An Integrated Management System for Quality and Information Security in Healthcare

Sinovuyo Tyali
An Integrated Management System for Quality and Information Security in Healthcare

by

Sinovuyo Tyali

Dissertation

submitted in fulfilment of the requirements for the degree

Magister Technologiae

in

Information Technology

at the

School of Information and Communication Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Supervisor: Prof. Dalenca Pottas

January, 2012
DECLARATION

I, Sinovuyo Tyali (20313918), hereby declare that this dissertation submitted for the degree to be awarded, is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another University or for another qualification.

SINOVUYO TYALI
Abstract

Health service organizations are increasingly required to deliver quality healthcare services without increasing costs. The adoption of health information technologies can assist these organizations to deliver a quality service; however, this again exposes the health information to threats. The protection of personal health information is critical to ensure the privacy of patients in the care of health service organizations. Therefore both quality and information security are of importance in healthcare.

Organisations commonly use management system standards to assist them to improve a particular function (e.g. quality or security) through structured organizational processes to establish, maintain and optimise a management system for the particular function. In the healthcare sector, the ISO 9001, ISO 9004 and IWA 1 standards may be used for the purpose of improving quality management through the establishment of a quality management system. Similarly, the ISO 27001 and ISO 27799 standards may be used to improve information security management through the establishment of an information security management system. However, the concurrent implementation of multiple standards brings confusion and complexity within organisations.

A possible solution to the confusion is to introduce an integrated management system that addresses the requirements of multiple management systems. In this research, various standards relevant to the establishment of management systems for quality and security are studied. Additionally, literature on integrated management systems is reviewed to determine a possible approach to establishing an IMS for quality and information security in healthcare.

It will be shown that the quality management and information security management standards contain commonalities that an integration approach can be based on. A detailed investigation of these commonalities is done in order to present the final proposal of the IMSQS, the Integrated Management System for Quality and Information Security in healthcare.
Dedication

My sincerest gratitude and appreciation are extended to:

• **God Almighty**, for bestowing his favour upon me throughout my studies;

• My Supervisor, **Professor Dalenca Pottas** for her trustworthiness, support; and for working tirelessly to ensure that this dissertation is completed;

• My **Mom Nomangesi** for being my pillar of strength and for her continuous support and love;

• My sister **Luleka** and **Brother Xhanti** for keeping me sane throughout my studies;

• My **Family and Friends** for their support; and

• Finally, to **Debbie** for all the time and effort she invested in proofreading this dissertation.
# Table of Contents

Chapter 1 .............................................................................................................. 1

1.1 Background .......................................................................................................... 1
1.2 Importance of quality in healthcare ...................................................................... 2
1.3 Importance of information security in healthcare .................................................. 6
  1.3.1 Privacy, Confidentiality, Integrity and Availability ........................................... 8
1.4 Management system standards ............................................................................. 11
1.5 Integrated management systems .......................................................................... 13
1.6 Problem Statement ............................................................................................... 14
1.7 Research objectives ............................................................................................... 15
1.8 Delineation of Research ....................................................................................... 15
1.9 Research Methodology ......................................................................................... 15
  1.9.1 Research Methods ........................................................................................... 16
  1.9.2 Research process ............................................................................................. 18
1.10 Structure of the Dissertation ................................................................................. 19
1.11 Conclusion ........................................................................................................... 21

Chapter 2 ................................................................................................................. 22

2.1 Introduction ........................................................................................................... 22
2.2 Types of healthcare services .................................................................................. 24
  2.2.1 Primary Healthcare ......................................................................................... 24
  2.2.2 Secondary and Tertiary healthcare .................................................................. 25
  2.2.3 Private Healthcare vs. Public Healthcare ....................................................... 26
2.3 Healthcare Information ......................................................................................... 27
2.4 Health Information Systems .................................................................................. 29
2.5 Quality of service delivery in healthcare .............................................................. 32
2.6 Information Security Requirements in Healthcare ................................................. 34
2.7 Conclusion ............................................................................................................ 36
## 5. Security in Healthcare

5.1 Introduction ........................................................................................................... 75
5.2 IMSQS: GP1 - Management responsibility and leadership ........................................ 76
5.3 IMSQS: GP2 - Resource management .................................................................... 78
5.4 IMSQS: GP4 - Audits ............................................................................................. 79
5.5 IMSQS: GP5 - Documentation and records control ............................................... 80
5.6 Conclusion ............................................................................................................. 81

## 6. Conclusion

6.1 Introduction ........................................................................................................... 83
6.2 Chapter Overview ................................................................................................. 85
6.2.1 Chapter 1 – Introduction .................................................................................. 85
6.2.2 Chapter 2 – The Healthcare Milieu ................................................................. 85
6.2.3 Chapter 3 – Management Systems for Quality and Security ............................ 86
6.2.4 Chapter 4 – IMSQS: An Integrated Management System for Quality and Information Security in Healthcare ................................................................. 86
6.2.5 Chapter 5 – Conclusion .................................................................................... 87
6.3 Revisiting the research questions and objectives of the research ......................... 87
6.3.1 Research question and sub-objective 1 .......................................................... 87
6.3.2 Research question and sub-objective 2 .......................................................... 88
6.3.3 Research question and sub-objective 3 .......................................................... 88
6.3.4 Research question and sub-objective 4 .......................................................... 89
6.3.5 Research question and sub-objective 5 .......................................................... 90
6.3.6 Research question and sub-objective 6 .......................................................... 90
6.4 Benefits and Limitations of the Research ......................................................... 91
6.5 Future Research .................................................................................................. 93
6.6 Conclusion .......................................................................................................... 94
References ................................................................. 95

Appendix A ............................................................................. 109
List of Figures

Figure 1.1 Layout of Dissertation.................................................................20
Figure 3.1 Difference between the ISO 9001 and 9004 standards................39
Figure 3.2 Model of a process-based quality management system ...............46
Figure 3.3 Model for Health Service Organizations with Patient/Client as "Customer"........................................................................................................47
Figure 3.4 PDCA model applied to ISMS processes........................................52
Figure 4.1 Dansk Standard’s model for an Integrated Management System 62
Figure 4.2 High level overview of the IMSQS..................................................64
Figure 4.3 IMSQS: Integration approaches: policies.......................................77
Table 4.1  Informative sections: Common elements between the QMS and ISMS standards ................................................................. 65
Table 4.2  ISMS processes: Common elements between the QMS and ISMS standards ................................................................. 66
Table 4.3  Management resources: Common elements between the QMS and ISMS standards ................................................................. 67
Table 4.4  Resources required for performance improvement: Common elements between the QMS and ISMS standards ......................... 68
Table 4.5  Mapping: Generic processes ................................................................. 70
Table 4.6  Directives provided in the ISO 27799 (Section 6) but not stated in the ISO 27001 ................................................................. 74
Welcome to the new reality of quality, the world of integrated management systems. Unfortunately for you, this world is real. This is the world where you have to address the needs of not just the customer, but virtually everybody who has a direct or indirect contact with your company. This is the world of mushrooming management system standards (MSS), where for each such stakeholder there is at least one MSS covering the minimum requirements for assuring a good relationship with that stakeholder. This is the world where the only way to survive the onslaught of MSS birds is not to run away from them or deal with them one by one, but to tame them. In other words, integrate.

Karapetrovic (2003)
Chapter 1
Introduction

Chapter 1 briefly describes the purpose of the research and presents background information on the topics that are discussed in the dissertation chapters. The problem statement, research objectives and the research methodology are provided. A brief overview of each chapter is described and a graphical illustration of the chapter layout is presented.

1.1 Background

The healthcare sector is diverse and comprises of hospital, private nursing home, medical and dental practice work, ambulance transportation, complementary medicine and other human health activities, such as medical laboratories services, across a range of organisations within the public and private sectors (Lampsas, Vidalis, Papanikolaou, & Vagelatos, 2002). It encompasses a wide variety of practices and activities, and is supported by a number of industries devoted to providing resources to the medical community (Davies & Lowe, 1999).

The healthcare industry is an information- and knowledge-intensive sector (Willam & Herbert, 2009). This results in decision-making being information dependent and large volumes of data are collected, stored, analysed, transferred, and accessed on a daily basis by organizations, services and systems within the sector (Bath, 2008). The information that is collected continues to ensure that healthcare providers’ clients are properly cared for (Lampsas, Vidalis, Papanikolaou, & Vagelatos, 2002). This is the reason that information management is fundamental to healthcare delivery (Coulter, et al., 2006).

Healthcare remains a paper intensive and minimally automated and digitized industry. However, globally, the healthcare industry is searching for technology that can help to establish online clinical repositories that enable rapid access to shared
information that can help find cures for prevalent medical conditions (Omni MD, 2010). This means that healthcare providers will rely increasingly on information technology (IT) to acquire, manage, analyse, and disseminate healthcare information and knowledge (Willam & Herbert, 2009).

Information technology is essential to record the delivery of care because many patients will experience one or more transitions between healthcare providers during the course of their lifetime. A complete record of the medical history of the patient is important for quality care to be delivered (Blobel, 2007). The electronic tools developed and implemented in the healthcare domain to facilitate activities such as information gathering, storage, analysis, transmission and retrieval are known as health information systems (Smith & Eloff, 1999).

Health information systems are an integral component of healthcare systems because they provide the resources within which data collection, processing, analysis and reporting of health information takes place. They facilitate the development of appropriate healthcare indicators for monitoring and evaluating the performance of the healthcare system (Matshidze & Hanmer, 2009). Health information systems present the possibility of improving the accessibility of patient related information to healthcare professionals through the improved handling of medical records and providing the results of investigations faster (Sousa-Poza, Altinkilinc, & Searcy, 2009). In many countries health information systems are faced with the challenge of ensuring that high quality information is collected and stored efficiently to ensure that patient safety and the delivery of quality care is achieved (Jha, Doolan, Grandt, Scott, & Bates, 2008). Section 1.2 further discusses the importance of quality in health activities and health systems.

1.2 Importance of quality in healthcare

Quality of care is defined as the degree to which health services for individuals and populations increase the likelihood of desired health outcomes and are consistent with current professional knowledge (Chassin & Galvin, 1996). Quality is also defined as the degree to which care services influence the probability of optimal
patient outcomes (Wright & Shojania, 2009). It involves the consistent delivery of a product or service according to expected standards (Abdosh, 2006). This is true in the healthcare setting where patient satisfaction is an important component of service quality (Wright & Shojania, 2009).

Quality is seen as a process of meeting the needs and expectations of patients and health service staff (Sousa-Poza, Altinkilinc, & Searcy, 2009). Therefore, the main goals of a healthcare system should include a better quality of healthcare that is responsive to the expectations of the population (Kabene, Orchard, Howard, & Leduc, 2006). Quality needs to be ensured to satisfy patient needs. The assurance of quality in healthcare is achieved through the process of developing statements regarding inputs, processing and outcomes standards that the healthcare delivery system must meet in order for the country’s population of care to achieve optimum gains (Wright & Shojania, 2009). This means that the healthcare needs of the population are met with the best possible quantity and quality of services produced at minimum costs (Kabene, Orchard, Howard, & Leduc, 2006). However, although high quality care is desired, the realities within the healthcare sector are that healthcare continues to struggle with issues of quality, safety and responsiveness to the needs, legitimate demands and reasonable expectations of the people whom the healthcare systems were set up to serve (Kiguli, Okui, Mutebi, MacGregor, & Pariyo, 2009).

Healthcare quality is generally defined in two ways: technical quality and socio-cultural quality (Kiguli, Okui, Mutebi, MacGregor, & Pariyo, 2009). Technical quality refers to the impact that the available health services have on the health conditions of a population while socio-cultural quality measures the degree of acceptability of services and the ability to satisfy patients’ expectations (Kabene, Orchard, Howard, & Leduc, 2006).

There is a distinction between health systems in different countries even in those with similar levels of income, education, and health expenditure. They vary considerably in performance and in their ability to attain key health goals.
Healthcare professionals face many obstacles in their attempt to deliver quality health care to patients. Some of these constraints include budgets, absenteeism rates and the low morale of healthcare personnel (Kabene, Orchard, Howard, & Leduc, 2006). Some of these obstacles are self-evident with the scarcity of basic amenities of health services, such as the lack of clean waiting rooms or adequate beds and food in hospitals. These are aspects of care that are often highly valued by the population and which can impact on the healthcare professionals’ morale and ability to deliver quality health care (Leatherman, Ferris, Berwick, Omaswa, & Crisp, 2010).

The effect of poor quality service delivery is dissatisfied customers (patients) which can lead to a number of critical behaviours such as switching service providers, thereby, interrupting their continuity of care and influencing others in their perceptions of quality provided in health care (Kabene, Orchard, Howard, & Leduc, 2006). This may, in turn, disrupt planned healthcare interventions and studies that are conducted to better understand the problems that patients and healthcare professionals are faced with (Abdosh, 2006).

Quality can be improved in the healthcare sector by providing a conducive and comfortable environment for the people receiving health care; by the health practitioners healthcare environment being designed for comfort, safety and functionality; by providing access to social, emotional and spiritual support for patients and their families and for the staff of the facility (Abdosh, 2006). Healthcare improvements can include, among others, building more health facilities, providing more drugs, recruiting more health workers and training health workers through continuing medical education (Leatherman, Ferris, Berwick, Omaswa, & Crisp, 2010).

Health care quality assurance can be used as a means to improve healthcare quality and outcomes. It involves activities and programs intended to assure or improve the quality of care in either a defined medical setting or a program (Abdosh, 2006). The concept according to (Kabene, Orchard, Howard, & Leduc, 2006) includes:

- The assessment or evaluation of the quality of care;
• The identification of problems or shortcomings in the delivery of care;
• Designing activities to overcome these deficiencies; and
• Follow-up monitoring to ensure effectiveness of corrective steps.

Because quality of care is a multidimensional concept, individuals should not take decisions in isolation and practices should be evidence-based and adhere to best practices and standards that are adopted in the sector (Kiguli, Okui, Mutebi, MacGregor, & Pariyo, 2009).

Quality assurance and quality control are part of any successful quality management system (Yeung & LY, 1998). Quality management provides the principles and the methodological frame for operations, and coordinates activities to manage and control an organization with regard to quality (Maharashtra, 2010). It has been noted by many authors that an improvement in quality management progressively leads to more efficient internal operations, followed by satisfied external customers and eventually superior marketing and financial performance (Yeung & LY, 1998). Therefore, quality management is fundamental in the successful implementation of a quality management system. An example of a standard that can be used in the healthcare sector, to ensure that quality of care is achieved, is a quality management system standard.

A quality management system (QMS) in health care can be described as a structured organizational process that involves the staff at different levels in planning, measuring and assessing patient care in such a way as to provide optimal medical service to patients (Wardhania, Utarini, van Dijk, Post, & Groothoff, 2009). The QMS approach is often copied from the manufacturing industry or for-profit service providers (van Harten, Casparie, & Fisscher, 2000). It can, therefore, be considered as an emerging management technology in health care to address quality management issues (van Harten, Casparie, & Fisscher, 2000). Quality management and quality management systems are widely advocated in health care to address the following issues:

• The increasing complexity of health institutions and systems;
• The focus on efficiency and effectiveness;
• The pressure on cost-reduction; and
• The on-going process of sub-specialisation and individualisation and strengthening of the position of the client.

International and national regulatory bodies have developed standards that enable organizations to establish management systems for quality, environment and sustainable development, health, safety and social responsibility, among other functions to address the growing concern of the healthcare community and society with respect to aspects that affect the quality of life and the management of quality within the healthcare sector, (de Oliveira & Zouain, 2009). These standards include ISO 9001, ISO 14001, IWA 1 and the OHSAS 18001. Performance in accordance with standards such as the IWA 1 provide the cornerstone of quality assurance in healthcare and result in a wide range of quality assurance activities, including the accreditation of health facilities, external quality evaluation, and performance improvement (Marquez, 2001). A number of these standards, their purpose and how they assist in managing quality are discussed in section 1.4.

Some of the means of improving the quality of care includes the utilisation of IT in healthcare settings which allows for information to be readily communicated and shared among healthcare providers (Adler-Milstein & Bates, 2010). The main impact that IT had on the quality of care was to advocate for increasing adherence to guideline or protocol based care (Chassin & Galvin, 1996). It is evident, therefore, that IT has a major role in the delivery of quality healthcare pertaining to the electronic recording and sharing of information. In the following section, IT is further discussed with regard to the security aspects of recording health information in healthcare systems.

1.3 Importance of information security in healthcare

The use of IT to process information continues to evolve, and organisational dependence on information is continually increasing. This dependence on
information systems and services means organisations are more vulnerable to security threats (Analytix, 2009). The easier it becomes to access and exchange information, the more difficult it becomes to protect it.

Information security is an on-going concern for most healthcare providers (Wolfe, 2009). Healthcare records are vulnerable to a range of threats that will cause harm if the records are not adequately protected. Information security is the preservation of the confidentiality, integrity and availability of information (ISO/IEC 17799, 2005). The British Standards Institute (BSI) defines information security as a means to protect information held by organizations from a wide range of threats to ensure business continuity, minimize business damage and maximise return on investment and business opportunities (BSI, 2007). Information security is also defined as encompassing the systems and procedures designed to protect the organisational information assets from disclosure to any person or entity not authorized to have access to that information, especially information that is considered sensitive, proprietary, confidential, or classified, as in national defences (Wiant, 2005).

