DOKUZ EYLUL UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF BUSINESS ADMINISTRATION
BUSINESS ADMINISTRATION DOCTORAL PROGRAM
DOCTORAL THESIS
Doctor of Philosophy (PhD)

AN ANALYSIS OF THE RELATIONSHIPS AMONG INFORMATION SECURITY MANAGEMENT SYSTEMS, PATIENT SAFETY, AND QUALITY

Turan Tolgay KIZILELMA

Supervisor
Prof. Dr. Özkan TÜTÜNCÜ

İZMİR-2014

DOCTORAL THESIS
APPROVAL PAGE

University	: Dokuz Eylul University
Graduate School	: Graduate School of Social Sciences
Name and Surname	: TURAN TOLGAY KIZILELMA
Title of the Thesis	: An Analysis of the Relationship Among Information Security Management Systems, Patient Safety, and Quality
Defence Date	: 23/09/2013
Supervisor	: Prof.Dr.Özkan TÜTÜNCÜ

EXAMINING COMMITTE MEMBERS

Title,Name and Surname	University	Signature
Prof.Dr.Özkan TÜTÜNCÜ	DOKUZ EYLUL UNIVERSITY	.....
Prof.Dr.Ömür Nezcan ÖZMEN	DOKUZ EYLUL UNIVERSITY	.....
Assoc Prof.Dr.Sabri ERDEM	DOKUZ EYLUL UNIVERSITY	.....
Prof.Dr.Ali Necati GÖKMEN	DOKUZ EYLUL UNIVERSITY	.....
Assoc Prof.Dr.Selçuk B.HAŞILIOĞLU	PAMUKKALE UNIVERSITY	.....

Unanimity (✓)
Majority of votes ( )

The thesis titled as "**An Analysis of the Relationship Among Information Security Management Systems, Patient Safety, and Quality**" prepared and presented by TURAN TOLGAY KIZILELMA is accepted and approved.

Prof.Dr. Utku UTKULU
Director

DECLARATION

I hereby declare that this doctoral thesis titled as “An Analysis of the Relationships among Information Security Management Systems, Patient Safety, and Quality” has been written by myself in accordance with the academic rules and ethical conduct. I also declare that all materials benefited in this thesis consist of the mentioned resources in the reference list. I verify all these with my honour.

Date

…/…/…….

Turan Tolgay KIZILELMA

ABSTRACT

Doctoral Thesis

Doctor of Philosophy (PhD)

An Analysis of the Relationships among Information Security Management Systems, Patient Safety, and Quality

Turan Tolgay KIZILELMA

Dokuz Eylül University

Graduate School of Social Sciences

Department of Business Administration

Business Administration Doctoral Program

Information is considered as a vital asset for all organizations and businesses. Therefore, confidentiality, integrity, and availability of corporate and customer information is essential for competitive edge and times mandatory due to legal compliance for certain industries such as healthcare. Standards established such as ISO 27001 are aimed towards implementation of these information security related goals. In addition to information security, patient safety, which aims to prevent harm and negative outcomes of care and quality management, which promotes patent safety and better services are also key components of a well-designed healthcare system. The main aim of this dissertation is to evaluate the influence of these three key dimensions and their components on healthcare excellence by conducting a survey in a state research and training hospital in Turkey, based on current standards and frameworks. ISO 9000 quality and 27000 information security management system standards are used as a framework. The survey has been applied to hospital employees at various positions. 389 valid responses have been obtained for analysis. An exploratory factor analysis indicated general patient safety, unit patient safety, Kaizen (continuous quality improvement), general quality requirements, information security, and healthcare excellence dimensions. Multiple regression analysis showed patient safety, quality, and information security significantly affected healthcare excellence.

Keywords: Information Security, Patient Safety, Quality Management, ISO 27001, ISO 9001, Healthcare, Excellence, Health Information Technology.

ÖZET

Doktora Tezi

Bilgi Güvenliği Yönetimi Sistemleri, Hasta Güvenliği ve Kalite arasındaki İlişkilerin Analizi

Turan Tolgay KIZILELMA

Dokuz Eylül Üniversitesi

Sosyal Bilimler Enstitüsü

İngilizce İşletme Anabilim Dalı

İngilizce İşletme Doktora Programı

Bilgi, örgütler ve iş hayatı açısından önemli bir varlıktır. Dolayısıyla ticari ve müşteri bilgilerinin güvenliği, bütünlüğü ve ulaşılabilirliği, rekabetçilik ve hatta sağlık sektörü gibi alanlarda yasalara uyum açısından gereklidir. ISO 27001 gibi standartlar bu tür bilgi güvenliği odaklı amaçlara hizmet etmektedir. Olumsuz sonuçları ve zararları önlemeye yönelik hasta güvenliği ve hasta güvenliğini ve daha iyi sağlık hizmetlerinin önemini belirten kalite yönetimi de sağlık sektörünün önemli unsurlarındandır. Bu tezin ana amacı bu üç unsurun sağlık mükemmelliği üzerine olan etkilerini Türkiyedeki bir sağlık araştırma ve uygulama hastanesinde ISO 9000 kalite ve ISO 27000 bilgi güvenliğine dayalı bir anket çalışması yaparak değerlendirmektir. Anket değişik posizyonlardaki hastane çalışanlarına uygulanmış ve 389 geçerli anket kaydı elde edilmiştir. Açıklayıcı faktör analizi sonucunda genel hasta güvenliği, birim hasta güvenliği, KAIZEN, genel kalite gereksinimleri, bilgi güvenliği ve sağlık mükemmelliği faktörleri ortaya çıkmıştır. Çoklu regresyon analizi, hasta güvenliği, kalite, ve bilgi güvenliğinin sağlık mükemmelliğini etkilediğini ortaya çıkarmıştır.

Anahtar Kelimeler: Bilgi Güvenliği, Hasta Güvenliği, Kalite Yönetimi, ISO 27001, ISO 9001, Sağlık Hizmetleri, Mükemmellik, Sağlık Bilgi Teknolojileri.

AN ANALYSIS OF THE RELATIONSHIPS AMONG INFORMATION SECURITY MANAGEMENT SYSTEMS, PATIENT SAFETY, AND QUALITY

CONTENTS

CHAPTER TWO
PATIENT SAFETY

CHAPTER THREE
QUALITY

CHAPTER FOUR
QUANTITATIVE RESEARCH

ABBREVIATIONS

AMC	Academic Medical Centers
ARPANET	Advanced Research Projects Agency Network
CDSS	Clinical Decision Support System
CFA	Confirmatory Factor Analysis
CIA	Confidentiality, Integrity, Availability
CPOE	Computerized Provider Order Entry
CQI	Continuous Quality Improvement
CSI	Computer Security Institute
DV	Dependent Variable
EMR	Electronic Medical Records
ENISA	European Network and Information Security Agency
EU	European Union
EFA	Exploratory Factor Analysis
FMAQ	Flight Management Attitudes Questionnaire
GDP	Gross Domestic Products
HCI	Human Computer Interaction
HCIS	Healthcare Information Systems
EHR	Electronic Health Record
HFACS	Human Factors Analysis and Classification System
HIPAA	Health Insurance Portability and Accountability Act
HIS	Healthcare Information Systems
HIT	Healthcare Information Technology
HRSA	Health Resources and Services Administration
ICT	Information Communication Technology
IEC	the International Electrotechnical Commission
IOM	Institute of Medicine
IS	Information System
ISA	Information Security Architecture
ISMS	Information Security Management system
ISO	The International Organization for Standardization
ISS	Information Security Systems
IT	Information Technology
IV	Independent Variable

JCAHO	Joint Commission on Accreditation of Healthcare Organizations
LAN	Local Area Networks
NPSA	National Patient Safety Agency
NPSF	National Patient Safety Foundation
NRI	Networked Readiness Index
PDCA	Plan-Do-Check-Act
PDSA	Plan-Do-Study-Act
PDLC	Product Development Life Cycle
PFIRES	Policy Framework for Interpreting Risk in E-Business Security
PHR	Personal Health Record
PWC	PricewaterhouseCoopers
QMS	Quality Management Systems
QOS	Quality of Service
SARFIT	Structural Adaptation to Regain Fit Model
SDLC	Software Development Life Cycle
SME	Subject Matter Expert
	Small and Medium-sized Enterprises
TAM	Technology Acceptance Model
USA	United States of America
VPN	Virtual Private Networks
WAN	Wide Area Networks

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

INTRODUCTION

a. Background of the study

World Health Organization (WHO) states that, "*Health is a state of complete physical, mental, and social well-being and not merely the absence of disease or infirmity"* (World Health Organization, 1948). There are objections (Callahan, 1973: 77) as well as acceptance (Breslow, 1972: 349) of this definition. There may or may not be a perfect health definition, yet health is important for individuals and the society we live in. In fact for some people good health is indispensable part of life needed for the pursuit of happiness. Genes we inherit, environment we live in, and our own behavior are among the factors that influence health (Lohr, 1990: 19).

Health and healthcare[1] go together as healthcare has important consequences on health. In some cases it helps people preserve or restore their health and in some others it might just have a marginal impact. A variety of health problems occur beyond the individual's control. It is important as everyone needs it at some point in their lives. Healthcare is important to ensure a healthy body, a healthy workplace, and a healthy community.

Contrary to health, healthcare can be and is bought and sold. Although differences exist in healthcare policies and delivery of health services of every government and country, the cost aspect of the issue remains common for all. To obtain the maximum efficiency and effectiveness of the resources used providing healthcare services to those who need it, the healthcare system needs to be efficient and effective. Institute of Medicine (IOM) proposes six specific goals for improvement to achieve this efficiency and effectiveness. IOM states that, healthcare should be: "*safe, effective, patient centered, timely, efficient, and equitable*" (Institute of Medicine, 2001: 6).

Information systems and technology (hereinafter "IT"), patient safety, and quality management have all crucial roles in addressing these properties defined by IOM. These are the three important domains that form the main pillars of the healthcare industry.

[1] Health care and healthcare are often used to mean the same thing. But they have different meanings depending on the context. Health care as two words refers to what happens to a patient. Healthcare as one word refers to a system or systems to offer, provide, and deliver health care. However in our dissertation we'll use healthcare for simplicity.

IT nowadays has become integrated to our lives and is an essential if not an indispensable part according to many. Information is the essence of IT. In today's fast paced environment information is critical in every part of our day-to-day routines. Information is embedded in political, economic, social, technological, environmental, and legal aspects of our lives. It is only as good as its consequences. The main issue for any IT is to provide the right information to the right people at the right place and time. Within an organization information is merely useful to the degree it is shared and protected. With the sharing of information, security becomes a major issue which must be addressed properly. In a healthcare setting the security of information becomes especially important due to the increasing demands to improve the quantity and quality of information associated with the healthcare services provided. Developments and demands within the healthcare industry necessitate better sharing of information across boundaries of organizations while proper confidentiality is maintained (Higgs, 1997: 61).

Despite all the advances in IT and availability of all the security related tools, information security (IS) breaches are common to most organizations. The 2011 Computer Security Institute (CSI) Computer Crime and Security survey found 41% of the respondents experienced security incidents (Richardson, 2011: 11). Among these incidents 22% were targeted attacks. According to the survey, for 20% or less of the losses, 87.1% of respondents indicated malicious insiders where 66.1% attributed to non-malicious insiders. In a recent security survey, respondents identified internal crimes (34%) causing more damage than external attacks (31%) (PricewaterhouseCoopers, 2013a: 9).

Stories of security incidents causing much harm to companies confirm these types of security surveys which indicate that companies still are experiencing significant security breaches despite the existence of IS systems supposedly protecting their sensitive data. Along with many others, Heartland Payment Systems security breach causing possibly one of the largest incidents in the industry with 100 million credit and debit cards exposed to fraud is a good example that technical approaches alone to IS issues are not sufficient to prevent incidents like these (Brenner, 2009; Worthen, 2009).

Safety is a critical attribute of healthcare systems. Though healthcare information technology (hereinafter "HIT") plays a significant role, it doesn't affect patient safety alone as much as the interactions of people and technology in a given environment (Coiera, 2003: 206). Healthcare is a complex system prone to

accidents due to the way various components are linked to each other. Human error in healthcare like in any other industry is one of the main reasons contributing to accidents. When humans and machines interact within this complex system, creating unsafe states (Ash et al., 2004: 106), patients are harmed. Patient safety has been recognized as a major issue and researched by different institutions (Institute of Medicine, 2004; Joint Commission on Accreditation of Healthcare Organizations, 2014; National Patient Safety Agency, 2014; National Patient Safety Foundation, 2014).

How a given system operates has much to do with safety. Large systems consist of various complex components that fail due to multiple faults occurring at the same time. Therefore; safety considerations should be part of the systems process design and implementation, which have to do with the overall systems quality. Quality management systems (QMS) and standards help reduce errors within a given process increasing reliability of the process outputs.

Staff perceptions and attitudes about patient safety[2] of their hospitals and on their work units can influence the care they provide. Research on unit work climate (the measurable attitudes of staff) in human services organizations, which included social workers and nurses, has shown that an organizational climate of support for staff and responsiveness to priorities such as patient safety positively affects the quality and effectiveness of services (Hemmelgarn et al., 2001).

Clinical staff with a clear understanding of high priorities set for patient safety functions towards reducing or eliminating the beliefs and attitudes that risk patient safety (Singer, Gaba, et al., 2009). A better patient safety culture or safety climate would facilitate staff attitudes in adopting safe patient care behaviors such as following policies and procedures designed to protect patients, reporting errors in care, and communicating and collaborating with the healthcare team. The effects of these behaviors can be observed and measured by indicators of quality patient care.

Objective measures of the quality and safety of patient care offer the means to evaluate care processes and identify areas for improvement. For example, performance improvement programs can include educational programs that update staff on unit quality indicators, identify progress to the goals of the unit, and plan strategies to meet those goals as indicated. Linking outcomes to the culture of safety offers opportunities to create benchmarks and the exchange of approaches

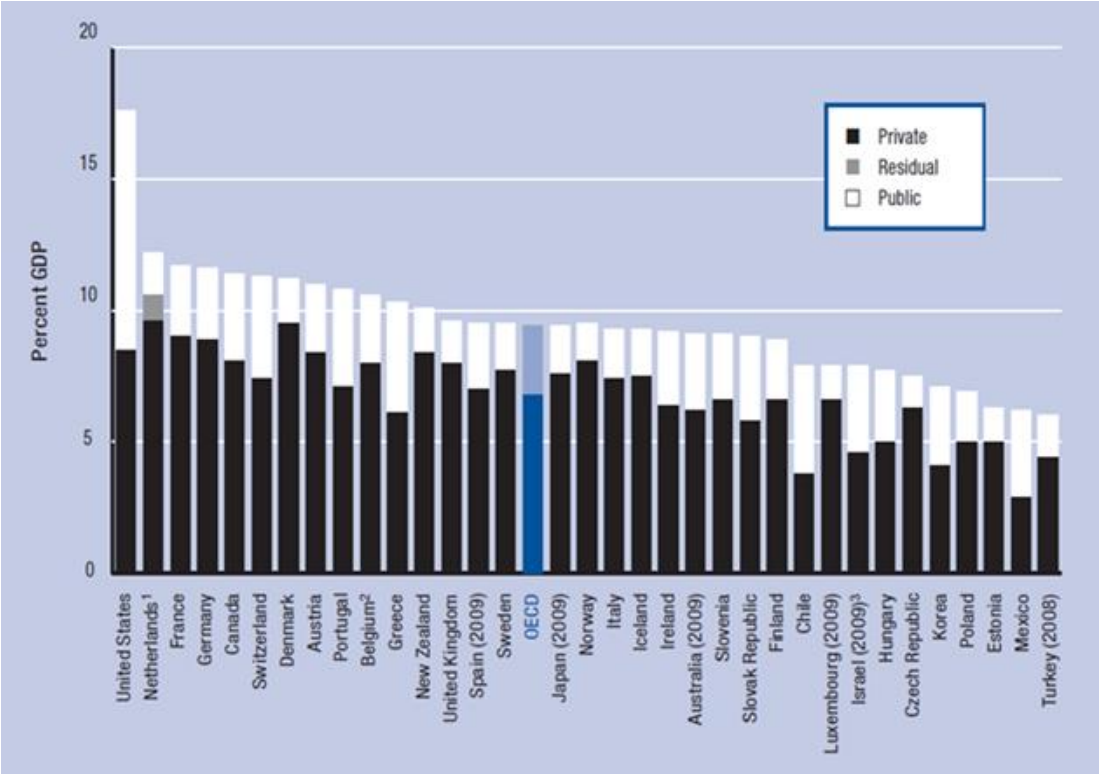
[2] Patient safety, patient safety climate, or patient safety culture might refer to the same concept depending on the circumstances.

within and across hospitals that improve patient safety (Singer, Lin, et al., 2009: 400).

Although questionnaires have been used to measure and describe hospital patient safety culture and climate, few studies have attempted to link climate to patient outcomes or other indicators of safe, quality patient care (Davenport et al., 2007; Thomas et al., 2003).

A healthcare system is responsible for a considerable proportion of public expenses. As shown in Figure 1, expenditures for healthcare related GDP health costs are also escalating in the western world (Adler-Milstein and Cohen, 2013: 83). As a result cost management has become a primary topic in healthcare. Improving the quality of healthcare and measuring the performance of care are major public and political issues challenging healthcare organizations.

Figure 1: Health Expenditure as a Share of GDP, OECD Countries



Source: OECD, 2012

In response to increasing concerns about quality and the rising need of expenditure accountability and improvement targets, a growing number of countries

and healthcare institutions have implemented quality management programs and applied quality standards. According to Hassan and Kanji (2007), Dranove et al. (1999; cited by Hassan and Kanji, 2007: 1) observed that nearly all hospitals in the United States were involved in quality improvement programs, noting that in 1997 almost all (98%) of about 2,000 hospitals had adopted the continuous quality improvement (CQI) policy. In the Netherlands, Wagner et al. (2003; cited by Hassan and Kanji, 2007: 1) found training programs in quality management for employees at 71% of the surveyed health care organizations.

b. Statement of the problem

Information security, patient safety, and quality are three critical key components of a well-designed healthcare system that aims for healthcare excellence. To date various studies have been done all addressing these factors individually within a healthcare environment. There also have been studies performed researching the relationship between safety and quality, security and safety, and security and quality, regarding healthcare excellence. Yet, despite the importance of these three critical factors within healthcare, there have been almost no study that accurately assess and examine the interrelationships among all three of these factors within a healthcare environment and the impact on healthcare excellence.

The expenditure on HIT is expected to increase globally to over $55 billion by 2017 (MarketsandMarkets, 2014). Use of resources effectively and efficiently within healthcare is important as healthcare organizations face complex issues related to effectiveness, efficiency and quality. Like in all other systems, "*in an effective and efficient healthcare system, organizational resources are used to get the best value for the money spent*" (Palmer and Torgerson, 1999: 1136). Patient safety is considered as a critical component of quality (Kohn et al., 2000), yet even in hospitals with programs heavily focused on improving patient safety, adverse events affecting hospitalized patients occur reducing the overall quality of care (Landrigan et al., 2010: 2125). IT can improve patient safety by reducing errors and harm from errors (Aspden et al., 2004; Bates et al., 1998; Kohn et al., 2000) and with better use of resources increase efficiency and quality.

In literature there is a bit of a confusion regarding the benefits or harms of HIT. Despite various studies indicating benefits of HIT, providing improvements to

patient safety and quality, certain others have not been able to provide benefits (Black et al., 2011; Garg et al., 2005; Reckmann et al., 2009).

c. Purpose of the study

The main aim of this dissertation is to attempt to predict the extent of the impact of the three key dimensions and their components of a healthcare system, i.e., information security, patient safety, and quality, on overall healthcare excellence using a quantitative approach and using survey questionnaire methods. The study aims to bring clarity to the existing issues and gaps related to the concepts being studied. Though there have been studies done on the relationship regarding safety, and quality, there has been no research done to analyze the relationships regarding all three dimensions in healthcare environment. The significance of the relationship is that it may provide an explanation of how information security, quality, and safety affect healthcare excellence, and may also confirm the positive correlations of quality and safety found in some of the very few studies done in healthcare (Tutuncu, 2008), allowing decision makers to implement proper security, safety, and quality related measures in the relevant healthcare settings.

d. Research questions

The purpose of this quantitative study is to find out the functional relationships of the three critical components including information security, patient safety, and quality within a healthcare system and their impact on healthcare excellence. The general research question (RQ) this research study addresses is:

To what extent do information security, patient safety, and quality influence healthcare excellence in the healthcare system?

The following research questions together with null hypotheses (H_0) and alternative hypotheses (H_a) expand the above general research question and serve as a guide to the study:

RQ1: To what extent is there a relationship between Information Security and Healthcare Excellence?

RQ2: To what extent is there a relationship between Patient Safety and Healthcare Excellence?

RQ3: To what extent is there a relationship between Quality and Healthcare Excellence?

e. Hypotheses

The following hypotheses were generated in order to answer and analyze the research questions of the study:

$H1_0$: There is no statistically significant relationship between information security, and healthcare excellence.

$H1_a$: There is a statistically significant relationship between information security and healthcare excellence.

$H2_0$: There is no statistically significant relationship between patient safety and healthcare excellence.

$H2_a$: There is a statistically significant relationship between patient safety and healthcare excellence.

$H21_0$: There is no statistically significant relationship between unit patient safety and healthcare excellence.

$H21_a$: There is a statistically significant relationship between unit patient safety and healthcare excellence.

$H22_0$: There is no statistically significant relationship between general patient safety and healthcare excellence.

$H22_a$: There is a statistically significant relationship between general patient safety and healthcare excellence.

$H3_0$: There is no statistically significant relationship between quality management system and healthcare excellence.

$H3_a$: There is a statistically significant relationship between quality management system and healthcare excellence.

$H31_0$: There is no statistically significant relationship between general quality requirements and healthcare excellence.

$H31_a$: There is a statistically significant relationship between general quality requirements and healthcare excellence.

$H32_0$: There is no statistically significant relationship between KAIZEN and healthcare excellence.

