's confidence and validation in relation to the organization's business security. All of the participants (100%) said that it certainly was a primary outcome of the implementation of the ISO 27001 standard.

Managing Business Risks Efficiently

We asked the participants whether managing business risks effectively and efficiently was a major or a minor benefit of the implementation of the ISO 27001 standard. Seven out of eight indicated that it was a primary benefit and only one considered it to be a secondary one.

The diagram in figure 4 below illustrates the most effective outcomes seen by the organizations after their implementation of the ISO 27001 standard.

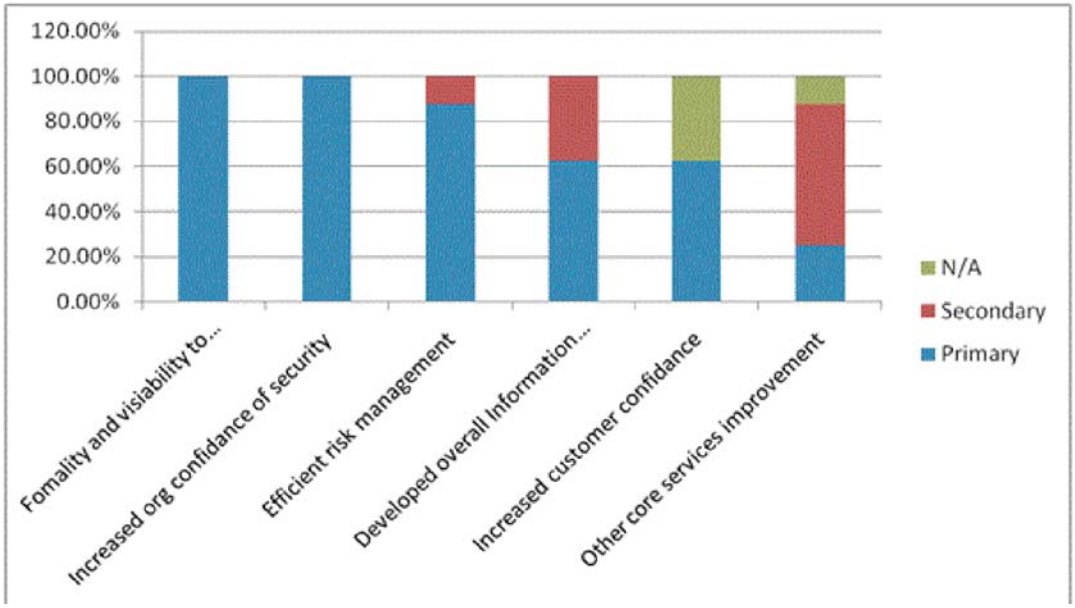

Figure.4 Outcomes of adopting ISO 27001 standard.

Lessons Learned

Just as we asked participants about what challenges and obstacles they faced during the implementation of ISO 27001, we also asked them about their success factors and the lessons that they had learned. The eight organizations stated that coherent planning from the inception to completion of the project, a sufficient budget, and their employees' positive attitude toward the project were the most helpful factors to achieve their goals of implementing the standard. Outstanding project management skills, top management's involvement and contributions, compatibility with existed policies and procedures, employee awareness of the importance of security, and the contribution of existing auditing functions came as secondary success factors, sequentially.

Figure 5 below illustrates the participants' responses about the success factors that they observed.