Information security is achieved through using control measures which are applied to lessen the threat to and reduce the vulnerability of the information asset. A lack of information security and its necessary control measures means that an organization may face the possibility of closure or even prosecution, because their information is a valuable business asset. This is equally true in the health sector, where the gathered patient information is regarded as confidential between doctor and patient and, therefore, it needs to be adequately protected or secured.

Security is a key issue in healthcare information systems, since most aspects of security become of considerable or even critical importance when handling healthcare information (Gritzalis, 1998).

Failure to properly protect healthcare information may result in undesirable consequences for both the doctor and the patient. Information security principles require the health service provider to have security safeguards in place to protect the patient health information. These safeguards apply to personal information held in
paper form or electronically (Crompton, 2001). When attempting to introduce computerised healthcare information systems there should, therefore, be a guarantee of adequate protection of the confidentiality and integrity of the patient information.

Simultaneously, however, the patient information needs to be readily available to all authorised healthcare providers, to ensure the proper treatment of the patient (Smith & Eloff, 1999). When healthcare records are not adequately secured, issues such as the privacy, confidentiality, integrity and the availability of information are raised. In the next section, these issues are discussed to get an in-depth understanding of these terms and how they pertain to securing information.

1.3.1 Privacy, Confidentiality, Integrity and Availability

Health and medical information, which includes medical records, prescription histories, patient data, surgical records, and so on, are obviously the types of information that have long been considered to be personal and deserving of privacy protection (Waldo, Lin, & Millett, 2007). There is a universal notion that the need for privacy in the medical and health arena is important. The need to keep private the health information about a patient health is recognized as a requirement. However, often measures to secure the information on healthcare records are absent and the information within them is vulnerable (Rowlingson, 2006).

Privacy refers to the limited access to identifiable information about individuals (Smith, 2004). Privacy concerns exist wherever personally identifiable information is collected and stored - in digital form or otherwise. Bhattacharyya & Roy (2008) define privacy as the right of individuals to hold information about themselves in secret, free from the knowledge of others. Improper or non-existent disclosure control can be the root cause for privacy issues. Privacy violations include breach of confidentiality, disclosure, secondary use and insecurity of information (Rowlingson, 2006).

An example of healthcare records being compromised is if the press would obtain
information about someone’s HIV status from a hospital and publish their status without their knowledge or permission.

Three key factors in information security are to preserve data confidentiality, integrity, and availability of organizations’ information (The Information Security Glossary). As mentioned above healthcare and medical data continue to become increasingly computerized and centralized, therefore, the difficulty of access is largely removed. With the convenience that comes with healthcare information being stored electronically, there are information security issues and privacy violations that occur which are potentially the most important threat to the effectiveness of electronic data storage (O’Brien & Yasnoff, 1999).

Confidentiality is concerned with ensuring that information is accessible only to those authorized to have access and is one of the cornerstones of information security (Bhattacharyya & Roy, 2008). Confidentiality is also defined as the assurance that information about identifiable persons is not disclosed without consent, except as allowed by law because its release would constitute an invasion of privacy for any person (O’Brien & Yasnoff, 1999). It is one of the most important aspects of data collection in healthcare (Quynh L., 2005). Microsoft (2009) state that confidentiality becomes a requirement in the following scenarios:

- When data is stored on a medium (such as a computer hard drive) that can be read by an unauthorized individual;
- When data is backed up onto a device (such as a tape) that can fall into the hands of an unauthorized individual; and
- When data is transmitted over unprotected networks.

From the perspective of the patient, confidentiality is essential to the relationship between a patient and a health care provider. Patients may be reluctant to disclose sensitive information that may be crucial to their correct treatment or they may refrain from seeking treatment because they are unsure whether their personal information will be distributed against their wishes (Whiddetta, Huntera, & Engelbrechta, 2006). Whether medical records are traditionally in hard copy or in electronic format, their
confidentiality may become a risk due to theft or personal abuse by those people who have access to it, e.g. file keepers or data capturers (Quynh L., 2005). Confidentiality is one of the cornerstones of information security.

Data integrity is the assurance of non-alteration, i.e. that the data (either in transit or in storage) has not been undetectably altered (Microsoft, 2009). “Data integrity implies that data have not been changed inappropriately, whether by accident or deliberately; it also includes ‘origin’ or ‘source’ integrity -- that is, that the data actually came from the person or entity you think it did, rather than an imposter”, according to (Miller, 2008). The integrity of data is critical to prevent disruption, unexpected modification, or loss of information. It ensures that data is never lost and that the operations executed on the data are accurate, fully completed and properly managed (MySql, 2005). Health service providers need to take reasonable steps to ensure the reliability of personal information when they collect, use or disclose it (Crompton, 2001).

Availability represents the requirement that an asset be accessible to authorized people and devices. As a general rule, the more critical a component is, the higher its availability will be (Purdue University, 2004). Data availability ensures that data is accessible at the service levels required for an application. This includes high availability to prevent unplanned downtime, online backups to enable hot administration, and the ability for a database to deliver high performance and scalability necessary for the most demanding applications. Security measures or controls must be implemented to ensure that security and privacy breaches do not occur.

There are various mechanisms that can be used to ensure that an organization’s information is adequately secured to achieve proper management and control of the information. One of these is to establish an information security management system (ISMS).

Management system standards should be used to ensure that a process is followed to ensure the proper management of both quality and information security in an
organisation. These standards define the approaches and principles to be followed to ensure the proper management of quality and information security. They provide a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached consensus as being the international state of the art (ISO, 2010). The standards for quality and information security management in healthcare as relevant to this study are briefly discussed in the next section.

1.4 Management system standards

Management system standards are used in organisations to manage different aspects of organisations’ activities and services (Macinati, 2008). According to the ISO (The International Organisation of Standardisation), “Management system standards provide the organization with a model to follow in setting up and operating the management system”. Standards are published documents outlining specifications and procedures designed to ensure products, services and systems are safe, reliable and consistently perform as they were intended to (Arifin, Aiyub, Awang, Jahi, & Iteng, 2009). Therefore, management system standards provide a standardised and accepted approach to establishing and maintaining management systems in the organisational context. Examples of management system standards can be found in the ISO 9000 (addressing quality) and ISO 27000 (addressing information security) series of standards.

The ISO 9000 international standards are designed as generic documents that outline the minimum requirements for quality systems of organizations in all industries (Karapetrovic & Willborn, 1998). These standards describe the concepts of a quality management system (QMS) and define the fundamental terms used in the ISO 9000 family (International trade center, 2001). The ISO 9001 and ISO 9004 are part of the ISO 9000 series of standards and are briefly discussed.

According to ISO 9000, the ISO 9001 and 9004 standards are based on eight quality management principles. These principles were chosen because they can be used to improve performance and achieve success (Frost, 2006). While ISO 9001
represents a model for quality assurance in design, development, production, installation and servicing of products, it is equally applicable to service industries. (Karapetrovic & Willborn, 1998). The ISO 9004 is recommended as a guide for organizations whose top management wishes to move beyond the requirements of ISO 9001, in pursuit of the continual improvement of performance (IWA 1, 2005).

In addition to the 9000 series of standards that addresses quality management, the IWA 1:2005 provides supplementary guidance for any health service organization involved in the management, delivery, or administration of health service products or services, including training and/or research (Frost, 2006).

The ISO 27000 series of standards are specifically reserved by ISO for information security (ISO, 2010). They are intended to assist all types of organizations to recognize the fundamental principles and concepts to improve the protection of their information assets. ISO 27001 and ISO 27799 are part of the ISO 27000 series, and are subsequently discussed.

The ISO 27001 standard provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system (ISMS). The adoption of an ISMS should be a strategic decision for an organization (ISO / IEC 27001, 2006). The ISO 27799 specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. This is achieved by implementing this standard in healthcare organizations and by other custodians of health information. They will be able to ensure a minimum requisite level of security that is appropriate to their circumstances and will maintain the confidentiality, integrity and availability of the personal health information (ISO / IEC 27799, 2008).

As described in section 1.4, it is evident that various management system standards can be used to ensure the proper management of quality and security. Since there are a number of standards that an organisation can use, confusion and an increased workload may result when implementing the various standards concurrently. To counter the confusion and increased workload that a number of standards being
used in one organisation can lead to, these standards can be integrated and be used as an integrated management system, in order to manage both the security and quality needs of a healthcare organisation.

As previously stated, there are a number of management systems that can be used by organisations, depending on their needs. A few of the management systems provided by ISO are the ISO 9001, ISO 9004, IWA 1, ISO 27799, ISO 27001 and ISO 14001, (Karapetrovic & Casadesu, 2009). These management systems may be integrated to form a single management system. Integration can be summarised as a process of linking different standardized management systems (MS) into a unique MS with common resources aiming to improve business operation (Jørgensen, Remmen, & Mellado, 2006). Consequently, integrated management systems are discussed in the next section.

1.5 Integrated management systems

An integrated management system is described as a single integrated structure derived from multiple separate management systems. It can be used by an organization to manage its processes that transform inputs of resources into a product or service which meet the organizational objectives. It will equally satisfy the stakeholders’ needs for quality, health, safety, environmental health, security, ethics or any other identified requirement (Wilkinson & Dale, 1999).

De Oliveira and Zouain (2009) define an integrated management system as one that integrates all the systems and processes of an organization into a complete framework which enables it to work as a single unit with unified objectives. Management systems can be integrated because with the revisions and new editions of the different standards, the management systems have an increased number of similarities (Jackson, 1997). This integration of management systems is continuing to expand as many organizations are integrating their management system standards, for example, ISO 9001, ISO 27799 and other relevant standards to continue to gain efficiencies (Leonard & McGuire).
Jorgensen, Remen and Mellado (2006) state that integration may be seen as a solution to many different problems, e.g. the problem of many management systems being implemented separately in one organisation. The integration of management systems is often necessary when there are many management systems that are implemented from different sources. This is because these systems may sometimes create a confusing situation for organisations wishing to remain competitive (Jackson, 1997). The most commonly found integrated management systems in literature are those that address the integration of environmental management systems (EMS), occupational health and safety management system (OH&SMS) and quality management system (QMS) (Wilkinson & Dale, 1999). In the literature that was investigated, currently, there is no published IMS for quality and security in health care and this research will attempt to address this need.

1.6 Problem Statement

Multiple stand-alone management systems may be combined to form an integrated management system to reduce the complexities of implementing multiple management systems in an organisation. The main problem addressed in this research is that there is no documented integrated management system for quality and information security in the health sector. In order to investigate this properly the following research questions must be answered:

• What are the information requirements of the healthcare sector?
• What are the quality and information security requirements of the healthcare sector?
• Which management system standards can be used to address these quality and security needs?
• What are the requirements of establishing an integrated management system?
• Which similarities can be identified within the management system standards?
• How can management systems for quality and information security be integrated for the healthcare context?
1.7 Research objectives

The main objective in this research is to propose an integrated management system for quality and information security in the healthcare sector. The following relevant sub-objectives will be addressed based on the primary objective:

• Establish the information requirements of the healthcare sector;
• Determine the quality and information security requirements of the healthcare sector;
• Investigate the management system standards that can be used to address quality and information security needs in healthcare;
• Determine the requirements to establish an integrated management system;
• Ascertaining similarities between the identified management system standards;
• Compile an integrated management system for quality and information security in the healthcare setting.

1.8 Delineation of Research

The integrated management system for quality and information security proposed in this research is based on the ISO 9001 (2008), ISO 9004 (2000), IWA 1 (2005), ISO 27001 (2005) and the ISO 27799 (2008) standards. In particular, only the editions as indicated were considered. These standards were chosen to be included in the research as the ISO standards are internationally accepted and well known. Additionally, the standards were available to the researcher and sufficed for the purpose of exploring the establishment of an integrated management system. The fact that the IWA 1 and the ISO 27799 provide guidelines contextualized for health service organizations, further strengthened the case to use these standards.

1.9 Research Methodology

Research can be defined as scientifically and methodically delving into the unknown to provide information for solving problems (May, 2001). When conducting research,
a process must be followed and explained (Dam-Jensen & Carmen, 2009). The methods section should describe what was done to answer the research question and describe how it was done (Kallet & FAARC, RRT, 2004), i.e. the research methods that were used.

The research process involves several chronological steps, but this does not mean each step must be completed before the next step is undertaken (Reference for business, 2011). Furthermore, the process of research is dynamic and may change as the research progresses. The goal of the research process is to produce new knowledge, or to add to the body of knowledge that already exists (Dam-Jensen & Carmen, 2009). The research methods and processes are subsequently discussed in sections 1.9.1 and 1.9.2 respectively.

1.9.1 Research Methods

In this study the research methods used include conducting an extensive review of literature to obtain relevant data about the research topic and how to solve the identified problem. Another method used is a comparative analysis, where quality and information security management standards were compared to identify their similarities to assist with compilation of an integrated management system. Finally solid arguments were utilised to argue towards an Integrated Management System for Quality and Information Security in healthcare (IMSQS). The methods of literature review, comparative analysis and argumentation are subsequently discussed.

1.9.1.1 Literature review

A literature review is an account of what has been published on a topic by accredited scholars and researchers (Hart, 2006). The idea is to give an overview of research that has been conducted on facets of the problem that is being investigated (Olivier, 2004). Writing a literature review allows the researcher to gain and demonstrate skills in two areas such as information seeking which is the ability to scan the literature efficiently, using manual or computerized methods, and critical appraisal,
the ability to apply principles of analysis to identify unbiased and valid studies (Hart, 2006). It is important that a literature review should be organized around and related directly to the thesis or research question that is being developed (Machi & McEvoy, 2008).

For this study an extensive literature review was undertaken to accomplish the objectives of this research. The literature was reviewed regarding topics relevant to this research, which include:

- The health sector and its information requirements;
- Management systems for both quality and information security in the healthcare sector;
- Management system standards; and
- The integration of management system standards.

The sources used in the literature review were selected based on their availability and trustworthiness. A clear understanding of the health sector was established and the importance of quality and information security within the sector. A chapter on management system standards for quality and information security was written to expound the standards that can be used to achieve quality and information security in the health sector. Integrated management systems were outlined and discussed, because of their relevance to the study. In order to achieve the IMSQS, the integration of management systems standards was thoroughly investigated. Various techniques that are found in literature for the integration of management system standards were uncovered and laid out. In the next section the second research method that was used is further explained.

1.9.1.2 Comparative analysis

To determine whether the standards could be integrated, a comparative analysis of the ISO 9001, ISO 9004, IWA 1, ISO 27001 and ISO 27799 standards was undertaken. This served the purpose of discovering similarities in terms of corresponding sections (elements) and generic processes in the standards. By
interrogating the standards for similarities, the comparative analysis method was used as a basic platform for the integration of the standards. It further served the purpose of highlighting contextual requirements specific to the healthcare environment, provided in the IWA 1 and ISO 27799.

When constructing a comparative analysis the researcher investigates in a focused and systematic manner two or more items in depth and compares them to find the reasons for differences or similarities (Hofstee, 2006). In this research the results of the comparative analysis standards seeks to integrate the standards based on identified corresponding elements and generic processes.

1.9.1.3 Argumentation

Argumentation is a possible strategy, technique or method particularly suited to information technology research (Hart, 2006). A good argument should be integrated with, and acknowledge other arguments (Olivier, 2004). An argument should be well integrated with itself, and be related to other established arguments or facts (Mast, 2011). An argumentative research paper gives a lot of emphasis to the analysis of the issue (Olivier, 2004).

For the purpose of this research, Chapter 4 is dedicated to the integration of the relevant management system standards, through the use of the comparative analysis method. In Chapter 4 arguments are presented to reason towards the integrated management system for quality and information security in the healthcare context. The aim is to assist healthcare organisations with the integration of their quality and information security management systems.

The application of the three methods, namely literature review, comparative analysis and argumentation during the research process, is subsequently described.

1.9.2 Research process

An extensive literature review was carried out investigate the healthcare sector, its quality and information security needs and how these needs can be addressed in an
integrated manned by utilising integrated management systems standards. The ISO 9001, ISO 9004, IWA 1, ISO 27001 and ISO 27799 standards were thoroughly studied to obtain relevant information about how to address quality and information security. This led to the realization that these quality and information security management system standards could be addressed in an integrated manner, which led to the review of literature that addresses the integration of management systems.

The literature showed that through the commonalities found within management systems standards, the integration of the management systems is enabled. It was revealed that there are various methods of integrating management systems. This research implemented one such method that was identified during the literature study. This is the integration of management systems standards through the use of identified common elements and generic processes. This research finding led to a comparative analysis of the relevant management system standards to find the commonalities within the standards. The commonalities were used to argue towards how the individual management systems can be implemented as an integrated management system.

1.10 Structure of the Dissertation

The layout of the dissertation is shown in Figure 1.1. The first chapter provides an introduction to the dissertation which includes the problem statement, research objectives and methods and process used in conducting the research. Chapter 2 explores the health sector as an area of application; various threats to healthcare information are explored and the importance of both quality and information security in healthcare. The third chapter expands on the second chapter by introducing the concepts of quality and information security management system standards as a means to reduce the security related risks as described in chapter two and to ensure that quality is maintained in healthcare.

