Information Security Management Systems in the Healthcare Context

S. Tyali and D. Pottas

School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
e-mail: dalenca@nmmu.ac.za

Abstract

The ISO/IEC 27799 standard for information security management in health was released in 2008. The standard contains a substantial section (Section 6) covering information security management systems in the healthcare context. This raises the question whether the ISO/IEC 27799 purports a difference between the generic standard for information security management systems (as embodied in the ISO/IEC 27001) and what is contained in Section 6 of the ISO/IEC 27799 standard. The aim of this paper is to determine whether this is the case, based on a comparative analysis that was conducted between the ISO/IEC 27001 and ISO/IEC 27799 standards. The results of the comparison are summarized and the additional directives provided by the ISO/IEC 27799, categorized to explain their purpose.

Keywords

Information Security Management, Information Security Management Systems, Health Information Security

1. Introduction

The healthcare sector is an information-and knowledge-intensive enterprise, and healthcare providers rely increasingly on information technology (IT) to acquire, manage, analyse, and disseminate healthcare information and knowledge (William and Herbert, 2009). IT solutions serve as a tool to improve decision- making, to promote information exchange among peers, for self care and professional support, to enhance the effectiveness of health institutions and to collect patient information electronically (Economic Commission for Africa, 1999). Information that is collected regarding a patient's health is called personal health information. It may include information about a person's health, disability, use of health services, or any other relevant personal information (Office of the privacy commissioner, 2001). This health information is stored and accessed electronically in systems known as health information systems. A health information system (HIS) is an integral component of any healthcare system. It provides the context within which data collection, processing, analysis and reporting of health information takes place and facilitates the development of appropriate healthcare indicators for monitoring and evaluating the performance of the healthcare system (Matshidze & Hanmer, 2007). However, the collection and storage of data using HISs can cause problems with information security which do not normally occur in the traditional paper-based data collection approach (Quynh, 2005). Health information systems that store patient information must be managed adequately from an information security point of view. This embodies the concept of information security management.

The purpose of information security management (ISM) is to ensure business continuity and to reduce business damage by preventing and minimising the impact of security incidents (Krause and Tipton, 2003). The purpose of an information security management system (ISMS) is to establish, implement, operate, monitor, revise, maintain and improve information security (Simtex-OC Web Site, 2009). According to Ashenden (2008), an ISMS is often implemented in an organisation to ensure that there is a consistent, repeatable and auditable means of addressing information security issues or risks.

The ISO/IEC 27001 (ISO 27001, 2005) is an internationally recognized standard that provides a specification for information security management systems. One of the standards that supports the implementation of ISO/IEC 27001 is the ISO/IEC 27002 - Code of practice for ISM (ISO 27002, 2005). This standard provides implementation guidance in support of the security controls specified in its clauses and is cross-referenced for this purpose in the ISO/IEC 27001 (ISO 27001, 2005).

In 2008, a new standard was published for information security management in health. The ISO/IEC 27799 international standard provides guidance to healthcare organisations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of their information by implementing the ISO/IEC 27002 standard (ISO 27799, 2008). Notably, the ISO/IEC 27799 contains a lengthy section (Section 6) which addresses information security management systems. The section contextualizes ISMS for healthcare environments. Arguably, it provides directives that are not explicitly discussed in the ISO/IEC 27001 because it is a generic standard for implementing an ISMS within an organization. The aim of this paper is to determine whether this is the case, based on a comparative analysis that was conducted between the requirements posed by the ISO/IEC 27001 standard versus Section 6 of the ISO/IEC 27799 standard.

The rest of this paper is organized as follows. In Section 2 a brief introduction is provided of the healthcare milieu, followed by a discussion of information security management systems in Section 3. Section 4 presents the results of the comparison, which are summarized and the additional directives provided by the ISO/IEC 27799, are shown to resort into two main groups that represent the nature of the directives. An envisaged future research plan is discussed in Section 5. The last section concludes the paper and emphasizes the importance of ISMS directives for healthcare environments. It should be noted that for the sake of brevity, further reference to the standards are denoted as ISO 27001 and ISO 27799.

