Readiness of Information Security Management Systems (ISMS) Policy on Hospital Staff Using e-Patuh System

Waidah Ismail[1], Najwa Haayati Mohd Alwi[1], Roesnita Ismail[1], Mahadi Bahari[2], Omar Zakaria[3]
[1]*Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Negeri Sembilan,Malaysia*.
[2]*Faculty of Computing, Universiti Teknologi Malaysia (UTM), Johor, Malaysia*.
[3]*Pusat Pengajian Siswazah, Universiti Pertahanan Nasional Malaysia (UPNM), Kuala Lumpur, Malaysia*.
waidah@usim.edu.my

***Abstract*—ISO 27001:2013 is the best-known standard providing requirements for information security management systems (ISMS). An ISMS is a systematic approach to manage sensitive information through people, processes and IT systems. In a hospital, a patient's individual medical record is highly private and sensitive. This study performed qualitative questionnaire based on the ISO27001:2013 policy. Seven hospitals in Malaysia were involved in this study. This study focus on the Data Center as it contains a high risk server. This study reveals the non-compliance issues among the sampled hospitals in Malaysia. The participation of the hospitals in trainings related to information security awareness and education were still not adequate due to lack of support from the top management. The Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), the Ministry of Health Malaysia and the top management in hospitals in Malaysia play vital roles to educate and ensure the compliance of ISO 27001:2013.**

***Index Terms*—Data Centre; Hospital Information Security Management Systems; ISO 27001:2013; Malaysia.**

I. INTRODUCTION

Information security refers to the process to protect information assets which includes software, hardware and human awareness. The key characteristics of the information security are confidentiality, integrity and availability that need to be managed properly throughout any organisation.

Within the health industry, it is the requirement to adopt the information security management systems (ISMS) for continuous operation and protection of personal data. This is also the way forward in applying for the accreditation for ISO 27001:2013 [1]. ISMS will ensure a comprehensive approach to information security in the organisation where the effect of security events can be reduced by timely detection and reporting. In addition, ISMS will ensure better planning and investment in areas where proper management and elimination of security threats are needed to prevent losses and to take care of the organisation's good name, its brand and reputation.

A patient's individual medical record is highly private and sensitive. Negligence and reporting errors on patient medical report might change the treatments and can cause patient harm. Good management of patient medical records protects physicians and hospitals against claims of negligence as well as protects patient. This study focuses on the readiness of ISMS policy among Malaysian hospitals' staff using e-Patuh system.

The remainder of this paper is organized as follows. The related work is presented in Section II. Section III explains the research methodology used in the study. The result and analysis is discussed in Section IV. Finally, conclusion is drawn in Section V.

II. RELATED WORK

Information is a valuable asset [2] and has value to an organisation. It needs to be protected against misuse, disclosure and destruction. Information security is not just a simple matter of having usernames and passwords [3]. Regulations on data privacy and data protection policy impose a raft of obligations to organizations [4]. Information security is achieved by implementing a suitable set of controls or countermeasures to ensure the integrity and security of the information they use to make critical business decisions [5]. This could be organizational countermeasures (i.e., policies, practices, procedures, organisational structures and awareness), and technical countermeasures (i.e., hardware and software functions). These controls need to be established to ensure that the specific security objectives of the organisation are met.

Information security awareness has been developed in in European countries. American consumers have come to demand an assurance that their personal privacy is protected and awareness of their medical information. There are two Acts in America, i.e. The Health Insurance Portability and Accountability Act (HIPPA) of 1996 for medical information and the Gramm-Leach-Bliley Act for 1999 for financial information [2]. Recently, Michael Schumacher's medical files have been stolen and offered for sale to the media, the files are thought to have been stolen from his hospital in Grenoble [6]. In Seoul, the hacking attack brought down the servers of South Korean broadcasters YTN, *Munhwa Broadcasting Corporation* (MBC) and *Korean Broadcasting System* (KBS) as wells as two major commercial banks, Shinhan Bank and Hong Hyup Bank. It took five days to recovery from the attack in Mac 2013 [7].