Chapter 4 constitutes the solution of the dissertation and presents the Integrated Management System for Quality and Information Security in healthcare (IMSQS). It proposes the components that an integrated management system for quality and information security in the healthcare context should contain.
Chapter 1
Introduction

Chapter 2
The Healthcare Milieu

Chapter 3
Management Systems for Quality and Information Security
- ISO 9001, ISO 9004, IWA 1
- ISO 27001, ISO 27799

Chapter 4
IMSQS: An Integrated Management System for Quality and Information Security in Healthcare

Chapter 5
Conclusion

Fig 1.1 Layout of the dissertation
Chapter 5 provides a conclusion summarizing the research and the achievement of the objectives stated in Chapter 1. Suggestions are provided for future research in this area.

1.11 Conclusion

The intention of this chapter was to introduce the reader to the broader research area of this project and to narrow the discussion to the problem statement. It goes further to specify the proposed solution to the problem statement, by looking at the main and sub-objectives of the research. In Section 1.9 the research methods were discussed. A high-level outline of the dissertation was provided in Section 1.10. In the next chapter this groundwork is further expanded by reporting on the literature study conducted about the healthcare sector in regard of quality and security.
Chapter 2
The Healthcare Milieu

Chapter Two explores the healthcare sector, the information that is essential for the proper care of patients and the health information systems that store that information. The quality of service delivery in health care is examined. The importance and necessity of information security when storing patient information electronically, especially within the healthcare sector, is investigated.

2.1 Introduction

Health is seen as a state of complete physical, mental and social wellbeing, and not merely the absence of disease or sickness. It is understood to be a fundamental human right, therefore, the attainment of the highest possible level of good health is important worldwide (Alta, 1978). Healthcare is an important segment of the economy and a key component of human welfare and society and governments are willing to commit a reasonable number of resources to explore and improve it (Zinkhan & Balazs, 2004).

The healthcare sector, as defined by Investopedia, is a category of supply relating to medical and healthcare goods or services. It incorporates hospital management firms, healthcare maintenance organizations, biotechnology and a variety of medical products (Investopedia, 2009). Mahmud and Parkhurst (2007) define the healthcare sector as one that includes a wide range of businesses such as drug manufacturers including the pharmaceuticals and biotechnology industries, diagnostics and device manufacturers, hospitals, insurance providers, and health technology and information providers. These definitions describe the healthcare sector as an information-and knowledge-intensive enterprise (Willam & Herbert, 2009), that generates huge volumes of data from hospitals, primary care surgeries, clinics and laboratories on a daily basis (Grimson, 2001).

The healthcare sector, as indicated in the afore-mentioned definitions, comprises
various types of healthcare services providers. These include private hospitals and day surgeries, medical practitioners, pharmacists, and complementary therapists, gyms, weight loss clinics and many others (Office of the privacy commissioner, 2001).

The environment of the professional healthcare organization is changing (Armoni, 2002). The provision of effective and appropriate health care is becoming complex. Its challenges include the frequent rapid changes in the patterns of healthcare service delivery and the changing demographics of the people served (Hellesø, Lorensen, & Sorensen, 2004). Healthcare has evolved into a business entity that requires strategic planning, financial management, operational control, and functional specialties to maintain its viability (Brogan, 2009). Its growth and change are driven by rising expectations and demands from people who are seeking a prolonged quality of life, effective treatments and by a rapidly developing science base which is enabling new diagnostics and treatments to be developed (Bartlett, et al., 2003).

The healthcare sector is currently experiencing a number of pressures, both internally and externally. The continuing innovation in medicine and healthcare technologies has resulted in new methods and tools in healthcare (Tsiknakis, Katehakis, & Orphanoudakis, 2004). The pressures faced by the healthcare sector influence the way in which its services are provided (Grimson, 2001).

The pressure for improved access to healthcare and the expectation of providing health care at lower cost together with the development of vertically and horizontally integrated delivery systems are creating dramatic changes in the roles and responsibilities within the healthcare sector (Hasman, 1998). The cost of health care is rising rapidly in most industrialized nations and there is concern that, despite high levels of spending, the quality and efficiency of care is at times inadequate (Jha, Doolan, Grandt, Scott, & Bates, 2008). These factors cause governments, worldwide, to be confronted by the urgent need to limit this rise in healthcare costs without compromising quality, equity and access. As a result, new ways to organise and deliver health services are being investigated and experimented with (Tsiknakis, Katehakis, & Orphanoudakis, 2004).
In many regards, the response of the healthcare sector to these changes and pressures has been deemed as inadequate. This is because the sector fails to anticipate and often responds inappropriately with too many resources that arrive too late or too many resources in the wrong place when responding to immediate healthcare challenges (World Health Organization, 2008). Despite a strong commitment to delivering quality healthcare, problems that involve medical errors and ineffective treatment continue to badly affect the industry (William & Herbert, 2009).

An important development in healthcare includes the movement towards shared or integrated care in which the traditional, single doctor to patient relationship is moving towards one where the healthcare of the individual is the responsibility of a team of professionals across all sectors of the healthcare system (Grimson, 2001). Due to the continuous development within the sector, service delivery needs constant monitoring. This is done to evaluate the effectiveness of delivery and to measure customer satisfaction. Both measures are important to enhance the effectiveness of service delivery and control healthcare costs (Balazs & Spotts, 2000).

There are various types of services provided by the healthcare sector. These include primary, secondary and tertiary healthcare. These services are explored in the next section.

### 2.2 Types of healthcare services

#### 2.2.1 Primary Healthcare

Primary Healthcare, as defined by the World Health Organization (WHO) in 1978, is essential healthcare. It is based on practical, scientifically sound, and socially acceptable methods and technology. It is universally accessible to all in the community through their full participation, at an affordable cost and is geared towards self-reliance and self-determination (WHO, 1978). The College of Medicine, University of Saskatchewan (2011), defines primary healthcare as shifting the emphasis of healthcare to the people themselves and their needs. This reinforces
and strengthens their capacity to shape their lives, hospitals and primary healthcare centres. It is seen as a task-oriented process that deals with common health problems in communities with a number of stakeholders that are involved in providing primary healthcare (Hanson, et al., 2008).

Primary healthcare forms an integral part both of the national health system of which it is the central function and main focus, and the overall social and economic development of the community (Aboriginal health & medical research council, 1999). One of the key elements of primary healthcare is to be responsive to the community needs (Weitzman, Kaci, & Mandl, 2009). This is possible because primary healthcare shifts the emphasis of healthcare to the people themselves and their needs (University of Saskatchewan, 2011).

Primary healthcare is that element within healthcare that focuses on services provision, including health promotion, illness and injury prevention (Weitzman, Kaci, & Mandl, 2009). Primary healthcare, in the developed countries, is usually provided by a medically qualified physician, however, in the developing countries, the first contact of care is often, but not always, provided by non-medically qualified personnel (Encyclopedia Britannica, 2009).

2.2.2 Secondary and Tertiary healthcare

Secondary healthcare refers to the service provided by medical specialists who generally do not have first contact with the patient. These services are established to diagnose and treat illness and disease (Brogan, 2009). Secondary healthcare is the provision of a specialized medical service by a physician specialist or a hospital on referral by a primary care physician (Mosby's medical dictionary, 2009). Its primary goal is to detect illness in its early stage and expedite treatment to prevent further disease or illness (Aboriginal health & medical research council, 1999). Secondary healthcare services are more general health services that are provided at hospitals (Brogan, 2009). Secondary healthcare services may include specialist hospitals, rehabilitation hospitals and psychiatry or old age hospitals.
Tertiary Health care refers to specialised services provided by medical practitioners (Aboriginal health & medical research council, 1999). These services focus on restorative care designed to restore an individual back to an optimal level of health. The goal of this type of care is to decrease the risk of permanent disability related to disease or illness (Brogan, 2009). Common examples of tertiary healthcare are physical therapy, speech therapy and respiratory therapy.

Primary, secondary and tertiary services are provided according to a provider funding model, known as the public and private sector. The public and private healthcare sectors are discussed in more detail.

2.2.3 Private Healthcare vs. Public Healthcare

It is important, when discussing private and public healthcare, to consider that countries have their own models for the public and private sectors. Therefore, these two sectors are discussed in general and do not pertain to any particular country.

Private healthcare can be defined as a process in which non-governmental actors become increasingly involved in the financing or provision of healthcare services (Uplekar, 2000). Private healthcare providers cater for a large proportion of the population in most low- and middle-income countries. This is where a considerable amount of the total healthcare expenditure is absorbed. Private healthcare plays an important role when under-resourced public healthcare fails to provide quality healthcare to all of the population (Lönnroth, Thuong, Duy Linh, & Diwan, 1998). Private health care, without any waiting time, is an option for the patient trying to avoid the public sector healthcare queue (Hoel & Sæther, 2001).

Privatisation involves changes to the public and private roles and responsibilities in the health sector, and generally includes changes in actual ownership of the means of financing and providing healthcare (Uplekar, 2000). The public sector would be unable to function without the private sector. This is because the private sector has the resources that can provide a higher level of care than that offered by the public sector. In some countries the public and private sectors are forming new kinds of
cooperative networks with the aim of providing more efficient healthcare services of a better quality for patients who have increasing expectations (Länsisalmi, Mika, Aalto, & Ruoranen, 2006). The public sector is discussed next.

The term “public health” means different things to different people. Many people understand public health to mean attention to clean drinking water, good sanitation and the control of rats, mosquitos and other diseases (Madden, 1999). The public health sector implies coordination and cooperation between individuals, government agencies and private and community-run organisations. Publicly delivered healthcare is provided by non-profit public-sector practitioners in publicly owned facilities. The funding for these systems typically comes from the public sector (Blanchette & Tolley, 2001).

The security of the public health sector, worldwide, depends on their capacity to act effectively and contribute to the health of all. The world is rapidly changing and information moves faster than previously which makes the sharing of essential health information one of the most feasible routes to global public health security (Prentice & Reinders, 2007). The history of the public sector in medical care shows movement towards increasing government involvement (Cutler, 2002).

In countries with dominantly public health care, there are often queues for some types of treatments. The waiting time in the public health system is explained by referring to limited public resources (Hoel & Saether, 2003). The main difference between the private and public sector is that the former attempts to maximize its profits, share or volume, while the role of public sector maximizes the sum of its benefits to society (Grundgeigera & Sandersona, 2009). In both the public and private sectors, patient information, including personal details and healthcare conditions, needs to be stored. In the following section, the information pertaining to the patient is discussed. This is termed healthcare information.

### 2.3 Healthcare Information

Historically, critical health information for a patient seeking treatment, for a variety of
conditions such as allergies, current treatments or medications, has been scattered across paper-records kept by different healthcare service providers in a variety of locations. This made it difficult for a healthcare clinician to access all the health information for a patient at the time of care (Hufnagel, 2009). This has made access to this critical data challenging and it is difficult for healthcare clinicians to make the most informed decisions on treatment options which may potentially put the health of the patient at a greater risk (Hufnagel, 2009).

The information that is collected about the health of an individual is called health information (Office of the privacy commissioner, 2001). It may be a combination of demographics, administrative, and clinical data captured during a healthcare encounter (Brogan, 2009). It includes but is not limited to data such as medical information, personal details, such as a name, address, admission and discharge dates, billing information and genetic information (Kon & Gvozdanovi, 2006). It may include information about the next of kin and other identifying information (Waldo, Lin, & Millett, 2007). It includes the information collected by a healthcare service provider during the course of providing treatment and care to an individual (Brogan, 2009). The healthcare information that is collected by healthcare providers is important for healthcare workers to best ensure that their clients, the patients, are properly cared for (Matshidze & Hanmer).

Healthcare information can be obtained from different sources or repositories that are spread over multiple locations. This information is often in differing forms, for example, completed patient records; hand-written prescriptions; reports by a physician, a consultant or a laboratory (Waldo, Lin, & Millett, 2007). Other sources of healthcare information include news from the media, government documents, reports, announcements and research publications (Quynh, 2005). Furthermore, information is combined for secondary purposes, such as the management of local health services, the monitoring and surveillance of diseases, and for planning the delivery of health services at regional, national and international levels (Bath, 2008).

The healthcare information of a patient is used in the practitioner-patient interaction and by other numerous, spatially dispersed third-parties. Such third-parties include
the following:

- The medical practitioners who are given access to the medical data of the patient in the context of shared medical care;
- The administrative bodies charged with the management of healthcare services; and
- Other third-parties such as insurers and employers.

These third-parties deem this health information as essential for planning and decision making at all levels of the healthcare spectrum (Matshidze & Hanmer). Additionally, healthcare information can be used in assisting patients to anticipate and understand how their illness can affect their health and life in general (Deering & Harris, 1996).

The problems that people can have with health information, as stated by Deering & Harris (1996), include:

- How to interpret conflicting or differing information;
- How to judge reliability; and
- How to decide what to do when given many choices.

A considerable improvement is evident with the enhanced availability of health information in an electronic format (Barrows & Clayton, 1996). Easy access to and the organisation of information can be provided by the automation of healthcare records, but the availability of the information depends on whether the practitioners actually collect and record the healthcare information from the patient (Tang & Hammond, 1997).

2.4 Health Information Systems

The healthcare record is captured either in a paper-based or computer-based format. Paper-based records were used prior to the application of (computers) machines to
the healthcare sector (Brogan, 2009). In some countries the computer-based medical record has replaced the paper-based medical record as the primary source of information for health care and it meets all the clinical, legal, and administrative requirements (Dick, Steen, & Detmer, 1997). Quynh (2005) states that this integrated, electronic, health record system is needed for the following reasons:

- Patients do not always know their health conditions and remember their health treatment history;
- There is a need for health workers to access the same information from a common source so they have adequate information about their patients;
- Testing and related results held at different health centres should be made available via a common e-system; and
- An integrated health record system can be of great interest to research, health management and administration.

A health information system is defined as the unified collection of different types of information systems used by clinicians in health services (Fernando & Dawson, 2009). HIS are important support tools in the management of healthcare services delivery in both the developed and less developed countries. An adequate HIS is essential to assess the health needs of populations and groups, and to plan and implement health interventions (Azubuike & Ehiri, 1999). Health information systems are increasingly being developed within healthcare institutions, in broad areas of application (Gritzalis, 1997). They provide great processing power, extensive repositories of patient data, and convenient client-based user interfaces (Giuse & Kuhn, 2003). Healthcare staff depend increasingly on these computerised HIS to perform their everyday functions such as diagnosing, the recording of medical information or to assist in patient treatment (Katsikas, 2000).

Healthcare information systems are used to (Economic Commission for Africa, 1999; Wua, Chen, & Greenese, 2009; Glaser, Drazen, & Cohen, 1986):

- Promote better health behaviour;
- Improve decision making, to promote information exchange among peers;
• Enhance self-care and professional support;
• Improve the effectiveness of health institutions;
• Attain the provision of optimal communication with all healthcare service providers;
• Deliver high-quality and efficient health care;
• Limit the problem of medical errors (e.g. through increased accuracy and legibility of information);
• Facilitate point-of-care decision support;
• Streamline workflow (e.g. through a reduction in the number and kinds of forms to be completed);
• Reduce costs; and
• Improve the patient–physician relationship.

However, there are specific challenges relating to the use of electronic storage of information in health. These challenges as reported by Grimson (2001) include:

• Multimedia complexity of medical data;
• Data capture for unstructured text;
• Terminology;
• Coding and classification issues;
• The absence in many countries of a unique national patient identifier;
• A general lack of awareness of the benefits;
• Risks;
• Wariness due to a number of highly publicised failures; and
• Security and confidentiality concerns.

Adequate and reliable HIS have been recognised as essential in the achievement of the goals of health for all. They can be crucial in the planning and delivery of national healthcare priorities. Lack of an effective HIS can have undesirable consequences on health service delivery, particularly in the public health sector and in primary health care, as apparent in the following areas (Azubuike & Ehiri, 1999):

• Health needs assessment: Among the responsibilities of any given health
ministry or department is the assessment of the health needs of the population it serves;

- Monitoring of disease trends: Reliable information is essential in understanding any changes in spatial disparity of diseases or conditions. This would have significant implications in designing appropriate interventions to minimise their impact; and

- Effective planning of health interventions: This involves the proper assessment and prioritisation of needs. The achievement of these interventions is largely dependent on the availability of adequate health information.

The absence of a reliable HIS will make the afore-mentioned tasks difficult to achieve.

It is evident from the afore-going discussion on HIS that these systems have the potential to address many of the problems and concerns experienced in healthcare, as highlighted in this chapter. With the understanding gained of the broader healthcare sector, its information needs and the systems used to store, process and access healthcare information, the rest of this chapter will focus on quality of care and the security and privacy of healthcare information. Quality of care is an important aspect in health, therefore, the quality of healthcare service delivery and its benefits are discussed next.

2.5 Quality of service delivery in healthcare

As stated in section 2.1, pressure is being exerted upon healthcare institutions to improve their efficiency and competitive advantage in relation to cost effectiveness and the quality of care (Wardhania, Utarini, van Dijk, Post, & Groothoff, 2009). Quality of service delivery affects financial performance in terms of profitability, by reducing costs and increasing revenues (Macinati, 2008). However, in the healthcare sector, the introduction of quality programs lags behind that in other industries, e.g. the manufacturing industry (van Harten, Casparie, & Fisscher 2002). Both in
manufacturing and in health care, quality allows organizations to pursue their own objectives (Wardhana, Utarini, van Dijk, Post, & Groothoff, 2009).