$H32_a$: There is a statistically significant relationship between KAIZEN and healthcare excellence.

f. Nature of the study

The focal point of this quantitative predictive study was to explore the relationships among the three key components, i.e., information security, patient safety, and quality management system and their impact on healthcare excellence in healthcare via a study conducted in Turkey in a state research hospital, as well as the potential influences they had on each other. Literature has been reviewed for security, safety, quality and similar objectives were taken into consideration for establishing the survey and techniques. The non-experimental design of the study allowed responses obtained within a relatively short time frame through a drop-off survey with a structured questionnaire distributed to the employees of a state research hospital in Denizli, Turkey. The overall methodology was effective, efficient, and relatively inexpensive.

Prior studies (Upfold and Sewry, 2005; Yeniman Yildirim et al., 2011) that used validated set of dimensions were taken as references for the design of the information security construct. For this part, the security construct, ISO/IEC 27001 Information Security Management System and its objectives and clauses were used to form the items (ISO-27001, 2005) on the questionnaire. The safety items on the questionnaire were based on the Safety Attitudes Questionnaire (SAQ) (Sexton et al., 2006) which was an improvement over the Intensive Care Unit Management Attitudes Questionnaire (Sexton et al., 2000; Thomas et al., 2003). The Flight Management Attitudes Questionnaire (FMAQ) (Helmreich et al., 1993; Helmreich and Merritt, 1998) was the main reference for the intensive care study. The quality related items were based on established quality related research (Tutuncu et al., 2009).

The questionnaire used an interval-scale for scoring (1 = Never, 2 = Rarely, 3 = Sometimes, 4 = Often, 5 = Always).

g. Significance and relevance of the study

This study contributes to the knowledge base within healthcare by exploring the interrelationships among the three key components and their impact on the healthcare excellence. There is a gap in literature regarding the impact of three important components in healthcare; information security management systems, patient safety, and quality on overall healthcare excellence. Very few studies to date

have researched the impact of HIT, especially information security, on safety and quality resulting in major gaps in our knowledge regarding how HIT affects safety and quality. The patient safety, quality, and information security are the building blocks of a well-designed healthcare aiming at providing excellent care.

In addition to the theoretical contribution there is also the practical relevance as the study can contribute to better management of healthcare organizations especially from a strategic perspective. Given the increasing reliance on HIT, the security related consequences in healthcare are extremely important along with the quality and safety.

h. Limitations and delimitations of the study

Survey participants' understanding of the IS concepts in parallel to quality and safety is one of the main constraints of the study. Due to the general nature of the hospital personnel, their involvement with IT and IS might be limited. For certain participants of the survey, the responses to the questions may not reflect their true thoughts due to concerns of being reprimanded. Though it is clearly mentioned that this is an academic research, answers to certain management related questions may not reflect the accurate thoughts of the personnel.

The unit of analysis was a delimitation of this study. The field study is conducted in one hospital. In order to get more meaningful results, the study can be applied to multiple healthcare institutions and comparative analysis can be conducted (Yin, 2009).

Another important limitation of the study was the cancelation of the ISO 27001:2005 standard on which the IS questions were based. The new ISO 27001:2013 information security standard that was published on September 25, 2013 cancels and replaces ISO/IEC 27001:2005 version. The questionnaire was distributed and results were obtained before the new version of 2013 became active. Although the control groups of the standard are very similar, a future version of the study can be conducted in different settings using the new ISO 27001:2013 version.

i. Organization of the remainder of the study

Within introduction, background of the study, problem statement, purpose of the study, research questions and hypotheses, as well as significance, limitations

are provided. The need for further research related to relationships of information security, patient safety, and quality and their impact on overall healthcare excellence is discussed by providing current state of the issues. In chapter one, a comprehensive review of the literature related to information security is presented in regards to healthcare excellence. Each topic is presented within a separate section addressing various important concepts regarding the issues. Information security is presented starting with the use of IT in healthcare, complexity of the healthcare system, the effect of Internet on our lives, security related concepts, risks, cultural and human factors, as well as some theories, standards and regulations. Patient safety is reviewed on chapter two touching the safety concept, errors, risk factors, systems and accidents, safety culture and ending with human factors in safety. Chapter three deals with quality related issues in healthcare addressing the history and important concepts in quality such as Total Quality Management (TQM), CQI, methods and frameworks, barriers, problems, and factors influencing quality improvement efforts. Chapter four provides in detail the quantitative research, methods, population, the data, and findings presented through various statistical analyses performed, and finally chapter five finishes with a discussion, conclusion and implications for practice and further research.

The first three chapters cover the main topics and their sections; Information Security Management Systems, Patient Safety, and Quality within a healthcare environment. The first chapter is a discussion of information security management systems and the related topics such as HIT, standards and frameworks, threats, human and cultural factors. The second chapter will discuss patient safety related topics which then will be followed with the third chapter with quality related topics that exist within a healthcare environment followed by quantitative methods explained in chapter four and finally a conclusion will be presented.

CHAPTER ONE
INFORMATION SECURITY MANAGEMENT SYSTEMS

1.1. INFORMATION TECHNOLOGIES

Leaders in healthcare recognize the need for what has been called "*knowledge in the world"* (Norman, 2002: 56), which is information retrievable when needed, replaces the need for detailed memory recall, and is continuously updated on the basis of new information.

Information relies on the usage of IT. Looking back at the IT history one can see the progressive evolution. Multiple turning points exist in the computer technology, which later became to be known as the IT industry. According to Press (2013), the major milestones in the IT history are:

- June 30 1945: John Von Neumann published the "f*irst Draft of a Report on the EDVAC*", the first documented discussion of the stored program concept and the blueprint for computer architecture to this day.
- May 22, 1973: Bob Metcalfe distributed a quickly drafted memo inventing Ethernet at Xerox, Palo Alto Research Center (PARC).
- March 1989: Tim Berners-Lee circulated "*Information management: A proposal*" at CERN in which he outlined a global hypertext system.

Based on these milestones IT industry's past can be categorized briefly into eras such as mainframes, PCs, Internet, and Post-PC. Though these milestones form the different eras of the IT industry's past, a quick look into the details of these milestones will reveal more.

Early 1950's were a time for large scale computers, which were placed in huge air-conditioned offices operated by a small number of technical people. No online users existed and as a result no user accounts or passwords were required to use these systems. Programs were run in batches with physical control. Both hardware and software interruptions were handled by in-house IT professionals. Small scale-computers with "*dumb terminals*" gave multiple users access to system resources via their defined user ID and passwords. Time-sharing, multi programming, and online data storage were among the main highlights of the mid-60s, which also brought the potential of computer security breaches. Due to complex programs, operating systems, and databases in a multi-user environment,

system and data protection had to be provided against unintentional or intentional errors.

In the 70s, the development of microprocessors and network technologies accelerated the deployment and usage of computers. Compared to the large scale mainframes, microprocessors enabled faster and inexpensive computers on a wider scale. The Kenbak-1 was the first personal computer and it was listed for sale for $750 in the Scientific American magazine in 1971 (Computer History Museum, 2006). Late 70s witnessed general availability of first generation personal computers such as TRS-80, Commodore, and Apple II which were designed to be used by single individuals and didn't have any IS impact. In 1969 ARPANET (Advanced Research Projects Agency Network) in US was established for national defense purposes which would later provide the foundations of the global network, which we today know as Internet. The ARPANET connected four nodes and computers were interconnected via dedicated leased lines which for the first time in IT history exposed the systems to outside world and computers from different locations were able to communicate with each other providing a variety of benefits. Information sharing was the main benefit. In addition to the physical controls to the systems, logical controls were put in place to provide authorized access to computing resources via remote terminals for individuals in other locations.

Mass production of personal computers took place in the 1980s. Along with the computers, a variety of applications such as spreadsheets and text editing applications running on PCs made them popular within the home and office environments. Data sharing was still an issue due to complexities of the technology as these computers were geared more towards individual usages and were not connected to each other in a mainstream. This issue was later resolved with the development of local area networks (LAN), which created its own set of security related issues.

In the 80s, the personal computers due to advances in technology started to become affordable for the consumers. The increased availability of applications such as spreadsheets along with inexpensive computers provided the means for consumer to purchase them and use them at homes and offices. Despite the convenience factor, sharing data among users of the systems was not easy. In order to solve this issue, LANs were developed. LANs provided users a way of accessing data hosted on a more powerful computer called server or workstation. Though convenient, issues such as security within this new platform emerged.

With the rapid advances in network technologies, 90s experienced the wide scale interconnectivity especially via the wide area networks (WAN). Introduction of World Wide Web with unrestricted access to masses opened another phase in the IT computing environment introducing the E-commerce concept. Internet made it possible and convenient to buy, sell, communicate, and share information. All these major technological changes in the 90s as well as the wireless technologies of the early 2000 brought IS issues along, as it was possible to connect to different computer systems running various business related applications using Internet and other WAN/LAN technologies from anywhere in the world.

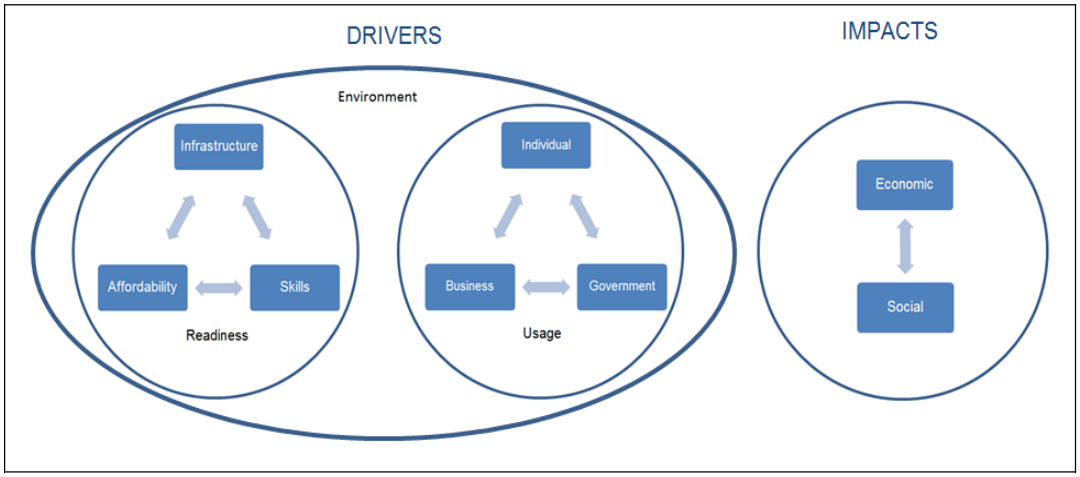
The world of IT is constantly evolving, expanding and deeply changing our lives. Nowadays IT is everywhere integrated to our daily lives in various formats. There is an ongoing transformation from the old technology to new technology. High resolution cameras, webcams, displays, wearable devices such as Samsung's watch, Google's glass and other handheld portable devices including laptops, tablets, smartphones, phablets utilizing all the latest processors and software along with the high bandwidth of broadband availability now make IT part of our daily lives more than ever.

Organizations are also being forced to utilize IT to restructure core business processes, to increase productivity and effectiveness and to gain competitive advantage due to continuing innovations and global pressures (Zwass, 1997). In many cases, IT is required to run businesses (Zviran and Haga, 1999: 162).

Advances in technology have provided access to digital world. The new platforms and concepts such as cloud computing have made the competitive gap between small and large companies even smaller, with low barriers to enter, making innovation is no longer limited to large enterprises. It is now apparent IT provides new opportunities to bring value by effectively and efficiently utilizing organizational resources (Bilbao-Osorio et al., 2013: xi). In addition to academic research, many organizations have also attempted to measure the benefits IT provides to economy and society (Bilbao-Osorio et al., 2013: xii).

The 2013 global information technology report presents a framework to utilize for assessing and measuring impact of IT for nations taking certain factors such as, infrastructure, skills, affordability, individuals, businesses, and government present in an environment as illustrated in Figure 2 (Bilbao-Osorio et al., 2013).

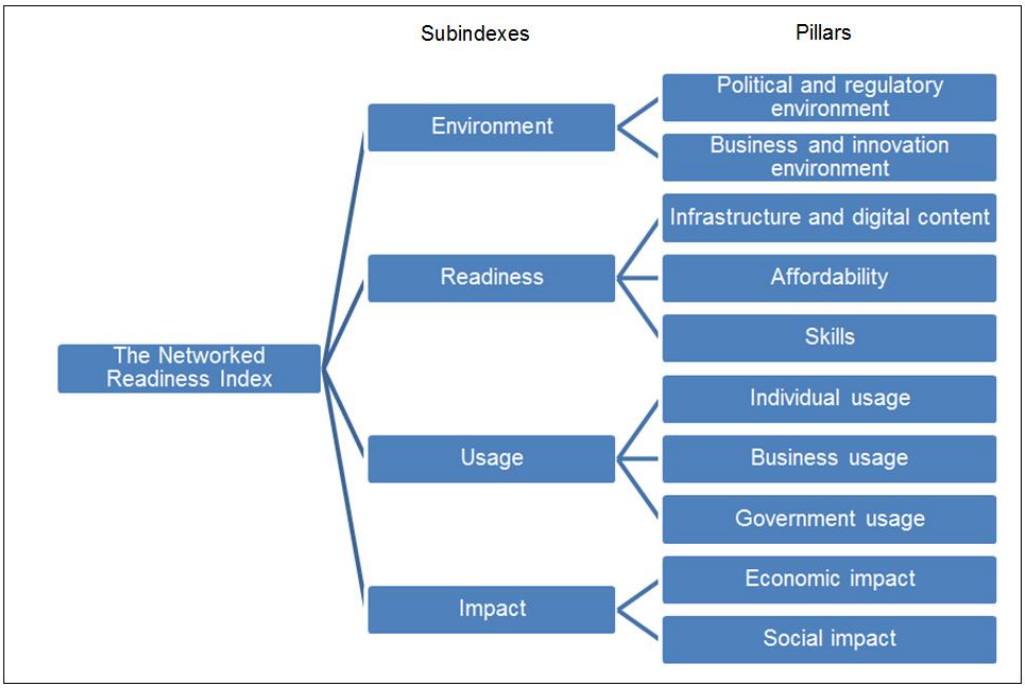
Figure 2: The Networked Readiness Index Framework



Source: Bilbao-Osorio et al., 2013: 5

The Network Readiness Index (NRI) shown in Figure 3, consists of four component indexes aimed at measuring from an IT perspective; the environment; the readiness, the usage; and, the impacts. The environment, readiness and usage all drive the impact IT provides to economy and society.

Figure 3: The Networked Readiness Index Structure



Source: Bilbao-Osorio et al., 2013: 6

1.1.1. Healthcare Information Technology

It is not easy to define the terms used for healthcare information systems and technologies as they cover a wide array of applications, solutions, and components and have contextual meanings. Health (care) IT is a common term used along with other terms like health information systems, healthcare information systems, health (care) information and communication technologies, health (care) informatics. "*The terms cover a wide range of applications from many disciplines including but not limited to; medicine, computer science, management science, statistics, biomedical engineering, among many others*" (Raghupathi, 1997: 82). Other definitions focus specifically on the technology aspect such as; "*computer hardware and software that deals with the storage, retrieval, sharing, and use of healthcare information, data, knowledge for communication and decision making"* (Jones et al., 2011: 43).

A wide range of products, including electronic health records (EHR), patient engagement tools (e.g., personal health records), and software for medical devices are also part of the HIT. HIT encompasses an array of techniques, applications, tools, processes, systems, software, hardware, operating within a larger socio-technical context including people, organizations, workflows, processes.

IT advancements play an important role in every aspect of the modern societies, impacting all industries including but not limited to finance, healthcare, defense, education, and energy. HIT expenditures are expected to increase all over the world. In North America alone, the figure is expected to be around $35 billion in 2014 due to government imposed regulations (Technology Business Research, 2013). Globally, the spending is expected to exceed $56 billion by 2017, an increase of $16 billion from the 2012 figure of 40.4 billion at a compound annual rate of 7% (MarketsandMarkets, 2014). Increased pressure on governments to reduce healthcare costs, healthcare systems integration and high return on investment expectations are among the reasons for the increased rate of growth. The fragmented nature of the HIT industry, high costs of HIT initial investments as well as maintenance costs, and the discrepancy of the regulations between developed and developing countries are also the factors slowing down a faster growth.

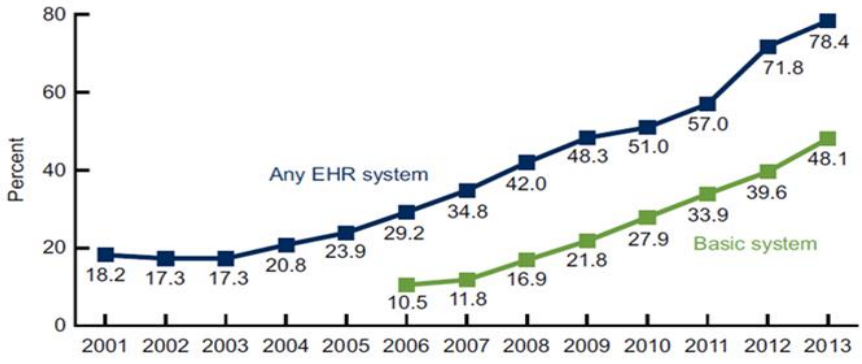
Due to this high investment in HIT, one of the main goals of the sector is to make sure safety of care is improved as well. HIT can play an important role for this improvement in healthcare by reducing errors and costs, as well as providing better

information to patients. HIT can also provide controls for adverse medical reactions, timely communication to patients, and preventive screening services.

The assumption that use of HIT provides these benefits needs further testing. In addition, efforts to achieve one benefit might bring implications to promote the other (Institute of Medicine, 2012). Advances in HIT in addition to the benefits can also create failures which may not be identified properly or noticed easily unless these advances in technology are well established. The reasons of the failures introduced by the new technologies need to be examined properly in order to analyze the impact of new technology on safety (Woods, 2010).

Use of HIT, along with advances in technology is increasing due to high demand for automation and benefits as well. Use of increased electronic medical records (EMR), computerized provider order entry systems (CPOE), and Internet also contributes to this high demand. Government imposed regulations also increase HIT usage in order to streamline and limit increases in healthcare costs (Reis, 2012). As shown in Figure 4, the significant increase in adoption of HIT in the USA within the last decade is another indicator for this high demand (Hsiao and Hing, 2012).

Figure 4: % of Office Based Physicians with EHR Systems in USA



Source: Hsiao & Hing, 2012, based on National Ambulatory Medical Care Survey and Electronic Health Records Survey

Various barriers and challenges including complexity of training needed for systems integration, cost of HIT, lack of resources, especially qualified IT labor, and concerns regarding privacy and confidentiality of health data (Cain et al., 2000) prevent the existing healthcare environment to take full advantage of the advances

in HIT. On top, lack of national and governmental standards for processing health data increases the barriers even more.

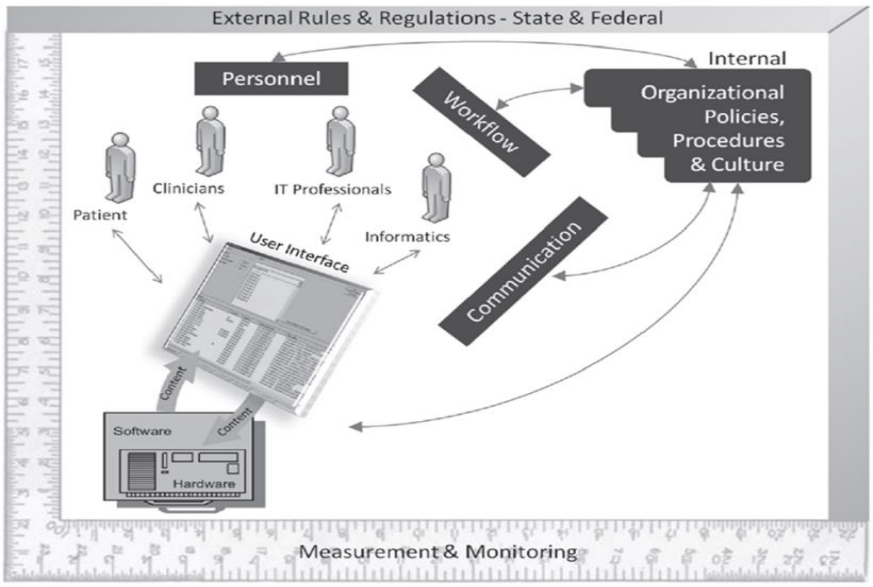
1.1.2. Healthcare Information Technology - Complexity

Healthcare is a complex environment presenting challenges and also opportunities for IT. A variety of models have been introduced to address the inherent challenges and adapt IT into complex adaptive healthcare environment to better utilize. The main models that have been developed for this purpose include Hutchins' theory of distributed cognition (Hazlehurst et al., 2003; Hutchins, 1995; Patel et al., 2008), Rogers' diffusion of innovations theory (Ash, 1997; Gosling et al., 2003; Rogers, 2010; Venkatesh et al., 2003), Reason's Swiss Cheese Model[3] (Lederman and Parkes, 2005; Reason, 2000b; Van Der Sijs et al., 2006), Venkatesh's unified theory of acceptance and use of technology (Holden and Karsh, 2010; Kijsanayotin et al., 2009; Venkatesh et al., 2003), Norman's seven-step human computer interaction (HCI) model (Malhotra et al., 2007; Norman, 2002), and 8-dimension socio-technical Model (Sittig and Singh, 2010). All of these models each cover one or more aspects of the IT implementation in healthcare. When compared, among all these models, Sittig's 8-dimension socio-technical model has taken a full range factors into consideration utilizing the limited views of the other models.

The 8-dimension socio-technical model as illustrated in Figure 5 represents the key interdependent dimensions critical to a successful HIT implementation as; *Hardware and software computing infrastructure, Clinical, Human-computer Interface, People, Workflow, Internal organizational policies, procedures, and culture, External rules regulations and pressures, System measurement and monitoring"* (Sittig and Singh, 2010: i69).

[3] See section 2.4.3

Figure 5: The 8-Dimension Socio-technical Model



Source: Sittig and Singh, 2010: i69

HIT usage in healthcare environment is among the many reasons why healthcare is considered as a complex system (Begun et al., 2003; Sittig and Singh, 2010). The interdependencies of the factors present in these complex systems need to be researched within their own context in order to understand the system itself. Otherwise a hierarchical decomposition (Rouse, 2003: 154) of a complex system for the purposes of trying to understand how it functions doesn't work for HIT due to its adaptive nature (Rouse, 2008: 18).