2. The Healthcare Milieu

Health is a state of complete physical, mental and social wellbeing, and not merely the absence of disease or sickness; it is a fundamental human right, and the attainment of the highest possible level of health is a most important worldwide social goal whose realization requires the action of many other social and economic sectors in addition to the health sector (World Health Organization, 1978). The healthcare sector is defined as a category of supply relating to medical and healthcare goods or services which includes hospital management firms, health maintenance organizations, biotechnology and a variety of medical products (Investopedia Web Site, 2009).

There are various types of healthcare services provided by the health sector. These include traditional health service providers such as private hospitals and day surgeries, medical practitioners and pharmacists (Office of the privacy commisioner, 2001). In recent years healthcare organizations worldwide have undergone major reorganization and adjustments to meet the demand of improved healthcare services accessibility and quality; in addition, the use of information technology to process health data continues to grow and more than ever critical information stored electronically is needed by healthcare administrators, providers and other users (Eder, 2000). Health information is essential for planning and decision making at all levels of the healthcare spectrum (Matshidze & Hanmer, 2007).

The sensitive nature of health-related information cannot be disputed. While the protection and security of personal information is important to all individuals, corporations, institutions and governments, there are special requirements in the health sector that need to be met to ensure the confidentiality, integrity, auditability and availability of personal health information (ISO 27799, 2008). Therefore custodians of health information should ensure that proper ISM practices are followed. Through the establishment of an information security management system, an organization can ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties (ISO 27001, 2005).

3. Information Security Management Systems

An ISMS enables an organization to systematically operate its management system for information security. By implementing an ISMS an organization can measure and manage their information security processes in a structured manner and control and hone their system to meet their business needs (Pattinson, 2007). This will ensure that a coordinated approach rather than a piecemeal approach is followed. This is conducive to continuous improvement, a core characteristic of a management system.

Introducing an ISMS into an organization calls for commitment and continued support from senior management. This commitment should be encouraged through all levels of management down to the individual system administrators and users, therefore making each person accountable to a degree for ownership and the success of the ISMS (Broderick, 2006). When the ISMS is effectively addressed, confidence is established to internal (such as managers) as well as external stakeholders (Ashenden, 2008).

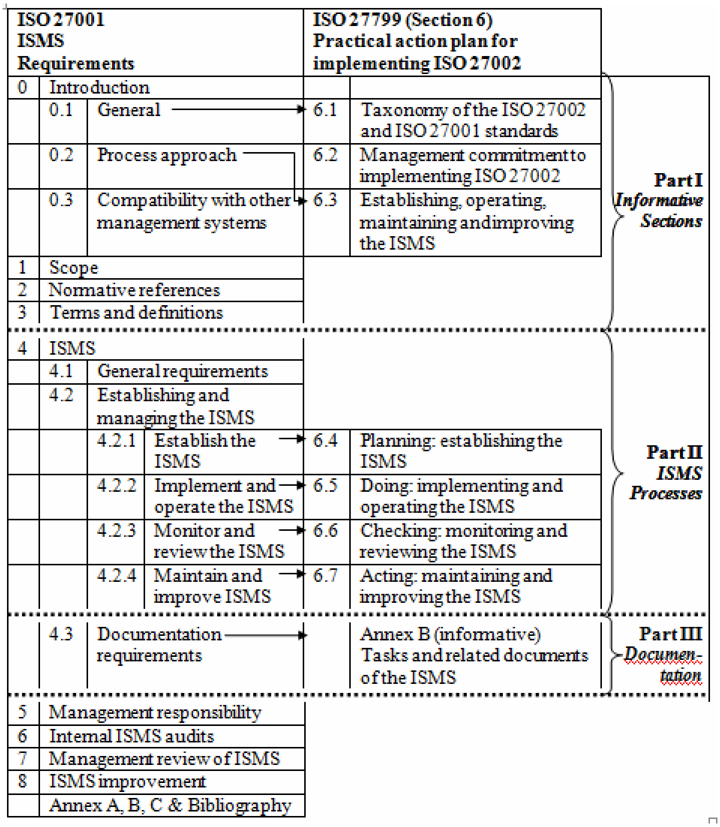
Operating an ISMS is subdivided into a four phase process, namely: Plan; Do; Check and Act (Cavalli et al., 2004). These processes are known as the PDCA model. The