Quality of health care is defined as the degree to which the provision of health services for individuals and populations increases the likelihood of desired health outcomes and is consistent with current professional knowledge (Cooperberg, Birkmeyer, & Litwin, 2009). Poor healthcare service quality wastes resources that could be used to treat more patients (Øvretveit, 2003). When quality initiatives are implemented, they lead to process improvement, which results in cost reduction and can improve clinical output (Macinati, 2008). Quality initiatives are being introduced because the public is increasingly critical of the quality of hospital service delivery (Øvretveit, 2003).

Health care quality problems are classified into 3 categories and examples provided by Chassin and Galvin (1996):

- Underuse is the failure to provide a health care service when it would have produced a favourable outcome for a patient. An example of overuse is missing a childhood immunization for a disabling disease like polio.
- Overuse occurs when a health care service is provided under circumstances in which its potential for harm exceeds the possible benefit. Prescribing an antibiotic for a viral infection, for which antibiotics are ineffective, constitutes overuse.
- Misuse occurs when an appropriate service has been selected but a preventable complication occurs and the patient does not receive the full potential benefit of the service. A patient who suffers a rash after receiving penicillin for strep throat despite having a known allergy to that antibiotic is an example of misuse.

According to Chassin and Galvin (1996) evidence from careful research studies demonstrates a large number of serious problems in each of these categories. Poor quality health care may discourage patients from using the available services. If the healthcare system cannot be trusted to guarantee a threshold level of quality, it will
remain underutilized, be bypassed, used only for minor ailments, or used as a measure of last resort (Andaleeb, 2001).

The core of this discussion centres on the theme of ensuring quality service in the delivery of health care and one way to facilitate this is by utilising information systems to store healthcare information. In the context of the healthcare milieu, it is unlikely that quality healthcare information can be maintained without using electronic systems. Information systems can play an important role in reducing inefficiencies in healthcare by ensuring that the right information is available in the right place at the right time (Hasman, 1998). The benefits of maintaining quality healthcare information include its reliability in supporting informed decisions about healthcare and treatment and its role in facilitating continuity of care when a new health service provider becomes involved (Crompton, 2001).

While the benefits of healthcare records are numerous, inter alia in the improvement of quality of care, these records are particularly sensitive to the information security aspects of confidentiality, integrity and availability (Cavalli, Mattasoglio, Pincioli, & Spaggiari, 2004). When an HIS is used to store patient information, there are undoubtedly security issues that arise (Bakker, 1999). In the following section the importance of securing information in the healthcare sector is discussed.

### 2.6 Information Security Requirements in Healthcare

In section 2.3 it was established that patient healthcare information can be shared by a wide range of people, both in and out of the healthcare industry. The electronic availability of healthcare information on multiple systems is important because it allows the patient health information to move with them from provider to provider, regardless of where the information originated (Knol, 2009). However, its access should be obtained only when the patient agrees to let others view their information. It is necessary to agree to the sharing of health information when wanting to obtain care e.g. in case of emergency or to qualify for health insurance. Permission must be granted for access, however, the information also has to be available when needed (Rights, 2008). The availability and accessibility of information is becoming important
as society moves towards an approach where patients can receive care from several providers in cross-border healthcare (Wallin & Xu, 2008).

Anderson (2003) states that “Information security encompasses the use of physical and logical data access controls to ensure the proper use of data and to prohibit unauthorized or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets”. Apart from secure communication mechanisms, systems used in healthcare are faced with high demands for privacy and medical data confidentiality, clinical documents integrity and validity checking and data persistency (Kon & Gvozdanović, 2006).

Ahlfeldt (2006) emphasises the aims concerning information security in healthcare, namely to reach a high level of security, but also to reach a high level of patient privacy. As explained in section 1.3, security is often referred to in terms of the confidentiality, integrity and availability of information, while privacy refers to the patient’s right to decide about the disclosure of their personal information.

Xu (2008) states that the patient is the most important factor in healthcare, and therefore, the patient information must be kept secure from any security breach. Healthcare organisations should aim to provide strict requirements that ensure high levels of data security because healthcare information is particularly sensitive. Williams (2008) confirms that information security is important in any organisation but particularly where personal and medical information is routinely recorded. The collected healthcare information is potentially vulnerable to misuse from both authorized and unauthorized users who inappropriately access patient information for their own personal or economic gain (Mandil & Darbellay, 2003).

A formal approach to managing the use and disclosure of personal health information is in the best interests of patients, individual researchers, organizations and society (Cooper & Collman, 2005). The risks of ignoring good security and privacy practices are substantial. It should be noted that information security cannot
be achieved only through technical means but should be supported with management processes (Cavalli, Mattasoglio, Pincioli, & Spaggiari, 2004).

2.7 Conclusion

Health care organizations generally adopt information technology to reduce costs as well as improve efficiency and quality (Cooper & Collman, 2005). However, this places new demands on the healthcare sector to maintain a sufficient level of information security and to strive to maintain patient privacy (Ahlfeldt, 2006).

The aim of Chapter 2 was to explore the healthcare sector and the benefits and challenges that health information systems have brought to the sector. The different providers within the healthcare sector were discussed, namely healthcare providers from the private and public sectors. The information needs and the systems used to store information in the healthcare sector were discussed. The quality of service delivery in health was discussed and the need for quality in healthcare, especially in relation to the healthcare service provided to patients. The use of technology to store healthcare information and the security challenges arising from this were discussed.

The two main themes carried forward to Chapter 3, are quality and information security in the healthcare context. Both quality management systems and information security management systems were introduced in Chapter 1 as structured organizational processes to improve quality and information security respectively. These management systems are the focus of Chapter 3 and form the base of argumentation towards an integrated management system for quality and information security in Chapter 4.
Chapter 3
Management Systems for Quality and Security

The aim of Chapter 3 is to investigate management systems and management systems standards for quality and information security. Initially, an overview of the ISO 9000, 9001, 9004, IWA 1, ISO 27001 and ISO 27799 is presented. A more detailed discussion of the IWA 1 is provided to illustrate the characteristics of quality in the healthcare sector. The ISO 27001 is examined to illustrate how the characteristics of security can be achieved using this standard.

3.1 Introduction

A management system can be defined as a composite of personnel, resources, policies and procedures interacting in an organised way to ensure a given task is performed, or to achieve or maintain a specified outcome as a set of common elements in an effective and efficient manner (Karapetrovic & Willborn, 1998). Traditionally, management systems for quality, environmental, information security and occupational health and safety management are operated independently by different departments in organisations (Wilkinson & Dale, 1999). At the operational level, each management system has unique processes which are undertaken (Jackson, 1997). A number of standards have emerged to guide systematic implementation of various management systems, some of which have gained global recognition – such as ISO 9001 and ISO 14001 (Asif, De Bruijn, & Fisscher, 2010).

3.2 Management Systems Standards: Quality and Security

In accordance with the delineation of the research mentioned in section 1.8, the following standards will be considered in the areas of quality and security:

- Quality (section 3.2.1): ISO 9001, ISO 9004 and IWA 1; and
3.2.1 Management system standards for quality

The ISO 9001 and ISO 9004 standards both form part of the ISO 9000 family of standards which define the requirements for quality management in organizations. The ISO 9001 and ISO 9004 standards are subsequently discussed.

3.2.1.1 ISO 9001

The ISO 9001 is a standard for quality management systems (Yoo, et al., 2006). Van Houten (2000) states that ISO 9001 is an internationally recognized quality management system (QMS) standard used by organisations to ensure that quality standards are maintained. ISO 9001 is based on the process approach and the eight quality management principles of customer focus, leadership, involvement of people, process approach, systems approach to management, continual improvement, factual approach to decision-making and mutually beneficial supplier relationships (Yoo, et al., 2006).

The ISO 9001 specifies the requirements for a QMS for use by organisations for internal application, certification or contractual purposes (Yoo, et al., 2006). The purpose of the ISO 9001 QMS is to provide businesses with a model to grow systematically while assuring the quality of their products (Aldowaisan & Youssef, 2006). It, therefore, applies to the processes that create and control the products and services an organisation supplies. It prescribes systematic control of activities to ensure that the needs and expectations of customers are met (BSI, 2007).

The ISO 9001 and ISO 9004 were created as a consistent pair of standards so that businesses that wanted to exceed the requirements of 9001 could use the principles of 9004 to move towards business excellence (Boys, Karapetrovic, & Wilcock, 2004). This leads to a discussion about the ISO 9004.

3.2.1.2 ISO 9004

The ISO 9004 standard provides guidance for the continuous improvement of existing quality systems beyond the minimal ISO 9001 requirements (Boys,
Karapetrovic, & Wilcock, 2004). This international standard promotes the adoption of a process approach when developing, implementing and improving the effectiveness and efficiency of a QMS to enhance interested party satisfaction by meeting their requirements (ISO 9004, 2000).

When compared to ISO 9001, the objectives of customer satisfaction and product quality are extended to include the satisfaction of interested parties and the performance of the organization (Boys, Karapetrovic, & Wilcock, 2004). The ISO 9004 standard is applicable to the processes of the organization and consequently the quality management principles on which it is based can be deployed throughout the organization (Chan, Neailey, & Ip, 1998). Its focus is the achievement of on-going improvement, measured through the satisfaction of customers and other interested parties (ISO 9004, 2000). The ISO 9004 consists of guidance and recommendations and is not intended for certification, regulatory or contractual use or as a guide to the implementation of ISO 9001 (Boys, Karapetrovic, & Wilcock, 2004). Figure 3.1 succinctly summarizes the difference in emphasis between the ISO 9001 and 9004 standards.

Fig 3.1 – Difference between the ISO 9001 and 9004 standards (Wilson Mar, n.d.)
In addition to the general requirements and guidelines for management systems which are independent from specific industries, sector-specific management system standards or guidelines are occasionally developed by a particular industry to address specific needs or requirements. The ISO International Workshop Agreement (IWA) 1 guideline to implement a QMS in healthcare is one such example. An International Workshop Agreement (IWA) is an alternative to a full International Standard, and is offered by ISO for cases where rapid development and publication are required (ISO, 2005). The IWA 1 (2005) is subsequently introduced briefly in section 3.2.1.3. This discussion is expanded in section 3.3 to describe the document in more detail.

3.2.1.3 IWA 1

The IWA 1 is the first quality management standard developed for healthcare provider organisations. (Dyro, 2004). The IWA 1, “Quality management systems – Guidelines for process improvements in health service organizations” is based on the ISO 9004:2000, “Quality management systems – Guidelines for performance improvements” (Reid, 2001). The guidelines include much of the text of ISO 9004 supplemented by text specifically aimed at assisting health service organizations to implement a QMS, regardless of whether they decide to pursue certification to ISO 9001 (ISO, 2005).

The document provides a framework for the design and improvement of process-based QMS by health care organizations (Reid, 2001). The guidelines are voluntary and are not intended for certification or accreditation. (Dyro, 2004). In summary, the IWA 1 guidance document is a unique tool that the healthcare industry can adopt and begin implementing to help increase operational efficiencies, reduce errors and adverse outcomes, and experience a greater patient/client focused culture (Sporidis, 2007).

The standards that are discussed in the following section are the management system standards for information security, as relevant to this study. The discussion commences with a brief overview of the ISO 27000 family of standards.
3.2.2 Management system standards for security

The ISO standards for information security management are within the 27000 et seq. numbering scheme and comprise an extensive suite of standards. The ISO 27799 is the industry-specific rendition and companion guide to the ISO 27002. The ISO 27001 standard focuses on the processes required to implement an ISMS (Wolfe, 2009), which is the focus of this research. Therefore section 3.2.2 focuses first on the ISO 27001 standard and thereafter considers the requirements for information security management in healthcare as described in the ISO 27799.

3.2.2.1 ISO 27001

An Information Security Management System (ISMS) is a set of coordinated activities to direct and control the preservation of confidentiality, integrity, and availability of information (Carlson, 2008). An ISMS allows the senior management to monitor and control their security, minimise the residual business risk and ensure that security continues to fulfil corporate, customer and legal requirements (Analytix, 2009). The ISMS provides processes and controls for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the system and managing documents and records within the context of the overall business risks of the organisation (ISO27001). The ISO 27001 is a generic model that can be used when establishing an ISMS, but because the healthcare sector has unique characteristics the ISO 27799 standard is discussed.

3.2.2.2 ISO 27799

The ISO 27799:2008, “Health informatics – Information security management in health using ISO/IEC 27002”, addresses the issue of the highly sensitive area of personal health information and how to protect its confidentiality and integrity while assuring its availability for healthcare delivery (Maillard, ISO, 2008). The standard provides guidance to health organizations and other holders of personal health information on how to protect such information via the implementation of ISO27002 (Fraser, 2006). This will enable healthcare organizations and other custodians of
health information to ensure a minimum requisite level of security that is appropriate to their size and circumstances (IHS, 2008).

The increasing use of wireless and Internet technologies in healthcare delivery, and the consequent growth of electronic exchange of personal health information between health professionals, heightens the need for effective IT security management in healthcare (Maillard, ISO, 2008). For the proper management of information security in healthcare, a minimum set of requirements must be met (Fraser, 2006). The benefit of meeting the minimum requirements is to adopt a common reference for information security management in healthcare (Maillard, ISO, 2008).

ISO 27799 is a companion to ISO/IEC 27002, “Information technology - Security techniques - Code of practice for information security management” (IHS, 2008). Together, ISO 27799 and ISO 27002 define what is required in terms of information security in healthcare, but they do not define how these requirements are to be met (ISO / IEC 27799, 2008). This is done in the ISO 27001.

In section 6 of the ISO 27799, the establishment, operation, maintenance and improvement of an ISMS in healthcare is discussed using the ISO 27001 as frame of reference.

For the sake of clarity, it is appropriate to mention the reason for providing an expanded discussion on the IWA 1 and ISO 27001 in sections 3.3 and 3.4 respectively.

Each section of the IWA 1 document is tied to its counterpart in ISO 9004 containing all the requirements of ISO 9001 (IWA 1, 2005). It is therefore appropriate to consider the IWA 1 in terms of this research. In contrast, the ISO 27799 was created as a companion for the ISO 27002 (although a limited discussion of the ISO 27001 is provided in section 6 of the ISO 27799). Therefore it is appropriate to consider the ISO 27001 rather than the ISO 27799 in more detail for the purpose of investigating the creation of an integrated management system. After gaining this clarity, Chapter
4 makes provision for input about the aspects in section 6 of the ISO 27799 which are relevant to this research.

For each of the IWA 1 and ISO 27001, the purpose, benefits, process approach and certification issues are subsequently discussed.

### 3.3 IWA 1

The guideline that is specifically designed for use in healthcare to manage quality is the IWA 1:2005. To reiterate, the IWA 1 entitled “Quality Management Systems – Guidelines for Process Improvements for Health Service Organizations”, is based on the ISO 9004:2000. This is confirmed by van Harten, Casparie and Fisscher (2000) who state that the guidelines used in the IWA 1 include those of the ISO 9004:2000 supplemented by text specifically aimed at assisting health service organizations to implement a QMS. It was developed in an international workshop organized under the aegis of ISO, by a joint committee of experts from the American Society for Quality (ASQ) Health Care Division and the Automotive Industry Action Group (AIAG) which is a global industry association representing automotive manufacturers (Frost, 2006).

It was necessary for the IWA 1 document to be created to address quality needs in the healthcare sector. The IWA 1 provides guidance specifically “for any health service organization involved in the management, delivery, or administration of health service products or services, including training and research, in the life continuum process for human beings, regardless of type, size, and the product or service provided” (Sporidis, 2007). The IWA 1 guidance document is, therefore, a useful tool and helps to create an opportunity for hospitals and other health service providers to reduce waste, increase operational efficiencies, reduce patient errors, and enhance the patient/client focus throughout the organization, among many other things (Takeda, et al., 2003).

#### 3.3.1 Purpose of a QMS in health

The IWA 1 aids in the development or improvement of a fundamental QMS for health
service organizations that provides for continuous improvement, emphasizing error or adverse outcomes prevention, the reduction of variation and organizational waste, for example non value added activities (IWA 1, 2005). It defines expectations about how a particular healthcare activity will be performed to produce the desired results (Marquez, 2001). It focuses on the achievement of on-going improvement, measured through the satisfaction of customers and other interested parties (IWA 1, 2005).

Performance in accordance with standards is the end result of a wide range of quality assurance activities, including the accreditation of health facilities, external quality evaluation, and performance improvement (Yeung & Y, 1998). The IWA 1 provides guidelines by considering both the effectiveness and the efficiency of a QMS, and consequently the potential for improvement of the performance of an organization (IWA 1, 2005).

The ISO 9004, which the IWA 1 is based on, addresses the improvement of both the effectiveness and efficiency of a QMS, while ISO 9001 is limited to the assessment of effectiveness (Boys, Karapetrovic, & Wilcock, 2004). The IWA 1 provides opportunities to increase operational efficiencies throughout any health service organization and these efficiencies become significant once top management is committed to its implementation (Yeung & Y, 1998). The literature in quality management suggests that the improvement of quality management practices is a continuous process (Yeung & Y, 1998). In the following section, the benefits of a QMS in healthcare are discussed.

