9th International Workshop on Frontiers in Availability, Reliability and Security (FARES 2014),
University of Fribourg, Swizerland, Sep 11, 2014

Evaluating the effectiveness of ISO 27001:2013 based on Annex A

Bahareh Shojaie, Hannes Federrath
University of Hamburg
{shojaie,federrath}@informatik.uni-hamburg.de

Iman Saberi
Hamburg, Germany
isaberi@gmail.com

***Abstract*—The part of the management system of an organization dealing with information security is called Information Security Management System (ISMS). The most adopted ISMS standard is ISO 27001:2005. The 2005 version of the standard has been updated in 2013 to provide more clarity and more freedom in implementation, based on practical experiences. This paper compares ISO 27001:2005 and the updated 2013 standard, based on Annex A controls. We classify the controls into five categories of *data, hardware, software, people* and *network*. All of the controls defined in Annex A, regardless of their objectives, can easily be allocated to at least one of these categories. Classifying the controls to known categories offers an integrated view of the updated standard and presents a suitable guide for evaluating the performance and efficiency of the updated standard.**

Keywords—Information Security Management Systems, ISMS

I. INTRODUCTION

An Information Security Management System (ISMS) contains all instruments and methods the management should use to satisfy information security in all tasks and activities. In order to protect assets within an organization, the concept of the ISMS provides a set of policies, procedures, guidelines, related resources and activities to be managed. The establishment and implementation of the ISMS in an organization is based on the needs, objectives, processes, size, structure, and unique security requirements. In the general management structure, it is crucial to consider the ISMS as an important part of an organization, which is implemented in different organizations with different motivations. The most important reasons for implementing this security management system are market assurance and governance.

The idea of developing a code of practice for information security was first introduced by the British Standards Institution (BSI) and UK in 1995 as BS7799. The standard was split into two parts in 1999, which covers both, code of practice (BS7799-1) and specifications for certification (BS7799-2). In 2000, BS7799-2 was adopted as 17799 by ISO as a best practice for information security [12]. ISO 17799 consists of management level recommendations for IT security management. ISO 17799 and ISO 27002 [14] were merged in the beginning of 2007 [6].

Important ISO standards before the ISO 2700x family of standards were ISO 13335 and the already mentioned ISO 17799. ISO 13335 is a reference point for IT security management, which consists of general guidelines and instructions.

During a revision in 2005, ISO 27001 was developed as specifications [13] and ISO 27002 was recognized as a code of practice for ISMS. ISO 27002 contains a set of management level recommendations to define a framework for security management in an organization.

Alison Anderson and Dennis Langley developed a security management system [1] based on the security studies of different organizations, and proposed three groups for monitoring the internal security policy implementation:

- Information system,
- Information system assets, and
- Information system environment.

In 2006, STOPE (Strategy, Technology, Organization, People and Environment) was introduced by [20]. This approach is based on "six sigma" by using ISO 17799:2005 for evaluating and continuously improving ISMS.

In December 2011, more than 17000 certificates were issued around the world, which shows the significance of having ISMS certificates in industry [7]. ISO 27001:2005 was technically revised for the first time in October 2013 [16]. Discovering and studying the reasons behind this update can help organizations to examine and evaluate their current security management systems.

This paper leads organizations to practical improvements in their ISMS by categorizing the controls defined in the updated standard to five groups of *data*, *hardware*, *software*, *people* and *network*. The five categories provide a better understanding and allow a new classification of controls. The benefits of this categorization are fully described in Section III.

An organization can benefit from this categorization and can finally identify which part of their organization needs more attention regarding relevant vulnerabilities. The results from several recent security surveys are used for each category to find out whether the updated standard considers certain security breaches in the modified (updated) controls.

The remainder of the paper is organized as follows: Section II compares ISO 27001:2013 and ISO 27001:2005 based on their specifications and contents. Section III, which is the main contribution of the paper, discusses Annex A controls. First, the five categories are described, and then the controls that have been changed in ISO 27001:2013 are investigated. Section IV demonstrates the results of the analysis of several security surveys. Section V concludes the paper.