ISO 27001 standard adopts the Plan-Do-Check-Act approach or cycle which is applied to structure all the ISMS processes and requirements for continual improvement (ISO 27001, 2005). According to Humphreys, the ISO 27001 standard is used worldwide by organisations, both commercial and government, as the foundation for the management of the organisation's policy and implementation of information security (Humphreys, 2008). Since this standard for information security management systems is designed to be flexible, it can be used by all types of organizations and because of this has become the de facto ''common-language'' for information security management systems. Because the standard is so generic, guidance is required as to its application in the health domain. The ISO 27799 standard for information security management in health includes a section (Section 6) which describes ISMSs quite comprehensively. The standard emphasizes the importance of healthcare organizations establishing an ISMS, and states that "to be truly compliant", an operational ISMS is required "in which there are appropriate compliance auditing processes" (ISO 27799, 2008). This leads to the objective of this research, namely to consider Section 6 of the ISO 27799 critically as compared to the ISO 27001, in order to determine any additional requirements that may be embodied in this section. The comparison that was conducted to this effect is summarized in Section 4.

4. Comparative Analysis: ISO 27001 vs ISO 27799 (Section 6)

4.1. High-level Overview

The aim of Section 4.1 is to provide a structure for further discussion based on a high-level overview of the standards. Table 1 clarifies, at a glance, the sections contained in the ISO 27001 versus the sub-sections of Section 6 of the ISO 27799. Arrows are used to denote the areas of correspondence.



ISO 27001 ISMS Requirements				ISO 27799 (Section 6) Practical action plan for implementing ISO 27002		
0	Introduction					**Part I** *Informative Sections*
	0.1	General		6.1	Taxonomy of the ISO 27002 and ISO 27001 standards	
	0.2	Process approach		6.2	Management commitment to implementing ISO 27002	
	0.3	Compatibility with other management systems		6.3	Establishing, operating, maintaining and improving the ISMS	
1	Scope					
2	Normative references					
3	Terms and definitions					
4	ISMS					**Part II** *ISMS Processes*
	4.1	General requirements				
	4.2	Establishing and managing the ISMS				
		4.2.1	Establish the ISMS	6.4	Planning: establishing the ISMS	
		4.2.2	Implement and operate the ISMS	6.5	Doing: implementing and operating the ISMS	
		4.2.3	Monitor and review the ISMS	6.6	Checking: monitoring and reviewing the ISMS	
		4.2.4	Maintain and improve ISMS	6.7	Acting: maintaining and improving the ISMS	
	4.3	Documentation requirements			Annex B (informative) Tasks and related documents of the ISMS	**Part III** *Documentation*
5	Management responsibility					
6	Internal ISMS audits					
7	Management review of ISMS					
8	ISMS improvement					
	Annex A, B, C & Bibliography					

Table 1: High-level overview of the ISO 27001 standard vs the ISO 27799 (Section 6)

For the purpose of this paper, the high-level overview shown in Table 1, delimits the structure into three parts. Part I, denoted as the informative sections, explains the purpose of the standards and the ISMS approach. Part II, denoted as ISMS processes, provides more detailed discussion of the processes required to establish, implement, operate, monitor, review, maintain and improve an ISMS. Part III, denoted as documentation, discusses the required documentation. This structure (Parts I, II and III), is used in the following three sections of the paper to discuss the results of the comparative analysis.