Thus, there is an awareness increase on the need to protect the information systems that are crucial to continue daily business function. In order to address all areas of security concerned, businesses need to approach it more holistically to cover network security, personnel, physical and environment security, and business continuity [8]. This approach includes prescribing to recognised certification

standards–a security policy of sorts that can help organisations measure their security policies and procedures against universally accepted codes of practice. Therefore, certification standards laid, would provide the framework around which an organisation can create its security strategy and develop security best practices. The comparison has been listed between five standards i.e. ISO27001, BS7799, Payment Card Industry Data Security Standard (PCIDSS), Information Technology Infrastructure Library (ITIL) and Control Objectives for Information and related Technology (COBIT) [2]. These standards playing its own role and position in implementing ISMS. For example ISO 27001 and BS7799 focus on information security management system while PCIDSS focus on information security related to business transactions and smart card. ITIL and COBIT focus on information security and its relation with the Project Management and IT Governance.

In Malaysia, Information Technology and Internet Government (JITIK) Bil 1/2006 dated 8 May 2006 agreed that Standard ISO/IEC 27001:2005 Information Security Management System (ISMS) related with Information Communication and Technology Security Management should be implemented in Government sectors. In 27 July 2012, the Ministry of Health received their accreditation by Malaysian Administrative Modernisation and Management Planning Unit (MAMPU). Malaysia is in the 13th place on the status of accreditation of ISO 27001 [9] (see Table 1).

Table 1
List of Country and ISO 27001 Accreditation [9]

Status	Country	Total	Status	Country	Total
1	Japan	4152	8	Korea	107
2	UK	573	9	USA	105
3	India	546	10	Italy	82
4	Taiwan	461	11	Spain	72
5	China	393	12	Hungry	71
6	Germany	228	13	Malaysia	66
7	Czech Republic	112	14	Poland	61

However, the implementation of ISMS is not being fully enforced to all hospitals in Malaysia. MAMPU reveals the number of information security threats occurred since 2010 to October 2013 and intruder was reported as the highest security treat in 2011 (see Table 2).

Table 2
Incident Occurrence in 2010 - 2013[9]

No	Incident Classification	Incident Occurs			
		2010	2011	2012	2013 (as at Oct)
1	Intrusion	214	393	337	201
2	Malicious Code	6	5	1	2
3	Harrassment/ Threat	0	0	0	0
4	Attempts/Hack Threat/ Information Gathering	1	12	4	0
5	Physical Loss	0	0	0	0
6	Spam	3	1	2	0
7	Forgery	0	0	1	0
8	Denial of Service	0	2	2	0
9	Violation of Policy	3	6	0	0
	Total Incident	228	419	347	203

III. Research Methodology

Figure 1 shows the process of conducting the study where it started with reviewing the policy of ISO27001:2013, then designed and developed the questionnaire based on the ISO27001:2013. Next, the printed questionnaire was distributed to the Head of Information Technology in seven public hospitals around Klang Valley in Malaysia. To uphold the secrecy, those hospitals were named as A, B, C, D, E, F and G respectively. The collected data was analysed to find the gaps between the hospitals that did not comply with ISMS. E-Patuh system is the first step in introducing the awareness of ISMS among the staffs in Ministry of Health (MOF).

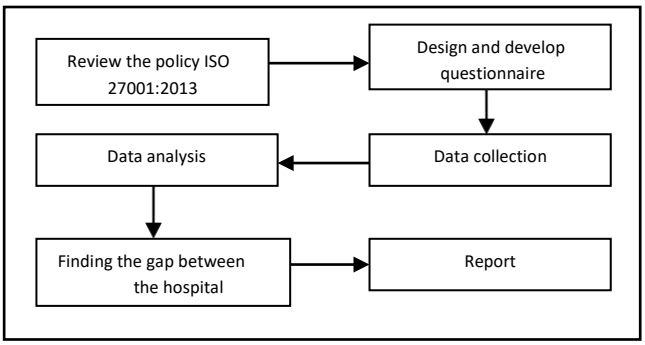

Figure 1: Research process in conducting the study

IV. Result and Analysis

The result and analysis are divided into three sections based on the awareness of ISMS, source of knowledge of ISMS and its compliance.

A. Awareness of ISMS

Among the seven sampled hospitals, the results revealed that 86% of the hospitals were aware about the ISMS. Although the policy ISMS ISO:27001 2013 was released in Malaysia during October 2013 [10], it was very surprised to find out that majority of the hospitals (82%) in this study did not aware on the implementation of ISMS ISO:27001 2013. The results revealed that three sampled hospitals were using the local information security policies namely "Dasar Keselamatan ICT" developed by the Ministry of Health Malaysia (see Figure 2). Another two hospitals have developed their own security policies and the remaining two hospitals indicated that they were using Quality Management policy, "Akta Kerajaan Elekronik 1997", email policy and others. Thus, it reflects that some hospitals are still confuse and did not know the differences between the Quality Management policy and the ICT policy. However, all the seven hospitals at least have one of the Business Contingency Plan, Disaster Recovery Planning, Security Audit, Risk Management server.