Regardless of the existing models, there is a common belief that HIT can be a positive transformative force when done right creating an environment of safer care with a variety of side benefits such as clinical performance increase, better decision support, improved communication among patients and caregivers, administrative cost reductions, innovations in clinical studies by following patterns based on data obtained from patients with similar diagnosis resulting new solutions to existing diseases.

On the other hand, potential to maximize the administrative economic benefits, the inadequate design, test, application, and implementation of HIT creating hazardous safety environments within an already complex setting, as well as risks to patients as a result of the heterogeneity within the HIT products and solutions are among the serious concerns for the negative consequences.

1.1.3. Healthcare Information Technology - Benefits

Despite the adoption challenges and sophistication of HIT, done properly, IT can provide an environment of healthcare that is of high quality, safer, more responsive to patient's needs, and more efficient (Adler-Milstein and Cohen, 2013).

In general, health IT is not one unique end product but is consisted of elements that are designed, applied, and used differently by various vendors, healthcare settings, and users (Häyrinen et al., 2008: 292). These differences influence healthcare processes including workflow, design, and procedure, hence the quality and safety of the care delivered.

Patient safety reliability can be increased through designing and implementing a proper HIT (Dorr et al., 2007; Niazkhani et al., 2009; Shah et al., 2006). In addition, this proper implementation, provides the platform to support research (Blumenthal and Kilo, 1998: 625), extract medical knowledge from patient care using automated clinical data (Hewitt and Simone, 2000).

The diversity of the adverse events inherent in the healthcare environment is one reason why much of the literature studying HIT and patient safety has focused on error avoidance and prevention. IT can improve patient safety by reducing errors and harm from errors (Aspden et al., 2004; Bates et al., 1998; Kohn et al., 2000). A variety of studies on electronic prescribing of medications offer strong evidence of improved patient safety via lowered frequency of medication errors, which might significantly be able to reduce avoidable adverse drug events (Kaushal et al., 2003; Shamliyan et al., 2008; Wolfstadt et al., 2008). Yet the degree to which HIT can reduce these errors varies widely among the different electronic prescription applications used (Nanji et al., 2011: 769).

HIT can improve patient safety by utilizing medical evidence with patient specific clinical data and clinical decision support systems available when needed for patient care (Berner et al., 1999; Classen, 1998; Hunt et al., 1998). In addition as part of the decision support systems, automated clinical data provides assistance to clinicians and patients with their decisions in diagnosis and evaluations regarding treatment options (Burger, 1997; Weed and Weed, 1999).

In addition to improving coordination among clinicians, and increasing accountability for performance (Blumenthal and Kilo, 1998), HIT help make quality measurements timely and accurate (Schneider et al., 1999: 1184). One of the other

major effects of HIT on quality of care is its role in increasing adherence to guideline- or protocol-based care (Wu et al., 2006: 742).

EHR, an important component of a complex HIT consists of mainly four core elements (Institute of Medicine, 2012: 38): electronic clinical documentation, electronic prescribing, results reporting and management , and clinical decision support (DesRoches et al., 2008; Jha et al., 2009; Jha et al., 2006) as well as barcoding systems and patient engagement tools. The EHR provides other uses in accounting, reporting, surveillance, and quality improvements. Table 1 summarizes the benefits and safety concerns commonly found in the literature (Institute of Medicine, 2012: 39).

Table 1: Benefits and Safety Concerns - Literature Summary

HIT Components	Potential Benefits	Safety Concerns
Computerized Provider Order Entry (CPOE): An electronic system that allows providers to record, store, retrieve, and modify orders (e.g., prescriptions, diagnostic testing, treatment, and/or radiology/imaging orders).	– Large increases in legible orders – Shorter order turnaround times – Lower relative risk of medication errors – Higher percentage of patients who attain their treatment goals	– Increases relative risk of medication errors – Increased ordering time – New opportunities for errors, such as: • fragmented displays preventing a coherent view of patients' medications • inflexible ordering formats generating wrong orders • separations in functions that facilitate double dosing • incompatible orders – Disruptions in workflow
Clinical Decision Support (CDS): Monitors and alerts clinicians of patient conditions, prescriptions, and treatment to provide evidence-based clinical suggestions to health professionals at the point of care.	– Reductions in: • relative risk of medication errors • risk of toxic drug levels • time to therapeutic stabilization • management errors of resuscitating patients in adult trauma centers • prescriptions of non-preferred medications – Can effectively monitor and alert clinicians of adverse conditions – Improve long-term treatment and increase the likelihood of achieving treatment goals	– Rate of detecting drug–drug interactions varies widely among different vendors – Increases in mortality rate – High override rate of computer generated alerts (alert fatigue
Bar-coding: Bar-coding can be used to track medications, orders, and other healthcare products. It can also be used to verify patient identification and dosage.	– Significant reductions in relative risk of medication errors associated with: • transcription • dispensing • administration errors	– Introduction of workarounds; for example, clinicians can: • scan medications and patient identification without visually checking to see if the medication, dosing, and patient identification are correct • attach patient identification bar-codes to another object instead of the patient • scan orders and medications of multiple patients at once instead of doing it each time the medication is dispensed
Patient Engagement Tools: Tools such as patient portals, smartphone applications, email, and interactive kiosks, which enable patients to participate in their healthcare treatment.	– Reduction in hospitalization rates in children – Increases in patients' knowledge of treatment and illnesses	– Reliability of data entered by: • patients, • families, • friends, or • unauthorized users

Source: Institute of Medicine 2012: 39

A research conducted in 1997, aimed at identifying the frequency of adverse drug events screened more than 90 000 hospital admissions (Classen et al., 1997: 303). The study found that 2.4% of the admissions were associated with adverse drug events causing an increase in costs of $2262 due to 1.9-day additional stay.

A reduction of medical errors associated with quality was due to the HIT. Multiple studies from LDS Hospital regarding CPOE (Evans et al., 1999 ; Evans et al., 1998: 234) showed significant decreases in adverse drug events and medication errors (Bates et al., 1998: 1316). In addition to the patient safety and quality related effects, there is also the financial side of the equation where HIT has an impact to the overall bottom line. Various studies observed that EMRs can provide a positive financial return on investment (Johnston et al., 2004; Wang et al., 2003).

IOM (2001) provides the definition adapted from Hunt et al., (1998: 1339) for clinical decision support system (CDSS) as "*software that integrates information on the characteristics of individual patients with a computerized knowledge base for the purpose of generating patient-specific assessments or recommendations designed to aid clinicians and/or patients in making clinical decisions."*

According to IOM, CDSSs provide assistance to clinicians and patients regarding prevention and monitoring of tasks, prescription of drugs, and diagnosis and management. Application related to prevention and monitoring tasks and prescription of drugs use decisions based on simple rule based logic that's often based on practice guidelines (Delaney et al., 1999; Shea et al., 1996). On the other hand, diagnosis and management of applications require detailed patient data, up-to-date clinical information and sophisticated mathematical models.

1.1.4. Healthcare IT - Harmful Consequences

Despite varies studies that HIT can assist providing improvements to patient safety, certain others have not been able to provide benefits (Black et al., 2011; Garg et al., 2005; Reckmann et al., 2009). It is clear that current HIT implementations are often complex, cumbersome, and brittle in ways that may also have negative effects on clinician performance (Armijo et al., 2009; Belden et al., 2009). When HIT changes the workflow, there is a potential negatively affecting clinicians' abilities to communicate patient information (Niazkhani et al., 2009: 543). It may also cause increased workload for clinicians ignoring information generated by computers, and therefore continue to rely on many traditional ways of

communication creating unsafe workarounds, and spending more time dealing with HIT than with patient care (Ash et al., 2009: s72).

Medication safety due to HIT use might be the only specific area of benefits as the potential benefits of HIT is weaker in other areas (Bates and Gawande, 2003: 2533). Research in literature is also limited in establishing advantages of HIT on healthcare outcomes (Black et al., 2011; Garg et al., 2005; Reckmann et al., 2009). In addition recent data suggest HIT can cause new safety challenges into the healthcare system (Magrabi, Li, et al., 2010; Magrabi et al., 2012).

Though HIT is central to providing improvements to safety and quality of health services, new evidence suggests it might also bring additional risks (Ash et al., 2004; Magrabi, Ong, et al., 2010; Magrabi et al., 2012; Magrabi et al., 2011; Sittig and Singh, 2011). According to Food and Drug Administration (FDA) in US, 42 reported patient harms as well four deaths in 436 critical events took place in nearly three years from 2008 to 2010 that had to do with HIT (Magrabi et al., 2011: 853).

HIT generally includes computer hardware and software used by health professionals and consumers to support care which might have physical and logical components that fail in time. The safety of these components used in HIT needs to be urgently addressed (Coiera et al., 2012; Institute of Medicine, 2012). HIT problems also disrupt clinical work contributing to new types of errors leading to delays and re-work (Hanuscak et al., 2009; Harrison et al., 2007; Magrabi, Ong, et al., 2010; Perry et al., 2005; Wetterneck et al., 2011).

Despite HIT's promise in improving safety, research indicates potential safety issues related HIT use called "*e-iatrogenesis"* (Weiner et al., 2007: 387). HIT caused harm might result in injuries and potential deaths due to errors in dosage, failures detecting fatal illnesses, and avoiding or delaying treatment (Aleccia, 2011).

For example, Koppel et al., (2005: 1199) describe major types of previously unexplored medication-error sources in Table 2 facilitated by a CPOE application of a commercially available EHR system.

Table 2: CPOE Based Errors

• Assumed Dose Information • Medication Discontinuation Failures • Procedure-Linked Medication Discontinuation Faults • Immediate Orders and Give-as-Needed Medication Discontinuation Faults • Antibiotic Renewal Failure • Diluent Options and Errors • Allergy Information Delay

- Conflicting or Duplicative Medications
- Patient Selection
- Unclear Log On/Log Off
- Failure to Provide Medications After Surgery
- Post-surgery "Suspended" Medications
- Loss of Data, Time, and Focus When CPOE Is Nonfunctional
- Sending Medications to Wrong Rooms When the Computer System Has Shut Down
- Late-in-Day Orders Lost for 24 Hours
- Role of Charting Difficulties in Inaccurate and Delayed Medication Administration
- Inflexible Ordering Screens, Incorrect Medications

Source: Koppel et al., 2005: 1199

1.2. INTERNET

March 2014 marked the 25th anniversary of the creation of the World Wide Web (WWW) by Tim Berners-Lee. During this quarter of a century, the adoption of Internet has contributed and greatly influenced the way we live our lives including "*the way people get, share, and create news; the way they take care of their health; the way they perform their jobs; the way they learn; the nature of their political activity; their interactions with government; the style and scope of their communications with friends and family; and the way they organize in communities*" (Fox and Rainie, 2014: 4).

The Internet has rapidly grown from an academic network into a resource of disruptive technology that continues to have a revolutionary effect on our lives. With the technological advances, especially within the last 15 years, for most people Internet became an indispensable part of the daily routines. The rapid and radical transformation brought by the Internet can be seen in all aspects of our society affecting all industries. Access to relevant Information on a given subject from anywhere anytime using a variety of devices undoubtedly is one of the ways Internet altered how we utilize technology. People access their financial, health governmental and any other private information over the Internet in a secure way. In addition many social networks on the Internet now allow people to socialize in many ways that would have been impossible before. Businesses use Internet to conduct business, promote products and services, similarly consumers use Internet to buy products and services. Businesses customize their products and services according to the consumers' preferences on the fly. Financial transactions don't require physical presence anymore as money can be transferred from one account to another easily in different forms online for the various products or services offered to consumers. For any product or service manufactured, ordered, distributed and

finally delivered, the entities involved such as the buyer, the seller, the manufacturer, the distributer, the financial institutions involved; they all can be in different parts of the world and do not need to even contact with each other as every process involved can be automated over the Internet. In healthcare using robotics, remote surgeries are done where the patient and doctor are in two different locations.

With all the advances, more and more people access and use Internet for various purposes. Table 3 provides certain Internet related use figures in US, based on PewResearch 2014 Internet project (Fox and Rainie, 2014: 5).

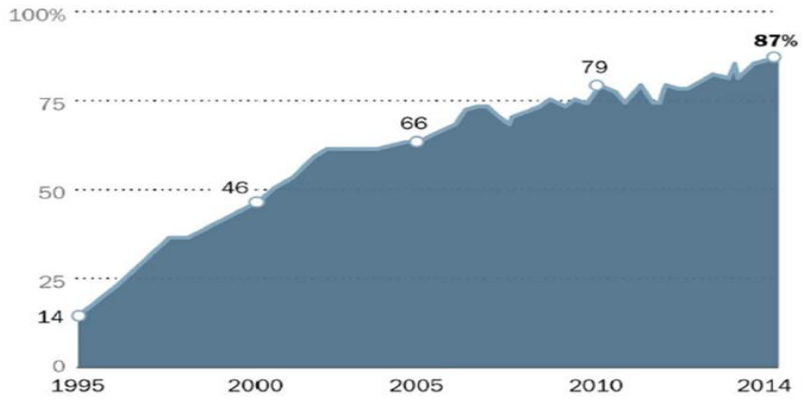
Table 3: US Internet Use Statistics

• 87% of American adults use the Internet
• 97% of Young adults ages 18-29 use Internet
• 68% of adults connect to the Internet with mobile devices like smartphones or tablet computers
• 90% of Internet users say the Internet has been a good thing for them personally
• Only users of the Internet and mobile phones made clear those technologies feel increasingly essential, while more traditional technologies like landline phones and television are becoming easier to part with:
• 53% of Internet users say the Internet would be, at minimum, "very hard" to give up, compared with 38% in 2006
• 49% of cell phone owners say the same thing about their cell, up from to 43% in 2006.
• Adult ownership of cell phones has risen from 53% in 2000 to 90% in 2014

Source: Fox & Rainie, 2014: 5 based on Pew Research Center Surveys, 1995-2014

Figure 6 shows the high increase rate of Internet use over the years since 1995. It has increased from 14% in 1995 to 87% in 2014.

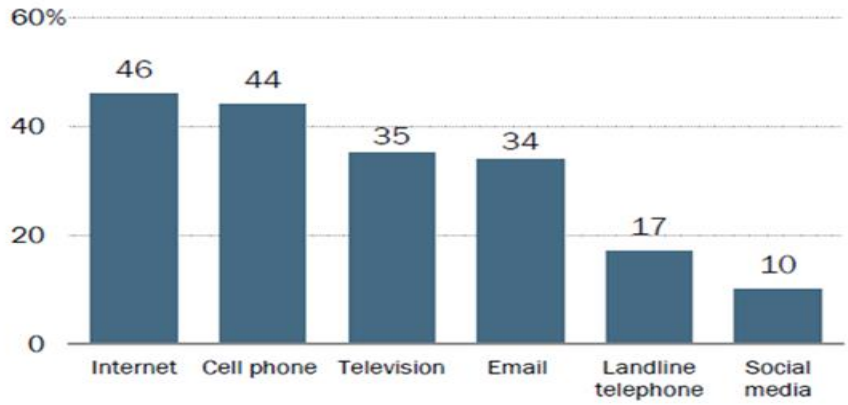
Figure 6: Internet Use in US, Over Time



Source: Fox & Rainie, 2014: 4 based on Pew Research Center Surveys, 1995-2014

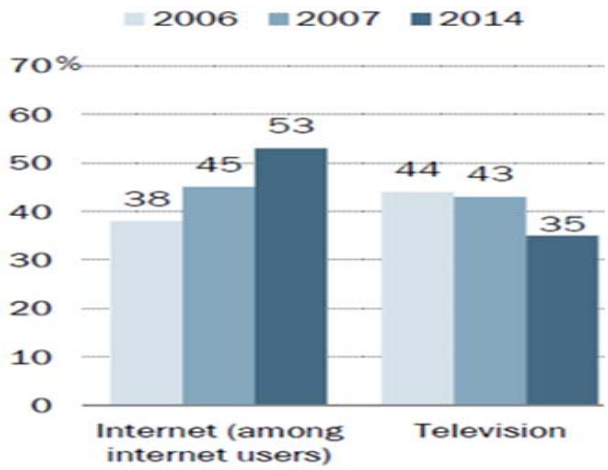
Figure 7 shows as technology advances, people use Internet more and rely on mobile devices to access Internet anywhere anytime. This reliance on new technology is also reflected in people's preferences. Percentage of people who consider Internet and mobile phones hard to give up is much more than those who use Television and landlines as shown in Figures 8 and 9.

Figure 7: Technologies Very Hard or Impossible to Give Up



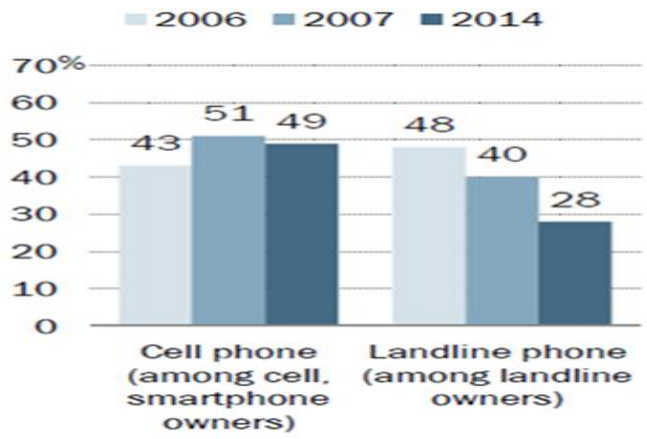
Source: Fox & Rainie, 2014: 6 based on Pew Research Center Survey 2014

Figure 8: Internet vs. Television



Source: Fox & Rainie, 2014: 20 based on Pew Research Center Surveys

Figure 9: Mobile Phones vs. Landlines



Source: Fox & Rainie, 2014: 21 based on Pew Research Center Surveys

Most western countries made considerable amount of progress regarding ubiquitous broadband access with increased amounts of bandwidth (National Telecommunications and Information Administration, 2013). Technology industry leads the way in revolutionizing the nature of Internet use through mobile devices. According to Pew Internet Report, over one billion smartphone users worldwide carry the global network in their pockets, surpassing the 41% who use traditional mobile phones. Smartphones are widely used for health related matters via mobile applications. 31% of cell phone owners, and 52% of smartphone owners, have used their phone for health related medical information. Exercise, diet, and weight apps are among the most popular health applications used (Fox and Duggan, 2012).

More and more, patients are seeking information on the Internet regarding medical conditions or treatments (Fox and Jones, 2009). Regarding the health related matters, patients look for answers on the Internet more than they communicate with their doctors about healthcare questions (Elkin, 2008: 2). The Internet also provides consumers easy access to their personal health records including consultations, diagnoses, lab results, prescriptions. According to the Pew Report, 72% of Internet users indicate they searched for health information online in 2011, specific diseases or conditions; treatments or procedures; and doctors or other health professionals being the most searched for (Fox and Duggan, 2012).

According to IOM report (Institute of Medicine, 2000: 36), potential uses of Internet in regards to healthcare are listed in Table 4.

Table 4: Functions Commonly Performed Over the Internet

• Search for consumer health information • Participate in chat/support groups • Exchange electronic mail between patients and care providers • Access biomedical databases and medical literature • Find information about health plans, select physicians • Purchase pharmaceuticals and other health-related products • Transfer medical records among affiliated health organizations • Transfer claims data to insurers and other payer organizations • Conduct remote medical consultations (limited) • Send medical images (X rays, etc.) to remote site for interpretation • Broadcast medical school classes over campus networks • Videoconferencing among public health officials • Remote surgery or guidance of other procedures • Public health surveillance/incident reporting • Home-based remote medical consultations • In-home monitoring of patients

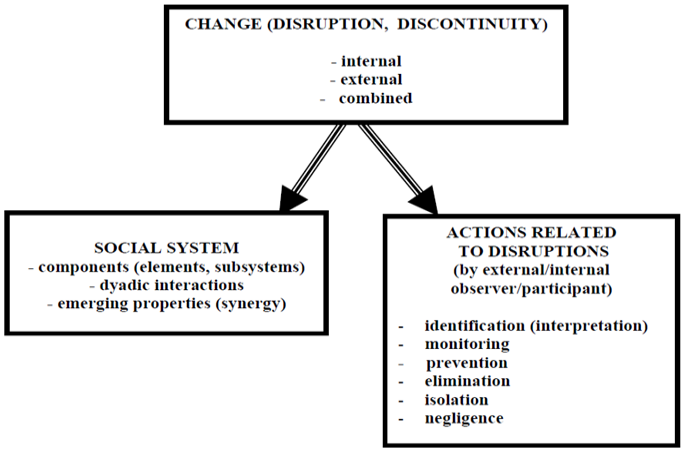
Source: Institute of Medicine, 2000: 36

1.3. SECURITY

The word "security" in English covers a broad range of meanings including "*to feel safe and to be protected"* and is used to describe a situation without any risks or worries (Mesjasz, 2004: 4). The term *security-securitas* in Latin means tranquility and freedom of care which Cycero termed the absence of anxiety upon which the fulfilled life depends (Liotta, 2002: 477). Arnold Wolfers (1960; cited by Mesjasz, 2004: 5) provided a more inclusive definition of security as "*Security, in an objective sense, measures the absence of threats to acquired values, in a subjective sense, the absence of fear that such values will be attacked"* which later became a standard definition in International relations (IR) theory (Møller, 2000).

Mesjasz (2004) defines the main concept of security as presented in Figure 10 which relates to certain components such as *threat, risk, danger, vulnerability, uncertainty* and can be further used to develop a wider concept of security that researches the interrelationship between security defined as a characteristics of social systems and different concepts labeled as systems thinking, or systems approach (Mesjasz, 2004: 7).