4.2. Part I: Informative Sections

The focus of the informative sections is to explain (a) the purpose of an ISMS and (b) the processes relevant to ISMSs. In the case of the ISO 27001, the purpose of the standard is explained and the process approach to ISMS is introduced in Sections 0.1 and 0.2 respectively. The ISO 27799 introduces the concept of an ISMS in Section 6.1 and explains the ISMS process approach in Section 6.3. The importance of management commitment is stressed in Section 6.2 of the ISO 27799. Other than the ISO 27799 recommending that health organizations should integrate their ISMSs with information governance processes, there is nothing unique as pertaining to ISMSs for health care evident from the comparative analysis of the informative sections.

4.3. Part II: ISMS Processes

Section 4 of the ISO 27001 is dedicated to discussing the requirements for ISMSs in detail. The discourse is presented in a prescriptive format (e.g. "The organization shall establish ...") due to the mandatory nature of the stated requirements seen from a certification point of view. The corresponding discussion in the ISO 27799 can be found in Sections 6.4 to 6.7. The discourse in these sections is not prescriptive, but adopts an informal, guiding approach. It is in these sections, where directives that are not explicitly discussed in the ISO 27001, can be found. These directives are summarized in Table 2.

ISO 27799 Sub-section	**Summary of Additional Directives Pertaining to the Healthcare Domain as Provided in the ISO 27799**
6.4.3	A unique forum called an information security management forum (ISMF) should be established to manage and direct the information security management system activities within the healthcare sector. When organizing the ISMF within the healthcare sector stakeholder views need to be accommodated and regulatory obligations are to be met.
	A scope statement may be used in various types of organizations, but in the case of health organizations, the scope statement should be publicised widely, reviewed, and adopted by the organization's information, clinical and corporate governance groups. Some health organizations seek comments on the scope statement from clinicians' professional regulatory bodies, which may be aware of other organizations pursuing compliance or certification.
6.4.4.2	Information security risk assessment is important in the healthcare sector because the sector carries high risk due to having facilities such as laboratories, emergency departments and operating theatres. Both qualitative and quantitative factors need to be considered when assessing information security risks in these environments. Examples of issues to consider when designing valuation guidelines are: recognising the importance of patient safety; uninterrupted availability of emergency services; professional accreditation; and clinical regulation.
6.4.4.4	Information custodianship, ownership and responsibility are issues that are raised when risk assessment is to be undertaken in the healthcare sector. For effective information security risk assessment to be achieved in the healthcare sector, the knowledge and skills listed below are necessary: a) clinical and nursing process knowledge, including care protocols and pathways; b) knowledge of the formats of clinical data and the capability for the misuse of this data;

ISO 27799 Sub-section	**Summary of Additional Directives Pertaining to the Healthcare Domain as Provided in the ISO 27799**
	c) knowledge of external environment factors that could exacerbate or moderate any or all of the levels of the risk components described previously; d) information on IT and medical device attributes and performance/failure characteristics; e) knowledge of incident histories and actual case impact scenarios; f) detailed knowledge of systems architectures; g) familiarity with change management programmes that would change any or all of the risk component levels.
6.4.5.3	There are numerous factors to be taken into account to define criteria for the acceptance of risks. A selection from these factors includes: a) Health sector, industry or organizational standards b) Clinical or other priorities c) Cultural Fit d) Reactions of subjects of care (patients) e) Coherence with IT, clinical, and corporate risk acceptance strategy
6.4.6	The organization's information security officer, data protection officer or risk manager should be responsible for the security improvement plan of the organization on behalf of the ISMF. The plans should be made available to clinical and other staff; they are useful in demonstrating progress and process improvement. These plans are sometimes effective in minimizing interruptions to operations when integrated with information security improvement, planned changes in IT facilities and healthcare.
6.5	Because of the critical nature of health information systems it is especially important to define responsibilities and action steps in the initial phase of response because events can unfold quickly and this leaves little time for reflection as a security incident unfolds.
6.5	In the health context the ISMF is further responsible for making sure that the risk treatment plan is carried out. In healthcare approving the risk treatment plan may involve both information governance and clinical governance.