II. ISO 27001:2005 VS. ISO 27001:2013 BASED ON THEIR STRUCTURE AND CONTENT

ISO 27001:2013 looks structurally and fundamentally different from ISO 27001:2005. The updated standard is based on

Annex SL, which is the main reason for this notable distinction. Annex SL is a guideline to integrate ISO management system standards. All the revised management system standards have to integrate and adapt to this high level structure (Annex SL) as well. For instance, ISO 22301:2012 on business continuity and ISO 27001:2013 (as mentioned) are already published with conformance to Annex SL and ISO 9001 (quality management system) [5].

The requirements for establishing, implementing, maintaining and continually improving ISMS are defined in different clauses of ISO 27001:2013. For conformity to ISO 27001:2013, any exclusion of the requirements from clauses 4 to 10 is not acceptable. These requirements are defined in a way to provide a variety of choices for implementation. For example, preparing an inventory of assets is no longer a requirement for risk assessment. The titles and the contents of the clauses 4 to 10 in the updated standard are different from ISO 27001:2005. Every clause defines a document requirement, based on the definition and specifications of each clause, for example the document requirements for clause 4 is "scope" and for clause 8 is "the results of risk treatment plan". Clauses 4 to 7 specify requirements for establishing ISMS, while clauses 8 to 10 identify the implementation requirements.

In ISO 27001:2013, each requirement is mentioned only one time and there are no duplicate requirements (for instance preparing a list of documents is no more required). The order of requirements in these clauses is not important for the implementation. As a result, the specification part of ISO 27001:2013 is more practical.

Besides, the terminologies and terms are changed, for instance, instead of "preventive action", the term "actions to address risks and opportunities" is used [7]. The requirements for "management" are replaced with "leadership". Totally, the contents of the updated standard are simpler, which makes it easier to understand. The updated standard is not based on the Plan-Do-Check-Act (PDCA) cycle anymore. Therefore, related phrases and concepts are changed, such as "continual improvement" instead of PDCA.

ISO 27001:2005 is a process-based approach, which is compatible with ISO 9001:2000 and ISO 14001:2004. In ISO 27001:2005, the terms and definitions were mentioned in the body of standard and the normative reference (that is deriving from this standard) is ISO 27002:2005. ISO 27000:2013 is mentioned as a normative reference for ISO 27001:2013. Additionally, in ISO 27001:2013, the name of ISO 31000:2009 is mentioned as a reference to determine the internal and external context of the organization. To adapt to ISO 31000, the priority of outlining assets, threats and vulnerabilities for defining risk is eliminated, which gives more freedom to organizations in practice.

According to ISO 27001:2005, Annex A is a checklist to make sure all essential controls are considered and no necessary control is ignored by the organization. However, ISO 27001:2013 recommends that controls have to be selected in the progress of risk treatment. Based on this fact, a risk treatment plan has more priority than Annex A controls, which presents the results gained from the risk treatment. It also defines the necessary controls that need to be implemented to protect an organization from determined risks. ISO 27001:2013 is more flexible with different risk assessment methodologies [2] as there is no prerequisite for identifying risk.

The Statement of Applicability (SOA) contains the organization's information security control objectives and controls. In ISO 27001:2013, the SOA will have more clarity based on the definition of the controls by the risk treatment process, because it puts more emphasize on objectives, monitoring and measuring the performance, as the ISMS registration does not guarantee the quality of performance [3].

According to the "2013 information security breaches survey" referenced in [11] which defines UK companies' damages in cyber space, 32% of the organizations did not measure the effectiveness of information security. Therefore, the updated standard pays more attention to efficiency and performance of the implemented controls. Based on the ISO 27002:2013 guidelines referenced in [17], there is a connection between the implementation requirements of each control with other relevant controls. For example, ISO 27002 mentions A.5.1.1 "policies for information security" and A.8.1.2 "ownership of assets" as supportive controls for implementing A.6.1.1 "information security roles and responsibilities" control.

