A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors

Zaidatulnajla Hamdi1*, Azah Anir Norman1, Nurul Nuha Abdul Molok2, Farkhondeh Hassandoust3

1Dept. of Information Systems Faculty of Computer Science and Information Technology University of Malaya Kuala Lumpur, Malaysia
2Dept. of Information Systems Kuliyyah of Information and Communication Technology International Islamic University of 4Malaysia (IIUM) Kuala Lumpur, Malaysia
3Auckland University of Technology Auckland, New Zealand

*najelahamdi@gmail.com

Abstract. Organizations have different takes on Information Security Management Systems (ISMS) since security measurements vary according to their business relevance. One way to assure ISMS is being well-implemented is by having a standard compliance such as the ISO 27000 series. The ISO 27000 series is a family of standards that provides a framework for best practice ISMS that helps organizations keep their information assets secure. This paper intends to seek how organizations in different business sectors implement ISMS in their practices. By identifying which organization attains a higher number of ISO requirements, it is anticipated that the characteristics that increase the chances of an organization being certified can be distinguished. This paper reviews case studies regarding the ISMS implementation based on ISO 27000 series between organizations in different business sectors. The result of this paper presents the state of ISO compliance of the organizations. The findings also discussed the characteristics of organizations that are applicable for certification. Through the findings, it is found that the organization, which fulfilled the highest number of ISO requirement, has a stronger possibility of being certified. However, ISO standards should be more dynamic to support diverse business environment thus avoiding generalization to get compliance.

1. Introduction
   A. Background

In these days, information plays an important role for an organization. It is a key asset that guides organization in making decisions and solving problems. Without the right information, an organization is bound to commit errors. Hence, information must be managed properly so that organizations can improve their operations. Information systems is a tool that is used in order to achieve high levels of proficiency and efficiency in business operations. They are generally intended to help in a particular process or to do a specific analysis. Collecting, storing and analyzing information without a proper security measurement will only makes the organization becomes more vulnerable to cybercrimes. No matter the sizes of an organization is, it is essential to create a plan to ensure the security of its information assets. [1] mentioned in his paper that information and information systems are an essential establishment for organizations especially when internal and inter-company data transfer are increasing.
There is no doubt that transferring data is a highly important process in modern business networking, but this key process may actually be the culprit in opening the doors for vulnerabilities and threats.

Information security management does not solely depend on the technical implementations, but also on the administrative efforts. It is a challenge itself to understand how authorities, individuals, and technical elements can work thoroughly in influencing the security of an organization. One of the ways to ensure that information security is being handled properly is by having a compliance towards the international standards. Standards for information security management specify the requirements and processes to enable a business to establish, implement, review and improve information security [2]. There are quite a number of standards exist including COBIT, NIST SP 800 and ISO 27000 series. Being certified based on ISO standards would provide organizations with better credentials and assurance towards its users that their information is safely protected. However, to become ISO compliant requires a lot of controls to be implemented, where some of them may or may not be appropriate for certain business structures.

2. Literature Review

A. Information Security Management Systems

Information Systems Management Systems or ISMS is a set of policies and methods that is used by the management to protect the information security in their daily organization activities. It is based on how proper an organization carries out its risk assessment and measuring its risk acceptance levels to manage risks and vulnerabilities [3]. The definition of ISMS varies throughout the research area. According to [4], ISMS should be considered as an important part of an organization even though the motivation of its implementation varies among different types of organizations. Information security is designed to protect the CIA triad of its data which are confidentiality, integrity and availability from unauthorized access [5].

In structuring the ISMS processes, the plan-do-check-act (PDCA) cycle is often used [6]. The stages of the cycle are [1]:
- PLAN: Designing ISMS
- DO: Implementing and operating ISMS
- CHECK: Monitoring and reviewing ISMS
- ACT: Maintaining and enhancing ISMS.