Figure 10: The Core Concept of Security

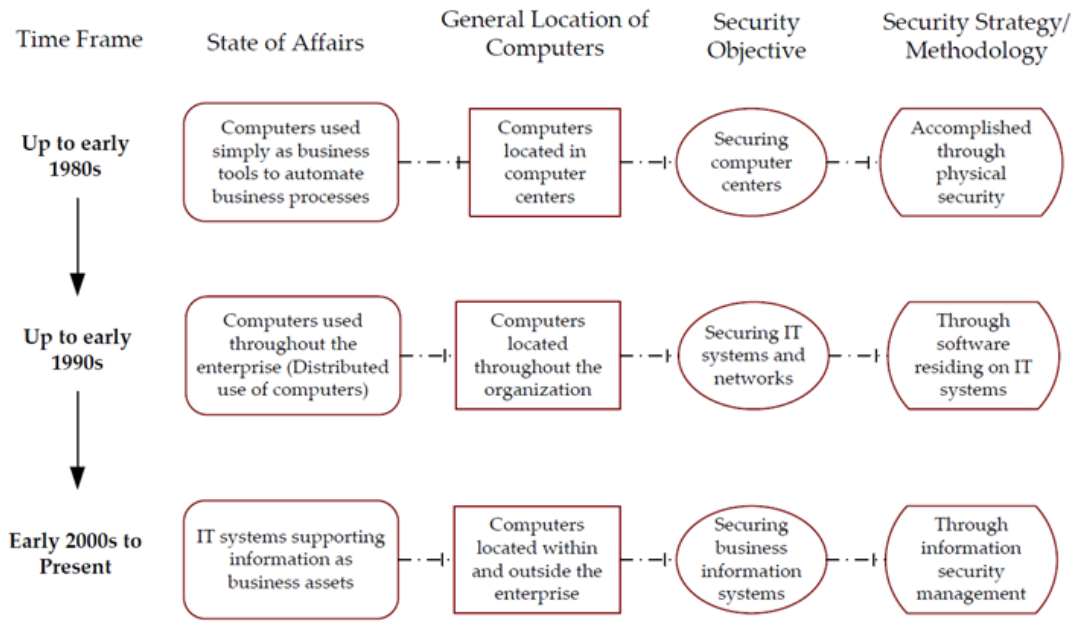


Source: Mesjasz, 2004: 7

1.3.1. Information Security

Looking back to the advances in the history of IT helps us evaluate the different phases IS went thorough. Despite the various complex dimensions of the current state of IS, the main security focus for organizations was simply on physical protection of the computing assets in the early years of computing which included securing and protecting data from natural disasters and malicious activities (Nnolim, 2007). The evolution of computer and IS strategies is shown in Figure 11 (Nnolim, 2007: 1; Vermeulen and Von Solms, 2002).

Figure 11: Evolution Security in IT



Source: Nnolim, 2007: 1

The progress of IS can be seen through the characteristics of the IT computing eras, starting with the mainframes and midrange computers in the early 50s to 70s then to personal computers used at homes and offices in the early 80s which brought the LANs and WANs of network connections as well as database and server farms in the late 80s - 90s, and eventually the Internet era with complete interconnectivity where IT systems supporting information as a business asset. The evolution was from physical security of computers, to security of IT and networks, and eventually to security of business information systems. Widespread usage of personal computers which later utilized the LAN/WAN communication technologies introduced different aspects of the information security issues. The Internet era further accelerated the IS to a whole different level without any boundaries and made it a critical function of any business information system along with the challenges it brought along.

As the number of security related incidents increase, more needs to be done to face these overwhelming security challenges. Recent studies show that security needs to be tightened to deal with these increasing breaches in organizations (Workman et al., 2008: 2813). Companies failing to manage their information security properly will more than likely to face the negative consequences. "*The*

organizations' integrity will be compromised, and there will be a loss of money, trust and competition; furthermore, people will lose confidence and trust in one another" (Blakley et al., 2001: 100).

James Andrew from CSIS indicated that the global GDP was about $70 trillion in 2011 according to the World Bank, while ballpark figure on the cost of cybercrime and cyber espionage was $300 billion to 1 trillion globally and $24 billion to $120 billion in the US (Lewis and Baker, 2013). In the same report, according to the United Nations Office on Drugs and Crime (UNODC), identity theft was stated as the most profitable form of cybercrime, generating perhaps $1 billion per year in revenue on a global basis and that the cost of identity theft using cyber techniques in the US was $780 million (Lewis and Baker, 2013).

Cost of security according to some studies has been increasing and expenditures on cyber security should be considered as part of the total cost of cyber espionage and cybercrime (Anderson et al., 2012). According to one study, governments and companies spend maybe 7% of their IT budgets on security. Another study predicts annual global spending on cyber security software at around $60 billion, increasing around 8% each year (Perlroth, 2012). Despite the increase in cost for implementing security strategy for the purposes of protecting business assets, nearly 30% of companies participated in a PwC survey didn't have a plan, of the 56% who have, 26% fail to test it (PricewaterhouseCoopers, 2013a).

Total cost of malicious cyber activity would also include the opportunity costs such as forgone opportunities, or lost benefits that would otherwise have been obtainable for activities in cyberspace. An example to an opportunity cost would be the additional money spent on cyber security that otherwise would not be needed in a more secure environment. Reduced sales and lost productivity are other examples to opportunity costs. In addition to the monetary costs, security breaches cause other non-financial damages to businesses. According to the PwC study, the cost of security related incidents can be classified into three categories: monetary, productivity, and indirect. Internal procedures and communication can be impacted lowering the productivity, along with reduced competitive advantages. Information security incidents, in addition to causing economic damage may also have a negative impact on reputation, goodwill, and trust (Hoffer and Straub, 1989; PricewaterhouseCoopers, 2013a).

In another 2008 study commissioned by the European Network and Information Security Agency (ENISA), it is mentioned that "*growing public concerns*

about information security hinder the development of both markets and public services" (Anderson et al., 2009: 1). From this perspective, in addition to the costs, malicious cyber security activities impact consumer behavior as well. According to a survey cited in the European Commission Cyber security Strategy Document, almost a third of Europeans are not confident in their ability to use the Internet for banking or purchases because of security concerns (TNS Opinion & Social, 2012). In the EU (European Union) majority of Internet users (61%) are concerned about experiencing identity theft as 12% of Internet users across the EU have experienced online fraud, and 8% have experienced identity theft while 13% have not been able to access online services because of cyber-attacks (TNS Opinion & Social, 2012).

The proliferation of the IT has increased the importance of information security in businesses making it a critical component. Objectives are set forth to protect this critical business component by ensuring the data confidentiality, integrity and availability within IT (Schultz et al., 2001; Smith, 1989). As businesses spent millions of dollars to protect their assets and have specific positions created such as IS officers, IT security director, Chief Security officer and allocate budgets for the purposes of protecting their business assets a proper definition of information security is needed.

A general definition is given in ISO/IEC 27001:2005 standard as "p*reservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved"* (ISO-27001, 2005: 2).

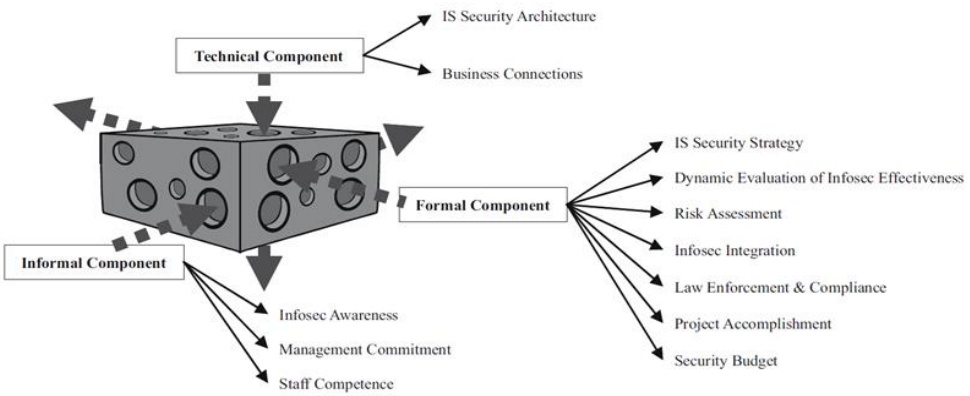
In the business context, information security is defined as "*the application of any technical methods and managerial processes on the information resources (hardware, software, and data) in order to keep organizational assets and personal privacy protected"* (Hong et al., 2003: 243). IS, therefore, is concerned with protecting and securing business information resources. Vermeulen & Von Solms (2002) elaborate on IS from an architectural management framework perspective indicating that "*information security management refers to the structured process for implementation and ongoing management of information security in an organization"* (Vermeulen and Von Solms, 2002: 120) where an architectural framework may be looked at as "*set of tools, methods, processes, and vocabulary that can be used for developing a broad range of different IT architectures"* (Perks and Beveridge, 2003: 437). Taking the historical developments and decades of evolution of IT into consideration along with the increased interaction across multiple computers,

networks, and organizations without any geographical boundaries, the existing inadequate business IS strategies focusing on the perimeter of network controls and risk reduction needed to be reviewed and new security management strategies be developed to reflect on the new technology platforms (Rungta et al., 2004: 304).

The Open Group (2011) looks at IS from a viewpoint perspective where *view* is defined as "*a representation of a whole system from the perspective of a related set of concerns"* (The Open Group, 2011: 374). According to the Open Group, security viewpoint includes various areas including physical, data, information, application, and infrastructure within the enterprise where enterprise is the highest level in an organization including organizational goals, objectives, mission, vision, business strategies, and all other organization functions and activities (The Open Group, 2011).

Torres et al. (Torres et al., 2006: 532) define IS as "*a well-informed sense of assurance that information risks and technical, formal and informal controls are in dynamic balance*." They refer to "*technology, process, and people"* aspects aligned with the terms "*technical, formal, and informal"*. Figure 12 shows the model of the critical success factors in security management information systems (SMIS) as explained using the Swiss-Cheese model (see section 2.4.3) developed by Reason (Reason, 1997).

Figure 12: Critical Success Factors in SMIS



Source: Torres, Sarriegi, Santos, & Serrano, 2006: 533

The IS domain has a wide coverage of concepts. Protection of information in order to provide the confidentiality, integrity, and availability of information is important and various tools and mechanisms are used for this purpose. The authorized or unauthorized use of the information resources, certain attacks such as

denial of service against the system where information resides are also concepts associated with IS. Security in this sense also implies the existence of valuable assets, - the information -, to be protected from unauthorized access. The concept of a security perimeter is often times referred and used for protecting assets inside from threats outside by means of devices used on the perimeter such as firewalls filtering incoming and outgoing network traffic. The notion of perimeter makes an explicit distinction between inside and outside, where inside is a trusted zone and outside is not. This approach is similar to an analogy with safes, access control in buildings, and other means of physical control. Here physical boundaries are created in which the assets are contained. The containing perimeter has a limited number of gates, which also limit the traffic that can go through using, e.g., keys (Pieters, 2011: 327). This approach of securing information assets has been the accepted view in the past as the design for protection of IT followed a similar pattern of containment (Franqueira et al., 2009; Scott, 2004) along with the exposure, weaknesses or gaps of the system to outside threats. The term *exposure* is used to describe what part of the *inside* is accessible from the *outside* (Dragovic and Crowcroft, 2004: 58). This perimeter-based security focused on containment brings the issue of threats from the trusted inside where individuals inside the perimeter misuse their authorized level of access to the systems disrupting and posing a threat to the system (Probst et al., 2007: 127).

In addition, as the demand to access to inside information resources increases via usage of virtual private networks (VPNs), the boundaries or the perimeter concept seem to disappear. More and more the concept of cloud technology is proliferating into our lives, where the valuable information assets to be protected now reside somewhere on the Internet and therefore the protection should be as close to the data as possible. Protection may no longer be based on the physical separation of networks through a firewall, but rather on digital separation of the data by means of encryption such as sticky policies (Karjoth et al., 2003). These encryption policies can allow people from various organizations access to the data through different routes with different access credentials, however the physical and digital protection of IS still remains an issue to be further explored.

1.3.2. Confidentiality, Integrity, and Availability

In many studies, confidentiality, Integrity, and availability concepts form the foundations of the IS principles and methods. The commonly accepted viewpoint is security encompasses confidentiality, integrity, and availability (Bertino and Sandhu, 2005; Lindqvist and Jonsson, 1997). Confidentiality refers to the protection of data against unauthorized disclosure; integrity refers to the prevention of unauthorized and improper data modification; and availability refers to the prevention and recovery from errors and system failures (Bertino and Sandhu, 2005: 2).

"Information security is the protection of information and information systems from unauthorized access, use, disclosure, modification or destruction. Information security is achieved by ensuring the confidentiality, integrity, and availability of information" (Blobel, 2002; cited by Orel, 2013: 196). A more in depth definition for these terms is given by Tudor (2002: 1); confidentiality, integrity, and availability (CIA) is defined as follows:

> *Confidentiality relates to the protection of information from unauthorized access, regardless of where the information resides or how it is stored. Information that is sensitive or proprietary needs to be protected through more stringent control mechanisms. Authentication and authorization are two mechanisms used to ensure the confidentiality of information. Policies must be in place to identify what information is confidential and the period of time it should remain confidential. A Framework must be developed for classifying information according to its characteristics and should include associated security requirements for each confidentiality ranking.*
>
> *Integrity is the protection of information, applications, systems, and networks from intentional, unauthorized, or accidental changes. It is also important to protect the processes or programs used to manipulate data. Information should be presented to information owners and users in an accurate, complete, and timely manner. Key to achieving integrity is management controls that provide the appropriate separation of duties as well as testing and validation of any changes that are made to systems and processes. Also important are the identification and authentication of all users accessing information, applications, systems, and networks through the use of manual and automated checks. A framework needs to be developed for classifying the integrity of data according to its characteristics and should include associated security requirements for each integrity ranking.*
>
> *Availability is the assurance that information and resources are accessible by authorized users as needed.*

In healthcare confidentiality, integrity, and availability as well as security and privacy generally mean the following (Blobel, 2002; cited by Orel, 2013: 196):

• *Confidentiality* – the property that electronic health information is not made available or disclosed to unauthorized persons or processes. It is the controlled release of personal health information to a care provider or information custodian under an agreement that limits the extent and conditions under which that information may be used or released further.

• *Integrity* – the property that electronic health information have not been altered or destroyed in an unauthorized manner.

• *Availability* – the property that electronic health information is accessible and useable upon demand by an authorized person.

• *Privacy:* The right and desire of a person to control the disclosure of personal health information.

• *Security:* A collection of policies, procedures, and safeguards that help maintain the integrity and availability of information systems and control access to their contents

In order to evaluate the electronic health information confidentiality, integrity, and availability, a general understanding of health IT within a healthcare institution is required (Orel and Bernik, 2013).

1.3.3. IS Policies, Methods and Models

Security policies and guidelines are viewed as the starting point of IT security (Whitman, 2004: 52). A security policy prescribes how an organization manages its IT security. More specifically security policy "…*consists of a set of rules and practices that regulate how the organization manages, protects, and distributes its key information assets*" (Walker, 1985: 62). Generally speaking, a good security policy should clarify the following aspects: individual responsibility, authorized and unauthorized uses of IT, how users report suspected threats, and penalties for violations (Whitman, 2004: 52).

The effectiveness of the existing strategies of policies and models has been questioned due to lack of theories. According to Hong et al. "*Because of the lack of an information security management theory, there are few empirical studies conducted to examine the effectiveness of management strategies and tools"* (Hong et al., 2003: 243). Hong also pointed out the lack of consistent security polices might be one of the reasons causing a gap of theoretical framework in IS (Hong et al., 2003: 244). Table 5 shows theoretical polices on IS highlighting major themes.

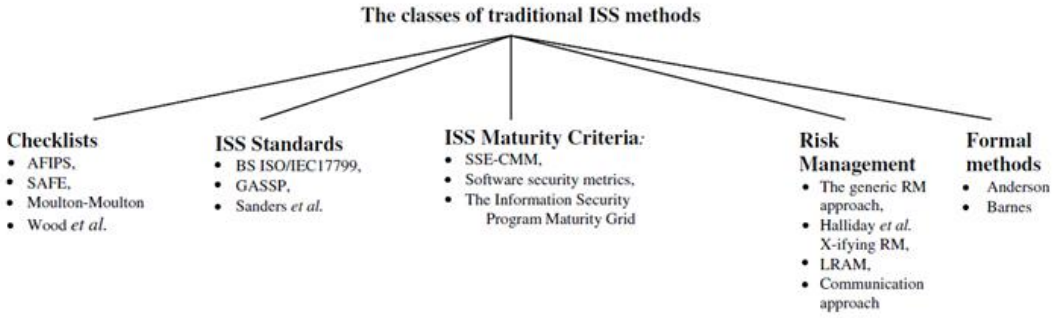
Table 5: Theoretical Policies on Information Security

Kabay (1996) - policy theory	Rees et al (2003) policy life cycle	Flynn (2001) e-policy	(Doherty and Fulford, 2006) Component based Security Policy	Knapp et al. (2009)Repeatable organizational process
to assess and persuade top management	*policy assessment*	*comprehensive e-audit*	Personal usage of information systems	risk assessment
to analyze information security requirements	*risk assessment*	*e-risk management policy*	Disclosure of information	Policy development
to form and draft policy	*policy development and requirements definition*	*computer security policy*	Physical security of infrastructure and information resources	Policy Review
to implement the policy	*review trends and operations management*	*cyber insurance policy*	Violations and breaches of security	Policy approval
to maintain the policy		*email policy*	Prevention of viruses and worms	Policy awareness & training
		Internet policy	User access management	Policy implementation
		software policy	Mobile computing	Monitoring
			Internet access	Policy enforcement
			Software development and maintenance	
			Encryption	
			Contingency/continuity planning	

Source: Adapted from Hong et al., 2003: 244

Despite the development of several new modern IS methods by scholars, the traditional methods have been used more in practice. In contrast to the first generation with three classes (Baskerville, 1988, 1993) and second generation (Siponen, 2005) with five classes of traditional IS methods, there seems little evidence of usage for the more modern methods. "*Information systems security (ISS) checklists, standards, maturity criteria, risk management (RM), and formal methods (FM), are among the most commonly used ISS methods"* (Siponen, 2005: 304) as shown in Figure 13.

Figure 13: The Five Classes of Traditional ISS Methods

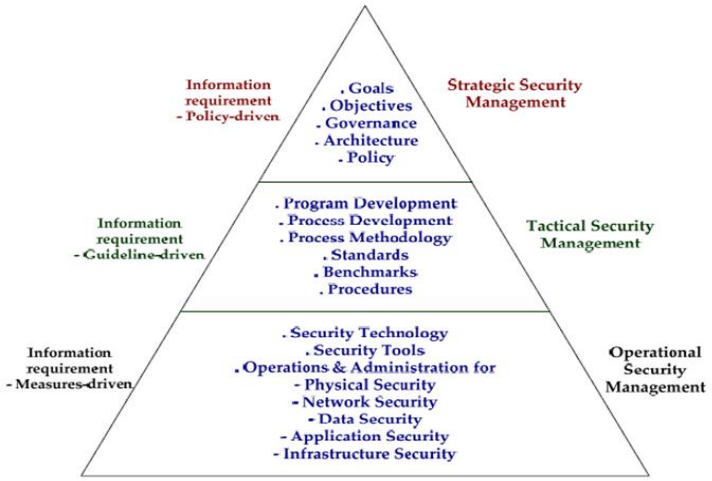


Source: M. T. Siponen, 2005: 304

Varying organizational levels also affect IS. Strategic, tactical, and operational levels form the underlying structure of the IS that deal with the corresponding types of security issues concerning senior management within the organization (Belsis et al., 2005: 193). The requirements for IS management should be policy driven on a strategic level, guideline-driven on tactical level, and measures-driven on an operational level.

Among these three organizational levels that deal with IS, corporate strategy is managed by the strategic level, processes and methods used for IS by the tactical level, and the implementation, and operation of security tools and measures by the operational level (Belsis et al., 2005: 193). This level of security management among different layers within an organization is shown in Figure 14 (Belsis et al., 2005; Nnolim, 2007).

Figure 14: Security Management among Different Layers



Source: Belsis et al., 2005: 193; Nnolim, 2007: 10

Slewe and Hoogenboom indicated the operational level from a logical and technical point being focus for majority of security related measures (Slewe and Hoogenboom, 2004: 60). However as IT environment is changing and becoming more complex, organizations are shifting the focus for IS efforts on to the tactical and strategic levels.

1.3.4. Information Security Threats

Threats to business IT systems take advantages of the weaknesses, gaps or lack of proper controls within the security systems and exploit vulnerabilities. According to Peltier, as a result of these exploitations, technology instead of supporting, damages or impacts the organization (Peltier, 2005) leading to loss of revenues, assets, or reputation.

Table 6 shows a variety of studies that have been done regarding the types of threats that exist within IT. Loch, Car, and Warkentin (1992) conducted a survey about the concerns IT executives had regarding a variety of organizational information threats, which were categorized into eleven groups. The senior managers seem to think the treats were moderately low in impact and also thought others to be in greater risk than they were, showing a naive belief that bad things only happen to other people (Loch et al., 1992). Hutt (1995) In his *Computer Security Handbook* categorized threats into seven groups while (Rannenberg et al., 1999) studied IT security in the healthcare industry and came up with four IS threats. Peltier (2003) identified six kinds of information threats.

Table 6: Threats within Information Technology

Loch et al. (1992)	Hurt (1995)	Rannenberg et al. (1999)	Peltier (2003)
Ineffective controls	Management failures	Unauthorized information gain	Computer Virus
Natural disasters	Physical hazard	Unauthorized modification of information	Hackers
Computer Virus	Equipment Malfunction	Unauthorized impairment of functionality	Denial-of-Service
Accidental bad data entry	Software Malfunction	Unauthorized noncommitment	E-mail Mistakes
Accidental data destruction by employee	Human Error		Disgruntled Employees
Hackers	Misuse of Data		Industrial Spying
Internal unauthorized access	Loss of Data		
Poor control over manual handling of I/O			
Intentional data destruction by employee			
Intentional bad data entry by employee			
Unauthorized access by competitors			

Source: Peltier, 2005

The common theme among all these categories is the human, element; in other words employees working internal to the organization, as well as people external to the organization seem to be a common factor. Rules and procedures, physical elements, and any software related issues also seem to exist within all categories. The classifications of threats within the IT environment also reflect the different phases the IT industry went through; pre-PC, PC, Post PC/network and Internet.