### 3.3.2 Benefits of a QMS in health Care

Marquez (2001) states that health service providers are interested in improving the quality of care and service they provide to their patients/clients. The objectives as outlined in the IWA 1:2005 document, are the goals that many organizations in the healthcare industry have set for themselves and are looking for the best possible ways to achieve them. These goals, which also demonstrate benefits to the organization, include (IWA 1, 2005):

- Minimize / reduce burden on the organization;
• Improve delivered health service quality and safety to complement existing accreditation or aid in achieving accreditation;
• Provide process improvements to increase the value added to the organization and the patient/client;
• Improve the image of the organization, increase patient/client confidence in the organization, and have a tool to reward quality;
• Maintain consistency in approach through the use of a globally recognized and accepted standard; and
• Develop / incorporate a process that is actionable.

Other benefits of implementing a QMS in healthcare as described by Reid (2001) include increases in organisational effectiveness and efficiency, standardisation of work and documentation and reduction of risks and errors. The ISO 9004 states that successful use of the eight management principles by an organization should result in benefits to interested parties. These benefits include improved monetary returns and the creation of value and increased stability (ISO 9004, 2000).

The benefits of implementing a QMS in healthcare have been highlighted; subsequently the process approach which is followed to establish a QMS is outlined.

3.3.3 The Process Approach

The IWA 1 international standard promotes the adoption of a process approach when developing, implementing and improving the effectiveness and efficiency of a QMS to enhance interested party satisfaction by meeting their requirements (IWA 1, 2005). The process approach of the IWA 1 is shaped by the principles that underlie the ISO 9001 and were adopted as the underlying framework for ISO 9004 (Boys, Karapetrovic, & Wilcock, 2004). Both the ISO 9001 and the ISO 9004 state that they promote the adoption of a process approach when developing, implementing and improving the effectiveness of a QMS, to enhance customer satisfaction by meeting customer requirements (ISO 9004, 2000). In the same way that the process approach is a continuous cycle in the IWA 1, so is the ISO 9001 because it requires
that the organisational processes undergo continuous improvement (Yoo, et al., 2006).

In Figure 3.2, a model of a process-based QMS is shown. In this regard it is important to understand the concepts of a process and a process approach. The IWA 1 (2005) concisely describes a process as “an activity using resources, and managed in order to enable the transformation of inputs into outputs”. The ISO 9001 (2008) explains that a ‘process approach’ is “the application of a system of processes within an organization, together with the identification and interactions of these processes, and their management to produce the desired outcome”.

Figure 3.2 - Model of a process-based quality management system (ISO 9001, 2008; ISO 9004, 2000; IWA 1, 2005)
The model shown in Figure 3.2 is a generic model which does not show the processes at a detailed level. However, it can be seen that customers (and other interested parties) provide a significant input in defining the requirements for the organization’s product. Customer satisfaction is monitored through a process of measurement leading to continuous improvement of the product.

Within the health service organization, an understanding must be gained of the QMS in its own context in order to lead to patient satisfaction. The IWA 1 presents a diagrammatic view of a QMS model for health service organizations. This is shown in Figure 3.3.

![Model for Health Service Organizations with Patient/Client](image_url)

*Figure 3.3 - Model for Health Service Organizations with Patient/Client as “Customer” (IWA 1, 2005)*
A process-based model is depicted that shows how the “interested party” – the patient/client – requesting health service is the input to the next process of diagnosis, and so on. It is clear that the primary beneficiary of the health service is the patient. There is on-going monitoring of the patient/client satisfaction levels to ensure the organization is meeting the required health service expectations.

### 3.3.4 QMS Certification

As stated previously, the IWA 1 international standard consists of guidance and recommendations and is not intended for certification, regulatory or contractual use, nor as a guide to the implementation of ISO 9001 (IWA 1, 2005). Reid (2001) affirms this by proclaiming that the IWA 1 guidelines are voluntary and are not intended for certification or accreditation. The IWA 1 does not require certification because it is only a guidance document, which means that its implementation is in addition to the implementation of the ISO 9001 and ISO 9004 standards (Yoo, et al., 2006). Organizations that pursue certifications will be certified against the requirements of the ISO 9001.

This concludes the discussion on the IWA 1 standard. In section 3.4 the ISO 27001 ISMS standard is discussed using the same sections as for the IWA 1, viz. the purpose, benefits, process approach and certification issues. It was established in section 3.2 that management system standards include generic features. Some of these characteristics will be apparent when discussing the ISMS standard in the following section.

### 3.4 ISO 27001

According to Humphreys (2008), the ISO 27001 standard is used worldwide by organisations, both commercial and government, as the foundation for the management of the organisational policy and the implementation of information security. It provides a specification for an ISMS. The ISO 27001 specifies the necessity for an organization to introduce adequate controls, personalized to its
needs (Dion, 2008). Information security management ensures the security of information through the proactive management of information security risks, threats and vulnerabilities. Consequently, information security management should be built into the daily business operations rather than being treated as an optional extra (Kritzinger & Smith, 2008). An ISMS extends the concept of ISM by espousing an overarching management process to ensure that the information security controls continue to meet the organization's needs. Section 3.4.1 discusses the purpose of an ISMS.

### 3.4.1 Purpose of an ISMS

According to Simtex OC (2009), an ISMS is a management system based on the approach of the risks to which a company is exposed and its purpose is to establish, implement, operate, monitor, revise, maintain and improve the information security. An ISMS is a management system, not a technical information security standard, consequently, many organizations have introduced an ISMS to improve information security management (Broderick S. J., 2006). The ISMS is implemented in an organisation to ensure that there is a consistent, repeatable and auditable means of addressing information security issues or risks (Ashenden, 2008). Information security and the management thereof, should be an integral part of the organisational operating and business culture (Mirela & Maria, 2009).

ISO 27001 is intended to serve as a reference point for identifying a range of controls needed to align information systems with business objectives, and it addresses organizational, administrative, and procedural aspects of security (McGee, Bastry, Chandrashekhar, Vasireddy, & Flynn, 2007). The management system includes the organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources (Howie, 2006). The identification of risks is a crucial part of the planning of every ISMS (Cavalli, Mattasoglioa, & Pincirol, 2004). Assessing the risks involves identifying the assets, the threats and their vulnerabilities. The ISMS should ensure that adequate and proportionate security controls are selected to protect information assets against the identified threats and vulnerabilities and give confidence to third parties (Ashenden,
Inevitably this will be beneficial for the implementing organization and all interested parties.

### 3.4.2 Benefits of Implementing an ISMS

The benefits of adopting a common framework for security management are numerous (Broderick J. S., 2006). Selected benefits include (UQAZ, 2009):

- Provides satisfaction and confidence that customers’ information security requirements are being met;
- Allows for focused staff responsibilities;
- Improves the effectiveness of the information security environment;
- Allows for market differentiation due to a positive influence on company prestige and image, as well as a possible effect on the asset or share value of the company;
- Reduces liability and risk due to implemented or enforced policies and procedures, which demonstrate due diligence; and
- Provides competitive advantage and reduction in costs connected with the improvement of process efficiency and the management of security costs.

An ISMS brings structure to the information security program with clear direction, authorization and roles that are understood (Carlson, 2008). By using an ISMS an organization can be sure that they are measuring and managing their information security processes in a structured manner and that they can control and hone their system to meet their business needs (Pattinson, 2007).

An ISMS may serve as a market differentiator, and serve to enhance perception and image (Ashenden, 2008). When an organisation implements an information security management system and acquires certification to ISO 27001 by an accredited third party certification body, it gives the organisation an independent and unbiased view of the appropriateness and effectiveness of the implemented ISMS and demonstrates the organisation’s capability to the outside world (LLoyds register
quality assurance, 2006). It serves as a public statement of its ability to manage information security properly (Saint-Germain, 2003).

Similar to the ISO 9001’s QMS, the ISO 27001 adopts a process approach to establish, implement, operate, monitor, review, maintain and improve an information security management system.

### 3.4.3 The Process Approach

The ISO 27001 adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure all ISMS processes (ISO 27001, 2005). The PDCA approach or cycle ensures continuous improvement because the management system is regularly monitored and reviewed to verify that the controls to manage the risks are still efficient and if they are not, then improved controls are implemented (Humphreys, 2008). It is a part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (Simtex Oc, 2009). The Plan, Do, Check, Act cycle serves as a guide when planning the action of what needs to be done and how best to go about it. The needed controls are established, progress is monitored and the system is improved by taking preventive and corrective actions and identifying areas for improvement (Pattinson, 2007).

In the Plan phase, the policies, objectives, targets and processes relevant to controlling risk are established (Cavalli, Mattasoglio, & 2004). McGee et. al (2007) suggest that for the Plan phase, to establish the ISMS, it is necessary to understand the business objectives and establish the high-level management policy covering security considerations, identify the risks, and select control objectives and controls for the treatment of risks.

The Do phase implements identified controls and procedures from the Plan phase. Allan (2008) describes the Do phase as to implement and operate the ISMS policy, controls, processes, and procedures. During this phase, the requirements of the policy are implemented, for example, the implementation of password procedures
(Eloff & Eloff, 2005).

An evaluation of the controls implemented in the Do phase is carried out in the Check phase of the PDCA cycle and metrics used to measure identified problems and measure results (Visitask, 2009). The Check phase ensures that periodic reviews are conducted to verify the effectiveness of the ISMS, to review the levels of acceptable and residual risk and periodically conduct internal ISMS audits (Saint-Germain, 2005). Corrective actions may be needed to improve the solution where necessary, in the Act phase of the PDCA cycle (Mind Tools, 2009).

The PDCA cycle is illustrated in the Figure 3.4. It can be seen that the ISMS takes as input the information security requirements of interested parties or stakeholders, and through the necessary actions and processes produces information security outcomes that meet those requirements and expectations (ISO 27001, 2005).

![Figure 3.4 - PDCA model applied to ISMS processes](image)

The process approach promoted by ISO 9001, which systematically identifies processes that are part of the quality system and identifies the interactions between
them, is actually based on the Plan-Do-Check-Act cycle (PDCA) which can be applied to all processes (ISO 9001, 2008).

Once an organization has developed, implemented, and documented the ISMS, an accredited certification body can perform a third-party audit (Saint-Germain, 2003).

### 3.4.4 ISMS Certification

ISO certification has become an important issue for organizations. Many organizations attempt to obtain ISO 27001 certification (Karabacak & Sogukpinar, 2006) because it provides guidelines for implementing a constructive risk management process, setting up policies, and ensuring a secure infrastructure is in place (Overill, 2008). By adopting a reliable guideline, organizations demonstrate their commitment to secure business practices (Siponen & Willison, 2009).

It is necessary to use an independent and accredited third party known as a certifying body to ensure that meaningful and repeatable assessments are done against the standard (Pattinson, 2007). Security auditors assess the organisational ISMS scope and whether it covers all aspects of operation (Saint-Germain, 2003). An accreditation body is responsible to ensure that the certification bodies reach the necessary standards for consistently assessing that an ISMS implementation is meeting the ISO 27001 standard (Pattinson, 2007).

The certification of ISMS is designed to show that a structured procedure has been respected. This procedure allows the organization to establish and assure independently, through a registry, a level of confidence to interested parties, on the adoption of appropriate controls throughout the organization (Dion, 2008).

### 3.5 Conclusion

In recent years, a number of specifications for function-specific management systems have been released, specifically in the form of standards. The International
Organisation for Standardisation has developed some of these standards, for example in the areas of quality management, environmental management and information security management. The purpose of these management systems is to enable organisations to address various stakeholder requirements in a systematic manner (Asif, Fisscher & de Bruijn, 2010).

This chapter was primarily aimed at investigating management systems in general and specifically management systems for quality and security. The IWA 1 standard was investigated, together with the ISO 9004 and the ISO 9001 which it is based on, to understand the implementation of a QMS in healthcare. The purpose, benefits, process approach and QMS certification were discussed to obtain a broader understanding of how the QMS is constructed and its uses.

The ISO 27001 and the ISO 27799 standards for information security management system were discussed to obtain a clearer understanding of how the ISMS is implemented in the healthcare sector. An overview of the purpose, benefits, process approach, and ISMS certification was given.

When multiple management systems are implemented in an organisation, confusion may arise because of the different implementation criteria of the standards. This problem may be solved by integrating the management systems used in an organisation. The topic of integrated management systems is investigated in chapter 4 and an integrated management system proposed for quality and information security in healthcare.
Chapter 4
IMSQS: An Integrated Management System for Quality and Information Security in Healthcare

The aim of Chapter 4 is to present an integrated management system for quality and security (IMSQS) in healthcare. The chapter begins by exploring the concept of integrated management systems to show that multiple management systems may be integrated to form an IMS. Next, integrated management systems case studies are discussed to demonstrate the benefits that organisations derive from integrating their management systems standards. Various approaches to the integration of management systems are summarised to show methods that can be utilised when integrating management systems. The IMSQS is presented by illustrating the IMS at a high level. The common elements of the QMS and ISMS are identified. The generic processes of the IMSQS are discussed to show how an IMSQS may be implemented in the healthcare context, with special emphasis afforded to the importance of contextualisation. Finally the purpose and findings of the chapter are summarised.

4.1 Integrated Management Systems

Organisations may choose to implement multiple Management System Standards (MSSs) to improve organizational performance in quality, safety, security and a number of other aspects or functions (Bernardo, Casadesus, Karapetrovic, & Heras, 2009). The implementation of multiple MSSs may lead to confusion for organisations because of their different implementation criteria (Jørgensen, Remmen, & Mellado, 2006). The problem of organisations implementing different standalone management systems may be solved by implementing an IMS.

An integrated management system (IMS) describes several previously separate management systems grouped together to form a single system (Tang & Hammond, 1997). It is a single integrated structure used by an organization to manage its processes or activities. These transform the inputs of resources into a product or
service which meet the organizational objectives and satisfy the quality, health, safety, environmental, security, ethical or any other identified requirement of the stakeholder (Wilkinson & Dale, 1999).

The aim of an IMS is to streamline processes and avoid duplication (Griffith, 2000). An IMS, besides providing a mechanism to cope with all of the different management system requirements, provides focus on business needs and provides added value to businesses (Jackson, 1997). An IMS supports an organisation by taking a holistic approach to management systems (Pojasek, 2006). In addition to providing internal improvements, an integrated approach to management systems will be less costly than implementing numerous systems for different requirements (Wilkinson & Dale, 1999).

Due to the confusion that separate management systems pose when implemented in a single organisation, various authors have proposed an IMS as a solution to the problem. Authors such as Jørgensen (2008), Karapetrovic and Casadesu (2009), and the IBM organisation (Standards Malaysia, 2009) report on case studies of companies that implemented an IMS. A few of these case studies are discussed to illustrate the benefits that an IMS can bring to an organisation.

4.2 IMS Case Studies

4.2.1 The Dansk Standard Approach for an IMS

Jørgensen (2008) discusses the implementation of an IMS by the Danfoss group in Denmark. The company develops and produces mechanical and electronic products and controls, e.g. refrigeration and air conditioning, heating and water and motion controls. They chose to integrate the quality, environment and health and safety management systems, due to the number of common elements in the systems. The focus of the IMS is placed on the system and the processes, not on specific areas such as quality, environment, occupational health and safety, and social accountability.
The main reason for integrating the management systems, as stated by the organisation, is to meet customer expectations; to streamline and simplify the management systems to avoid conflicts between the systems, and to improve awareness and reduce confusion among its employees. The company based their integration approach on the IMS standard developed by the Danish organization for standardisation, viz. Dansk Standard.

4.2.2 Filtros Anoia, S.A. Model of an IMS

The second case study is Filtros Anoia, S.A. organisation, a Spanish manufacturer of paper filters for industrial, analytical, laboratory and special uses. They introduced management systems to re-establish their major investments in technology and improvements in quality management. The company initially implemented the ISO 9001 quality management system, and later integrated the ISO 14001 into the quality management system. From the organisation’s point of view, integrating the management systems proved to be a rational decision because the individual standards share some common requirements (Karapetrovic & Casadesu, 2009). Their rationale to implementing the integrated management system is to assist in improving the organisation and its customer relations.

4.2.3 IBM Case Study

Organisations such as IBM, one of the leading information technology companies, have implemented IMS to reduce the complexity and cost of managing multiple management systems in one organisation. IBM initially implemented the ISO 9001 and then the ISO 14001 management standard. Later, they integrated their QMS with the environmental management system into their business management system. They utilised a process approach to address management system standards integration. Their decision to integrate the management system standards was as a result of the number of management systems that existed as well as others that were envisaged to be implemented. The initiative to integrate the management systems minimised the difficulty in the maintenance of managing separate management
system standard certifications, and simplified how the management system standard requirements were fulfilled (Standards Malaysia, 2009).

A number of benefits arise from integrating management systems as is evident in the discussion of the case studies. These benefits can be summarised as follows. IMSs assist to:

- Meet customer expectations;
- Streamline and simplify the management systems;
- Avoid conflicts between the management systems;
- Improve awareness and reduce confusion among employees;
- Assist in improving the organisation and its customer relations;
- Minimise difficulty in the maintenance of managing separate management system standard certifications; and
- Simplify how the management system standard requirements are to be fulfilled.

Karapetrovic (2003) emphasizes that integration is not only about the benefits that can be attained, but about the inevitable increase in management system standards which can only be “survived” by following an integration approach. Various approaches to creating integrated management systems are evident in literature. These include, but are not limited to the compatibility approach (Jørgensen, Remmen, & Mellado, 2006), the risk analysis based approach (Labodova, 2004), the two step integration approach (Jonker & Karapetrovic, 2004) and the Dansk standards approach (Jørgensen, Remmen, & Mellado, 2006). These approaches are subsequently discussed to show the ways in which management systems can be integrated.