For transition to the updated version, documents and contexts have to adapt to the new structure, and the new controls need to be implemented and finally efficiency and usefulness of the controls have to be measured [7]. There are some areas, which do not require any changes, such as control of documentation. Nevertheless, there are some other areas that require a rethink like objectives of the management system [5]. The objectives in the updated standard are defined based on all relevant functions and all levels. Careful planning plays an important role for a successful transition to the updated standard.

III. ISO 27001:2005 VS. ISO 27001:2013 BASED ON THE CONTROLS DEFINED IN ANNEX A

The main part of both ISO 27001 and ISO 27002 is Annex A, which plays an important role in the ISMS implementation procedure. ISO 27001:2005 Annex A consists of 133 controls defined in 11 control objectives. The updated standard has deleted, rewarded and merged some controls, which makes the grouping of the controls more logical. As a result, ISO 27001:2013 has 114 controls defined in 14 control objectives.

A. Categorization

ISO 27001 consists of two parts: The first part defines the specifications, requirements and definitions, and the second part is Annex A, that illustrates the control objectives and controls. Once an organization decides to implement an ISMS based on ISO 27001:2013 or to update its current management system, the responsible personnel face high-level controls in various control objectives.

In the following, both versions of ISO 27001 (2005 and 2013) are compared based on their controls by using our five categories (*data, hardware, software, people* and *network*). These categories are general enough to provide freedom in implementation and specific enough to prevent any confusion by different interpretations. Categorizing the controls to five

easy classifications brings a better understanding of the reasons for update. If the number of the controls is increased or decreased in one category, it generally gives the impression that there are some issues related to these controls, which require an update.

An organization will also benefit from our five categories by classifying their revealed security flaws into these five categories in order to determine their level of security in a classified and systematic manner. The results of different security surveys, such as "information security breaches survey 2013" [11], are also useful to share and communicate the global weaknesses, based on the type of the organization. These investigations support the aim of ISO 27001 as a common business language to help organizations to share the same controls for similar risks.

Furthermore, categorizing the controls makes it especially easier for small and medium organizations/enterprises (SMEs) to implement the necessary and relevant controls based on their own business requirements. SMEs – compared to large companies – have different characteristics, and ISO 27001:2005 provide special recommendations for them [15], taking into account their budget and their relevant threats. Most of the SMEs cannot afford to establish an ISMS in the entire organization. Thus, SMEs are the main target of our categorization, which guides them to select efficient controls based on existing security gaps.

The three main versions of ISMS standards (as mentioned) are BS7799:1999, ISO 27001:2005 and ISO 27001:2013. This paper compares the number of controls defined in each of these three standards, based on our five categories (*data*, *hardware*, *software*, *people* and *network*). However, the main focus of the paper is on the comparison of ISO 27001:2005 and ISO 27001:2013. Due to limited space we only present an aggregated view.

The assignment of the controls to our five categories can be found at https://svs.informatik.uni-hamburg.de/annexApaper/.

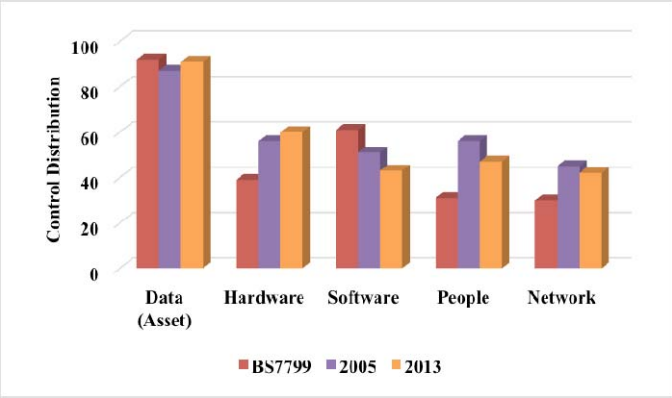

Figure 1. Comparison between BS7799, ISO 27001:20005 and ISO 27001:2013 based on our five categories.

The comparison between ISO 27001:2005 and ISO 27001:2013 based on five main categories shows a remarkable difference between the highest category (*data*) and the lowest category (*network*) (see Fig. 1). Apart from the focus of the controls of both standards, the contents of the updated standard controls are distinctive based on the requirements of new developed or improved relevant technologies.