In order to deal with threats properly an effective security implementation requires numerous technical, policy, and people safeguards. According to PwC (PricewaterhouseCoopers, 2013b: 34), below are the ten essential safeguards for an effective IS:

- A written security policy
- Back-up and recovery/business continuity plans
- Minimum collection and retention of personal information, with physical access restrictions to records containing personal data
- Strong technology safeguards for prevention, detection, and encryption
- Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data
- Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records
- Ongoing monitoring of the data-privacy program
- Personnel background checks
- An employee security awareness training program
- Require employees and third parties to comply with privacy policies

1.3.5. Information Security in Healthcare

Due to the advanced evolution of technology within the last twenty years, it is apparent that IT is now an indispensable part of our daily lives and has been widely applied in every aspect of our society including business, education, healthcare, finance, government, and national defense. IS has emerged as an important component of this IT evolution. As IS becomes a required business function, not all organizations are equally affected by the problems of information security. In certain

industries, where information is intensive and critical, the security issue is more serious and must receive more attention (Peltier, 2003). The demands of healthcare with regard to security and availability are both more stringent and more varied than those of other industries (Donaldson and Lohr, 1994). For example, in the banking, financial, insurance, and healthcare industries, information protection is typically more important than in farming, mining, and manufacturing industries. Healthcare organizations due to inherent vulnerability of sensitive information are particularly concerned with security of information assets.

According to many, information privacy and IS means the same. However there are differences between IS and privacy. This is especially an important concept that needs to be distinguished in healthcare. According to Kang (1998), privacy related to IS, refers "*an individual's control over the acquisition, disclosure, and use of personal information"* (Kang, 1998: 1203). In other words privacy aims to keep the information private while IS manages the steps taken to keep the information secure. Along the same lines of privacy and security, access to data is related to the need to know. Who is going to access under what conditions is important and needs to be made clear. If this need to access data is not clearly specified, then attempts to access information might be considered illegal or unauthorized. "*The authority to create and view data of a certain type would be vested with the user and the permission to use that authority to access and update specific records should be vested with the patient or with the patient's representative*" (Higgs, 1997: 61).

The interplay between privacy and security begs the question of what specific information do we want to keep private and secure? For many individuals, personal health information such as medical records, in addition to financial information is the most valuable protected sensitive information**.** Confidentiality, security and privacy affect consumers and patients whereas ethical and legal factors mostly affect all the other players of the system. So governance of information is critical as individuals prefer to keep their health related medical information private and secure. In addition to certain mundane information, medical records also contain a lot of sensitive information about individuals such as fertility, abortions, emotional problems, sexual behaviors and preferences, physical and substance abuse, HIV status, psychiatric care and others (Rindfleisch, 1997: 94). The wide proliferation of HIT makes these sensitive medical records available in various databases and certainly accessible to many people within the healthcare

environment. In order for these records to stay private and secure, access needs to be controlled to prevent any harm as a result of any disclosure. This harm might come in the form of social embarrassment or prejudice, or affect our insurability, or limit our ability to get and hold a job. There might also be legal consequences regarding privacy of identifiable health information, reliability and quality of health data, and tort based liability (Hodge Jr et al., 1999: 1467).

National policies pertaining to privacy, security, and confidentiality as well as standards for the coding and exchange of clinical information contribute to the overall automation of clinical information (Dwyer, 1999; Kleinke, 1998). Yet safeguarding privacy and information security has the potential to be a barrier for the free flow of health information much needed for research, outcome analysis, and other public health activities. In addition, people due to increasing levels of concerns and fear of violations of privacy may forego seeking necessary healthcare services or withhold personal information from clinicians (Goldman, 1998: 49). Carefully balanced privacy protections will maximize the use of IT as well as satisfy the requirements for consumers (Detmer, 2000). If these privacy protection policies are too stringent the adoption of many IT applications that are critical to addressing healthcare quality concerns might be impeded (Detmer, 2000). As developments within the healthcare require better sharing of information across organizational boundaries, proper confidentiality should be maintained (Higgs, 1997: 61), while detailed policies can be setup providing timely and authorized access to those with a valid purpose. Policies related to information security technologies are available to provide safe occurrence of these activities such as encryption, authentication (Detmer, 2000; National Research Council Board on Biology, 1998).

Information is only as good as its consequences. The core problem for any information system is to provide the right information to the right person at the right place at the right time. The sensitive protected information is only useful when it is shared within the healthcare system and the medical providers. Doctors, physicians, and clinicians, who are highly mobile need to access to this protected sensitive information from many different locations in order to diagnose diseases, to avoid unnecessary, risky duplicative tests, and to come up with an effective treatment plan taking many factors into account.

Technological advantages include improved data to assist in making more informed decisions about insurance, providers, products, and procedures. It can also contribute to improved care through more expedient and accurate research and

diagnosis, and the ability to disseminate expert advice to underserved areas (Hodge Jr et al., 1999: 1466). It also provides challenges to the protection of private health information. Data can be accessed, changed, viewed, copied, used, disclosed, or deleted easily by both authorized and unauthorized individuals. In such circumstances healthcare organizations are especially concerned with security matters such as inherent vulnerability of sensitive data (e.g., personal health records) in health informatics. The integrity and availability of sensitive and confidential information contributes to high quality care, which makes the protection an important issue in healthcare. With the increasing use of IT in the healthcare domain today, hospitals are interconnected to share medical data, thereby providing a distributed environment for storing and accessing medical data. As data is accessed from various locations in such distributed environment, security becomes a major concern because security lapses such as unauthorized access, eavesdropping, masquerading, intrusion, and data integrity violation could easily occur. A study by Kroll Advisory Solutions (2012: 6) indicate that majority (79%) of the security breaches related to patient data at US hospitals are caused by employees, with unauthorized employee access.

In assessing electronic health information, confidentiality, integrity, and availability requires the medical professional first to understand health IT environment of a hospital, private practice or some other medical institution. This includes technologies used for both clinical and administrative purposes. It is important that those technologies are physically used and located, and to know how they are used during various healthcare processes. When evaluating health IT environment one should think about situations that may lead to unauthorized access, use, disclosure, disruption, modification or destruction of electronic health information.

Due to this relationship between privacy and IS, there are several laws and regulations imposed by governments to safeguard IS and privacy such as the ones in the US; the Health Insurance Portability and Accountability Act of 1966 (HIPAA), the Privacy Act of 1974, and Security Breach Notification Law (Wong and Thite, 2009). HIPAA, with its mandates for data security, was expected to trigger HIPAA-covered entities to deploy novel information security processes and practices (Appari et al., 2009). Recent research, however, indicates that this has not been the case (Appari et al., 2009; Brady, 2011). Literature on HIPAA and IS has identified a number of factors that contribute to security behavior and security effectiveness.

These factors include *management support* (Logan and Noles, 2008; cited by Brady, 2011: 1), *security awareness* (Lending and Dillon, 2007; Medlin and Cazier, 2007; cited by Brady, 2011: 1), *security culture* (Ma et al., 2008; cited by Brady, 2011: 1), and c*omputer self-efficacy* (Chan et al., 2005; cited by Brady, 2011: 1; Lending and Dillon, 2007; Womble, 2007). Additionally, *security effectiveness* (D'Arcy and Hovav, 2009; cited by Brady, 2011: 1) and *security behavior* were found to be valid predictors of each other as well.

Understanding the factors affecting the effectiveness of security countermeasures has been a consistent theme in the literature (Chang and Lin, 2007; Knapp et al., 2007). IS effectiveness has been researched as a result of the continued security related incidents causing substantial financial losses (Chang and Yeh, 2006: 351). This is another reason why more effective policies need to be developed to address compliance with HIPAA and other security related regulations. Effectiveness of IS has been studied often in the literature. Straub indicated IS effectiveness as "*the ability of IT security measures to protect against the unauthorized and deliberate misuse of assets of the local organizational information system by individuals, including violations against hardware, programs, data, and computer service*" (Straub, 1990; cited by Brady, 2011: 1). The theoretical foundation for IS effectiveness was improved by developing and testing an integrative model of IT security effectiveness (Kankanhalli et al., 2003: 140). Chang and Lin stated that organizational culture and support of management positively influences security effectiveness (Chang and Lin, 2007: 451). They also indicated that confidentiality, integrity, and availability were significantly correlated to security effectiveness.

1.3.6. Impact of Information Security Breaches

With the increased dependency on IT, the consequences for society can be enormous (Rogers, 2001: 2). Issues such identity thefts, security of transactions over the Internet, viruses, spyware, security breaches of confidential information, securing networks and databases, corporate accountability are all part of the security related matters that affect all of us. Reported data regarding information security related breaches tend to be *measures* rather than real *metrics* due to incompleteness (Walker, 2012: 11).

According to the 2010 survey commissioned by the Information Security Europe organization (Potter and Beard, 2010: 2), there has been an increase from 72% of security breaches in 2008 to 92% in 2010 with a median number of incidents reported as 45 compared to 15 in 2008. As a result of the increase in incidents costs of security incidents also increase. In large organizations the losses were as much as £280,000 to £690,000, compared to £90,000 to £170,000 in 2008. Smaller organizations with staff less than 50 also experience security related issues costing them £27,500 to£55,000 in 2010 versus £10,000 to £20,000 in 2008.

Information security and privacy are major concerns in the healthcare domain (Huang et al., 2008: 11) and according to Herold, data security breaches related to privacy in healthcare organizations continue to increase (Herold, 2009). The absence of sound IS management processes and practices together with the healthcare industry's increasing reliance on HIT, contribute to threats to the integrity of patient data (Netschert, 2008: 121). According to the 2009 HIMSS Security Survey, one-third of the respondents reported that their organization had at least one known case of medical identity theft, with only one-half having a plan in place for responding to security breach threats or incidents (Healthcare Information and Management Systems Society, 2009: 15).

Regarding the impact of information security breaches, more attention needs to be given to the social and behavioral aspects especially among academic medical centers. A variety of user acceptance models have been identified in the literature focusing on workplace behavior, including the Technology Acceptance Model (TAM) and TAM2 (Venkatesh and Davis, 2000: 186). Generalizability of factors within technology acceptance model focusing on user behavior in IS requires further research. Many information security breaches in the workplace have been attributed to the failure of employees to comply with organizational security policies (Chan et al., 2005). In two industries where IT is heavily used similar to healthcare, a study conducted including 104 employees found IS breaches generally as a result of non-compliant employee behavior (Chan et al., 2005; cited by Brady, 2011: 2).

1.3.7. Information Security Risk

IS, an important concept that manages and ensures risks to IT, is identified and managed in alignment with the business objectives. Anderson (Anderson, 2003:

310) defines information security as "*a well-informed sense of assurance that information risks and controls are in balance*."

Despite the high interest, and an increasing number of academic and business focused research on IS, limited studies have been conducted on IS in healthcare (Appari and Johnson, 2010: 297). In their overview of the literature, they conclude that "*surprisingly little research has been published about the use, effectiveness and availability of information security risk management methods in healthcare organizations."*

As risks in information security present a wide variety of challenges in different complex settings, they should be examined from a wider perspective (Dhillon and Backhouse, 2001; Dourish and Anderson, 2006; Gerber and von Solms, 2005; Pieters, 2011; Thompson and Kaarst-Brown, 2005) where risk management activities include the acceptance, mitigation, or assignment of risk. Risk management is especially important in healthcare, a complex environment difficult to define boundaries for due to multiple factors such as technology, people, and scope of services.

1.4. ORGANIZATIONAL FACTORS

Many efforts have been made within the last decade to explore and address the IS related issues. Researchers (Chang and Ho, 2006; Eloff and Eloff, 2003; Sittig and Singh, 2010) generally agree that IS management encompasses many domains, including managerial, technical, social and organizational aspects that must all be effectively addressed. Similarly, other studies also indicate that IS issues similar to safety and quality are more of social rather than technical issues involving business, organizational, management, and people elements (Dhillon and Backhouse, 2000; Dutta and McCrohan, 2002; Mader and Srinivasan, 2005). Solms identifies the issue as one of the 10 sins stating as "*not realizing that the protection of information is a business issue and not a technical issue"* (von Solms and von Solms, 2004: 372). The socio-technical nature of information security is also emphasized by Björck and Siponen (Björck, 2004; Siponen, 2006; cited by Coles-Kemp, 2009: 181) and the human dimension to both IS practice and technology design is recognized (Coles-Kemp, 2009: 181). Lampson (2004) and Lacey (2010; cited by Bess, 2012: 11) support the view that IS management is a *people* problem,

not just a technology problem, as it is people who will implement, manage, and use the IS policy within an organization.

Still, some research in business to manage and define IS indicate more attention is given on a technical and operational level without a formal framework or methodology (Hong et al., 2003). Additional research confirms that IS has been regularly measured as a technological problem with a technological solution (Ruighaver et al., 2007: 56), All these studies focusing on finding technological solutions to prevent vulnerabilities and attacks tend to overlook human and organizational aspects and do not adopt a socio-technical approach which involves human and organizational aspects (Dhillon and Backhouse, 2001: 140).

Having a training culture that brings awareness to issues as well as solid procedures and policies in place before any problem occurs is important. Similarly user feedback on policies and procedures is essential to improve their effectiveness. Kenneth et al. (2009) state that, when individuals are not motivated to follow procedures and protect information, security fails. Theodorakis (1994) indicate that employees indirectly cause majority of the problems by violating and neglecting existing organization IS policies.

From a theoretical perspective, information security systems (ISS) have "*technical, socio-technical*, or *social organizational roles*." According to the technical view, information security is a technical artifact and the emphasis in regards to security is on technical matters, with social implications in second place if at all exist. (Iivari and Hirschheim, 1996: 553). Technical view where users have no direct responsibility in ISS development measures considers poor technical quality and user resistance as the main causes for IS problems. The socio-technical view on the other hand considers both technical and organizational factors equally important, and points out the non-existence of an asymmetry between social and technical systems as the source of ISS problems (Iivari and Hirschheim, 1996: 556). Compared to technical view, users in socio-technical view have moderate participation and responsibility related to ISS activities. Finally the social view stresses the importance and priority of the development of organizational systems in respect to technical matters, where fulfilling users' preferences have major impact on the success of the ISS efforts.

As IT is designed and used by humans, human computer interaction (HCI) is very important, and IS solutions that do not consider how users will react to and comply with them are likely to fail. One of the main characteristics of socio-technical

studies is its consideration of the interaction between the technology that is constructed and the people who affect and are affected by the technology including the HCI component. The socio-technical view emphasizes *human* factors in security management. According to this approach, risks are separated as human risks and technical IS risks. Due to the sociological nature, risk is seen as subjective rather than objective. A variety of theories from different disciplines such as psychology and sociology have been used as a reference for exploration of IS risk management (Appari and Johnson, 2010).

A wide variety of models have been developed under various studies trying to examine the factors in IS. Kankanhalli et al. (Kankanhalli et al., 2003: 141) focus on prevention methods pointing out that deterrent and preventive efforts using control procedures are one way to deal with non-compliance and misuse of systems by employees. Torres et al. (Torres et al., 2006) outline some success factors based on current IS literature and security experts' perspectives. Reason (1997) focuses on safety factors that in certain cases prevent incidents such as human errors contributing to IS issues. Ives and Olson, (1984) identify user participation as an important element in IS risk. Fulford and Doherty (2003: 106) summarizes key factors (Siponen, 2000: 31; Von Solms, 1998: 174) contributing to effective IS management as: "*the commitment and support from information security management; conducting assessment of potential security risks and threats; the implementation of appropriate controls to minimize risks and threats; and the communication of security issues."*

A four-factor (Purpose, People, Plan, Progress) view is proposed by Tucker and Mohammed (1996) that leads to a successful implementation of IS. According to Mak, (2001: 263), planning, involvement, leadership, awareness, organic growth and teamwork are among the seven critical elements of an information model needed for successful IS implementations.

According to von Solms (von Solms, 2001: 504), information security is a multidimensional discipline integrating corporate governance. The information possessed by organizations is among its most valuable assets and is critical to its success. The top level management, which is ultimately accountable for the organization's success, is therefore responsible for the protection of its information (von Solms, 2001: 505). The important aspect of IS governance, which is crucial for enterprise wide effectiveness of information security, is the responsibility of top level

management. IS governance must be an integral and transparent part of corporate governance and should be aligned with the corporate governance framework.

Major factors found to influence IS in organizations are (Waly et al., 2012: 4); lack of awareness, lack of defining roles and responsibility, lack of communication and documentation, lack of reward and sanction systems, lack of reinforcement and practice.

1.4.1. Organizational Culture

It would make sense to also cover the organizational culture briefly before we delve into the separate domains of information security, safety, and quality cultures in each separate section. The short-hand, well-known, common, and simplest definition of organizational culture is "*the way things are done here"* (Bower, 1966; cited by Smit and Dellemijn, 2011: 23). According to Robbins (2001), organizational culture can be considered as the personality of the organization (Robbins, 2001; cited by Da Veiga and Eloff, 2010: 198) and is the social glue that binds the members of the organization together (Kreitner and Kinicki, 1992; cited by Da Veiga and Eloff, 2010: 198).

Organizational culture can be viewed as a combined effort between anthropology (Roethlisberger and Dickson, 1939; cited by Scott et al., 2003: 924) and sociology (Parsons, 1977; cited by Scott et al., 2003: 924), which also contributed to the scientific management techniques of Frederick W. Taylor and his successor Frank B. Gilbreth. These two underlying approaches form the platform for various theories and/or paradigms that study organizations (Burrell and Morgan, 1979; cited by Scott et al., 2003: 924). Anthropology uses interpretivism to explain culture via a metaphor for organization, defining organizations as being cultures. Sociology however uses functionalism to define culture, as something an organization owns. Pettigrew introduced the term "*organizational culture"* to literature in an article in "*Administrative Science Quarterly"* (Pettigrew, 1979: 572) even though Jaques referred to it as "*culture of factory"* as early as 1951 (Jaques, 1951; cited by Scott et al., 2003: 924).

Pettigrew's empirical study of a private British boarding school highly influenced by Burton Clark (Clark, 1970) emphasizes the influences of leaders and leaderships, which stresses the influence of Selznick's *Leadership in Administration* (Selznick, 1957). According to Selznick, two ideal types of enterprise exist; a rational

instrumental *organization* implying a technical instrument to gather human energies and direct them towards set goals and a value-infused *institution* implying an organic social entity, or culture.

Though roles, norms, and values all have been mentioned by Katz and Kahn in their "*The Social Psychology of Organizations"* (1978: 5), it wasn't until the late 80s when organizational culture according to (Scott et al., 2003: 925) has been defined by various scholars (Davies et al., 2000; Ott, 1989; Schein, 1988). The definitions include a wide range of social phenomena, such as language, behavior, beliefs, values, norms, assumptions, symbols of status and others. Among all these definitions, Edgar Schein's (Schein, 1985; 1988: 7) definition that utilizes a functionalist view seems to have the most acceptance and usage. Schein defines culture as "*The pattern of basic assumptions that a group has invented, discovered or developed, to cope with its problems of external adaptation or internal integration that have worked well and are taught to new members as the way to perceive, think, feel and behave."*

According to Schein, practices and behaviors, values and beliefs, and underlying assumptions form the three levels of culture. Practices and behaviors, which are hard to measure deal with organizational attributes, and are observed, felt, and heard within an organization by individuals. Values and beliefs which deal with goals, ideal norms, standards, and moral principles are measured through survey questionnaires. Underlying assumptions form the essence of the organizational culture.

1.4.2. Information Security Culture

IS culture requires more attention as social and cultural aspects of employee interactions within workplace and technology is an issue as reported by many (Guzman et al., 2008). Research indicates organizational culture and information systems management in general are correlated, which includes IS (Smit and Dellemijn, 2011: 31).

The compliance behavior is reported to be influenced by organizational subcultures causing conflicts within departments. Studies indicate for the compliance of IS, security culture plays an important role (Ma et al., 2008). Winkel defined security culture as "*the system of collective moral concepts, mindsets and behavior patterns anchored in the self-conception of a social unit and instructing its*

members in dealing with security threats" (Winkel, 2007: 223). Rotvold indicated security culture provided a positive effect on security compliance (Rotvold, 2008). Chang and Lin, examining the overall influence of organizational culture on the IS management implementations (Chang and Lin, 2007: 453) indicated that favorable organizational culture is needed for a suitable and effective IS management implementation, as well as technology and management's support.

Better understanding, developing and managing a proper information security culture inside an organization is not easy to accomplish. Industry researchers and academic scholars (Drevin et al., 2006; Ruighaver and Maynard, 2006; Van Niekerk and Von Solms, 2010; von Solms, 2006) agree that developing an appropriate IS culture is an effective way to manage user behavior to achieve a more effective IS program. Properly developed communication channels increase the effectiveness of IS matters on employee behavior (Bess, 2012: 162). What has not been made clear is how to develop and manage an appropriate IS culture. IS culture is defined as *the "collective norms, values and beliefs which control the behavior of the individuals within the organization with respect to information systems security"* (Van Niekerk and Von Solms, 2010: 478). IS culture is considered to be a subculture or a subset of the overall organizational culture (Schlienger and Teufel, 2003), and develops due to behavior of employees, in the same way that an organizational culture develops due to the behavior of employees in the organization (Hellriegel et al., 2001; Robbins et al., 2003).

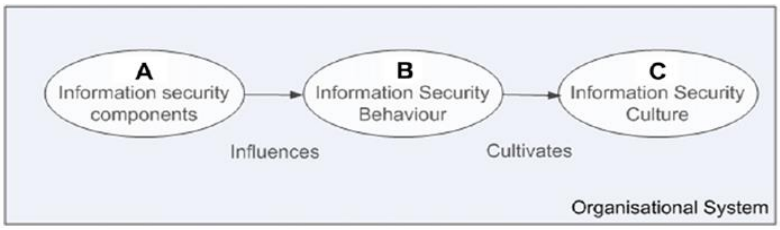
Why is Information security culture such an important component to IS? IS programs are ultimately dependent upon the organizational members to implement and maintain the technical and administrative controls in such programs. Because of this dependency, it is the human element that presents the greatest risk to an organization's security program (Chang and Lin, 2007; Van Niekerk and Von Solms, 2010; cited by Bess, 2012: 3). Since it is ultimately the human behavior, or people's actions which will operate the IS program then it becomes important to understand how the security related behaviors of the organizational members can be better understood and governed. Organizational culture has been found to be a significant factor in guiding and governing human behavior within an organization. Early research by Vroom and von Solms (2004) indicated that embedding security practices within the organizational culture could have a positive influence on IS (Vroom and von Solms, 2004). Because of this significant role, organizational

culture will influence the operational effectiveness of the IS program (Da Veiga et al., 2007).

The literature has commonly adopted Schein's (1985) organizational culture theory when addressing the topic, ignoring other critical dimensions of IS culture (Schein, 1985). Examples of these other critical dimensions include culture's ability to both enable and constrain an individual's behavior or actions as well as how an individual may think about things around them.