4.3 Approaches to the Integration of Management Systems

4.3.1 Compatibility Approach

The compatibility approach, as suggested by the name, focuses on similarities
between management system standards to achieve integration. According to Jørgensen, Remmen and Mellado (2006), the compatibility approach achieves integration at three levels of increasing difficulty. This is explained as follows by the authors:

- At the first level, termed the **corresponding level**, there is increased compatibility with cross-references between parallel systems.
- The second level, the **coordinated and coherent level**, achieves integration through generic processes with the focus on tasks in the management cycle, viz. the plan, do, check, act cycle.
- At the most advanced (third) level, termed **strategic and inherent**, an organisational culture of learning, continuous improvements of performance and stakeholder involvement related to internal and external challenges, are achieved.

At the **corresponding level**, the compatibility of cross references and internal coordination reduce the add-on problems of different parallel management systems. They reduce both the duplication of paperwork and confusion between demands of different standards (Jørgensen, 2008). Jørgensen, Remmen and Mellado (2006) suggest that from an administrative point of view, the benefits listed below, could be obtained from implementing this level of integration:

- Minimisation of documentation and records;
- Less bureaucracy and reduction of paperwork;
- Cost savings by optimisation of time and resources assigned to the system; and
- Simplification of internal and external audits.

The **coordinated and coherent level** goes one step further (Wilkinson & Dale, 1999). It suggests that an IMS has to be based on the generic aspects of management: policy, planning, implementation, corrective action and management review, i.e. the plan do check act (PDCA-cycle) previously discussed.
The benefits of the coordinated and coherent level are (Jørgensen, 2008):

- More focus on interrelations - synergies as well as trade-offs - between quality, environment, occupational health and safety, and social accountability;
- Objectives and targets are set up, coordinated and balanced; and
- Organisation and responsibilities are defined in one place.

Jørgensen, Remmen and Mellado (2006) state that the third level, the **strategic and inherent level**, is seen as the most difficult (and unlikely) to achieve and is also difficult to describe in detail. The authors indicate that to achieve this level, management commitment, employee motivation and participation, changes in routines and traditions, etc. will constitute challenges. The focus of the integrated management system has to be customer-based quality, product-oriented environmental management and inclusive of corporate social responsibility to reach this level (Jørgensen, 2008).

### 4.3.2 Risk Analysis Based Approach

Labodova (2004) proposes a risk based approach that is supported by a risk analysis, as a strategy to integrate multiple management systems. It develops objectives and targets in the IMS where the risk assessment is based on financial terms. Risk can be used as an integrating factor, for example, risk to the environment, risk to the life and health of employees and surrounding population, and the risk of economic losses.

Labodova (2004) further states that by using this approach, the implementation of a management system consists of two parts: First, the initial review which assesses the actual situation regarding risks and the actual technology and organisation present. Secondly, the introduction of a management scheme following the PDCA approach.
4.3.3 Two Step Integration Approach

Karapetrovic and Jonker (2004) discuss a two-step integration strategy based on the implementation of a QMS and environment management system (EMS). This approach uses elements of the compatibility approach, but attempts to extend the IMS to include management systems other than a QMS and an EMS.

In the first step there are three options that can be used, according to the authors. The QMS and EMS can be established in one of the following ways:

- The QMS first and the EMS second;
- The EMS first and the QMS second; or
- The QMS and the EMS simultaneously.

In the second step, (Karapetrovic & Casadesu, 2009) address the integration of management systems other than QMS and EMS. They subsequently discuss an integration strategy for companies who have more than the QMS and EMS implemented. Based on the first option mentioned above, namely establishing the QMS first and the EMS second, the sequence could be:

1. Integrate the QMS and other MSs that are based on the process approach;
2. Integrate the EMS and other MSs that are based on the PDCA model; and
3. Link, align and integrate these function-specific management systems.

4.3.4 The Dansk Standard Approach

As mentioned in section 4.2.1, the Danish organization for standardisation, developed a standard for IMSs. The Dansk model defines a three step approach to implementing an IMS. A graphical representation of the Dansk IMS model is shown in Figure 4.1. The model includes a strategic layer because the Dansk standardisation organization felt that organisations in general do not place enough emphasis on overall corporate governance. Therefore, special attention was drawn to this issue by illustrating it as a separate level at the top of the diagram. The
second level is the common system and process elements which form a generic platform for IMS. The third level (at the bottom) represents the different fields of management, which an organisation can choose to integrate into an IMS, such as quality, environment, energy, occupational health and safety, food safety, risk, social responsibility, and economy.

<table>
<thead>
<tr>
<th>Excellent management of management systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common elements in an integrated management system</td>
</tr>
<tr>
<td>QUALITY</td>
</tr>
</tbody>
</table>

Figure 4.1- Dansk Standard’s model for an Integrated Management System (Jørgensen, Remmen, & Mellado, 2006)

A selection of approaches to implement an IMS were described previously in sections 4.4.1 through 4.4.4. An organisation wanting to implement an IMS may choose an approach that is suitable for their business needs.

4.3.5 Conclusion: Approaches to IMS

In general, the available literature about IMS is based on the integration of the ISO 9001 (the quality management system), ISO 14001 (the environmental management system) and the OHSAS 18001 (the occupational health and safety management system). Most of the published work concentrates on the integration of quality, environmental and occupational health and safety (Karapetrovic, 2006).

Healthcare organisations have been challenged to improve upon current levels of efficiency, and competitive advantage in relation to cost effectiveness and quality of care and patient confidence (Blobel, Nordberg, Davis, & Pharow, 2006). The reasons
behind this movement are the following (Wardhani, Utarini, van Dijk, Post, & Groothoff, 2009):

- The increasing complexity of healthcare organisations and the system;
- Intensity of competition in the healthcare industry;
- The on-going process of specialization of healthcare providers;
- Strengthening of the client position; and
- Increasing awareness on patient safety and information security.

Standards such as the IWA 1 and ISO 27001, which were discussed in Chapter 3 may be utilised to employ processes for continuous improvement to improve the effectiveness, security and quality of healthcare delivery. However, the implementation and use of multiple standards as mentioned in section 4.1, may be confusing and tap the resources of the organisation through unnecessary repetition in the various departments where the responsibility for each management system resides. In section 4.4 an IMS for quality and security in the healthcare context is proposed based on the integration of the relevant management system standards that were considered in this research.

4.4 IMSQS: Integrated Management System for Quality and Security

4.4.1 IMSQS: High Level Overview

A graphical illustration of the proposed integrated management system for quality and security is shown in Figure 4.2. It is adapted from the Dansk model illustrated in Figure 4.1 and the compatibility approach discussed in section 4.3.1.

The IMSQS suggests that for an IMS for quality and security to be achieved, the quality and information security management systems standards, represented at the lowest layer of the figure, should be integrated based on both the common elements of the standards and the generic processes. The integration approach is represented in the middle layer of Figure 4.2. The IWA 1 and ISO 27799, depicted in the bottom
layer, focus on the needs of healthcare which ensures that the IMS, at the top level, is contextualised for healthcare.

### Integrated Management System Contextualized for Healthcare

<table>
<thead>
<tr>
<th>Common Elements and Generic Processes from Quality and Information Security Management Systems</th>
</tr>
</thead>
</table>

Figure 4.2 - High level overview of the IMSQS

The IMSQS proposes special emphasis on the context of healthcare, which has not been proposed in other approaches to IMS, where the emphasis has generally not been on the context of implementation. Some examples are provided in section 4.4.4 to illustrate why a contextualized approach is considered important.

In section 4.4.2 the common elements between the QMS and ISMS are shown. The generic processes are introduced in section 4.4.3 with further discussion of the generic processes in section 4.5.

#### 4.4.2 IMSQS: Common Elements

A tabular format is used to outline the common elements between the standards considered in this research. The mapping between the ISO 9001 and the ISO 27001 as represented in the tables is provided in Annexure C of the ISO 27001 management system standard. The information shown for the ISO 9004, IWA 1 and ISO 27799 was prepared by the researcher.
For ease of reading, the comparison is reported in three tables. Table 4.1, termed the informative sections, shows the sections in the standards that explain the purpose of the standard, the management system approach, the scope of the standard, references to other standards (normative references) and terms and definitions used in the standard.

No detail is provided for the ISO 27799 standard, because the informative sections of this standard refer to information security management (ISM), based on the ISO 27002 standard (i.e. not the ISMS).

<table>
<thead>
<tr>
<th>QUALITY MANAGEMENT SYSTEM</th>
<th>INFORMATION SECURITY MANAGEMENT SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 9001</td>
<td>ISO 27001</td>
</tr>
<tr>
<td>ISO 9004</td>
<td>ISO 27799</td>
</tr>
<tr>
<td>0 Introduction</td>
<td>0 Introduction</td>
</tr>
<tr>
<td>0.1 General</td>
<td>0.1 General</td>
</tr>
<tr>
<td>0.2 Process approach</td>
<td>0.2 Process approach</td>
</tr>
<tr>
<td>0.3 Relationship with ISO 9004</td>
<td>0.3 Relationship with ISO 9001</td>
</tr>
<tr>
<td>0.4 Compatibility with other management systems</td>
<td>0.3 Compatibility with other management systems</td>
</tr>
<tr>
<td>1 Scope</td>
<td>1 Scope</td>
</tr>
<tr>
<td>1.1 General</td>
<td>1.1 General</td>
</tr>
<tr>
<td>1.2 Application</td>
<td>1.2 Application</td>
</tr>
<tr>
<td>2 Normative references</td>
<td>2 Normative references</td>
</tr>
<tr>
<td>3 Terms and definitions</td>
<td>3 Terms and definitions</td>
</tr>
<tr>
<td>3.1 Terms and definitions – Supplemental</td>
<td>3 Terms and definitions</td>
</tr>
</tbody>
</table>

Table 4.1 – Informative sections:
Common elements between the QMS and ISMS standards
Table 4.2, termed the ISMS processes, shows the sections in the standards that provide more detailed discussion of the establishment, implementation, operation, monitoring, review, maintenance and improvement of an ISMS.

<table>
<thead>
<tr>
<th>QUALITY MANAGEMENT SYSTEM</th>
<th>INFORMATION SECURITY MANAGEMENT SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 9001</td>
<td>ISO 27001</td>
</tr>
<tr>
<td>4 Quality management system</td>
<td>4 Information security management system</td>
</tr>
<tr>
<td>4.1 General requirements</td>
<td>4.1 General requirements – refers to 9001</td>
</tr>
<tr>
<td>8.2.3 Measurement and monitoring of processes</td>
<td>8.2.2 Measurement and monitoring of processes</td>
</tr>
<tr>
<td>8.2.4 Monitoring and measurement of Product</td>
<td>8.2.3 Monitoring and measurement of product</td>
</tr>
<tr>
<td>8.2.2 Measurement and monitoring of processes</td>
<td>8.2.2 Measurement and monitoring of processes</td>
</tr>
<tr>
<td>8.2.3 Monitoring and measurement of product</td>
<td>8.2.3 Monitoring and measurement of product</td>
</tr>
<tr>
<td>4.2 Establish the ISMS</td>
<td>4.2.3 Monitor and review the ISMS</td>
</tr>
<tr>
<td>4.3 Implement and operate the ISMS</td>
<td>4.2.4 Maintain and improve the ISMS</td>
</tr>
<tr>
<td>4.4 Monitor and review the ISMS</td>
<td>4.7 Act: Maintaining and improving the ISMS</td>
</tr>
<tr>
<td>4.5 Maintain and improve the ISMS</td>
<td>6.3 Establishing, operating, maintaining and improving the ISMS</td>
</tr>
<tr>
<td>4.6 Planning: establishing the ISMS</td>
<td>6.4 Planning: implementing and operating the ISMS</td>
</tr>
<tr>
<td>4.7 Checking: monitoring and reviewing the ISMS</td>
<td>6.5 Doing: implementing and operating the ISMS</td>
</tr>
<tr>
<td>6.6 Act: Maintaining and improving the ISMS</td>
<td>6.7 Act: Maintaining and improving the ISMS</td>
</tr>
</tbody>
</table>

Table 4.2 – ISMS processes:
Common elements between the QMS and ISMS standards

Table 4.3, termed the management resources, shows the sections in the standards that provide more detailed discussion of the resources or supporting elements that are required.
<table>
<thead>
<tr>
<th>QUALITY MANAGEMENT SYSTEM</th>
<th>INFORMATION SECURITY MANAGEMENT SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 9001</td>
<td>ISO 9004</td>
</tr>
<tr>
<td>4.2 Documentation requirements</td>
<td>– refers to 9001</td>
</tr>
<tr>
<td>4.2.1 General</td>
<td>4.2.4 Control of documents – Supplemental</td>
</tr>
<tr>
<td>4.2.2 Quality manual</td>
<td>4.2.4 Control of records – Supplemental</td>
</tr>
<tr>
<td>4.2.3 Control of documents</td>
<td></td>
</tr>
<tr>
<td>4.2.4 Control of records</td>
<td></td>
</tr>
<tr>
<td>ISO 9004</td>
<td>ISO 27001</td>
</tr>
<tr>
<td>– refers to 9001</td>
<td>4.3 Documentation requirements</td>
</tr>
<tr>
<td>IWA 1</td>
<td>4.3.1 General</td>
</tr>
<tr>
<td></td>
<td>4.3.2 Control of documents</td>
</tr>
<tr>
<td></td>
<td>4.3.3 Control of records</td>
</tr>
<tr>
<td>ISO 27001</td>
<td>ISO 27799</td>
</tr>
<tr>
<td></td>
<td>6.4.8 ISMS document set</td>
</tr>
</tbody>
</table>

5 Management responsibility

5.1 Management commitment
5.2 Customer focus
5.3 Quality
5.4 Planning
5.5 Responsibility, authority and communication

5 Management responsibility

5.1 General guidance
5.2 Needs and expectations of interested parties
5.3 Quality policy
5.4 Planning
5.5 Responsibility, authority and communication

5 Management responsibility

5.1 Management responsibility
5.2 Needs and expectations of interested parties
5.3 Quality policy
5.4 Planning
5.5 Responsibility, authority and communication

5 Management responsibility

5.1 Management commitment
6.2 Management commitment to implement ISO/IEC 27002

6 Resource management

6.1 Provision of resources
6.2 Human resources
6.2.2 Competence, awareness and training
6.3 Infrastructure
6.4 Work environment

6 Resource management

6.1 General guidance
6.2 People
6.2.2 Competence, awareness and training
6.3 Infrastructure
6.4 Work environment
6.5 Information (data)

6 Resource management

6.1 General guidance
6.2 People
6.2.2 Competence, awareness and training
6.3 Infrastructure
6.4 Work environment
6.5 Information (data)

6 Resource management

6.2 Resource management
6.2.1 Provision of resources
6.2.2 Training, awareness and competence
6.4.4.4 Required skills and contributions

5.2 Resource management
6.5 f) Managing resources

Table 4.3 – Management resources:
Common elements between the QMS and ISMS standards

The last table focusing on common elements is Table 4.4. The table focuses on resources required for performance improvement.
<table>
<thead>
<tr>
<th>QUALITY MANAGEMENT SYSTEM</th>
<th>INFORMATION SECURITY MANAGEMENT SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 9001</td>
<td>ISO 27001</td>
</tr>
<tr>
<td>8.2.2 Internal audit</td>
<td>6 Internal ISMS audits</td>
</tr>
<tr>
<td>8.2.1.3 Internal audit</td>
<td>6.6.2.3 Independent audits</td>
</tr>
<tr>
<td>5.6 Management review</td>
<td>5.6 Management review</td>
</tr>
<tr>
<td>5.6.1 General</td>
<td>5.6.1 General</td>
</tr>
<tr>
<td>5.6.2 Review input</td>
<td>5.6.2 Review input</td>
</tr>
<tr>
<td>5.6.3 Review output</td>
<td>5.6.3 Review output</td>
</tr>
<tr>
<td>8.5 Improvement</td>
<td>8.5 Improvement</td>
</tr>
<tr>
<td>8.5.1 Continual</td>
<td>8.5.4 Continual</td>
</tr>
<tr>
<td>improvement of the</td>
<td>improvement of the</td>
</tr>
<tr>
<td>organization</td>
<td>organization</td>
</tr>
<tr>
<td>8.5.3 Corrective actions</td>
<td>8.5.2 Corrective</td>
</tr>
<tr>
<td>actions</td>
<td>actions</td>
</tr>
<tr>
<td>8.5.3 Preventive actions</td>
<td>8.5.3 Preventive</td>
</tr>
<tr>
<td>actions</td>
<td>actions</td>
</tr>
<tr>
<td>8.2 Corrective action</td>
<td>8.3 Preventive action</td>
</tr>
<tr>
<td>8.1 ISMS improvement</td>
<td>8.1 ISMS improvement</td>
</tr>
<tr>
<td>8.1 Continual improvement</td>
<td>8.1 Continual improvement</td>
</tr>
</tbody>
</table>

Table 4.4 – Resources required for performance improvement: Common elements between the QMS and ISMS standards

Jørgensen, Remmen and Mellado (2006) state that compatibility, cross-references and internal coordination of the elements in multiple management systems are obvious first steps to an integrated management system. It can be gathered from the mapping provided in Tables 4.1 – 4.4 that it will indeed be useful to have such a cross-reference at one’s disposal when implementing multiple management systems. However, the mapping in itself does not constitute an integrated management system. The cross-references between the standards must be used to combine elements from the different management systems. However, Asif, Fisscher and de Bruijn (2010) warn that this approach may lead to a lack of integration at the strategic level which could result in the IMS as a parallel structure rather than an over-riding organisational IMS. This point relates to the compatibility approach discussed in section 4.3.1, which suggest that integration at the corresponding level, is a first step in integration. The next level, termed coordinated and
coherent, takes the integration effort further by considering generic processes, with a focus on tasks in the management cycle. The third section addressing the IMSQS therefore focuses on generic processes.