B. ISO 27001

ISO 27001 is one of the standards under the ISO 27000 series that is the most adopted by several countries and industries [7]. It is a process management and assessment standard [8] that provides specifications for an Information Security Management System (ISMS). This standard consists of two parts [4]: the first part provides the requirements for an ISMS to be implemented, maintained and improved [9], while the second part is annex A that defines the control objectives and security controls. Annex A catalogues a wide range of controls and other measures that are relevant to information security [10]. ISO 27001:2013 is a revised version of ISO 27001:2005. In the 2005 standard, the Annex A contains 133 controls in 11 categories while the revised version contains only 114 controls across 14 categories [11]. Table 1 shows the changes in Annex A domains.

The ISO body performs a survey of certifications to their management standards annually. The survey counts the number of certificates issued by certification bodies that have been accredited by members of the International Accreditation Forum (IAF). Based on the latest survey on 2017, it shows that there is a 7.9% increase in ISO 27001 certification globally [12].

| Table 1. Changes In Annex A Of Iso 27001 |
|------------------------------------------|
| **ISO 27001:2005 [13]**                  |
| **Revised version of ISO 27001:2013 [1]**|
| A.5 Security policy                      |
| Information security policies            |
| A.6 Organisation of Information Security |
| Organization of information security     |
3. Methodology
This paper follows the case study research methodology. The general definition of the term case study is an empirical method aimed at investigating contemporary phenomena in their context. This methodology is commonly used in areas like political science, social work, business, and community planning; with objectives to increase knowledge about individuals, groups, and organizations, in addition of understanding social, political and related phenomena [14]. This approach is suitable for use if the research is focusing to answer “how” and/or “why” questions [15]. Case studies are usually led in real world settings, which in such way have a high level of authenticity and realism. As said in [16] the stages of the methodology are as follows: (a) designing the case study protocol; (b) conducting the case study; (c) analyze the case study evidence; and (d) develop conclusions, recommendations, and implications based on the evidence.

The review process starts with finding the right case studies that are appropriate to the research objectives. The keyword search is “(ISO 27001” AND “gap analysis”). Gap analysis papers are chosen because they examine the current performances of organizations and compare them to their ultimate future goal. Only gap analysis papers of ISO 27001:2013 are accepted as the standard for 2005 is already obsolete. After narrowing down the collected papers, the case studies chosen are compared to find their similarities. Evidence from other literature are also gathered to support the results of the comparison. Finally, conclusions and recommendations are developed according to the results obtained.

The research questions expected to be answered in this paper are as follows:
RQ1: How do organizations in different business sectors implement ISMS in their practices?
RQ2: What are the characteristics that increases the chances of an organization to be certified?

4. Case Studies: Organization Background
This paper reviews four different case studies between a non-profit institute, an educational institute, small and medium (SME) enterprises and enterprises. The details are as explained in Table 2.
Table 2. Case Study Details

| Organization Case Study | Business Details | Author, Year |
|-------------------------|------------------|--------------|
| Non-Profit              | Performs information gathering from the cyberspace. Its business nature requires them to implement a good information systems security since they are depending on information technology to do their job. | Briliant, 2016 [17] |
| Educational Institute   | Provides learning services in graduate studies. As any other modern institutes, they use information systems and technologies in their daily operations. Therefore, there is a need for this organization to maintain their security in order to avoid threat exposal | Nasser, 2017 [11] |
| Enterprises             | A group of enterprises in health care, internet and telecommunication, distributor of equipment and hotels | Candiwan, 2014 [18] |
| Small and Medium Enterprises | The similarities are they have less than 250 employees. The characteristics of choice are learn & education, IT, IT & consultant and logistic & delivery | Candiwan, 2014 [18] |

5. Results And Discussion

In order to implement ISO 27001:2013, organizations are required to prepare and produced specific documents. The standard specified several clauses that are often called the “shall” clauses that are mandatory if the organization wants to be compliant to the standard [17]. As seen in Table 4, these clauses include the Annex A controls too. The levels of compliance are defined as follows [11]:

- Compliant: The organization is fully compliant with the ISO 27001 specifications.
- Partially compliant: The organization has taken several steps towards being compliant but still requires further work to be commenced.
- Non-compliant: The organization has not taken any controls to serve the ISO 27001 requirements.