Da Veiga and Eloff approach the IS issue by defining the IS culture framework (ISCF) as three levels that build upon each other as shown in Figures 15, 16, 17 (Da Veiga and Eloff, 2010: 198). Level I on a higher level points out the influence of IS factors such as policies, procedures on the behavior of employees impacting the resulting IS culture as shown Figure 15.

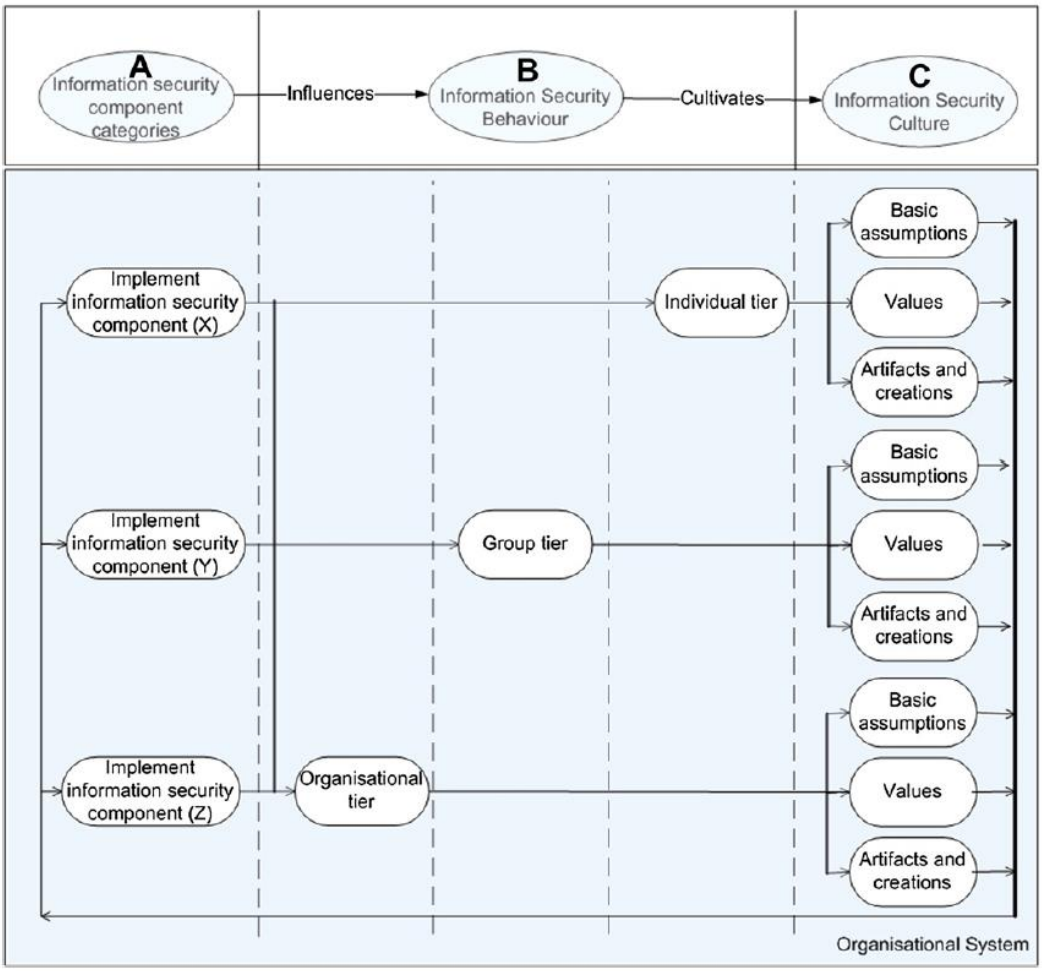
Figure 15: Level I of the Information Security Culture Framework



Source: A. Da Veiga & Eloff, 2010: 198

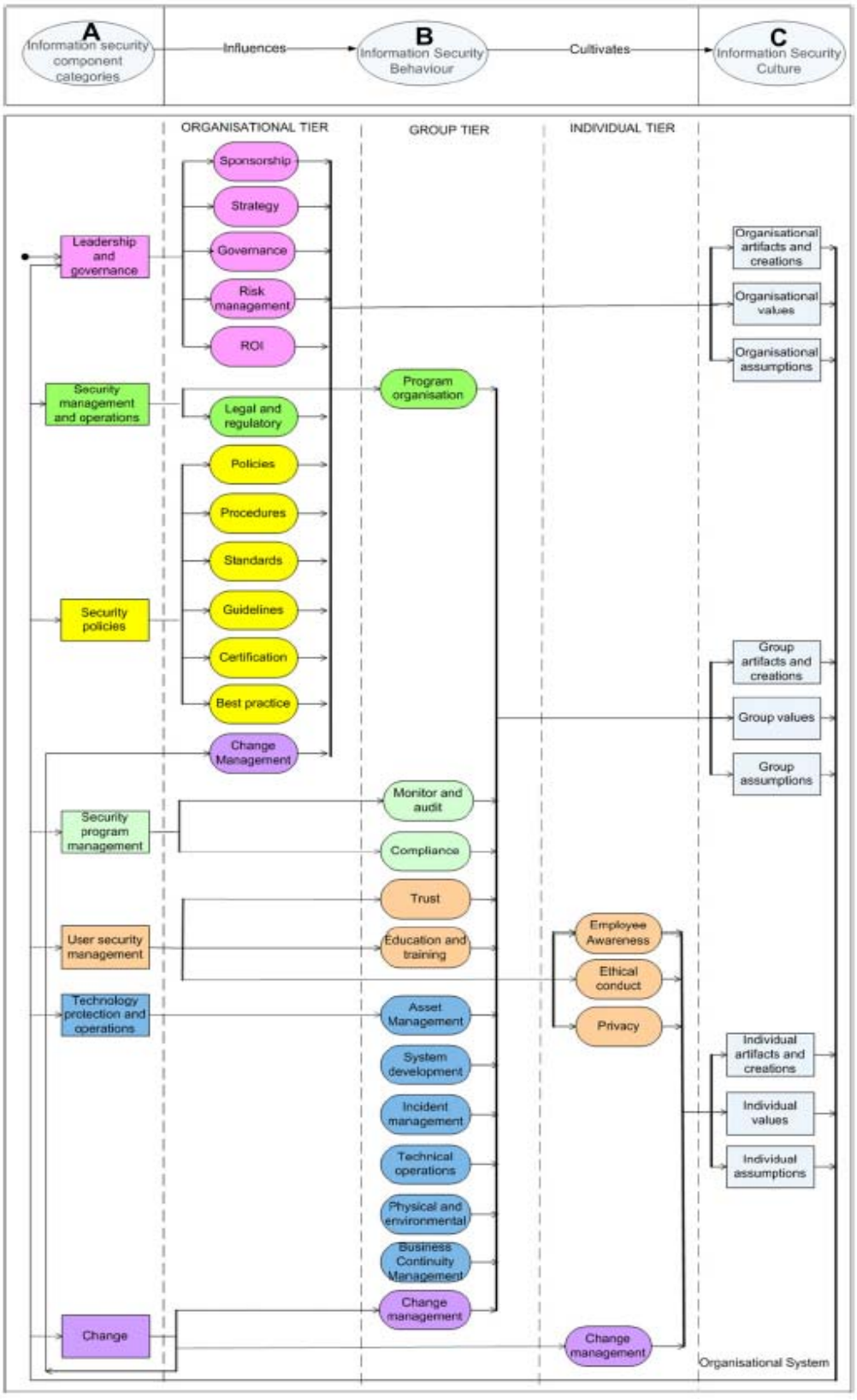
Decomposing level I into level II shows the interaction between different components of IS with the behavioral characteristics of the people either as individuals or as members of groups. This level also analyzes how groups function as well as the centralized versus decentralized operational structure of the organization. The security behavior sustained over time evolves into security culture with various assumptions, values, beliefs, practices and behaviors (artifacts). At the lowest level of decomposition, level III includes the seven categories of IS components defined from a previous study (Da Veiga and Eloff, 2007: 162). For each of the seven categories the corresponding behavioral entities for organizational, group and individual tiers are listed. From this behavioral list the corresponding behaviors, values, and assumptions are formed for organization, group and individuals.

Figure 16: Level II of the Information Security Culture Framework



Source: A. Da Veiga & Eloff, 2010: 199

Figure 17: Level III of the Information Security Culture Framework



Source: A. Da Veiga & Eloff, 2010: 200

1.5. THEORIES OF CONTINGENCY AND RATIONAL ACTION

Thompson defines an organization as a "*set of interdependent parts which together make up a whole*" (Thompson, 2011: 6,10). He perceives complex organizations as "*open systems, hence indeterminate and faced with uncertainty, but at the same time as subject to the criteria of rationality and hence needing determinateness and certainty."* Organizational structure of the organization is formed by the rational action to the environment where the ultimate goal is the survival of the system through an evolutionary process. The environment includes suppliers, customers, competitors, government regulatory agencies, public pressure that are all outside the organization's boundaries where the organization has little control, yet these environmental forces can potentially influence the organization's performance (Porter, 2008; Porter and Millar, 1985).

The contingency theory states that there must be a fit between the organizational structure and the organizational environment (Donaldson, 1995; Karlene and Martha, 1995). The degree of fit influences the performance and effectiveness level (Woodward et al., 1965; cited by Donaldson, 1995: 20). Changes in the environmental forces create a misfit with the organizational structure causing an imbalance, which eventually will reduce performance. In order to avoid this, an organization must respond to the changes in its environment in order to stay competitive and accomplish organizational goals by making rational adaptive changes to put the organization back to a balanced state. According to some researchers (Donaldson, 1995; Karlene and Martha, 1995), this is called as the *structural-adaptation-to-regain-fit model* (SARFIT).

The contingency model points out technology along with other environmental factors are the main components of organizational structure. According to Orlikowski (1992), technology has always been a central variable in organizational theory, informing research and practice. Barley (Barley, 1986, 1990) considers the way technology effect organizational structure as the trigger of structural change. Strategic adaption theory provides insights to this trigger of structural change. Miles and Snow (1978; cited by Croteau and Bergeron, 2001: 79) suggests "*Defenders, Prospectors, Analyzers, and Reactors"* are the four strategic types of organizations according to way they respond to adaptions of technology. The type of technological deployments vary with the chosen strategies (Croteau and Bergeron, 2001: 95).

The rational action perspective indicates that organizations are rational and reasonable and everything in the organization is planned, controlled, and orchestrated according to a business strategy where the outcomes are predictable (Thompson, 2011) and meet the needs of the organization. Many information researchers and practitioners have adopted the rational action approach in studying rationally planned strategies (Chan et al., 1997; Dhillon and Backhouse, 2001; Reich and Benbasat, 2000; Venkatraman et al., 1993). Specifically, the competitive strategy of Porter (Porter, 2008) and the value chain of Porter and Millar (Porter and Millar, 1985) have significantly influenced strategic thinking within the IT domain.

Together, the contingency theory and the rational action theory in addition to explaining why organizations have to act on the organizational IS change, they also state the process of this action is dynamic, and not static. Ironically, most security related best practices and management strategies are static, ineffective and dogma-based (Tippett, 2002).

1.6. INFORMATION SECURITY MANAGEMENT SYSTEMS

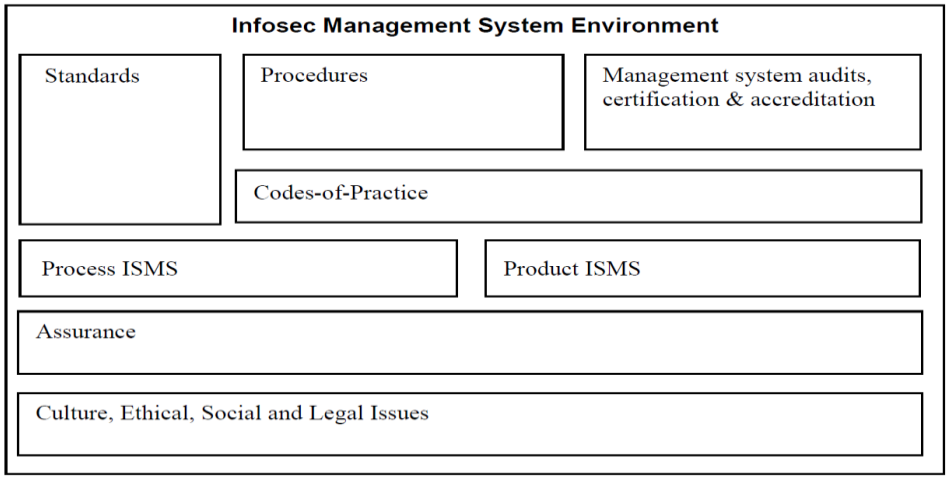
In order to address IS properly, organizations need to implement an IS management system (ISMS) or framework in some form or another. An ISMS as part of an organizational strategy includes several components such as processes, procedures, policies, resources, and planning activities regarding corporate governance, management issues, security culture, awareness, training, ethics and other human related issues, all within a business continuity, legal compliance, and a competitive edge perspective. In addition, as Werlinger, Hawkey, and Beznosov (2009) stated, ISMS or frameworks play an important role in safeguarding data and systems (Werlinger et al., 2009: 17). Research regarding the use of IS frameworks provide successful outcomes within a variety of IT domains and industries (Da Veiga and Eloff, 2010; Schweitzer, 1987; Straub and Welke, 1998). As an example, Straub and Wilke (1998) explained the benefits of using frameworks for risk management. Yet, despite the critical importance of IS, many organizations do not utilize existing security frameworks. According to the PwC survey, a great majority of participants indicated lack of methodology within their IS programs (PricewaterhouseCoopers, 2013a: 3).

Increased government interventions through regulations also cause increased IS requirements for many organizations (Gerber and von Solms, 2008:

125). As Moreira, Martimiano, Brandão, and Bernardes (2008); Tang (2008); and Williams (2008) stated, IS frameworks for information risk management are needed for compliance with government imposed regulations as well as efficient and effective IS systems (dos Santos Moreira et al., 2008; Tang, 2008; Williams, 2008). As a result of this increased security demand, many frameworks are available for organizations to explore and implement (Dunkerley, 2011: 16).

Among the various available conceptual models, Figure 18 below shows main components of an ISMS where process and products are handled separately (Eloff and Eloff, 2003: 131).

Figure 18: Components of ISMS



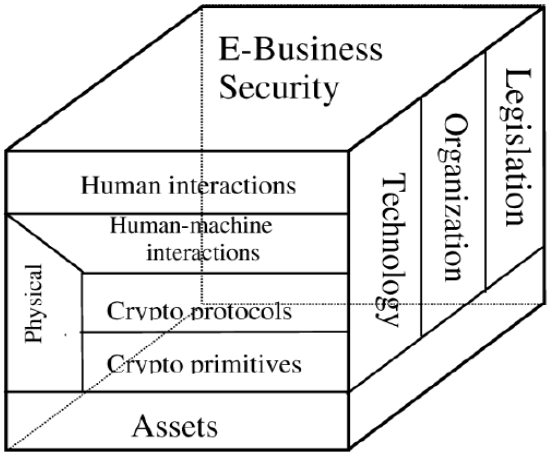
Source: Eloff & Eloff, 2003: 131

There are various models and approaches to ISMS (Eloff and Eloff, 2005). The ISO model, BS 17799 (ISO 17799) which was based on BS 7799 and later was renamed to ISO 27002 part of the ISO 27000 family is a guideline to implementing ISMS and functions based on a PDCA[4] (Plan-Do-Check-Act) cycle. The ISMS is a cyclic model that aims to ensure best practices are documented, reinforced, and improved over time. The layered multi-planes model proposed by Trček (2003: 337) integrates security related approaches. As shown in Figure 19, technological, organizational, legal issues along with e-security, human aspects, and physical assets are all part of the model. As protection and safeguarding of assets is the

[4] This model is explained in detail in section 3.4.1

primary focus, assets are central to the model. The main criticism about this model is that it does not address the strategic components but rather technical components.

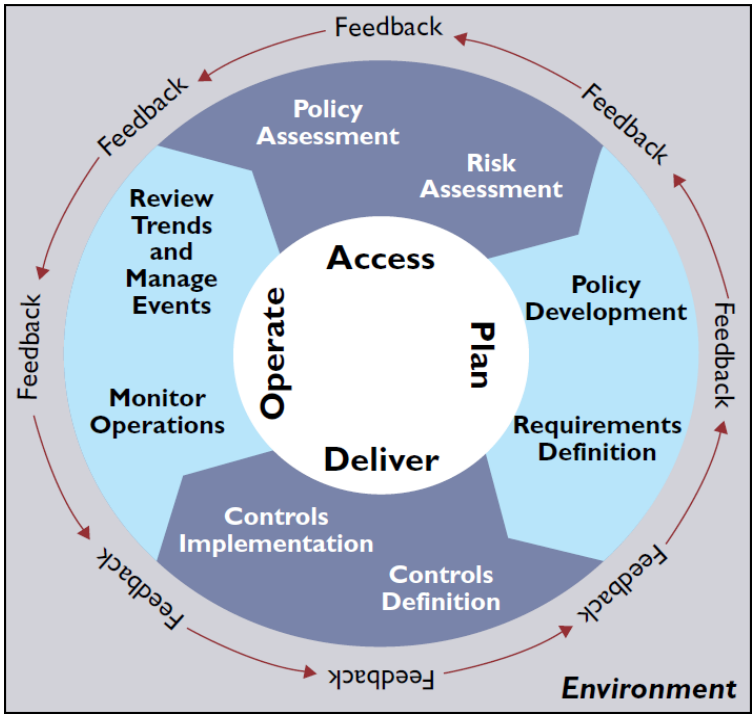
Figure 19: Layered Multi-Planes Model



Source: Trček, 2003: 337

Though it was initially developed for addressing e-commerce related security issues, the Policy Framework for Interpreting Risk in E-Business Security (PFIRES) Figure 20 (Rees et al., 2003: 102) has been applied to address general IS related matters of any organization. It was based on product and software development life cycle (PDLC, SDLC). The model consisting of four major phases: Assess Plan, Deliver and Operate similar to PDCA cycle was aimed at establishing information security. Due to its cyclic nature feedback is provided at all times throughout all four phases. As it is mainly aimed for establishing and maintaining IS, the model can be used as a starting point for a well-defined ISMS architecture.

Figure 20: PFIRES Life Cycle Model

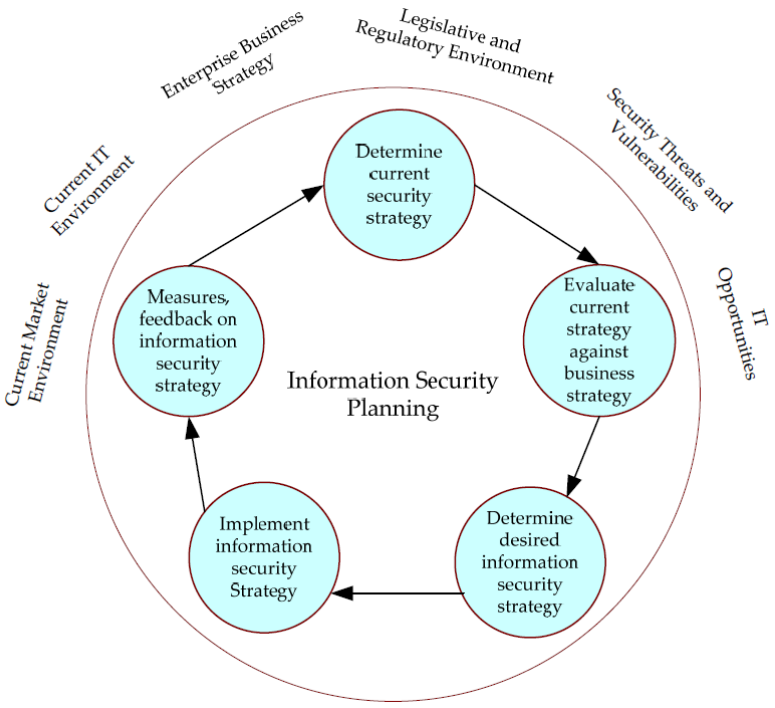


Source: Rees et al., 2003: 102

The model offered by META Security group as IS architecture (ISA) is similar to PDCA model and the four phases of the PFIRIS model. It consists of high-level objectives; roles and responsibilities; a policy framework; a process catalogue; a services framework; domain structure; trust-level definitions; tools, models and templates, and finally technology options. A different model Meta group provides other than the ISA allowing a strategic approach for IS matters consists of six components as; organization; management and governance; budget; policy management; processes, and technology (Meta Security Group, 2000; cited by Eloff and Eloff, 2005: 12).

IS planning model in Figure 21 developed by Perks & Beveridge (2003) highlights the external environmental factors affecting the IS systems as well as the internal actions to be taken in order to develop a security plan. The model points out legislative, regulatory, IT, market environments as well as business strategy and IT opportunities. It is based on a feedback cycle bringing continual improvements to the security plan.

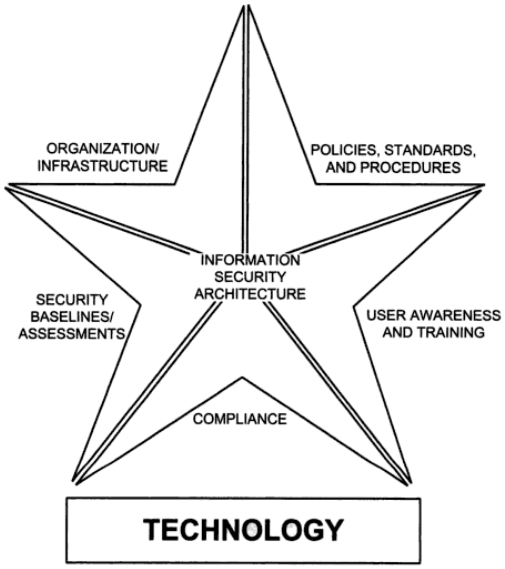
Figure 21: Information Security Planning Model



Source: Adapted from Perks & Beveridge, 2003

According Tudor (2002: 5), the model he proposes for IS has five main elements form for any IS architecture. He indicates that the security architecture is a process and is not something one can purchase (Tudor, 2002). As shown in Figure 22 the architecture is based on the five balanced components.

Figure 22: Information Security Architecture



Source: Tudor, 2002: 5

Though all three of Trček, Tudor, and the META Group emphasize the importance of an integrated approach, none provide a comprehensive set of multidisciplinary controls. The ISMS proposed by BS 7799 Part 2 (BS17799/ISO27002), the PFIRES, and the IS planning model are all based on a life-cycle approach consisting of four or five major cyclic phases.