In all three standards, the main focus is on *data* and the least emphasis is on *network*. In ISO 27001:2013, the number of controls relevant to *data* and *hardware* are increased. Nevertheless, the quantity of controls regarding *software*, *people* and *network* is decreased.

The fairly increase of *data* in ISO 27001:2013 (compared to the 2005 version) illustrates the significant importance of data assets. It is notable that additional controls are required for protecting the most important and sensitive asset, which can cause severe problems in case of loss. In both small (less than 50 employees) and large (more than 250 employees) organizations, business disruption had the most financial loss [11], which shows the critical concept of *data*. Anyway, *data* has a high priority in both versions of ISO 27001.

One of the reasons for updating ISO 27001:2005 was the growth and development of new information technologies and information security technologies, which are quite important for keeping data safe and secure. Besides that, an additional control group "cryptography" with two controls (crypto policy and key management) was introduced in ISO 27001:2013, which expresses a remarkable emphasize on safeguarding data assets in the updated standard.

The *hardware* related controls are reasonably increased in ISO 27001:2013. The important concept of physical security is one of the possible reasons for the grown number of relevant controls, which was probably not sufficiently considered in the past. Based on [11], 67% of the organizations cover both information and physical security, while fewer small organizations pay attention to physical and information security compared to 2012. This is one of the possible reasons for the increased number of *hardware* controls. Another possible reason is the development of information technology: Most of the communication and network devices such as switches, routers and firewall hardware just implement the lower layers – layer 2 (data link) and layer 3 (network) – of the OSI (Open Systems Interconnection) model [18]. However, since the concepts of information security management mainly focuses on the higher OSI levels – layer 4 (transport) up to layer 7 (application) –, these lower layers were not entirely covered in the ISO 27001 standards. In general, ISO 27001:2005 *data* and *hardware* controls were required to improve towards protecting these important assets from new security breaches presented by updated information technologies.

In contrast, the number of ISO 27001:2013 controls is dropped noticeably in category *software*. This reduction probably demonstrates that ISO 27001 is not well suited for software developers, although they have to consider security as one of the important issues of secure software design. Apart from that, viruses and malware affect fewer organizations regardless of their size, based on the 2013 security survey [11].

According to the CSI Computer Crime and Security Survey 2010/2011, the respondents who had security breaches believe, that enhanced security settings in their infrastructure can help to reduce security issues [9]. Moreover, the Security Tech Center [21] published some examples of *software* related security

breaches and improvements in Microsoft affected software, the relevant vulnerability impact and the restart requirement in November 2013 in order to improve the quality of relevant products. Oracle also provided several security solutions to safeguard its products. SAP as the third largest software company provides different security solutions such as identity management, access control and risk management. These mentioned developments help significantly to enhance the security of software related products, which leads to considerable revision in software related controls.

The attention of ISO 27001:2013 to *people* is also decreased fairly. In general, this illustrates an improvement in people's and employee's security behavior and knowledge. The people's security awareness seems increased in eight years (2005-2013), and in practice people pay more attention to information security. Consequently, a smaller amount of controls is required to manage people's activities, and the ISO 27001:2013 has removed some of the controls relevant to the minimum acceptable amount of security that has to be fulfilled. These outcomes probably show that ISO 27001:2005 was successful in improving people's security basic knowledge.

The number of controls focused on *network* almost remains constant in both – 2005 and 2013 – versions of the standards. The ISO 27001:2013 concentration on *network* is decreased gradually. This reduction demonstrates that ISO 27001:2005 focuses slightly more on *network* security. One of the possible reasons is the number of *network* relevant controls that were appropriate to provide acceptable level of security. In the 2013 standard, some of the *network* related controls are now merged or redundant controls are eliminated. However, the difference is not significant.

To summarize, the controls relevant to *data* and *hardware* categories are increased in ISO 27001:2013 since recent advances in IT – for instance A.10 "Cryptographic controls" or A.15 "Supplier relationships" – brought new security issues that had to be addressed in the updated standard. Besides, based on Deloitte Touche Tohmatsu Limited's 2013 annual report referenced in [10], the technology, media and telecommunication organizations challenge security issues presented by cloud computing and mobile technologies. On the other hand, the number of the controls relevant to *software* and *people* is decreased as the results of improvements in IT and people's security knowledge. Finally, *network* related controls remain approximately stable.