Table 3 shows the numbers of control requirements that are not fulfilled by the organizations. The red columns indicate controls that are not fulfilled at all (zero implementation), while the green columns indicate controls that are completely fulfilled. The phrase “completely fulfilled” here however, does not connote that they are compliant.

The higher percentage of not fulfilled in Table 3 shows that the organization is lesser compliant that the others. The percentage is calculated by taking the number of controls fulfilled divided by the number of requirements controls available in each domain.

Based on the gap analysis results in the case studies, none of the controls are 100% compliant. Organization B, for example, in domain (A.7), is only partly compliant on all six controls, implying 100% partly compliance. Organization C, on the other hand, in domain (A.5), albeit showing 0% requirements not fulfilled, is actually only 25% fully compliant [18].
Table 3. ISO 27001:2013 Gap Analysis Comparison Result

| Domains | Requirement Controls | Percentage of Controls Not Fulfilled (%) | Percentage of Each Domains Not Fulfilled (%) |
|---------|----------------------|------------------------------------------|---------------------------------------------|
|         |                      | A  | B  | C  | D  |                                  |                              |
| A.5     | 2                    | 100.0 | 100.0 | 0  | 0  |                                   | 50.0                         |
| A.6     | 7                    | 57.1  | 28.6  | 42.9 | 42.9 |                                   | 42.8                         |
| A.7     | 6                    | 33.3  | 0     | 16.7 | 16.7 |                                   | 16.7                         |
| A.8     | 10                   | 40.0  | 0     | 50.0 | 30.0 |                                   | 30.0                         |
| A.9     | 14                   | 64.3  | 7.1   | 35.7 | 35.7 |                                   | 35.7                         |
| A.10    | 2                    | 100.0 | 10.0   | 50.0 | 50.0 |                                   | 52.5                         |
| A.11    | 15                   | 20.0  | 0     | 40.0 | 26.7 |                                   | 21.7                         |
| A.12    | 14                   | 57.1  | 7.1   | 35.7 | 28.6 |                                   | 32.1                         |
| A.13    | 7                    | 71.4  | 14.3  | 42.9 | 42.9 |                                   | 42.9                         |
| A.14    | 13                   | 84.6  | 7.7   | 61.5 | 46.2 |                                   | 48.5                         |
| A.15    | 5                    | 100.0 | 20.0  | 60.0 | 80.0 |                                   | 65.0                         |
| A.16    | 7                    | 85.7  | 14.3  | 14.3 | 42.9 |                                   | 39.3                         |
| A.17    | 4                    | 100.0 | 0     | 50.0 | 25.0 |                                   | 43.8                         |
| A.18    | 8                    | 100.0 | 12.5  | 50.0 | 25.0 |                                   | 46.9                         |
|         |                      | 78.6  | 0.07  | 28.6 | 14.3 |                                  |                              |

It can be seen that organization A has the highest number of domains not fulfilled (A.5, A.10, A.15, A.17, and A.18) while organization C and D both are on par with all domains completely fulfilled. Although organization B does have one domain with 100% non-compliance, it has the greatest number of domains with 100% completely fulfilled (A.7, A.8, A.11, and A.17). The biggest difference that can be seen in these four organizations is in clause (A.5) which is information security policies. Both C and D completely fulfilled control (A.5), contrasting organization A and B that shows 100% non-compliance towards the same control.

It seems that organization A is the least compliance since the percentage of domains not fulfilled that is more than 50% is very high compared to the other three. It has 78.6% domains not fulfilled out of the 14 domains in Annex A. Meanwhile, organization B leads the chart with less than 1% that is not fulfilled, followed by D with 14.3% and C with 28.6%.