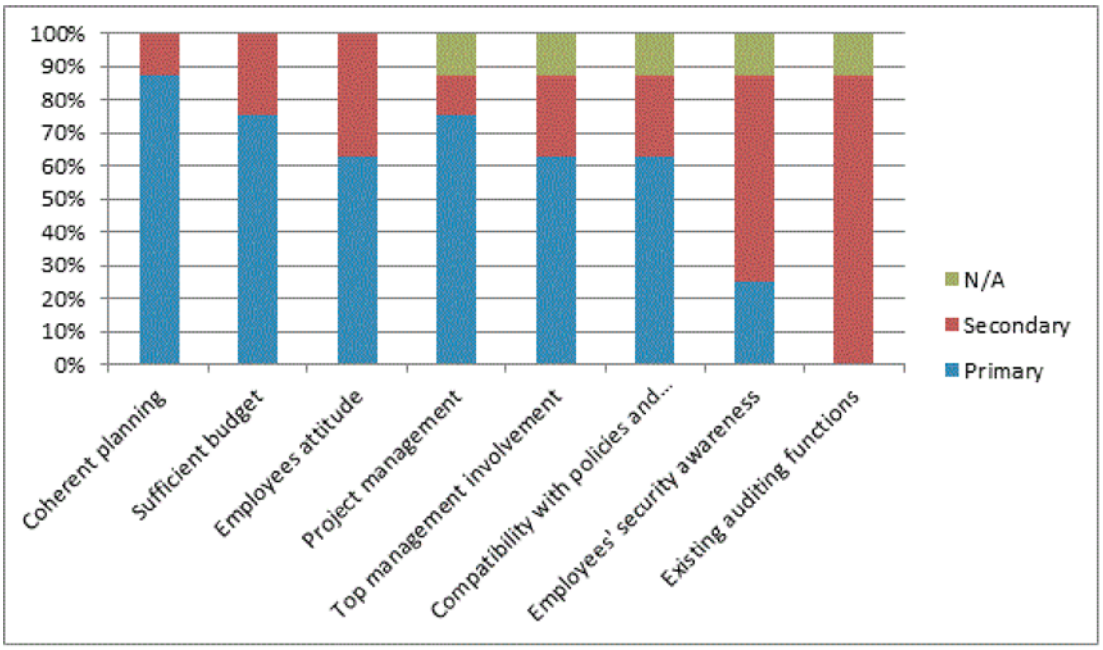

Figure.5 Success factors in implementing ISO 27001 standard.

Even though all of the participants indicated their satisfaction with the way they implemented the ISO 27001 standard, we asked them what they would do differently if they were to implement the standard over again. Almost all of the participants agreed on four primary things that they would do differently, starting with increasing the awareness of the benefits of an Information Security Management System (ISMS), then ensuring staff involvement from the inception to completion of the project, changing the risk assessment approach method, and finally reducing the reliance on external resources.

Figure 6 shows all of the options and their responses according to reported votes.

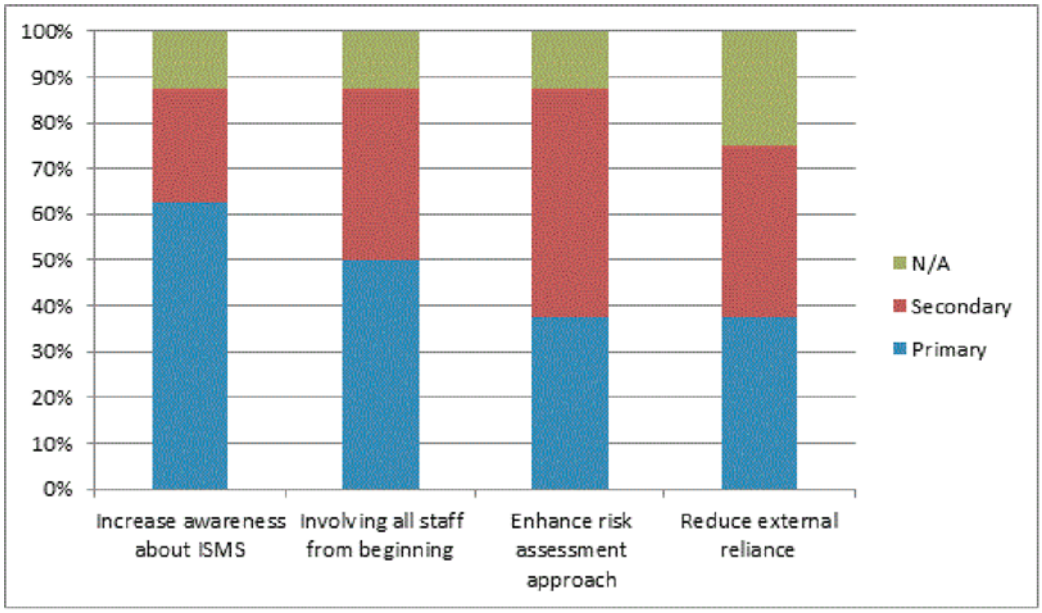

Figure.6 Suggestive changes to the implementation of ISO 27001 standard.