Table 2: Directives provided in the ISO 27799 (Section 6) but not stated in the ISO 27001

Based on the summary provided in Table 2, themes can be identified and classified into two groups, namely contextualization (i.e. of the healthcare environment) and structure (i.e. mechanisms used to implement the ISMS). Themes resorting in the contextualization group include high risk facilities (e.g. operating theatres), professional regulatory bodies, knowledge and skills for risk assessment, factors to define risk acceptance criteria, the critical nature of the environment (e.g. life / death) and legal obligations. These themes simply indicate issues that are inherent to the healthcare environment and should be considered when implementing an ISMS. It would, for example, be impossible to determine appropriate risk acceptance criteria if the stated factors (inherent to the healthcare milieu) are not kept in mind.

Themes resorting in the structure group include information governance and clinical governance, the information security management forum (ISMF), dissemination of the scope statement, responsibility for and dissemination of the security improvement plan, and responsibilities and action steps for the initial phase of responding to incidents. These themes indicate directives that are not simply included to contextualize the environment, but are additional to those provided in the ISO 27001.

The discussion now continues to the last part of the comparative analysis, which addresses the documentation requirements of ISMSs.

4.4. Part III: Documentation requirements

The documentation requirements for an ISMS are discussed in Section 4.3 and Annex B of the ISO 27001 and ISO 27799 respectively. The ISO 27001 provides the requirements in a listed format with each item referring to the relevant section of the standard. The ISO 27799 provides the same information, but in a more user-friendly format - depicted diagrammatically and related to the various phases, tasks and steps of the PDCA model. No additional directives pertaining to the establishment of an ISMS in healthcare environments, are provided.

5. Future Research Plan

This paper highlighted the specific requirements of establishing an ISMS in the healthcare domain through the consideration of the ISO 27799 (Section 6) versus the ISO 27001. The ISO 27001 is but one of various standards for management systems. Other such standards include ISO 9001 (Quality Management Systems), ISO 14001 (Environmental Management Systems) and OHSAS 18001 (Occupational Health and Safety Management Systems). In the healthcare context, the IWA 1 is the quality management system standard which provides guidelines for process improvements in health service organizations.

With the understanding gained of ISMS in the healthcare context through this paper, the next step is to gain a similar understanding of quality management systems in health care through consideration of the IWA 1. Conceivably the implementation of these management systems will be done by different departments in health service organizations if they should choose to implement both management system standards. This will be economically unreasonable particularly since an increasing overlap appears to be developing between management system standards as well as more focus on creating integrated management systems (IMSs) (Scipioni et al., 2001). The final phase of this research will therefore focus on an integrated management system for quality and information security in healthcare, incorporating the necessary directives for the distinctive operational circumstances of health service organizations.

6. Conclusion

Cavalli et al. (2004) state that because of the peculiarities of healthcare institutions and data, a lot of analysis and design work needs to be done when implementing the generic ISO 27002 standard in the healthcare context. It follows that the same applies to the ISO 27001 standard. It is important that generic standards such as the ISO 27001 and ISO 27002, are supplemented to create industry-specific renditions, such as the ISO 27799. This is because the fact that generic standards are not contextualized is often seen as a disadvantage.

The purpose of this research was to determine whether the ISO 27799 standard provides additional directives that are not covered as part of the ISO 27001, the international standard for information security management systems. Although the ISO 27799 is primarily aimed at information security management, the fact that it contains a substantial section on information security management systems raised the question of what exactly it does provide additionally, in terms of operating an ISMS in the healthcare domain.

The research was conducted by executing a comparative analysis of the relevant sections of the standards. It was found that the additional directives provided by the ISO 27799 resort in two main groups. One group clearly contextualizes ISMS in terms of health care, while the other group recommends the use of structures or mechanisms that are not mentioned in the ISO 27001.