B. Source of Knowledge on ISMS

It is useful to identify the source of knowledge on ISMS among the sampled hospitals. Figure 3 shows that most of the hospitals in this study learnt about ISMS from the Internet, MAMPU and their top management. This is parallel with the compliances section which also revealed that knowledge of ISMS from the top management has the highest compliances. This is true as the top management's role is important for the success of ISMS implementation.

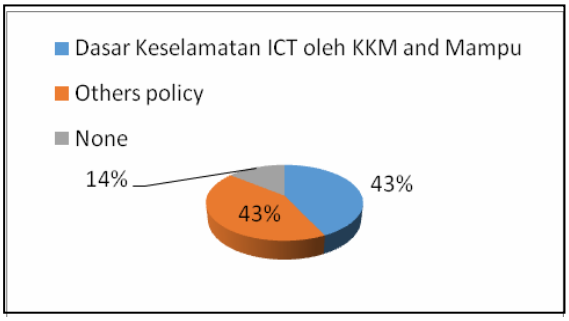

Figure 2: Type of policies that being implemented in hospital.

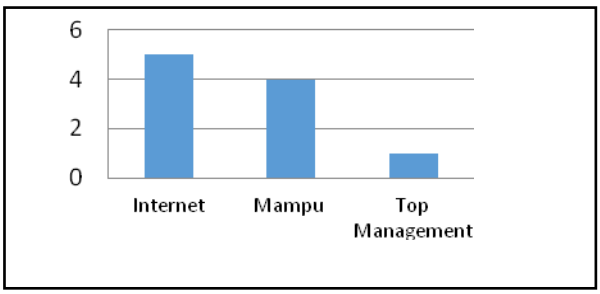

Figure 3: Sources of ISMS knowledge

Figure 4, on the other hand, shows that only 43% of the hospitals encouraged their staff to attend for any information security awareness, education and training. Top management should be responsible for the successful implementation of the ISMS and the well-being of the organisation. Creating an awareness program on ISMS requires numerous resources, a clear understanding of security within the organisation especially supports from the top management.

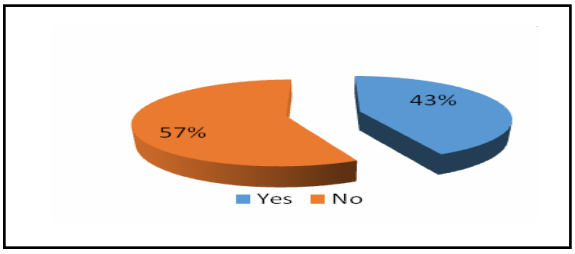

Figure 4: Information security awareness, education and training among hospital staff

C. Compliance

This section highlights the overall compliance status in the seven sampled hospitals. Figure 5 reveals that Hospital D has non-compliance issues. Hospital records and the patients' data are in the high risk information and can be categorized as private and confidential. Hospital F has the highest compliances of the ISO 270001:2013 where they learnt about ISMS from the top management. However, Hospital F is yet to apply for the certificate of ISO 270001:2013. Hospital A, E and G generally are compliance with the ISO 270001:2013 issues, respectively.

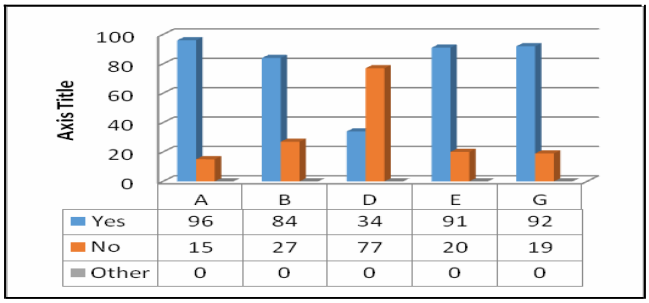

Figure 5: Overall Compliance ISO 27001:2013 that being implemented in hospital.