B. Inserted and deleted controls

This section mostly focuses on the modified controls in ISO 27001:2013. The modified controls are divided into two groups. The first group is controls that are eliminated from ISO 27001:2005 and the second is the inserted controls to the updated standard that were not mentioned before the 2013 version.

The overall number of controls in ISO 27001:2013 is decreased (133 to 114), although the number of control objectives is increased (11 to 14). Therefore, ISO 27001:2013 has 19 controls less than ISO 27001:2005, and uses 3 additional control objectives (cryptography, operations security, supplier relationship). In the updated standard, 20 controls are deleted and 11 controls are inserted. About 7% of the total 114 controls defined in the updated standard are mapped to more than one control in ISO 27001:2005 (merged). For instance, A.6.1.1 "Information security roles and responsibilities" in ISO 27001:2013 is mapped to two controls in ISO 27001:2005, namely A.6.1.3 "Allocation of information security responsibilities" and A.8.1.1 "Roles and responsibilities".

The new controls introduced in ISO 27001:2013 are mostly located in clause A.14, which defines "System acquisition, development and maintenance" [8]. A.14 comprises of two sub-clauses (classifications), "Security requirements of information systems" and "Security in development and support processes". However, most of the eliminated controls are from A.6 "Organization of information security", A.11 "Physical and environmental security", and A.12 "Operations security".

As the first step, the inserted controls are analyzed based on our five categories. The most concentration of the inserted controls is on *data*, while the least focus is on *network*. *Software* and *hardware* have the same level of distribution, followed by *people* (see Fig. 2).

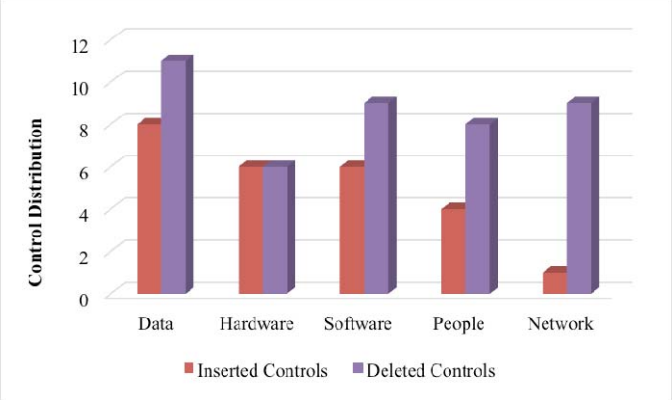

Figure 2. Comparison between deleted controls from ISO 27001:2005 and inserted controls into ISO 27001:2013 based on our five categories.

As the second step, the deleted controls are being investigated. As expected, the most focus of the deleted controls is on *data* and the least focus is on *hardware* (which has the same level as the inserted controls). Then, *software* and *network* have the same level, followed by *people*.

As Fig. 2 shows, the control distribution of deleted controls, based on our five categories, has higher values compared to inserted controls (except *hardware* related controls where both inserted and deleted controls has the same value). Most of the deleted controls are not brought into ISO 27001:2013, but were merged and distributed in the updated standard, based on recent development requirements (For example A.6.2.1 "Identification of risks related to external parties" is replaced by A.15.1.1 "Information security policy for supplier relationships").

There is a remarkable and sharp decrease of controls regarding *network*. This impressive result was predictable as ISO 27001:2013 controls have the least focus on *network*. This leads us to the assumption that the *network* relevant controls, which are eliminated from ISO 27001:2005, are not replaced in the updated standard. So, the inserted controls introduced by

the updated standard do not concentrate on this category *(network)* as expected.

These observations indicate that *data* relevant controls required the highest level of revision and/or became more important from the viewpoint of the editors of the updated standard. The improvements to *data* relevant controls can be divided into two groups. The first group is the withdrawn controls that were deleted from ISO 27001:2005. Most of these *data* related controls are not applicable in 2013 according to the improved IT and information security technologies that have been developed since 2005 (for example A.10.8.5 "Business information systems").