1.7. REGULATIONS AND ISO 27000

Gerber and von Solms point out, "w*ith information security being the focal point of business in the media and in legislatures around the world, organizations face complex requirements to comply with security privacy standards and regulations"* (Gerber and von Solms, 2008: 124). According to The American Heritage Dictionary (The American Heritage Dictionary, 2014), the definition of standard is given as "*An acknowledged measure of comparison for quantitative or qualitative value; a criterion. A degree or level of requirement, excellence or attainment".* According to ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), a standard is generally defined as "*document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the*

optimum degree of order in a given context" (ISO-IEC, 2004). Within an unregulated field of IT, standards are considered essential (Williams, 2006: 415). Standards are implemented to facilitate inter-organizational communication and co-operation. Their scope may vary depending on the type of information to be exchanged (Söderström, 2004).

Two types of standards exist in the form of *formal* and *de facto*. Government or official industry bodies develop formal standards while market use and vendor promotion dictate de facto standards. De facto standards in computing such as Microsoft Windows operating systems are the main force driving the change within the industry itself (Dennis, 2002; cited by Williams, 2006: 415).

In order to achieve certain levels of quality within any given industry, standards are followed and implemented. Within IT and technology domain, standards become even more important as a multitude of hardware, software, databases, operating systems and applications are the end result of a diverse environment with lack of standards. In such an environment proper legislation is difficult to create which is why legal requirements instead of regulations are integrated into formal standards (Williams, 2006: 415). Existing principles of IS can be viewed from legal and standard perspectives. Without the legal dimension of security, IS governance cannot be achieved properly (von Solms, 2001; von Solms and von Solms, 2004).

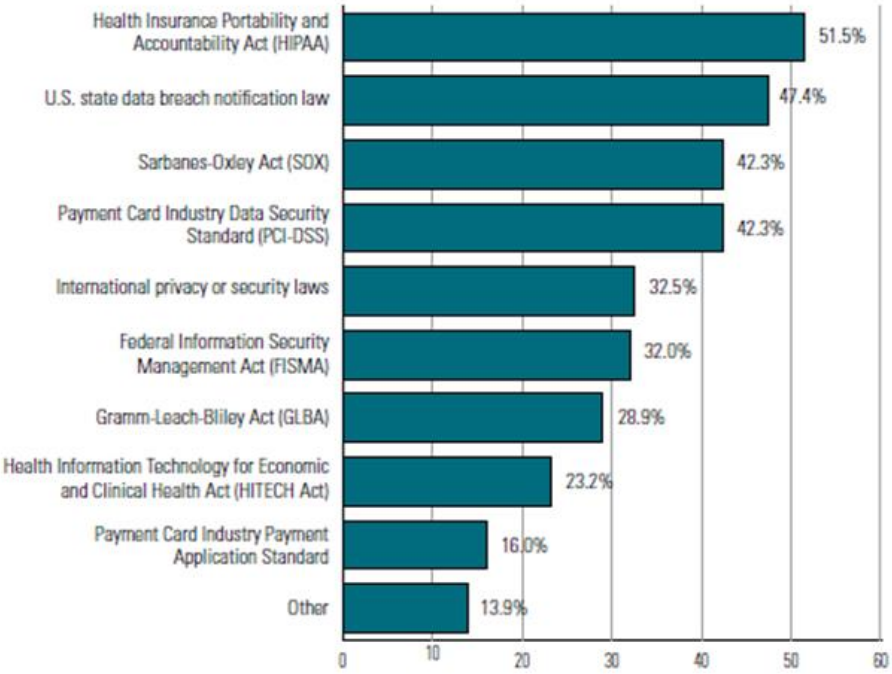
There is a difference between laws and standards as far as the computing landscape is concerned. While standards are set of rules and procedures documented by a set of experts within a given field that provide benchmark(s) for products or services, laws regulate the use, collection, development and ownership of data being used to protect the integrity and secrecy of information (Pfleeger, 1997). Standards are procedures and guidelines for best practices, consistency and interoperability among systems. Monitoring these guidelines and making sure the rules and procedures within are followed ensures their effectiveness. Laws indicate liability on the consequences of actions that can be enforced, which is why they are effective to the degree they are enforced.

Health is an important domain dependent on accurate and timely information for proper patient care and the management of health services. Standards are therefore crucial to the reliability information sharing, information compatibility and its effectiveness in healthcare. Although there are various standards worldwide, from a legal perspective most are not binding. In the United States, the *"Health Insurance*

Portability and Accountability Act (HIPAA) of 1996" is a legally binding, detailed health information protection policy which didn't take effect till 2005. HIPAA promoted the development of electronic healthcare transactions and specifically addressed the important issues of privacy and security for health related information (U.S. Department of Health and Human Services, 2014). In 2003 the US congress went further to enact the "*Standards for Privacy of Individually Identifiable Health Information"*, otherwise known as the "*Federal Medical Privacy Rule*." According to some, such level of detail integrated to the rule is hard to comply with given current medical information systems and a lack of understanding of even basic security measures in medical organizations (Lederman, 2004). As organizations have to comply with government imposed regulations and laws, IS frameworks that emphasize governance become more important. Research on the usage of these frameworks to accommodate HIPAA compliance is growing (Appari et al., 2009; Van Niekerk and Von Solms, 2010). The privacy and security aspect of HIPAA applies to any organization that interacts with data, therefore it is not only healthcare institutions or organizations but any other organization that deal with private data of individuals are also subject to HIPAA In this sense HIPAA has a bigger impact in the IS domain (Bilbao-Osorio et al., 2013).

According to the 2011 CSI Computer Crime and Security survey, majority of the participants were subject to a number of laws, regulations, and standards that deal with private data as shown in Figure 23 (Richardson, 2011: 6).

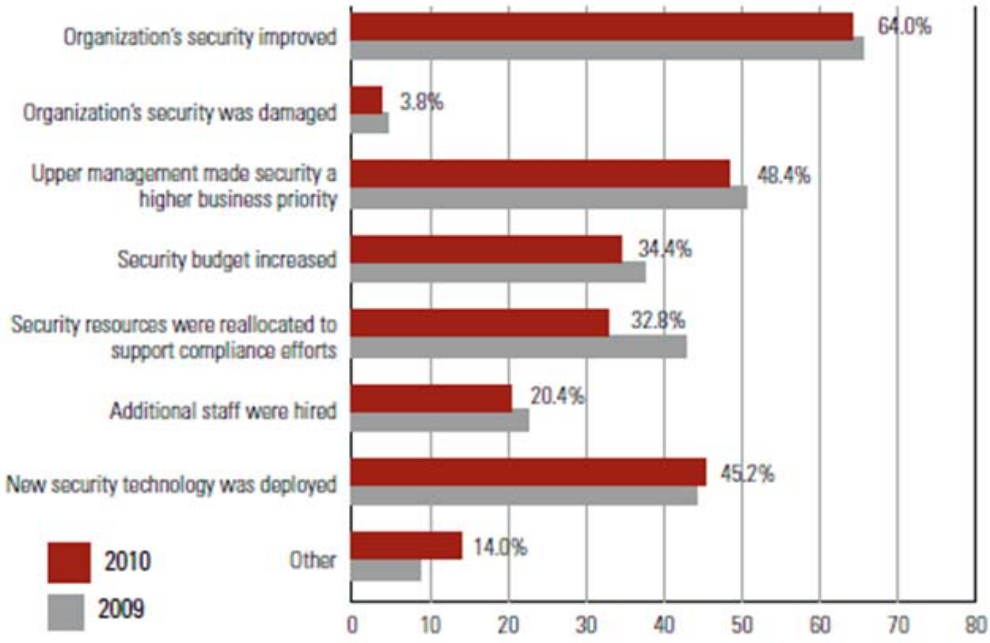
Figure 23: Laws and Industry Regulations Applicable to Organizations



Source: Richardson, 2011, based on 2010 CSI Computer Crime and Security Survey

The same survey indicated regulatory compliance efforts have had a positive effect on security programs as shown in Figure 24 (Richardson, 2011: 32).

Figure 24: Effect of Regulatory Compliance Efforts on Information Security



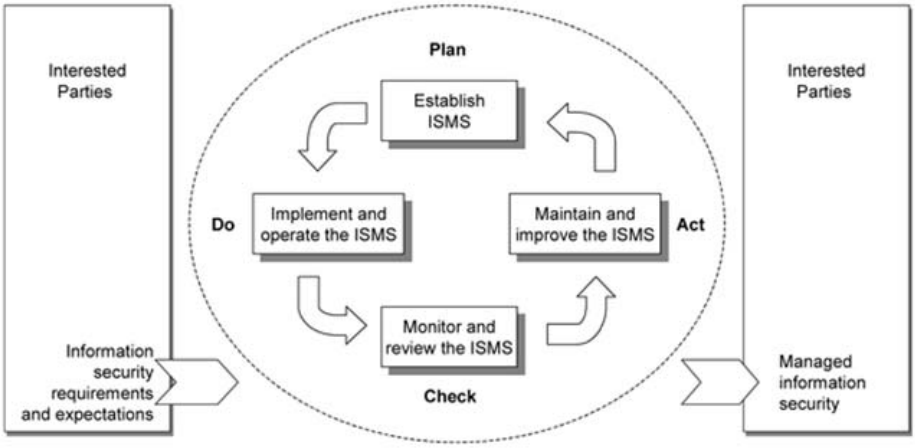
Source: Richardson, 2011, based on 2010 CSI Computer Crime and Security Survey

Regulation of HIT for the purposes of improving healthcare is also a hot topic. Regulatory requirements do not apply to HIT; specifically to standalone software applications not embedded in hardware such as electronic health records EHR or CPOE systems. However software embedded in a medical hardware is regulated (Young, 1987). IOM's report (Institute of Medicine, 2012) has few recommendations on the issue implying the technology exists in isolation (Longhurst and Landa, 2012). Depending on the improvements in healthcare the potential for a conditional control of HIT software by the US Food and Drug Administration similar to medical devices is suggested. The idea that HIT being regulated and controlled by FDA even with the proper framework is infeasible due the shortage of skilled health IT workforce (Goedert, 2011). This potential also has certain drawbacks as seen by the consequences of the regulation of blood bank software by FDA that began in 1994 (Weeda and O'Flaherty, 1998). Though the regulation provided quality improvements, major IT companies exited the industry due to regulatory requirements leaving small number of software vendors, which limited the innovations and advancements in blood banking software (MacPherson et al., 2009). Recommended strategies to address software safety are largely based upon increasing standardization and introducing mechanisms for oversight (Institute of Medicine, 2012; Singh et al., 2011; Walker et al., 2008), though some argue that such measures may hamper innovation (Longhurst and Landa, 2012).

International IS management standards are important factors and play a key role in managing and in most cases certifying IS systems of organizations (Siponen and Willison, 2009).

ISO/IEC 27000 is a family of international IS related standards prepared by Joint Technical Committee (ISO/IEC JTC 1) dedicated to the development of international management systems standards for IS, otherwise known as the IS Management System (ISMS) family of standards (ISO/IEC-27000, 2014). These standards are applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations). The main standard is the ISO/IEC 27001, the ISMS Requirements, that has two versions. The initial version was ISO 27001:2005 which focused on the PDCA cycle for the implementation of security measures as shown in Figure 25 below.

Figure 25: PDCA Model Applied to ISMS Processes



Plan (establish the ISMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.
Check (monitor and review the ISMS)	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

Source: ISO/IEC-27000, 2014, based on 27001:2005

The 27001-2013 version puts more emphasis on measuring and evaluating how well an organization's ISMS is performing (Quality Services Limited, 2013), and there is a new section on outsourcing emphasizing the fact that many organizations rely on third parties to provide some aspects of IT (British Assessment Bureau, 2013). The Plan-Do-Check-Act (PDCA) is not emphasized anymore like it was in 27001:2005.

Instead, other continuous improvement processes like Six Sigma's DMAIC (Define, Measure, Analyze, Improve , Control) method can be implemented (Dionach, 2011). Overall, 27001:2013 is designed to fit better alongside other management standards such as ISO 9000 and ISO 20000, and it has more in common with them (The Pragmatic Auditor, 2013). Following are the 14 main groups including the number of controls within each group part of the new version (Gamma, 2013).

- *A.5: Information security policies (2 controls)*
- *A.6: Organization of information security (7 controls)*
- *A.7: Human resource security - 6 controls that are applied before, during, or after employment*
- *A.8: Asset management (10 controls)*
- *A.9: Access control (14 controls)*
- *A.10: Cryptography (2 controls)*
- *A.11: Physical and environmental security (15 controls)*
- *A.12: Operations security (14 controls)*
- *A.13: Communications security (7 controls)*
- *A.14: System acquisition, development and maintenance (13 controls)*
- *A.15: Supplier relationships (5 controls)*
- *A.16: Information security incident management (7 controls)*
- *A.17: Information security aspects of business continuity management (4 controls)*
- *A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)*

ISO 27000 family of standards have been utilized heavily due to their increasing popularity. Within healthcare, it has been found to be a critical element in addressing compliance to HIPAA requirements (Myler and Broadbent, 2006). Healthcare organizations should consider implementing an ISO security framework to fully comply with legislative and regulatory requirements (Boynton, 2007; Harris and Cummings, 2007; Thomas and Botha, 2007). Saint-Germain, points out that ISO 27000 family of standards provides organized collection of practices and controls that can address the key concerns of CIA that are the focus of regulatory IT security efforts (Saint-Germain, 2005). According to a study Chang and Lin conducted to explore the use of standards assisting in HIPAA compliance, ISO 27002 was found to be a crucial element for an acceptable level of information assurance using the CIA concepts (Chang and Lin, 2007). ISO 27000 was designed to work across a wide array of organizations and is intended to help organizations cost effectively apply security controls aimed at protecting systems and data (Humphreys, 2006).

CHAPTER TWO
PATIENT SAFETY

As Sir Cyril Chantler of the Kings Fund said, "*Medicine used to be simple, ineffective, and relatively safe. Now it is complex, effective, and potentially dangerous*" (Institute of Medicine, 2012: ix).

2.1. SAFETY

Many dictionaries define safety with the following characteristics; "*Relative freedom from danger, risk, or threat of harm, injury, or loss to personnel and/or property, whether caused deliberately or by accident*" (BusinessDictionary.com, 2014); "*The condition of being safe; freedom from danger, risk, or injury*" (The American Heritage Dictionary, 2014); "*The condition of being safe from undergoing or causing hurt, injury, or loss*" (Merriam-Webster.com, 2012).

Though the term itself mostly draws attention to the human safety, the safety regarding environment and financial assets are also related due to the risk component of the definition.

According to Leveson, safety is defined as "*the absence of accidents, where an accident defined as an event involving an unplanned and unacceptable loss"* (Leveson, 1995; cited by Leveson, 2011: 57). Risk in the form of low and acceptable risk also is related to the safety (Ayyub, 2003; Harms-Ringdahl, 2003; Lowrance, 1976; Manuele, 2003, 2013; Misumi and Sato, 1999). The relation of risk with safety in the form of the lower the risk the higher the safety has been questioned by some researchers as well (Möller et al., 2006). The safety and risk considered by many as the antonym of each other is well analyzed by (Aven and Renn, 2009) indicating situations for broad risk perspectives that refer to uncertainties beyond probabilities and expected values hence, acceptable risk plays an important role defining safe and safety.

Associating risk with safety as the antonym provides simple definitions for safe and safety; although safety from this perspective is a subjective judgment depending on what is an acceptable risk and what is not (Aven, 2014). However approaching safety as absence of accidents, losses etc., illustrates a different picture for the definition. Dealing with future when events, consequences, and

uncertainties are all unknown, speaking of high or low safety is not possible. We can only refer to the probability of safety being high or low. Hence safety is observed as an event with no occurrence of undesirable events and consequences. The definition of risk is closely associated with this view defined by Rosa (Rosa, 1998; 2003; cited by Aven and Renn, 2009: 1) as "*a situation or event where something of human value (including humans themselves) is at stake and where the outcome is uncertain."*

The concept of security also is related with the safety. Security has to do with intentional incidents and events such as terrorist attacks, burglary, etc. whereas safety deals with accidental situations. In this view since risk as part of safety does not differentiate between intentional or unintentional events or consequences, it is safe to say security is associated with safety.

2.1.1. Patient Safety

The famous report "*To Err Is Human"* from Institute of Medicine (IOM) defines patient safety as "*freedom from accidental injury*."(Institute of Medicine, 1999: 4) This is the primary safety goal from the patient's perspective. The National Patient Safety Foundation has defined patient safety as "*the avoidance, prevention and amelioration of adverse outcomes or injuries stemming from the processes of healthcare*" (National Patient Safety Foundation, 2014). According to NPSF, safety does not reside in a person, device or department, but emerges from the interactions of components of a system. According to Leveson, safety is an emergent system property and needs to be addressed throughout the lifecycle of HIT systems (Leveson, 2011: 64). The safety of patients is not solely dependent upon HIT systems on their own but is influenced by their interactions with users and other technology in a given environment (Coiera, 2003: 210). Patients are harmed when interactions between system components (human and machine) create unsafe states (Ash et al., 2004). Safety issues involving IT are not unique to healthcare (Jackson et al., 2007), but this sector has lagged behind other industries in addressing such problems (Institute of Medicine, 2012).

There have been various studies regarding safety. Harvard Medical Practice Study 1, 2, 3 touched on the safety issue and specifically about adverse events, negligence, nature of adverse events, negligence malpractice, and adverse events (Brennan et al., 1991; Leape et al., 1991; Localio et al., 1991); however it was the

famous IOM report that had the most effect and triggered a new phase in patient safety within healthcare. The IOM report "*To Err Is Human"* estimated that 44,000-98,000 lives were lost every year in the US due to medical errors in hospitals and started a revolution to improve the quality of care (Institute of Medicine, 1999: 1). With an emphasis on improving quality which stated healthcare should be "*safe, effective, patient-centered, timely, efficient, and equitable*", better results were thought to be achievable (Institute of Medicine, 2001: 6).

New research indicates medical errors as the third leading cause of death in the United States, stressing the importance of patient safety (James, 2013).

Patient safety is considered as a critical component of quality (Kohn et al., 2000), yet further research documented deficiencies in the quality and safety of healthcare. According to McGlynn et al., evidence-based practice is only followed 55% of the time (McGlynn et al., 2003: 2642). Further studies have reconfirmed that medical errors continue to be prevalent, as more than 1.5 million preventable adverse drug events occur (Aspden et al., 2006).

According to Page, defenses against threats to patient safety are created when leaders and managers promote evidence based practice; when the capabilities of the workforce are understood and maximized; when work processes are designed to reduce errors in patient care; and when a culture of safety is created and sustained (Page, 2004).

Adverse events affecting patient safety can emerge as a result of the interaction with the care system during care delivery in all care settings. Human, systems, and technological errors can trigger these events, which are either a direct consequence of treatment or a failure to undertake an action that should have been completed.

Despite the big emphasis, safety especially during hospital stays continues to be an issue as various studies suggest. According to Classen et al., adverse events continue to occur in as many as one-third of hospital patients (Classen et al., 2011: 581). Even in hospitals with programs heavily focused on improving patient safety, adverse events affecting hospitalized patients occur (Landrigan et al., 2010). Compared to the inpatient care, ambulatory settings have even more safety related errors affecting patient safety as more medical care is delivered outside hospitals than inside (Institute of Medicine, 1999). This is further supported by a review of malpractice claims which concluded 52% of all paid malpractice claims for all

physician services involved ambulatory services, and almost two-thirds of these claims involved a major injury or death (Bishop et al., 2011: 2427).

The types of errors seen (Institute of Medicine, 1999), the relative importance of patient responsibility for following through on care decisions, and the different organizational and regulatory structures in place (Gandhi and Lee, 2010) are the major differences between inpatient and ambulatory settings regarding patient safety, which suggests interventions to improve hospital safety may not be applicable in the ambulatory settings (Hammons et al., 2001). According to a 10-year review of ambulatory patient safety literature, despite some progress, major gaps remain with virtually no experiments or demonstrations shown to improve patient safety in ambulatory settings (Lorincz et al., 2011).

2.1.2. Safety Culture

Within organizational research domain, there has been much debate regarding whether safety culture and safety climate refer to the same topics. These two concepts have been frequently used synonymously and interchangeably (Cox and Flin, 1998: 191) to describe organizational attributes that reflect safe work environments (Guldenmund, 2000). Various studies within the organizational literature about the nature, validity and applicability of the concepts of "*culture*" and "*climate*" do exist (Cooke and Rousseau, 1988; Flin et al., 2000; Guldenmund, 2000; Schein, 1984, 1990; Schneider, 1975).

The Chernobyl disaster back in 1986 triggered a high set of interest for the term "*Safety Culture*". In fact, the term is used by International Atomic Energy Agency (IAEA) investigators following the Chernobyl disaster (International Nuclear Safety Advisory Group, 1991) to classify various organizational gaps which contributed to the nuclear power accident (Mearns and Flin, 1999; cited by Palmieri et al., 2010: 102). Management's insufficient safety attentiveness and a lack of safety programs coined the term "*poor safety culture*" (International Nuclear Safety Advisory Group, 1991; cited by Palmieri et al., 2010: 102). The aviation industry's work on improving cockpit crew performance due to safety culture concerns (Helmreich and Wilhelm, 1991; cited by Palmieri et al., 2010: 102) and the aftermath of the nuclear accident together formed the proper setting for the early safety culture research (Sexton et al., 2000: 746).

Even before the Chernobyl disaster there was research being undertaken. Zohar (1980: 661) is given credit for the foundation of the organizational safety culture research, due to his work in Israel in manufacturing industry, studying occupational safety. He used the term *safety climate* referring to the organizational attributes contributing to employee safety. "*Safety climate refers to the perceptions and attitudes about safety as an integral part of the work environment"* (Zohar, 2002; cited by Palmieri et al., 2010: 102).

According to Zohar (2003: 125), "*safety climate relates to shared perceptions with regard to safety policies, procedures and practices*" while according to Flin (2007), culture as described in literature is less tractable and more complex than climate. Despite this ongoing debate, the concept of "*safety culture*" is accepted more as a valid construct to measure and develop improved safety performance in the form of injury rates, accident rates, and patient safety throughout a range of industries including but not limited to aerospace, manufacturing, healthcare, off-shore oil and gas, maritime, construction, highway safety, and agriculture.