4.4.3 IMSQS: Generic Processes

Arifin, Aiyub, Awang, Jahi, & Iteng (2009) identify the common processes of management system standards as:

- Management responsibility and leadership;
- Planning and review;
- Provision of resources;
- Communication;
- Operation control;
- Monitoring and evaluation;
- Management review; and
- Continual improvement.

Other authors such as Jørgensen, Remmen, & Mellado (2006) list the following as the generic processes in management system standards:

- Top management commitment;
- Definition of a policy;
- Planning of objectives and targets;
- Procedures for training of employees;
- Communication procedures;
- Audits;
- Documentation and records control;
- Control of non-compliance;
- Corrective and preventive actions; and
- Management review.
For the purpose of this research, the generic processes recommended by these authors are mapped in Table 4.5 to view commonalities between the suggested generic processes and to compile a list of generic processes for the IMSQS.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Top management commitment</td>
<td>Management responsibility and leadership</td>
<td></td>
</tr>
<tr>
<td>Definition of a policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Planning of objectives and targets</td>
<td>Planning and review</td>
<td></td>
</tr>
<tr>
<td>Procedures for training of employees</td>
<td>Provision of resources</td>
<td>Resource management</td>
</tr>
<tr>
<td>Communication procedures</td>
<td>Communication</td>
<td>Communication</td>
</tr>
<tr>
<td>Audits</td>
<td>Monitoring and evaluation</td>
<td>Audits</td>
</tr>
<tr>
<td>Documentation and records control</td>
<td>Operation control</td>
<td>Documentation and records control</td>
</tr>
<tr>
<td>Control of non-compliance</td>
<td></td>
<td>Control of non-compliance</td>
</tr>
<tr>
<td>Corrective and preventive actions</td>
<td></td>
<td>Corrective and preventive actions</td>
</tr>
<tr>
<td>Management review</td>
<td>Management review</td>
<td>Management review</td>
</tr>
<tr>
<td>Continual improvement</td>
<td>Continual improvement</td>
<td></td>
</tr>
</tbody>
</table>

Table 4.5 – Mapping: Generic processes

From Table 4.5 it is clear that there is close convergence between the processes suggested by the authors, with mainly a difference in terminology. Unfortunately the authors do not discuss the processes which makes the interpretation of what their intended meaning was rather subjective. Nevertheless, the implementation of MSs (and IMSs) in the organisational context is very specific to the needs of the organisation. The list of generic processes for the IMSQS is therefore suggested with the view that the proposal will be modified by organisations to suite their individual needs.

Further discussion of the generic processes is provided in section 4.5, with a view to providing examples. Before this more detailed discussion is presented, a discussion follows on the importance of contextualization. In section 4.4.1, Figure 4.2, the high-level overview of the IMSQS shows that there is a proposed focus on the needs of healthcare in the establishment of the IMS for quality and information security.
4.4.4 IMSQS: The importance of contextualization

In section 3.2.1.3 the IWA 1 was discussed in its capacity of being a quality management standard developed for healthcare provider organisations. The ISO 27799 was discussed in section 3.2.2.2 as a standard which defines the requirements for information security management in healthcare. Section 6 of this standard considers the information security management system, based on the ISO 27001, but contextualized for healthcare.

Although contextualization has not been emphasised in any of the literature on integrated management systems considered during this research, an argument is presented here as to why it is important to include it in the proposed IMSQS. The main argument is linked to the reason why standards for a specific context are created, i.e. to cater for the unique needs of that context.

In terms of the IMSQS, where the integration is proposed at the level of both common elements and generic processes, matters of contextualization will apply to both these levels. In order to illustrate the importance thereof, some examples are provided from the IWA 1 and the ISO 27799, where specific guidance is provided over and above the requirements of the normative standards (i.e. the ISO 9001, ISO 9004 and the ISO 27001).

IWA 1: Quality management systems – Guidelines for process improvements in health service organizations

The two examples from the IWA 1 listed below show sub-clauses that are provided over and above the requirements listed in the ISO 9001 and ISO 9004 standards.

6.3 Infrastructure

Clause 6.3.1 Hazardous waste handling

The organization should have a documented procedure for handling, disposal and removal of any hazardous materials, for example radioactive isotopes, sharps and/or needles, blood-born pathogens, in compliance with regulatory requirements and appropriate standards, and to safeguard those who may come into contact with such hazardous waste or substance.
7.1.3 Managing processes

Clause 7.1.3.2.1 Planning of realization processes

Planning for patient/client care should include a consideration of:

— Patient/client rights,
— initial patient/client evaluation/assessment,
— the initial status of patient/client health, for example high priority, urgent care needs,
— diagnosis and treatment design,
— specialty or ancillary treatment if required,
— the compatibility of the design of care to the delivery of care,
— the "error-proofing" of the processes to minimize medical error and variances, and
— follow-up requirements to prevent recurrence and/or maintain progress.

The fact that these sub-clauses are not included in the ISO 9001 implies that a health service organisation can be certified against the ISO 9001, without complying with the afore-mentioned specific requirements from the IWA 1. Considering the importance of for example hazardous waste handling in the health sector, the researcher proposes that this provides sufficient motivation for a health service organization to include contextual requirements for healthcare when implementing an IMS.

ISO 27799: Health informatics – Information security management in health using ISO/IEC 27002 (section 6)

Due to the fact that the ISMS requirements in the ISO 27799 are covered in one section only, the researcher was able to conduct a comprehensive comparative analysis of the ISO 27001 and the ISO 27799 (section 6) to determine the ISMS requirements which are unique to the healthcare sector. These contextual requirements are summarized in Table 4.6.

<table>
<thead>
<tr>
<th>ISO 27799 Sub-section</th>
<th>Summary of Additional Directives Pertaining to the Healthcare Domain as Provided in the ISO 27799</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.3</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>A scope statement may be used in various types of organizations, but</td>
</tr>
</tbody>
</table>
## ISO 27799 Sub-section

### Summary of Additional Directives Pertaining to the Healthcare Domain as Provided in the ISO 27799

<table>
<thead>
<tr>
<th>ISO 27799 Sub-section</th>
<th>Summary of Additional Directives Pertaining to the Healthcare Domain as Provided in the ISO 27799</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>6.4.4.2</td>
<td>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.</td>
</tr>
<tr>
<td>6.4.4.4</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>a) clinical and nursing process knowledge, including care protocols and pathways;</td>
</tr>
<tr>
<td></td>
<td>b) knowledge of the formats of clinical data and the capability for the misuse of this data;</td>
</tr>
<tr>
<td></td>
<td>c) knowledge of external environment factors that could exacerbate or moderate any or all of the levels of the risk components described previously;</td>
</tr>
<tr>
<td></td>
<td>d) information on IT and medical device attributes and performance/failure characteristics;</td>
</tr>
<tr>
<td></td>
<td>e) knowledge of incident histories and actual case impact scenarios;</td>
</tr>
<tr>
<td></td>
<td>f) detailed knowledge of systems architectures;</td>
</tr>
<tr>
<td></td>
<td>g) familiarity with change management programmes that would change any or all of the risk component levels.</td>
</tr>
<tr>
<td>6.4.5.3</td>
<td>There are numerous factors to be taken into account to define criteria for the acceptance of risks. A selection from these factors includes:</td>
</tr>
<tr>
<td></td>
<td>a) Health sector, industry or organizational standards</td>
</tr>
<tr>
<td></td>
<td>b) Clinical or other priorities</td>
</tr>
</tbody>
</table>
ISO 27799 Sub-section | Summary of Additional Directives Pertaining to the Healthcare Domain as Provided in the ISO 27799
---|---
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 4.6 - Directives provided in the ISO 27799 (Section 6) but not stated in the ISO 27001

Issues specific to health service organizations that are addressed in the ISO 27799 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.

As with the IWA 1, the contextual requirements summarized in Table 4.6 can be argued to be significant in the implementation of an IMS. For example, sub-clause 6.5 emphasises the critical nature of action in the initial phases of response, where it can be assumed that a patient’s life might be at stake. The impact of a negative outcome could have ruinous consequences for a health service organization.
This concludes the discussion of the IMSQS, which is based on common elements and generic processes from the quality and information security management systems, and also emphasises the importance of contextual factors. In section 4.5 further discussion is provided of the generic processes that were identified in section 4.4.3, before the chapter is concluded in section 4.6.

4.5 IMSQS: Generic Processes

4.5.1 Introduction

Jørgensen, Remmen, & Mellado (2006) indicate that an IMS which focuses on generic processes must inter alia provide a description of responsibilities, examine synergies and trade-offs and ensure alignment of policy objectives and targets to limit the problems related to managing MMSs across multiple functional units and departments.

In section 4.4.3 the proposed generic processes for the IMSQS were listed as:

- GP1: Management responsibility and leadership;
- GP2: Resource management;
- GP3: Communication;
- GP4: Audits;
- GP5: Documentation and records control;
- GP6: Control of non-compliance;
- GP7: Corrective and preventive actions;
- GP8: Management review; and
- GP9: Continual improvement.

The generic processes are numbered GP1 – GP9 in the list above to facilitate further discussion in the subsequent sections. A selection of these generic processes are discussed, viz. GP1, GP2, GP4 and GP5, to illustrate the integrated management system for quality and information security at the coordinated and coherent level as discussed in section 4.3.1.
4.5.2 IMSQS: GP1 - Management responsibility and leadership

The development of a policy is emphasised for both the quality and information security management systems. It forms part of the management responsibility and leadership generic process. In order to illustrate an approach that could be followed in the implementation of the IMSQS, the creation of the policy is now viewed from the perspective of the QMS, the IMS and the IMSQS.

Some of the requirements of a QMS is that a policy should be developed that is relevant to the type of environment that an organisation operates in. A policy should provide a framework for establishing and reviewing quality objectives. QMS standards require that the policy be communicated and understood within the organization, and is reviewed for continued relevance.

The ISO 27001 requires that the policy is aligned to the organisational strategic risk management strategy in which the establishment and maintenance of the ISMS is outlined. The policy should consider business, legal or regulatory requirements, and contractual security obligations. It is important for the ISMS policy to be continually reviewed by management and that management is responsible for the creation of the policy.

As is clear from the afore-going two paragraphs, the requirements for policy setting for quality and information security, although similar in some respects, are unique in other respects.

The integration approach for the quality and security policy should be clear and simple. Three possible solutions, illustrated in Figure 4.3, are:

- Two separate policies (two different documents reviewed separately);
- A single document with an introduction followed by a two declarations for quality and information security; or
- An integrated policy.
It should be noted that an organisation has the option to implement some aspects of an IMS separately in accordance with their requirements. For this reason the first option is included.

Figure 4.3 – IMSQS: Integration approaches: policies

The second option allows the organisation to make a unified statement on the integrated management system strategy, emphasising the integrated approach towards the quality and information security management systems. Thereafter, the policies will be handled separately. The last option allows for one policy for both quality and information security which is fully integrated.

Of importance is to note that independent from which approach is followed, the alignment of policy objectives and targets remains important. The content of the unified, partially unified or separate policies may not be contradictory.
4.5.3 IMSQS: GP2 - Resource management

The QMS requires that an organization determine and provide the resources needed for the implementation and maintenance of the QMS and continually improve its effectiveness. This is required to enhance customer satisfaction by meeting customer requirements. For example managers are required to ensure competence of the organisational quality resources such as personnel, by ensuring that job descriptions are prepared and qualifications are identified (and updated).

An ISMS standard requires that an organization should determine and provide the resources needed to improve an ISMS. It requires that information security procedures support the business requirements. The type of resources that organisations have include people, infrastructure, work environment, information, suppliers and partners, natural resources and financial resources.

Effective resource management is vital for successful IMS implementation. The organization should determine and provide the resources needed to implement and maintain the IMS for quality and security. The resource management function should provide and maintain the infrastructure needed to achieve conformity to both quality and security requirements. Management is responsible for understanding the types of resources that are necessary for routine business operations and special projects and to ensure that those resources are available when needed for the continuous improvement of the IMS (Jackson, 1997).

In section 4.5.1 the importance of responsibilities was mentioned. In terms of the generic process of resource management, it is suggested that convergence between resource requirements (e.g. in the allocation of responsibilities) should be attained with a view to minimizing the deployment of resources in the implementation, operation, maintenance and improvement of the IMS.

Another dimension of resource management comprises ensuring that employees are appropriately trained. The organization should ensure that all personnel who are assigned responsibilities defined in the IMS are familiar with both the QMS and the ISMS requirements as applicable to the execution of their work and are competent to
do the work as directed by the organisation’s aims and objectives. This can be done by determining the necessary competencies for personnel performing work affecting the IMSQS.

On-going awareness programs can be set up at different intervals to ensure that relevant personnel are aware of the relevance and importance of information security and quality activities and how they contribute to the achievement of the success of the integrated management system for quality and security. Management is responsible for identifying training and awareness needs of employees and the timelines for on-going awareness programs.

These measures should ensure that personnel are provided with adequate education and training for the proper implementation of their tasks. Annual reviews, goal setting, and the evaluation of personnel competence and performance should be conducted based on their knowledge of quality and security requirements. A skills audit record should be kept, pertaining to the quality and security knowledge of employees, for the review process to be conducted effectively by management. The training and awareness programs may be conducted for the IMS or for multiple implemented management systems.

4.5.4 IMSQS: GP4 - Audits

The QMS standard requires that audits should be conducted at planned intervals to ensure that it conforms to the set standards. It requires for an audit programme to be planned, taking into consideration the status and importance of the processes and areas to be audited, and the results of previous audits. It is required that a document be established to define the responsibilities and requirements to conduct audits and that a record of the results is maintained. In the audit process, management is responsible for the area being audited, and should ensure that any necessary corrective actions are taken without delay to eliminate detected nonconformities and their causes.
The ISMS standard requires that an internal ISMS audit be conducted at planned intervals. This is to determine whether the control objectives, controls, processes and procedures conform to the requirements of the standard, conform to the identified information security requirements, and are effectively implemented and maintained and perform as expected. Further, the standard requires that audit programmes should be planned according to the status and importance of the processes and areas under audit and the results of previous audits. The audit criteria, scope, frequency and methods should be defined together with the selection of auditors. An important aspect of audits is that their conduct should ensure objectivity and impartiality of the audit process. This means that auditors ought not to audit their own work. Management should ensure that actions are taken, without delay, to eliminate detected nonconformities and their causes.

The audit process can be done separately for each management system although an IMS approach is followed. The alternative to conducting separate audits for quality and security is a single audit plan that is carried out for the IMS. Audits, for this integrated IMSQS, should be planned by management at regular intervals. The ISO 9001 and ISO 27001 standards that form the foundation of this IMS share the same principles for the internal audit process of an organisation.

At the conclusion of any audit it should be stored and reviewed and discussed by management. The results should be reviewed in an integrated fashion addressing both quality and security. The management review of the audit process is done so that the possibility of corrective or preventive actions can be discussed to expose any continual improvement opportunities that may arise. If the audit action was performed as a single integrated audit plan then the review may be prepared in an integrated manner, however, if different audits plans were prepared then the review should be done separately as well.

4.5.5 IMSQS: GP5 - Documentation and records control

It is a requirement, when implementing a QMS, for records to be established and documented to provide evidence of conformity to requirements and of the effective
operation of the quality management system. An organization should establish a documented procedure (quality records procedure) to define the controls needed for the identification, storage, protection, retrieval, retention and disposition of records, for all records to remain legible, readily identifiable and retrievable.

The ISO 27001 requires that the documentation of the management system should include records of management decisions to ensure that actions are traceable to management decisions and policies, and ensure that the recorded results are reproducible. Furthermore, documents required by the ISMS should be protected and properly controlled. Records should be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS. Any relevant legal or regulatory requirements (regarding documentation) should be taken into account by the ISMS. All records should remain legible, readily identifiable and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records need to be documented and implemented. Documents of external origin are required to be identified and their distribution controlled. The storage and maintenance of documents should be outlined and classified according to their categories of classification. For example, documents may be classified as either controlled or uncontrolled records.

Care should be taken when choosing the procedures for documentation as required by the IMS for quality and security because the types of documents that are required will vary. This means that both the quality and the information security needs are to be addressed. Notwithstanding the effort required to consolidate the organisational record-keeping needs, the outcome will be less confusing and less time-consuming for employees. Therefore the benefits of a consolidated approach will be reaped when the consolidated requirements have been documented, implemented and accepted by all employees.

4.6 Conclusion

The proliferation of multiple function-specific management system standards leaves companies with few choices. However, the fact that current MSSs were largely
developed to be compatible with each other, it makes more sense to establish an integrated management system (Karapetrovic, 2003). The implementation of parallel management systems is 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 (Scipioni, Arena, Villa & Saccarola, 2001).

In this chapter, the concept of integrated management systems was explored. The reported literature revealed a range of approaches that can be used to integrate management systems.