The second group is the updated controls being inserted into ISO 27001:2013. These improvements bring new security issues that have to be addressed in the updated standard to replace the former relevant deleted controls (for example A.14.2.1 "Secure development policy" or A.6.1.5 "Information security in project management" that are inserted to the updated standard). Likewise, A.12.6.2 "Restrictions on software installation" by a user, A.14.2.1 "Secure development policy" or maintaining security in software development lifecycle are notable results of the recent improvements in software industry, as the second focus of both inserted and deleted controls.

IV. Discussion of Results of Security Surveys

Up to this section, the controls of the two latest versions of ISO 27001 were thoroughly analyzed. In this section, we investigate the results of several information security breaches surveys in order to find relations between security breaches and ISO 27001:2013 controls.

According to [11], there are three times more security breaches than 2012. 93% of large and 87% of small organizations had security breaches. As stated by [22], hacking is the most relevant security incidents that occur to both – small and large – types of organizations (small organizations have less than 1000 employees, while large organizations have more employees). However, large organizations mostly suffer from physical incidents. According to ISO 27002:2013 guidelines referenced in [17], the major reason for system failure is the inappropriate use of system administration privileges, which gives users unauthorized access or permission to system (*people* category).

According to [11], 93% of the companies had staff security breaches as a result of not understanding the policy perfectly [4]. The internal risks from employees and staff are also rising. In small organizations, attacks by unauthorized outsiders were the most reason for security breaches [11]. In large organizations, most attacks came from insiders (*people* category). These investigations indicate the importance of category *people* to information security, which might not been adequately controlled in recent years.

As said by [19], the countries that experienced the most costly data breaches spent the most effort on detection (investigation and assessing data breaches) and notification (such as IT activities for employing outsider experts). Accordingly, these organizations try to compensate the security breaches by improving the categories *network* and *people*.

According to [11], large organizations are weak in network security. Based on ISO 27002:2013, unauthorized access to network services is one of the weaknesses that can affect the whole organization. The other main weakness [17] is insecure connection to network services, which requires special attention while working with critical or sensitive business applications (*network* category).

Small organizations are weak in user education and awareness, home and mobile working, incident management, monitoring and removable media controls as well as network security [11]. According to [10], information security training and awareness as well as mobile security were the main drivers for improving information security in 2013 (*people* and *network* categories).

As a result of these findings, the updated standard is expected to give further emphasize on *people* and the important concept of "policy". There are two solutions regarding *people*, first, to increase and improve the awareness and training programs and forcing strict policies, and second, to improve the security of organizations infrastructures and to find out their security weaknesses. It might be helpful to concentrate on safeguards relevant to restricting and monitoring people's behavior and user access control with assistance of ISO 27001:2013 guidelines (covering both *people* and *network* categories). This advice is more useful in practice as external parties exploited most of data breaches [22] and the ability of attackers is unknown.

An increasing target of both, insider and outsider attacks, are small organizations [11]. Based on the general weaknesses according to small organizations, they have to focus on security flaws revealed in the process of risk assessment and use the Annex A as a checklist to ensure information security.

To sum up, for securing *hardware*, *software* and *data*, organizations can use the updated Annex A guidelines as a reference based on their requirements. Though, for protecting *people* and *network*, the ISO 27001:2013 controls are probably not sufficient, i.e. additional safeguards are required. According to the requirements and particular characteristics of each organization, further controls may be required to mitigate the relevant vulnerabilities based on the results of risk assessment and recommended best practices by experts. In general, providing the basic security principles and training the staff can be helpful to reduce security breaches.

V. Conclusion

This paper classifies the controls of ISO 27001:2013 into five categories, *data*, *hardware*, *software*, *people* and *network*, which can help organizations to improve and evaluate their ISMS performance and practical efficiency. Our classification is also useful to evaluate the efficiency of ISO 27001 based on the defined controls in Annex A in order to provide organizations with better insight and understanding of their current security management system and relevant security flaws.