D. Non-Compliance

Table 3 summaries the non-compliances issues for the seven seven selected hospitals in this study.

Table 3
Non-Compliances Issues

Item	Result	Discussion
A.5 Information Security Policy	All hospitals provide management direction and support for information security in accordance with business requirements, relevant laws and regulations except one hospital. Only one hospital is not timely reviewed to ensure its continuing, suitability, adequacy and effectiveness	Mostly all comply with the Management Directions for information security and only one hospital did not review the policy.
A.6 Organization of Information Security	One hospital does not have any appropriate contacts with other relevant authorities to ensure appropriate advice and action is taken in any security incident that might occur and segregation of work. All of the hospitals did not maintain contact with special interest groups. Only one hospital does not has any manage to define statutory, regulatory, policy or contractual requirement to control the implementation of information security in project management.	Mostly of the hospital comply with the item organization of information security but none of them have contact with special groups.
A.7 Human Resource Security	Four hospitals did not perform the verification checks on employee, contractors and third party based in the laws, regulation and ethics. Only two hospitals did not have terms and conditions of the responsibilities of information security of employees, contractors and third party to agree and sign. Only two hospitals did not have the involvement of the management require the employees, contractors and third party user to apply security in accordance with the policies and procedures established in the organizations. Four hospitals did not provide the information security awareness, education and trainings. One hospital does not have the disciplinary process for employees who have committed a security breach. Two hospitals did not have the termination or change of employment responsibilities.	Only one hospital comply all the items. Overall did not comply on the training and educate the staff.
A.8 Asset Management	One hospital does not have an information classification been defined and documented. Two hospitals did not have any proper management of removable media. Two hospitals did not have dispose the media securely and safely when no longer. And one hospital does not have procedure in transferring the physical media	Most of the hospital comply on the asset management such as inventory, ownership and acceptances of the assets

Item	Result	Discussion
A.9 Logical Security / Access Control	One hospital did not comply on the clearly define the access control matrix policies and policy on the use of network services. One hospital did not have any organisation restrict and control the allocation and use of privileges id. Only two hospitals did not review the user access rights. Only one hospital does not define and document the roles and responsibilities of the users. Three hospitals did not have the interactive systems for managing the password to ensure the quality of passwords. Three hospitals did not defines clearly and document the use of privileged utility program. Lastly in the items 9, only one hospital did not manage to log all the access activities on the program source code.	Most of the hospitals comply on the logical security and access control but they still need to define the matrix of the user, review the user privileges id, user access rights review and log activities on the program source code.
A. 10 Cryptography	All the hospital did not comply the key management to support the organisation's use of cryptographic techniques and except one hospital only comply the develop and implement a policy on the user of cryptographic controls for protection of information	All the hospitals did not implement the cryptography to protect the confidentiality, authenticity or integrity of information.
A.11 Physical and environmental Security	Only one hospital did not comply on the secure areas by prevent unauthorised physical access. Only one hospital did not implement by identify and define security controls to enable employee working in secure areas. Two hospitals did not comply by ensuring that the equipment, information software and physically destroyed or securely overwritten prior to disposal. Four hospital did not implement the off-site equipment considers the different risks of working outside the organization premises, storage equipment that contain sensitive data and licensed software are destroyed or overwritten to prior of disposal and in ensuring the unattended equipment has appropriate protection. All of the hospitals did not comply the adopt a clear desk policy for papers and removable storage media and also clear screen policy for information processing facilities except one hospitals	All of the hospitals comply on prevent of the secure area on the physical access of organisation's information and information processing facilities. Half of the hospital comply on prevent loss, damage, theft on assets and interruption in the organisations.
A.12 Operations Security	Only one hospital did not comply the operating procedures documented, maintained which available to all users, changes of information processing facilities and systems. Two hospitals did not comply on the control and manage any illegal installation or download activities that impact the capacity of the information processing. Only one hospital did not perform the protection of logging facilities and log information against the unauthorized access including the administrator, operator logs, and control of operational software and restriction on software installation. Two hospitals did not comply with clock synchronization. Three hospitals did not comply with the timely information about technical vulnerabilities of the systems. Only one hospital did not have check on the operational systems.	Mostly all the hospitals comply with the operational procedures and responsibilities in which to ensure the correct and secure operation of information processing facilities. All of the hospitals perform the protection from Malware and backup features. Most of the hospital perform the logging and monitoring to record events and generate evidence if there is any hacking or post-mortem. Almost of the hospitals have the information of protection of logging facilities, administration, operation logs, and software restriction on installation. The hospital that did not have the logging facilities cannot perform any checking on the operational systems.
A.13 Communi- cations Security	Only one hospital did not comply with all items in the Network security management. One hospital also did not comply with security of network services and segregation of works. Two hospitals did not comply with information transfer. Two hospitals did not comply with the secure communication or transition. One hospital also did not have the establishment with the non-disclosure agreement with the organization or external parties.	Most of the hospitals comply with the network security management. Most of the hospitals comply with the information transfer policies and procedures and agreement on information transfer.
A.14 System acquisition, development and maintenance	Only two hospitals did not comply with security requirements of information systems. Only one hospital did not comply with securing applications services on public networks. Only three hospitals comply all the security in development and support processes. Two hospitals did not comply with define clearly the secure. Development policy and control the implementation by the use of formal control procedures. And two hospitals did not perform the business critical review application and test to ensure there is no adverse impact and restrictions on changes to software package. Two hospitals did not define clearly the system development procedures including new development and change management policy. One hospital did comply with separate development environment with other environment, manage to control and monitor system planned, approved, tested and logged and lastly system acceptance testing. Only two hospital did not protection of test data where the select test data carefully, protect and control.	Only hospital outside Klang Valley did not comply with security requirements of information systems. Only three hospitals comply all the security in development and support processes. And only hospitals did not comply all. Only two hospitals did not comply three items in the section security in development. And one hospital complies two items in the section. Most of the test data comply with hospitals.
A.15 Supplier relationships	Five hospitals comply with security in supplier relationship and one hospital did not comply all of the items. One hospital did not comply with the information security policy for supplier relationships and addressing security within supplier agreements. Two hospitals did not comply with managing changes to supplier services, where take account of the critical of business systems and processes involved using re-assessment of risk.	Four hospitals comply with supplier relationships and only one hospital did not comply all of the items.
A.16 Information Security Incident Management	Three hospitals comply all of the items in the information security incident management where to ensure a consistent and effective approach with the management of information security incidents, including communication on security events and weaknesses. One hospital did comply all of the items. Two hospitals did not comply with the incident management committee to assess, manage and make decision and collection of evidence. Three hospitals did not comply with the learning from information security incidents and two hospitals did not comply with assessment and decision of information security events and response to information security incidents.	Three hospitals comply all the items in the information security incident management and one hospital did not comply all of the items. One hospital comply all the items except where the information security incidents to be quantified and monitored.