Table 4. Mandatory Requirements For ISO 27001 [17]

| Document | ISO 27001:2013 Clauses | Not Completely Fulfilled |
|----------|------------------------|--------------------------|
| 1        | Scope of the ISMS      | 4.3                      |
| 2        | Information security policy and objectives | 5.2 and 6.2 | X |
| 3        | Risk assessment and risk treatment methodology | 6.1.2 | X |
| 4        | Statement of Applicability | 6.1.3 d | X |
| 5        | Risk treatment plan    | 6.1.3 e and 6.2          | X |
| 6        | Risk assessment report | 8.2                      | X |
| 7        | Definition of security roles and responsibilities | A.7.1.2 and A.13.2.4 | X |
| 8        | Inventory of assets    | A.8.1.1                  |
| 9        | Acceptable use of assets | A.8.1.3 | X |
| 10       | Access control policy  | A.9.1.1                  |
| 11       | Operating procedures for IT management | A.12.1.1 | X |
Table 4 maps the mandatory clauses and its fulfilment with each organization. This list, however, does not portray the complete results as some case studies only reported as much. There is no information on organization B on which clauses does it fulfill. By comparing both Table 3 and Table 4, it can be concluded that none of these organizations are fully compliant towards ISO 27001. However, it is safe to say that organization B has the highest chances on getting certified since the number of controls fulfilled is the highest.

A as a non-profit institution concerns more on its human resources security, and physical and environmental security, but overlooked their information security policies, cryptography, supplier relationship, information security aspects of business continuity management, and compliance. On the other hand, B, as an educational institution focuses more on their human resources security, asset management, physical and environmental security, and information security aspects of business continuity management. However, as well as A does, B is also less concerning on its information security policies and organization of information security.

C and D, as their main characteristics are business organizations, differs the other two when they have 0% of domains not fulfilled, although most of them are only partially compliant. C as enterprises, contrasts A and B when its highest concern is on information security policies. D as small and medium enterprises, on the contrary, focuses most on its information security policies, and human resources security. Both C and D are low in concerning on systems acquisition, development and maintenance, and supplier relationship whereas C is also low in cryptography.

|   | Secure system engineering principles | A.14.2.5 |
|---|--------------------------------------|----------|
| 12 | Supplier security policy             | A.15.1.1 | X   |
| 13 | Incident management procedure        | A.16.1.5 |
| 14 | Business continuity procedures       | A.17.1.2 | X   |
| 15 | Statutory, regulatory, and contractual requirements | A.18.1.1 | X   |
| 16 | Records of training, skills, experience and qualifications | 7.2 |
| 17 | Monitoring and measurement results    | 9.1 |
| 18 | Internal audit program               | 9.2     | X   | X   |
| 19 | Results of internal audits           | 9.2 |
| 20 | Results of the management review     | 9.3 |
| 21 | Results of corrective actions        | 10.1    |
| 22 | Logs of user activities, exceptions and security events | A.12.4.1 and A.12.4.3 |

Figure 1. Average Percentage Of Domains Not Fulfilled
The least focused control among the 14 domains in Annex A as seen in Figure 1 is domain (A.15) which is supplier relationships. It shows a whopping number of 65.0% not getting fulfilled by organizations. This means that most of the organizations do not implement controls on what to include in agreements and how to monitor the suppliers. On the contrary, the most concerned control among all is domain (A.7) that is human resources security with only 16.7% not fulfilled. This implies that, no matter how an organization structure is, despite its variety of business objectives, human resources security is the main concern as employees are indeed the backbone of every organization. (A.7) is a control in which is related to controls prior to employment, during, and after the termination of employment. The next in line is domain (A.11) which is physical and environmental security with 21.7% non-fulfilment. This is a control that is related to defining secure areas, protection against threats, entry controls and equipment security.

6. Conclusions

Generally, all types of organizations do take concern on their information security as there are several security implementations that has been done. However, each and every one of them is still too far away from getting ISO 27001 certification. It can be concluded from the obtained results that the rank on getting compliance ready is led by an educational institution (B), followed by enterprises (C), then small and medium enterprises (D), and lastly is a non-profit institution (A). Non-profits tend to not put significant efforts in implementing information security even though they do handle sensitive information [19]. They have low awareness in securing information properly because of the mindset that a “do-good” organization will not be susceptible to cybersecurity attacks [20]. In order to avoid from security breaches or fraud potential, it is important for any type of organization to ensure that they have a continuous security management.

There are some limitations in completing this study as there are not much literature can be found in this area, especially case studies focusing on specific organization implementing ISO27001:2013. Gap analysis papers that are published using the 2005 standard is not relevant to answer the research questions.