In section 4.4 an integrated management system was proposed for quality and information security in the healthcare context. The IMSQS was discussed firstly through providing a high-level overview, which identified the main principles of the IMS. The integration layer of the IMSQS was proposed to be constituted by the common elements and generic processes of the quality and information security management systems. The importance of the inclusion and consideration of the healthcare context in the IMSQS was emphasised in sub-section 4.4.4. In section 4.5, a more detailed discussion was provided of a selection of the generic processes proposed for the IMSQS. This concluded the discussion of the IMSQS. In chapter 5 the dissertation is concluded.
Chapter 5
Conclusion

Chapter 5 concludes the research presented in this dissertation. An overview of how the objectives of the research were achieved is provided. The benefits and limitations of the research are considered. Lastly, the areas suitable for future research are suggested.

5.1 Background

Health information is “regarded by many as being among the most confidential of all types of personal information” (ISO 27799, 2008). Therefore, its protection is critical to ensure the privacy of patients in the care of health service organizations. Additionally, health service organizations are increasingly required to deliver quality healthcare services. Conceivably, the adoption of health information technologies can assist these organizations to deliver a quality service; however, this again exposes the health information to threats from both within and outside the organisation.

Management system standards are commonly used to assist organisations to improve a particular function (eg quality or security) through structured organizational processes to establish, maintain and optimise a management system for the particular function. In the healthcare sector, the ISO 9001, ISO 9004 and IWA 1 standards may be used for the purpose of improving quality management through the establishment of a quality management system. Similarly, the ISO 27001 and ISO 27799 standards may be used to improve information security management through the establishment of an information security management system. Notably, in the case of both quality management and information security management, additional requirements for the healthcare sector have been captured in the form of the IWA 1 and ISO 27799 respectively. The use of these standards ensures that sound quality and information security practices can be followed and applied in an organisation. By conforming to these standards, internationally recognised best
practises can be followed to address quality and information security issues that might arise in organisations in the healthcare sector. However, literature shows that organisations find it difficult to implement multiple management system standards, each with their own unique requirements, which have to be operationalized by different departments (Wilkinson & Dale, 1999; Jackson, 1997; Jørgensen, Remmen, & Mellado, 2006). Furthermore, the problem of multiple management systems is becoming worse due to an increase in these systems for specific functions (Karapetrovic, 2003).

A possible solution to the confusion is to introduce an integrated management system that addresses the requirements of multiple management systems.

In this research, various standards relevant to the establishment of management systems for quality and security were studied. These management systems standards include those specifically prepared for quality and information security in the healthcare sector. Additionally, literature on integrated management systems was reviewed to determine a possible approach to establishing an IMS for quality and information security in healthcare.

The compatibility of standards that will be integrated is essential as a basic platform towards an IMS (Jørgensen, Remmen, & Mellado, 2006). The increasing compatibility of management system standards promotes the integration of the systems at company level (Jørgensen, 2008). In the context of the ISO management system standards, Jackson (1997) indicates that this compatibility refers to the similarities between the ISO management system standards. The ISO 9001 declares that it is compatible with other ISO management systems and enables an organization to integrate its own QMS with related management systems. Further, it states that it is possible for an organization to adapt its existing management system(s) to establish a QMS that follows its guidelines because of this compatibility (ISO 9001, 2008).

While studying the management system standards, it was revealed that the quality management and information security management standards contain commonalities that an integration approach could be based on. This realization led to
a detailed investigation of these commonalities and the final proposal of the IMSQS, the Integrated Management System for Quality and Information Security in healthcare. The IMSQS addresses the main problem of this research which states that there is no documented IMS for quality and information security in the health sector. This, in turn, addresses the primary objective of this research as outlined in chapter 1:

The main objective of this research is to propose an integrated management system for quality and information security in the healthcare sector.

5.2 Chapter Overview

5.2.1 Chapter 1 – Introduction

Chapter 1 commenced by providing background about the healthcare sector and its various facets. The importance of quality and security in the sector and its dependence on health information and health information systems was outlined. Furthermore, the need for security and privacy regarding health / patient information was highlighted. The chapter introduced management system standards for quality and security and how these standards may assist in establishing, maintaining and improving organisational management systems. This led to the realization that if an organisation wants to implement different management systems e.g. for quality management and security management, a different management system standard would be applicable for each function. This could result in confusion when implementing multiple management systems. This led to a discussion about IMS and how they may be used to counter this confusion. This led to the motivation and formulation of the problem statement, objectives and methods used to meet the objectives of the research project.

5.2.2 Chapter 2 – The Healthcare Milieu

Chapter 2 provided an in-depth look at the healthcare sector, the nature and
activities of the sector. The services offered by the sector were explained, the funding model and the impact on the patient and health outcomes. This led to the discussion about health information, focusing on its delicate nature, its importance for both clinicians and patients and the purposes that it is used for. A discussion of health information systems and how they can assist in improving the delivery of quality healthcare followed. It was recognized that information security needs to be applied stringently. Finally, it was concluded that quality and information security are both vital to support healthcare services.

5.2.3 Chapter 3 – Management Systems for Quality and Security

Chapter 3 commenced by providing an overview of management systems. Management system standards for quality and security were introduced. This led to a detailed investigation of QMS and ISMS standards and their use. After providing an overview of the ISO 9001, ISO 9004, IWA 1, ISO 27001 and ISO 27799, the purpose, benefits, process approach and aspects of certification were discussed specifically in regard of the IWA 1 and the ISO 27001 standard.

5.2.4 Chapter 4 – IMSQS: An Integrated Management System for Quality and Information Security in Healthcare

Chapter 4 was dedicated to presenting the primary output of this research. The chapter proposed an IMS for quality and security in the healthcare sector. First, the concepts of multiple management systems and integrated management systems were broadly discussed. Case studies illustrating the use of IMSs were investigated and outlined. The compatibility of management system standards was investigated as a base for creating integrated management systems. It was discovered that the management system standards investigated in this research are compatible, possess common elements and apply generic processes. A table was used to illustrate the common elements between the relevant standards. Thereafter, a list of generic processes, based on literature, was suggested to be discussed in more detail later on. The importance of providing consideration for requirements unique to
the healthcare sector, as specified in the IWA 1 and ISO 27799, was emphasised. A detailed discussion of a selection of the proposed generic processes concluded Chapter 4.

5.2.5 Chapter 5 – Conclusion

The research project is concluded in this chapter. The benefits and limitations of the research and proposed future research directions are discussed.

5.3 Revisiting the research questions and objectives of the research

Six research questions and corresponding sub-objectives were identified in Chapter 1 of this dissertation. Each research question and matching sub-objective is now considered in order to show how the question was answered and consequently the sub-objective achieved through the execution of this research.

5.3.1 Research question and sub-objective 1

| What are the information requirements of the healthcare sector? | Establish the information requirements of the healthcare sector. |

This sub-objective was addressed through an investigation into the nature and constitution of the healthcare sector in Chapter 2. The types of healthcare services and the provider funding model (i.e. public vs private sector) were explored. It was established that recordkeeping is an integral requirement in healthcare due to the importance of patient health information in providing an effective healthcare service. Literature further showed that patient health information is required by various parties, including medical practitioners, administrative bodies and other third parties. An overview of health information systems showed that the availability of health information in electronic format (i.e. through the use of health information systems), will enhance accessibility to this information, which will enable better healthcare to
patients as they move between various healthcare providers.

5.3.2 Research question and sub-objective 2

| What are the quality and information security requirements of the healthcare sector? | Determine the quality and information security requirements of the healthcare sector. |

In Chapter 2 the need for increased access to healthcare at a lower cost together with concomitant pressures such as changing roles and responsibilities in the healthcare sector were highlighted. The World Health Organisation’s accusation that the healthcare sector fails to anticipate and respond to these pressures (World Health Organisation, 2008), emphasised the need for improvement of quality healthcare services. It was shown that quality problems in healthcare lead to underuse, overuse and misuse of health services. In the achievement of sub-objective 1, it was realised that electronic availability of personal health information can enhance the quality of healthcare services. However, Chapter 2 also brought to the fore the personal nature of health information and the need to ensure that health information is adequately protected from security threats.

Chapter 2 concluded that quality and information security needs in the healthcare sector can be met through the establishment of quality and information security management systems.

5.3.3 Research question and sub-objective 3

| Which management system standards can be used to address these quality and security needs? | Investigate the management system standards that can be used to address quality and information security needs in healthcare. |

Having established the utility of quality and information security management
systems, this sub-objective addressed the basic elements of management system standards for quality and security in Chapter 3. The standards relevant to quality and information security in the healthcare sector were investigated. It was discovered that there are various standards to direct the establishment, operation, maintenance and improvement of management systems. For the purpose of this research only the ISO 9001, ISO 9004, IWA 1, ISO 27001 and ISO 27799 standards were considered. Due to the fact that the IWA 1’s sections are mapped entirely to the sections of the ISO 9004, which expands on the ISO 9001, the IWA 1 was further investigated to establish the requirements for a QMS in healthcare. The ISO 27799, however, contains only one section which links to the ISO 27001, which specifies the requirements for an ISMS. Therefore the ISO 27001 was investigated in more detail in Chapter 3.

Having achieved the sub-objective of investigating management system standards for quality and information security, Chapter 3 concluded that the implementation of multiple management system standards can become a burdensome task within an organisation where each standard may need to be implemented by different departments. This can give rise to confusion and duplication of responsibilities and tasks.

5.3.4 Research question and sub-objective 4

| What are the requirements of establishing an integrated management system? | Determine the requirements to establish an integrated management system. |

The realisation that multiple management system standards are problematic to implement concurrently, led to an investigation into the requirements of establishing an integrated management system. A number of approaches to creating IMSs were considered and the requirements of each method outlined. Based on the researcher’s ability to propose an IMS using the information at hand, the compatibility approach which focuses on similarities between management systems was selected. The approach requires compatibility between the management system
standards, which implies that the researcher’s next step of action was to ascertain the similarities between the standards relevant to this research. The compatibility approach focuses on two requirements in terms of similarity, viz. common elements and generic processes.

5.3.5 Research question and sub-objective 5

<table>
<thead>
<tr>
<th>Which similarities can be identified within the management system standards?</th>
<th>Ascertain similarities between the identified management system standards.</th>
</tr>
</thead>
</table>

This sub-objective investigated the common elements and generic processes between the relevant management system standards. A tabular depiction of the common elements between the ISO 9001, ISO 9004, IWA 1, ISO 27001 and ISO 27799 standards was provided. However, it was emphasised that an IMS approach which focuses only on common elements, may lead to lack of integration within a parallel structure mentality. It was realised that the IMS must be extended to include integration at the level of generic processes. An investigation into literature enabled the researcher to identify a list of generic processes which are applicable to both the QMS and ISMS.

5.3.6 Research question and sub-objective 6

<table>
<thead>
<tr>
<th>How can management systems for quality and information security be integrated for the healthcare context?</th>
<th>Compile an integrated management system for quality and information security in the healthcare setting.</th>
</tr>
</thead>
</table>

The achievement of sub-objectives 4 and 5, allowed the researcher to propose an integrated management system for quality and information security in healthcare. The IMSQS was discussed according to its 4 main elements, viz. a high-level overview, common elements, generic processes and the importance of
contextualisation. Although the inclusion of contextual elements have not been found in IMS approaches addressed in literature, the researcher showed through examples from the IWA 1 and ISO 27799, why it is important to include contextual elements in an IMS for quality and information security in healthcare.

Having accomplished all the sub-objectives that this research set out to achieve, it is necessary to consider the benefits and limitations of the research.

### 5.4 Benefits and Limitations of the Research

From literature it is clear that integrated management systems are not viewed as a panacea for the problem of implementing multiple management system standards. However, an integration approach is viewed as more viable than retaining separate silos of responsibility in different departments when implementing MSSs.

To reiterate the benefits of IMSs from section 4.2, organisations can expect to have less difficulty to maintain and manage separate management system standards; the fulfilment of requirements will be simplified and streamlined with a reduction in conflicts between the management systems; there will be improved awareness and less confusion amongst employees; and as expected the organisational processes will be improved for the particular function (e.g. quality and security) with a resultant improvement in customer relations and meeting customer expectations.

The benefits of IMSs are therefore clear. However, literature also provides evidence of disadvantages of using an IMS, which should be considered. These are (Jorgensen, Remen & Mellado, 2006; Wilkinson & Dale, 1999; Khalil & Mahmood, 2006):

- An integration approach may lead to a ranking system for management system standards for the different functions, e.g. more attention may be paid to quality than to information security issues;
- The integration of management systems may lead to a reduction in the flexibility of the system. This may be the result of information interfaces being
tied together;

- The different disciplines (e.g. quality and security) are subject to integration differences on issues like objectives and requirements; and
- At times, the unwillingness of people to give up their culture and the control of their own discipline may influence the success of implementing an IMS.

It is acknowledged that the benefits and disadvantages of an IMS that have been discussed are not all-encompassing. However, the aim is to show that while an integrated approach is preferred, the use of IMSs do have disadvantages that should be considered.

In this research the problem statement was formulated as the lack of a documented integrated management system for quality and information security in healthcare. The main benefit of the research is therefore the documentation of a proposed approach for an IMS for quality and information security in healthcare. This output in itself has limitations, which are subsequently discussed.

The IMSQS is a theoretical solution to the problem, with no real world practical implementation. While this is understandable due to the impracticability of extending the scope of the research to include a case study, it nevertheless constitutes a limitation.

The common elements of the various management system standards were included in the formulation of the IMSQS. However, no consideration was afforded to the non-common elements. While it is evident that the non-common elements will be handled as separate (non-integrated) elements in the IMS, more detailed consideration should be afforded to this.

The IMSQS emphasises the importance of including contextualisation in the approach. The relevant analysis to highlight the contextual elements could be done comprehensively for the ISO 27799 due to its limited coverage in one section of the standard. However, the scope of the research precluded a detailed analysis of the IWA 1 to discover the additional contextual elements for a quality management
system in healthcare. Following from the limitations of the research, some suggestions are provided for future research.

5.5 Future Research

Four main limitations of this research were identified in section 5.4. These limitations are subsequently discussed in the form of suggestions for future research, based on the output of this research.

A valuable follow-up to this research will be a case study to implement an IMS for quality and security in the healthcare setting using the proposed IMSQS as a directive. The purpose of such a study may be purely to improve the level of detail included in the IMSQS as well as incorporate changes to improve the proposal. However, it would also be beneficial to gain inputs from managers in the healthcare organisational setting on both the proposed IMSQS and its implementation. This will be a logical outflow of conducting a case study as proposed above.

A second proposal for future research addresses the integration approach which depends on the use of common elements between the management system standards. In particular, the identification and handling of non-common elements between management system standards, as pertaining to the IMSQS, will be beneficial.

Lastly, the IMSQS did not address the “how” of including contextual elements in an IMS for quality and security. The research showed that the IWA 1 and ISO 27799 include requirements over and above those provided in the ISO 9001 and ISO 27001, which are unique to the healthcare setting. Examples were provided to show why it is important to include these requirements in an IMSQS for healthcare. However, not all of the unique requirements were identified and the utilisation of the unique requirements was included conceptually in the IMSQS, not illustrating how healthcare organisations should apply these in their context.
5.6 Conclusion

This research has made a contribution to the body of knowledge on integrated management systems, specifically for quality management and information security management in healthcare, through the proposal of the IMSQS. The approach was based on a compatibility approach, meaning that similarities between the management system standards were used to propose an integration approach. Whereas there is more than one approach that can be selected to implement an IMS, this dissertation presented a documented proposal, based on the compatibility approach, that can be used to implement an IMS for quality and information security in healthcare, thereby achieving the main objective of the research.

The dissertation was started with the following quote from Karapetrovic (2003), who in 2003 made this bold statement about the future of multiple management system standards and integrated management systems. It is considered appropriate to conclude the dissertation with the same excerpt, to ensure that the reader gains the intended meaning of Karapetrovic, having read this dissertation.

Welcome to the new reality of quality, the world of integrated management systems. Unfortunately for you, this world is real. This is the world where you have to address the needs of not just the customer, but virtually everybody who has a direct or indirect contact with your company. This is the world of mushrooming management system standards (MSS), where for each such stakeholder there is at least one MSS covering the minimum requirements for assuring a good relationship with that stakeholder. This is the world where the only way to survive the onslaught of MSS birds is not to run away from them or deal with them one by one, but to tame them. In other words, integrate.


Øvretveit, J. (2003, November). What are the best strategies for ensuring quality in hospitals?


Conference Paper Stemming from this Research

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


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 & Hamner, 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 commissioner, 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)

a. 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.

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

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.

b. 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.

c. 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.

<table>
<thead>
<tr>
<th>ISO 27799 Sub-section</th>
<th>Summary of Additional Directives Pertaining to the Healthcare Domain as Provided in the ISO 27799</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.3</td>
<td>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.</td>
</tr>
<tr>
<td>6.4.4.2</td>
<td>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.</td>
</tr>
</tbody>
</table>
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;
- 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.

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

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.

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.

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

<table>
<thead>
<tr>
<th>ISO 27799 Sub-section</th>
<th>Summary of Additional Directives Pertaining to the Healthcare Domain as Provided in the ISO 27799</th>
</tr>
</thead>
</table>
| 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;  
|                       | 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. |
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.

d. 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 (IMSSs) (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