The updated standard generally highlights and emphasizes the concepts of *data* and *hardware*, while controls relevant to *software*, *people* and *network* are decreased. The main focus of the new introduced controls (ISO 27001:2013) and deleted

controls (ISO 27001:2005) is mainly on *data* and *software*. Overall, *data* gets the greatest level of improvement. ISO 27001:2013 provides appropriate controls for the categories *data*, *software*, and *hardware.* For *people* and *network* categories, additional security controls are likely needed.

It is recommended to establish an acceptable level of security for *data*, *software*, and *hardware* categories (based on determined risk assessment criteria) and mainly to concentrate on the efforts to strengthen the *people* and *network* classifications, according to organizational features and business types.

REFERENCES

[1] Anderson, A., Longley, D., and Kwok, L.F., Security modeling for organizations, CCS '94 Proceedings of the 2nd ACM Conference on Computer and communications security, New York, 1994, p. 241- 250.

[2] Blakley, B., McDermott, E., and Geer, D., Information Security is Information Risk Management, NSPW '01 proceeding of the 2001 workshop on new security paradigms, New York, 2001, p. 97- 104.

[3] Boehmer, W., Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO 27001, The Second International Conference on Emerging Security Information, Systems and Technologies, 2008, p. 224 - 231.

[4] Bradley, D., and Josang, A., Mesmerize: an open framework for enterprise security management, ACSW Frontiers '04 Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalization, Australia, v. 32, 2004, p. 37- 42.

[5] Brewer, D., Understanding the new ISO management system requirements, BSI, London, 2014.

[6] Bundesamt fu□r Sicherheit in der Informationstechnik (BSI), BSI-Standard 100-1 Information Security Management Systems (ISMS), Bundesamt fu□r Sicherheit in der Informationstechnik, Bonn, Germany, 2008.

[7] British Standards Institution, Moving from ISO 27001:2005 to ISO 27001:2013, BSI, London, 2013.

[8] British Standards Institution, Mapping between the requirements of ISO 27001:2005 and ISO 27001:2013, BSI, London, 2013.

[9] Computer Security Institute, 2010/2011 Computer Crime and Security Survey, 2011, http://gocsi.com (January 10, 2014).

[10] Deloitte Touche Tohmatsu Limited, Blurring the lines 2013 TMT Global Security Study, 2013, http://deloitte.com (January 10, 2014).

[11] Department for Business Innovation and Skills, 2013 Information Security Breaches Survey, BIS, London, 2013.

[12] International Organization for Standardization/ International Electro technical Commission, ISO 17799:2000: Information technology – Code of practice for information security management, 2000.

[13] International Organization for Standardization/ International Electro technical Commission, ISO 27001:2005: Information technology – Security techniques – Information security management systems – Requirements, 2005.

[14] International Organization for Standardization/ International Electro technical Commission, ISO 27002: 2005: Information technology– Security techniques–Code of practice for information security management, 2005.

[15] International Organization for Standardization/ International Electro technical Commission, ISO 27001 for small businesses practical advice, ISO, Geneva, 2010.

[16] International Organization for Standardization/ International Electro technical Commission, ISO 27001:2013: Information technology – Security techniques – Information security management systems – Requirements, 2013.

[17] International Organization for Standardization/ International Electro technical Commission, ISO 27002:2013: Information technology – Security techniques – Code of practice for information security controls, 2013.

[18] International Telecommunication Union, X.200: 1994: Information technology – Open system interconnection – Basic reference model: the basic model, ITU, 1994.

[19] Ponemon, 2013 Cost of Data Breach Study: Global Analysis, 2013, http://ponemon.org (January 10, 2014).

[20] Saleh, M. S., Alrabiah, A., and Bakry, S. H., Using ISO 17799:2005 information security management: a STOPE view with six sigma approach, International journal of network management, v. 17, 2007, p. 85- 97.

[21] Security TechCenter, Microsoft Security Bulletin Summary for November 2013, 2013, http://technet.microsoft.com/en-us/security/bulletin/ms13-nov (January 10, 2014).

[22] Verison, 2013 Data Breach Investigations Report, 2012, http://verizonenterprise.com/DBIR/2013 (January 10, 2014).