Future work should endorse on how different organization structures set up affects the number of controls being compliant towards ISO 27001. Researchers are suggested to look into whether their main business operations map the requirements of ISO 27001 properly.

ACKNOWLEDGMENT

This work is financially supported by the grant RP044C-17HNE from University of Malaya, Kuala Lumpur, Malaysia.

References

[1] A. Z. Maingak and L. D. Harsono, “Information Security Assessment Using Iso / Iec 27001: 2013 Standard,” vol. 17, no. 1, pp. 28–37, 2018.
[2] R. van Wessel, X. Yang, and H. J. de Vries, “Implementing international standards for Information Security Management in China and Europe: a comparative multi-case study,” Technol. Anal. Strateg. Manag., vol. 23, no. 8, pp. 865–879, 2011.
[3] “INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and,” vol. 2018, 2018.
[4] B. Shojaie, H. Federrath, and I. Saberi, “Evaluating the effectiveness of ISO 27001: 2013 based on annex A,” Proc. - 9th Int. Conf. Availability, Reliab. Secur. ARES 2014, no. Fares, pp. 259–264, 2014.
[5] S. Alaboodi, “Towards evaluating security implementations using the Information Security Maturity Model ( ISMM ),” 2007.
[6] K. Haufe, S. Dzombeta, and K. Brandis, “Proposal for a Security Management in Cloud Computing for Health Care,” vol. 2014, 2014.
[7] B. Shojaie, H. Federrath, and I. Saberi, “The effects of cultural dimensions on the development of an ISMS based on the ISO 27001,” Proc. - 10th Int. Conf. Availability, Reliab. Secur. ARES 2015, pp. 159–167, 2015.
[8] A. N. Shivashankarappa, L. Smalov, R. Dharmalingam, and N. Anbazhagan, “Implementing it governance using COBIT: A case study focusing on critical success factors,” World Congr.
[9] R. Almeida and M. Mira, “A Model for Assessing COBIT 5 and ISO 27001 Simultaneously,” *2018 IEEE 20th Conf. Bus. Informatics*, vol. 01, no. July, pp. 60–69, 2018.

[10] B. David, B. Fbcs, and M. N. Fbcs, “Insights into the ISO / IEC 27001 Annex A,” no. December, 2010.

[11] A. A. Nasser, “Information security gap analysis based on ISO 27001 : 2013 standard : A case study of the Yemeni Academy for Graduate Studies , Sana ’a , Yemen,” vol. 3, no. 11, pp. 4–13, 2017.

[12] Laurent Charlet, “ISO Survey,” 2017. [Online]. Available: https://www.iso.org/the-iso-survey.html.

[13] I. Al-mayahi and S. P. Mansoor, “ISO 27001 Gap Analysis - Case Study,” *Secur. Manag. (SAM), 2012 Proc. Int. Conf.*, p. 1, 2012.

[14] P. Runeson and M. Höst, “Guidelines for conducting and reporting case study research in software engineering,” *Empir. Softw. Eng.*, vol. 14, no. 2, pp. 131–164, 2009.

[15] P. Baxter and S. Jack, “The Qualitative Report Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers,” *Qual. reporalutivat Rep.*, vol. 13, no. 2, pp. 544–559, 2008.

[16] R. K. Yin, *Case study research: Resign and methods*, 1st ed. Beverly Hills, CA: SAGE Publishing, 1984.

[17] O. C. Briliyant, “ISMS Planning Based On ISO / IEC 27001 : 2013 Using Analytical Hierarchy Process at Gap Analysis Phase ( Case Study : XYZ Institute ),” no. 4, pp. 4–9, 2016.

[18] Candiwan, “Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia,” no. 1, pp. 50–58, 2014.

[19] T. R. Imboden, J. N. Phillips, J. D. Seib, and S. R. Fiorentino, “How Are Nonprofit Organizations Influenced To Create and Adopt Information Security Policies ?,” *Issues Inf. Syst.*, vol. 14, no. 2, pp. 166–173, 2013.

[20] K. Rudolph, “Implementing a Security-Awareness Program,” *Comput. Secur. Handb.*, p. 49.1-49.47, 2015.