CONCLUSION AND FUTURE WORK

The aim of this study was to provide guidelines and enlightenment for Saudi organizations who are planning to become ISO 27001 certified, including the challenges and obstacles that they are likely to face during the implementation process, as well as efficient and effective ways to tackle these challenges. This should also give them a feeling of what to expect and the kind of benefits that they could achieve from implementing such a standard.

In this study, we tried to shed some light on the types of motivations, obstacles, and outcomes that Saudi Arabian organizations dealt with throughout the implementation phases of the ISO 27001 certification process.

All of the organizations seemed to agree that identifying the organization's assets was one of the major obstacles during the implementation phase, along with a lack of experience on the team. When it came to motivations, enhancing the organization's security level and obtaining competitive advantages were the most reported motivation factors.

All of the organizations expressed their satisfaction with the outcomes, with added formality and visibility for their information security practices along with raising the organization's confidence and validation of their business' security being the most reported benefits from implementing ISO 27001.

In the future, another survey could be conducted that will target small to medium size businesses in Saudi Arabia to explore the main reasons for not adopting the ISO 27001 certification standard.

REFERENCES

Boehmer, W. (2008). Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. *Emerging Security Information, Systems and Technologies, 2008. SECURWARE'08. Second International Conference on* (pp. 224-231). IEEE. Cap Esterel, France.

British Standards Institution. (1995). BS7799-1: Information Security Management Systems – Code of Practice for Information Security Management Systems.

British Standards Institution. (1999). BS7799-2: Information Security Management Systems – Specification with guidance for use.

Broderick, J. S. (2006). ISMS, security standards and security regulations. Information Security Technical Report, Elsevier, 11(1), 26 – 31.

ColesKemp, L. & Overill, R. E. (2006). The Information Security Ownership Question in ISO/IEC 27001 – an Implementation Perspective. *Proceedings of The 4th Australian Information Security Conference*. Perth, Australia.

Ekelhart, A., Fenz, S., & Neubauer, T. (2011). Interactive Selection of ISO 27001 Controls under Multiple Objectives. IFIP Advances in Information and Communication Technology (AICT), 278(278), 477-492.

Evans, R., Tsohou, A., Tryfonas, T., & Morgan, T. (2010). Engineering Secure Systems with ISO 26702 and 27001. *System of Systems Engineering (SoSE), 2010 5th International Conference on* (pp. 1-6). Loughborough, UK.

Fomin, V.V., Vries, H. (2008). ISO/IEC 27001 Information Systems Security Management Standard: Exploring the reasons for low adoption. *Proceedings of The third European Conference on Management of Technology (EUROMOT)*. Nice, France.

Hagen, J.M., Albrechtsen, E., Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. Information Management & Computer Security, 16(4), 377 – 397.

Henning, D. (2009). Tackling ISO 27001: A Project to Build an ISMS. GIAC GCPM Gold Certification, [http://www.iso27001security.com, Date Accessed: Mar 22, 2011]

Hong, K.S., Chi, Y.P., Chao, L.R., & Tang, J.H. (2003). An integrated system theory of information security management. Information Management & Computer Security, 11(5), 243-248.

International Organization for Standardization. (2005a). ISO/IEC 27001:2005(E) Information technology – Security techniques – Information security management systems – Requirements.

International Organization for Standardization. (2005b). ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management.

ISO (n.d). http://www.iso27001certificates.com/. [Date Accessed: Mar 22, 2011]

Mataracioglu, T, & Ozkan, S. (2011). Analysis of the User Acceptance for Implementing ISO/IEC 27001:2005 in Turkish Public Organizations. International Journal of Managing Information Technology (IJMIT), 3(1), 1-14.

Nabi, S.I., Mirza, A.A., & Alghathbar, K. (2010). Information Assurance in Saudi Organizations– An Empirical Study. Security Technology, Disaster Recovery and Business Continuity, 18-28, Springer.

Singh, L. P., A. Bhardwaj, et al. (2007). The Impact of ISO Implementation on Output Parameters in SME's in India. Management of Engineering and Technology, Portland International Center. Portland, OR.

Wander, T. (2008). Implementing the ISO/IEC 17799 standard in practice: experiences on audit phases. *Proceedings of the sixth Australasian conference on Information security-Volume 81*(pp. 115-119). Wollongong, NSW, Australia.