Item	Result	Discussion
A.17 Business Continuity	Five hospitals comply with information security aspects of business continuity Management and only hospitals did not comply all of the items. One hospital comply all except on the organization perform verification, reviewing and evaluation on the information security continuity that addresses each of area and responsible	Most of the hospitals comply with the business continuity.
A.18 Compliance	Four hospitals comply with the information security reviews to ensure that information security is implemented and operated in accordance with the organization policies and procedures. One hospital did not comply with all the items. Two hospitals did not comply with independent review of information security and one hospital did not perform the technical compliance inspection. All of the hospitals did not comply with regulation of cryptographic controls except one hospital. One hospital did not comply with the legal and contractual requirements. One hospital did not comply with identification of applicable legislation and contractual requirements. One hospital did not comply with the implementation of intellectual property rights and one hospital did not comply with privacy and protection of personal information.	Most of the hospital comply the compliance except the regulation of cryptographic controls. It shows that most hospital did not perform the cryptographic.

V. DISCUSSION AND CONCLUSION

The implementation of ISMS in any health providers or hospitals is more likely require support and commitment from the top to bottom and both (see Figure 6). The instruction and enforcement of the policy should be from the top management, thus the technical team will implement the policy and the user will adhere to the stated policy. However, this study revealed that most hospitals in the Klang Valley did not have their in-house developed policy and merely refer to Dasar Keselamatan ICT developed by the Ministry of Health and MAMPU. In contrast, hospitals that are located outside the Klang Valley are using the Quality Management System Policy. This study also revealed that the IT Personal are still confuse on which policy that they should implement in their hospitals.