It is concluded that the unique operating environment of healthcare organizations, warrants, in fact needs the provision of additional guidance for the establishment of effective and efficient ISMSs. If the additional directives are not considered, it is conceivable that there could be undesirable consequences. For example, if an information security risk assessment does not institute controls to ensure the continued and uninterrupted operation of emergency services in the event of a disaster, this could lead to a healthcare facility being incapacitated in offering such services when it is most needed. Such an incident could cause loss of life. Albeit a worst case scenario, it is a reality of healthcare environments which surely underscores the importance of designing and implementing proper information security management systems. This is supported by the ISO 27799 standard, the health context-specific version of the ISO 27001 and ISO 27002 standards, assisting the proper interpretation of the standards in the particular operational context.

7. References

Ashenden, D. (2008), “Information Security management: A human challenge?”, Information Security Technical Report, Vol. 13, Issue 4, 2008, pp. 195-201.

Broderick, J.S. (2006), “ISMS, security standards and security regulations”, Information Security Technical Report, Vol. 11, Issue 1, 2006, pp. 26-31.

Cavalli, E., Mattasoglio, A., Pinciroli, F., and Spaggiari, P. (2004), “Information security concepts and practices: the case of a provincial multi-specialty hospital”, International Journal of Medical Informatics, Vol. 73, Issue 3, pp. 297-303.

Economic Commission for Africa (1999), “Information and communication technology for health sector”, http://www.uneca.org/aisi/docs/pfshealth.pdf, (Accessed 15 June 2008).

Eder, L.B. (2000), Managing Healthcare Information Systems with Web Enabled Technologies, IGI Publishing, Hershey, PA, USA.

Humphreys, E. (2008). “Information security management standards: Compliance,governance and risk management”, Information Security Technical Report, Vol. 13, Issue 4, 2008, pp. 247-255.

Investopedia Web Site (2009), “Healthcare Sector”, http://www.investopedia.com/terms/h/health_care_sector.asp, (Accessed 13 October 2008).

ISO 27001. (2005). ISO/IEC 27001: Information Technology – Security Techniques – Information Security Management Systems - Requirements (1st ed.). Switzerland: International Organization for Standardization.

ISO 27002. (2005). ISO/IEC 27002: Information Technology – Security Techniques – Code of Practice for Information Security Management (1st ed.). Switzerland: International Organization for Standardization.

ISO 27799. (2008). ISO/IEC 27799: Health informatics — Information security management in health using ISO/IEC 27002 (1st ed.). Switzerland: International Organization for Standardization.

Krause, M. And Tipton, H.F. (2003), Handbook of Information Security Management, CRC Press LLC.

Mathur, A. (2003), “The role of information technology in designs of healthcare trade”, http://www.icrier.org/pdf/wp111.pdf, (Accessed 9 September 2008).

Matshidze, P. and Hanmer, L. (2007), “Health information systems in the private health sector”, http://hst.org.za/uploads/files/chap6_07.pdf, (Accessed 11 January 2009).

Office of the privacy commisioner (2001), “Health Information and the Privacy Act 1988: A short guide for the private health sector”, http://www.privacy.gov.au/materials/types/download/8683/6522, (Accessed 3 March 2009).

Pattinson, F. (2007), “Certifying Information Security Management Systems”, http://www.atsec.com/ downloads/pdf/CertifyingISMS.pdf, (Accessed 21 February 2009).

Quynh, L. (2005), “Issues on health data collection”, In: Creative Dissent: Constructive Solutions - AARE 2005, 27 Nov. – 2 Dec. 2005, Paramatta, NSW.

Scipioni, A., Arena, F., Villa, M., and Saccarola, G. (2001), “Integration of management systems”, Environmental Management and Health, Vol. 12, No. 2, pp. 134-145.

Simtex-OC Web Site (2009), “Certification of the Information Security Management Systems”, http://www.simtex.ro/lang_en/information-security.php, (Accessed 16 July 2009).

Willam, S.W. and Herbert, L.S. (2009). Computational Technology for Effective Health Care: Immediate Steps and Strategic Directions, National Academies Press, Washington, D.C.

World Health Organization. (1978). International Conference on Primary Health Care, Alma-Ata. The International Conference on Primary Health Care, (pp. 1-3).