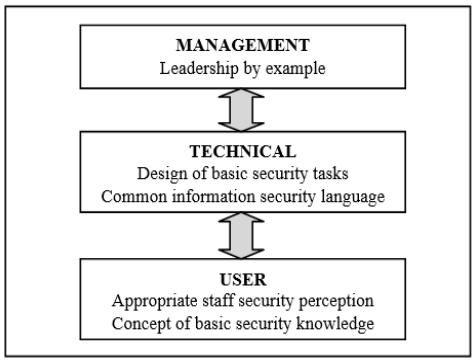

Figure 6: Information security groups in the three organization levels. [11]

Figure 7 shows the flow chart of ISMS implementation in hospitals in Malaysia. MAMPU has successfully enforced the Ministry of Health in accreditation of ISMS since 24th November 2010. The Ministry of Health received the ISMS accreditation with MS 27001:2007 on 27th July 2012. However, none of the hospitals in Malaysia have implemented ISMS or have their own developed policy. Moreover, the participation of the hospitals in trainings related to information security awareness and education were still not adequate due to lack of support from the top and seniors management. This is likely due to hospitals initially facing financial constraints.

This study revealed that the knowledge of ISMS among the urban hospitals was better than the rural hospitals. This is likely due to the latest cutting edge information related to ISMS thorough various source especially the Internet and support from the top management. Indeed, the top management plays vital roles to ensure the compliance of ISO 27001:2013. The Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) and the Ministry of Health Malaysia should educate and make aware on the importance of ISO 27001:2013 compliance among hospitals in Malaysia. The ISMS awareness and readiness should be educate among the IT Personal, medical staff as well as administrative staff within the hospitals. Good and secure management of patient medical records protects physicians and hospitals against claims of negligence as well as protect their patients' rights.

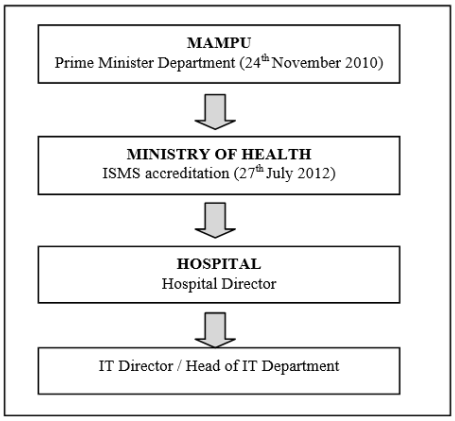

Figure 7: Flow chart of ISMS implementation in Malaysia

ACKNOWLEDGMENT

This research was supported by a research grant (PPP/UTG-0213/FST/30/12213) at the USIM and we greatly valued the participation of Hospital Universities in Malaysia in this research study.

REFERENCES

[1] ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems – Requirements, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed- 2:v1:en [Accessed 13 February 2015].

[2] Susanto Heru, Almunawar, Mohammad Nabil and Yong Chee Tuan (2011). Information Security Management System Standards: A Comparative Study of the Big Five, International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 05.

[3] Basie Von Solms And Rossouw Von Solms (2004). The 10 Deadly Sins Of Information Security Management. Computer & Security 23(2004) 371-376. Elsevier Science Ltd.

[4] Herd Susanto and Farhad Muhaya (2010). Multimedia Information Security Architecture Framework, Proceeding Future Information Technology (FutureTech) 2010, pp.1-6, 21-23 May 2010.

[5] Harord F, Tipton and Micki Krause (2003). Information Security Management Handbook (5th Edition).

[6] Daniel Johnson (2014). http://www.telegraph.co.uk/sport/motorsport/formulaone/michael-schumacher/10921311/Michael-Schumachers-files-stolen-from-hospital-and-offered-for-sale-to-the-media.html [Accessed 13 February 2015].
[7] Ju Min Park (2013). http://www.reuters.com/article/2013/03/21/us-korea-north-attack-idUSBRE92K02W20130321 [Accessed 13 February 2015].
[8] Alan See (2013). Security - holistic, certified and audited, 2013 http://www.e-cop.net/files/articles/20030218.pdf [Accessed 13 February 2015].
[9] Wan Hanisah Binti Mior Zainuddin, Pengurusan Sistem Keselamatan Maklumat MS/ISO/ IEC 27001:2007) Sektor Awam – Presentation slides.
[10] N. A.. http://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/ [Accessed 13 February 2015].
[11] OB Zakaria (2007). Investigating information security culture Challenges in a public sector Organization: A Malaysia case – OB Zakaria. Thesis PhD. Royal Holloway, University of London.