In order to measure perceptions about safety awareness of individuals, safety climate instruments were designed and created (Zohar, 1980). Soon after the IOM report (Kohn et al., 2000), the focus shifted to measurement of group level representing shared perceptions of workers in regards to management safety practices (Zohar and Luria, 2005).

There has been a variety of definitions of safety culture in the literature, each having their own perspective. According to Turner et al., safety culture is "*the set of beliefs, norms, attitudes, roles, and social and technical practices that are concerned with minimizing the exposure of employees, managers, customers, and members of the public to conditions considered dangerous or injurious"* (Turner et al., 1989). Von Thaden and Gibbons defined safety culture as *"the enduring value and prioritization of worker and public safety by each member of each group and in every level of an organization"* (von Thaden and Gibbons, 2008: 7). The most widely accepted definition of safety culture comes from the nuclear power industry (Advisory Committee for Safety in Nuclear Installations, 1993: 23).

> *The safety culture of an organization is the product of individual and group values, attitudes, perceptions, competencies and patterns of behavior that determine the commitment to, and the style and proficiency of, an organization's health and safety management. Organizations with a positive safety culture are characterized by communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of preventive measures*.

Safety attitudes and shared values also played key roles. According to Mearns et al., safety culture forms the environment within which individual safety attitudes develop and persist and safety behaviors are promoted (Mearns et al., 2003). The underlying norms, implied assumptions, and values about safety shared by the employees of the organization form the essence of organizational safety culture (Guldenmund, 2000; Mearns and Flin, 1999).

In their collaborative study of "*Safety Culture: An Integrative Review*", Wiegman et al. (2004: 123) indicate the following characteristics that are common to various definitions of safety culture found in the literature regardless of the industry;

- *Safety culture is a concept defined at the group level or higher that refers to the shared values among all the group or organization members.*
- *Safety culture is concerned with formal safety issues in an organization and closely related to, but not restricted to, the management and supervisory systems.*
- *Safety culture emphasizes the contribution from everyone at every level of an organization.*
- *The safety culture of an organization has an impact on its members' behavior at work.*
- *Safety culture is usually reflected in the contingency between reward systems and safety performance.*
- *Safety culture is reflected in an organization's willingness to develop and learn from errors, incidents, and accidents.*
- *Safety culture is relatively enduring, stable, and resistant to change.*

Safety culture also relies on certain theories such as high reliability theory (HRT) or normal accident theory (NAT). NAT represents a sociological perspective (Perrow, 1984; cited by Palmieri et al., 2010: 106), while HRT reflects an organizational psychology perspective (Roberts, 1990; Weick and Sutcliffe, 2001), and the so-called aviation framework (Helmreich et al., 1993) represents a quasi-theoretical human factors perspective (Gregorich et al., 1990). The common pattern among these three approaches is that culture is viewed as a key determinant for safety research in different ways. According to the sociological approach of NAT, safety is viewed as a system property not fully dependent on individual behaviors and performance (Perrow, 1994). NAT points out safety can be enhanced through organizational design and management, by reducing complexities, applying flexible policies, and procedures, and avoiding poorly designed processes and systems(Perrow, 1999). According to Perrow (1999: 354), "*the importance of safety culture is like the metaphor of an accident residing in the complexity and coupling of*

the system itself, not in the failures of its components which means some accidents are simply normal and unavoidable in the course of work." On the other hand, HRT is dependent on the ''*collective mindfulness''* of employees where circumstances are viewed from different angles and perspectives to avoid operational failures resulting in accidents (Weick and Roberts, 1993; Weick and Sutcliffe, 2006; cited by Palmieri et al., 2010: 107).

Aviation perspective differs from NAT and HRT in the sense that it does not utilize a theoretical framework to generate knowledge (Palmieri et al., 2010). It is based on methodologies related to critical incident (Flanagan, 1954; Woods and Shattuck, 2000; cited by Palmieri et al., 2010: 108) and critical decision (Klein et al., 1989), which present a deductive approach to cumulate knowledge via incident evaluation including describing the situation, recording possible influences, reviewing the preceding issues, and considering interactions (Carlisle, 1986; cited by Palmieri et al., 2010: 108).

Industrial safety studies whether (culture or climate) have a longer history than healthcare safety studies as they cover a timeframe of over 25 years. (Cooper and Phillips, 2004; Guldenmund, 2000; Zohar et al., 2007). Worker safety culture and climate have traditionally been the focus of industries such as steel manufacturing, oil and gas drilling, and high technology-use industries such as nuclear power plants, chemical processing plants, and the commercial aviation industry (Katz-Navon et al., 2005; Reason, 1998). Initially, studies of worker safety in the healthcare also have been the main focus attempting to show the effects of safety culture and climate in hospitals on worker's behaviors and performances (Flin, 2007; Gershon et al., 2000; Stone et al., 2006; Stone et al., 2007). Industrial studies aimed at the relationship between safety and safety performance try to reduce worker injuries and accidents, and to prevent large scale disasters (Cooper and Phillips, 2004; Guldenmund, 2000; Reason, 1998).

2.1.3. Patient Safety Culture

The patient safety culture is defined as the underlying assumptions of the priority of patient safety at the hospital and unit levels (Sexton et al., 2006; Zohar et al., 2007). Creating a culture of safety in hospitals requires the institutionalization and legitimization of patient safety as the priority concern for the organization and the interdisciplinary providers of care (McKeon et al., 2006).

Healthcare organizations, including hospitals, must develop a culture of safety in which the workforce and its patient care services are clearly focused on improving the reliability, quality, and safety of care (Kohn et al., 2000: 14). A culture of safety should include these components: (a) safety as a priority communicated by all levels of leadership; (b) frequent, open, and truthful staff communication by all levels of leadership; and (c) expressed organizational value in learning from errors and mistakes (Singer et al., 2003: 113).

Page has described a patient safety culture as one that vigilantly monitors for unsafe situations, cultivating attitudes and behaviors that enhance patient safety (Page, 2004: 289) indicating that an organizational culture among others is an important defense against threats to patient safety. The patient safety culture enforces a non-punitive error-reporting environment, and uses data analysis to understand causes of error. The safety culture is understood to be a "*performance shaping factor that guides the many discretionary behaviors of healthcare professionals in each patient interaction*" (Nieva and Sorra, 2003: ii17). Yet creating a culture of safety in healthcare organizations, specifically hospitals, has not progressed as rapidly as providers and consumers had anticipated (Brennan et al., 2005; Leape and Berwick, 2005; Page, 2004). Currently, a culture exists of "*naming, blaming and shaming*" that focuses on the individual rather than the systems that contributed to error (Page, 2004: 27). The focus has been on "who" was responsible, rather than "what" happened (Bagian, 2006: 289). Improving the quality and safety of patient care requires an organizational commitment to a culture of patient safety that maintains vigilance in monitoring for threats to patient safety (Nieva and Sorra, 2003; Scott et al., 2003).

In the healthcare literature, safety culture and climate, and attitude, are descriptions correlated for the same phenomena (Gaba et al., 2003) and are all suggested to appropriately represent the construct of safety culture (Nieva and Sorra, 2003; Sorra and Nieva, 2004). Human error is among the leading causes of accidents in major industries including healthcare (Bogner, 1994; Carayon et al., 2003; Cook and Woods, 1994; James, 2013; Kohn et al., 2000; Leape, 1994; Wears and Perry, 2002). A strong safety culture can help minimizing medical errors.

2.1.4. Patient Safety Risk Factors

Based on the findings of the famous IOM report "To Err is Human" (Institute of Medicine, 1999), Thompson (2002) in a statement given to U.S. Department of Health & Human Services stated that "*liability system and the threat of malpractice, which discourages the disclosure of errors affect patient safety negatively as most errors and safety issues go undetected and unreported, both externally and within healthcare organizations."*

Patients are an important part of the big safety picture. In addition to patients, there are other major factors that affect patient participation in safety related behaviors (Davis et al., 2007: 260);

- *Patient-related: patients' knowledge and beliefs about safety; emotional experiences with healthcare delivery and relevant coping styles; and demographic characteristics.*
- *Illness-related: stage and the severity of the patients' illness(es); symptoms; treatment plan; patients' health outcomes; and prior experience of illness (and prior experience of patient safety incidents).*
- *Healthcare professional (HCP)-related: healthcare professionals' knowledge and beliefs about safety and patients' involvement in it; and the way in which healthcare professionals interact with patients.*
- *Healthcare setting (HCS)-related: type of healthcare setting – primary, secondary or tertiary care setting; and admission process – emergency or elective.*
- *Task-related: the specific patient actions /behaviors required for involvement in safety.*

Healthcare worker safety and healthy workplace are contributing factors and are frequently linked with patient safety (Yassi and Hancock, 2005: 33). According to IOM, the work environment and its effect on healthcare employees play a key role in patient safety and outcomes (Institute of Medicine, 2004). The safer healthcare workers in their jobs are, the safer the patients will be. "*A healthy workplace is defined as one in which healthcare workers are able to deliver higher quality care, and worker health and safety and patient health and safety are mutually supportive*" (Eisenberg et al., 2001; Koehoorn et al., 2002; cited by Yassi and Hancock, 2005: 33). An important part of promoting patient safety must therefore focus on how to promote a healthy healthcare workplace (El-Jardali and Lagace, 2004; cited by Yassi and Hancock, 2005: 33).

Medication use processes are another factor all together affecting patient safety. The process of making sure that patient gets appropriate medication use is a complex process involving multiple organizations and professionals from various

disciplines; knowledge of drugs; timely access to accurate and complete patient information; and a series of interrelated decisions over a period of time. Related to medication, prescribing, dispensing, administering, monitoring, systems and management control are all potential risk areas where errors can affect patient safety (Nadzam, 1991).

2.2. ERRORS

According to Reason, an error is defined as *"the failure of a planned action to be completed as intended (i.e., error of execution) or the use of a wrong plan to achieve an aim (i.e., error of planning)"* (Reason, 1990; cited by Kohn et al., 2000: 28).

Adverse events are most of the time linked with errors. An adverse event is an injury caused by medical management rather than the underlying condition of the patient. Within the scope of adverse events, not all errors result in harm. Brennan et al. define an adverse event due to an error that do result in injury as a "*preventable adverse event*" (Brennan et al., 1991; cited by Kohn et al., 2000: 28). Preventable adverse events include negligent adverse events that satisfy legal criteria used in determining negligence (Leape et al., 1991; cited by Kohn et al., 2000: 28).

Errors can happen in all stages in the process of care, from diagnosis, to treatment, to preventive care. Analysis of errors in all these stages can provide much needed information especially regarding adverse events that result in serious injury or death. As a result improvements can be made to the overall system to avoid similar future events happening. Preventing errors contribute to the overall safety of the healthcare system at all levels. Building safety into processes of care prevents errors as well as improves quality. According to Deming, improving processes and preventing errors is the only way to improve quality (Deming, 1986). One of the efficient ways to accomplish this is to shift focus from blaming individuals for past errors to preventing future errors by designing safety into the system. According to Reason, error reporting is crucial to learning from mistakes to protect system integrity and prevent or mitigate failures (Reason, 1990, 2000). In parallel to HRT, employees are encouraged to support learning from errors in ''blame-free'' reporting systems, and that in poorly structured and insufficiently managed organizations, more errors are produced.

Adverse drug events are estimated to injure or kill more than 770000 people in hospitals annually (Lesar et al., 1997). Prescribing errors are the most frequent source (Kanjanarat et al., 2003; Kaushal and Bates, 2001; Kohn et al., 2000). According to Kohn et al., substantial body of evidence points to medical errors as a leading cause of death and injury (Kohn et al., 2000: 26). Kohn et al., indicate that

- medical errors harm a sizable amount of people,
- preventable adverse events cause majority of the death in the US,
- medical errors are costly,
- patient safety is as important as worker safety,
- medication-related errors mostly happen in hospitals,
- medication-related errors affect people outside hospitals as a result of wrong prescription, or patient not following instructions properly.

According to Leape et al., (Leape et al., 1993; cited by Kohn et al., 2000: 36) the errors that result in medical injury can be categorized as diagnostic, treatment, preventive, or other errors as seen in Table 7.

Table 7: Types of Errors

- Diagnostic
  - Error or delay in diagnosis
  - Failure to employ indicated tests
  - Use of outmoded tests or therapy
  - Failure to act on results of monitoring or testing
- Treatment
  - Error in the performance of an operation, procedure, or test
  - Error in administering the treatment
  - Error in the dose or method of using a drug
  - Avoidable delay in treatment or in responding to an abnormal test
  - Inappropriate (not indicated) care
- Preventive
  - Failure to provide prophylactic treatment
  - Inadequate monitoring or follow-up of treatment
- Other
  - Failure of communication
  - Equipment failure
  - Inadequate processes and procedures
  - Failure to follow standard procedures
  - Inadequate training
  - Poorly designed interface
  - Other system failure

Source: Lucian L Leape, Lawthers, Brennan, & Johnson, 1993

In order to understand why errors occur one need to understand normal cognition. A unitary framework proposed by Reason (Reason, 1990) for the cognitive theory indicates that much of the mental functioning is automatic, rapid, and effortless. Human brain has a huge amount of mental models "*schemata*" that are "*expert*" for automatic and unconscious processing. These schemata process

information rapidly, in parallel, and without conscious effort allowing people to act without thinking. In addition to this automatic unconscious processing, called the *schematic control mode*, cognitive activities can be conscious and controlled referred as the *attentional control mode*, which are used for problem solving as well as to monitor automatic function. On the contrary to the rapid parallel processing of the schematic control mode, processing in the attentional control mode is slow, sequential, effortful, and difficult to sustain.

Reason also emphasizes on the concept of *intention* as error is not meaningful without the consideration of intention. Errors depend on two kinds of failures; either actions do not go as intended or the intended action is not the right one. Reason using *intention* differentiates between slips or lapses and mistakes. A slip or lapse is an unconscious glitch in automatic activity and occurs when the action conducted is not what was intended. It is an error of execution. The difference between a slip and a lapse is that a slip is observable and a lapse is not. In a mistake however, the action proceeds as planned but fails to achieve its intended outcome because the planned action was wrong to start with.

In considering how humans contribute to error, it is important to distinguish between "*active and latent errors"* (Reason, 1990; cited by Kohn et al., 2000: 55). The consequence of active errors takes effect right away. These do occur at the frontline operator level and are sometimes called the sharp end (Cook et al., 1998; cited by Kohn et al., 2000: 55). Latent errors on the other hand are most of the time out of direct control of the operator and are due to poor design, incorrect installation, faulty maintenance, bad management decisions, and poorly structured organizations. These are called the blunt end. Contrary to active errors, latent errors are not easy to recognize and correct due to their inherent nature. According to Reason, current responses to errors tend to focus on the active errors by penalizing individuals instead of trying to discover and remove the latent errors. Focusing on active errors lets the latent failures remain in the system, and their accumulation actually makes the system more prone to future failure. Because system failures represent latent failures coming together in unexpected ways, they appear to be unique in retrospect. Since the same mix of factors is unlikely to occur again, efforts to prevent specific active errors are not likely to make the system any safer (Reason, 1990; cited by Kohn et al., 2000: 56).

The socio-technical model presents examples of errors related to the use of the EHR systems and the components where errors take place. See Table 8 for

examples of the types of errors (Sittig and Singh, 2011: 1282) based on the Socio-technical model (Sittig and Singh, 2010: i69).

Table 8: The Types of Errors Based on Socio-technical Model

Socio-technical Model Dimension	Examples of Types of Possible Errors
Hardware and software: required to run the healthcare applications	• Computer or network is not functioning
Clinical content: data, information, and knowledge entered, displayed, or transmitted	• Input data truncated (ie, buffer overflow); some entered data lost • Allowable item cannot be ordered • Incorrect default dose for given medication5
Human-computer interface: aspects of the system that users can see, touch, or hear	• Data entry or review screen does not show complete data (eg, missing patient name, medical record number, birthdate) • Two buttons with same label but different functionality • Wrong decision about KCl administration based on poor data presentation on the computer screen
People: the humans involved in the design, development, implementation, and use of HIT	• Two patients with same name; data entered for wrong patient • Incorrect merge of 2 patients' data • Nurses scan duplicate patient bar code taped to their clipboard rather than barcode on patient to save time
Workflow and communication: the steps needed to ensure that each patient receives the care they need at the time they need it	• Computer discontinues a medication order without notifying a human • Critical abnormal test result alerts not followed up
Organizational policies and procedures: internal culture, structures, policies, and procedures that affect all aspects of HIT management and healthcare	• Policy contradicts physical reality (eg, required bar code medicine administration readers not available in all patient locations) • Policy contradicts personnel capability • Incorrect policy allows "hard stops" on clinical alerts, causing delays in needed therapy
External rules, regulations, and pressures: external forces that facilitate or place constraints on the design, development, implementation, use, and evaluation of HIT in the clinical setting	• Billing requirements lead to inaccurate documentation in EHR (eg, inappropriate copy and paste)
System measurement and monitoring: evaluation of system availability, use, effectiveness, and unintended consequences of system use	• Incomplete or inappropriate (eg, combining disparate data) data aggregation leads to erroneous reporting • Incorrect interpretation of quality measurement data

Source: Sittig & Singh, 2011: 1282

2.2.1. Conditions That Create Errors

Errors, whether active or latent can occur as a combination of many factors. Factors can intervene between the design of a system and the production process

that creates conditions in which errors are more likely to happen. Reason refers to these factors as psychological precursors or preconditions (Reason, 1990; cited by Kohn et al., 2000: 61). Factors such as right equipment, well-maintained and reliable; a skilled and knowledgeable workforce; reasonable work schedules, well-designed jobs; clear guidance on desired and undesired performance, etc., are the precursors or preconditions for safe production processes. Any precondition can contribute to a large number of unsafe acts such as training deficiencies can show up as high workload, undue time pressure, inappropriate perception of hazards, or motivational difficulties (Reason, 1990).

Technology is one of the main preconditions contributing to errors one way or another in the form of latent failures embedded in the system. As humans create errors, the perception that humans are unreliable and inefficient is formed and recognized. The action to take has been to find the person creating errors and prevent him or her doing it again. A second response has been to increase the use of technology by automating processes to reduce human involvement hence reduction in errors. Technology changes the tasks that people do by shifting the workload and eliminating human decision making (Cook and Woods, 1994; cited by Kohn et al., 2000: 61). Where a nurse previously may have been in charge of medication and provided the medication to a patient mostly manually, he or she may intervene as needed due to fully automated medication devices. Yet there are still procedures that cannot be automated and he or she needs to be involved in the procedure, which usually involves having to monitor automated systems for rare, abnormal events (Reason, 1990).

As automation rarely fails, basic skills are not practiced and end up getting lost. If something goes wrong with the automated process even if it is very rare, it causes problems for people in charge. Automation makes systems more *opaque* to people who manage, maintain, and operate them (Reason, 1990). Processes that are automated are less visible because machines intervene between the person and the task and can handle more information. One of the advantages of technology is that it can enhance human performance to the extent that the human plus technology is more powerful than either is alone (Norman, 1993; cited by Kohn et al., 2000: 62). In medicine, automated order entry systems or decision support systems can question the actions of operators, offer advice, and examine a range of alternative possibilities that humans cannot possibly remember.

As technology allows more to be accomplished by fewer people, interaction among team member sharing the same tasks is reduced affecting the distributed nature of the job in which tasks are shared among several people and may influence the ability to discover and recover from errors (Norman, 1993; cited by Kohn et al., 2000: 63).

Working conditions also present challenges and can easily contribute to creating errors. According to Halbesleben et al., higher burnout scores, staff reporting lower perception of safety on the unit, lower frequency of reporting potential errors, and a lower patient safety grade for the unit are all related (Halbesleben et al., 2008: 564) . According to Moody et al., there is a positive correlation between supervisor and manager support of actions and expectations promoting safety, and the reporting of medication errors (Moody, 2006). In their study they found that when nurses had a higher patient workload more medication administration errors were reported.

2.2.2. Cost of Errors

Although medication-related errors do not result all in actual harm, the ones that do are costly. In a study conducted at two prestigious teaching hospitals in US, Kohn et al. found that with nearly 2% of admissions, a preventable adverse drug event occurred resulting in average increased hospital costs of $4,700 per admission or about $2.8 million annually for a 700-bed teaching hospital. When these findings are generalized, the increased hospital costs alone of preventable adverse drug events affecting inpatients are about $2 billion for the US alone (Kohn et al., 2000: 2).

Direct hospital costs represent only a fraction of the overall costs, as hospital patients form only a portion of the total population at risk. Ambulatory settings also incur costs for more and complex care. In addition to hospitals, surgical centers, private physician offices, clinics, pharmacies, nursing homes and other institutions incur as a whole due to errors.

Opportunity costs are another part of the picture, as money spent at repeated diagnostic tests or counteract adverse drug events is money unavailable for other purposes. In addition, society as a whole pay for errors when insurance costs and copayments are inflated by services that would not have been necessary had proper care been provided. In addition to higher direct healthcare expenditures,

there are also indirect costs that can't be measured as a result of errors. Loss of trust in the system, diminished satisfaction, lower morale, higher frustration at not being able to receive and give the proper care, longer hospital stay or disability causing physical and psychological discomfort, lost worker productivity, reduced school attendance by children, and lower levels of population health status, are among the many indirect costs employers, employees, patients and society as a whole pay for medical errors (Kohn et al., 2000: 3).

2.3. SAFETY AND ACCIDENTS

There have been numerous studies that link safety and accidents in literature. Normal accident theory (NAT) and High reliability theory (HRT) approach the issue from different perspectives. Perrow in his normal accident theory states that accidents are inevitable in certain complex systems. Due to the nature of processes, though rare, accidents are normal in complex, high technology industries. In contrast to exploring the reasons of accident and errors, other researchers have focused on the characteristics that make certain industries, such as military aircraft carriers or chemical processing, highly reliable (Roberts, 1999). According to the HRT, accidents can be prevented through good organizational structure, design and management (Sagan, 1993). Organizational commitment to safety, high levels of training, redundancy in personnel, and safety measures, and a strong organizational culture for continuous learning and willingness to change are among the main attributes of highly reliable industries (Roberts, 1999; Sagan, 1993).

HRT proposes that although accidents may occur, systems can be designed to be safer so that accidents happen rarely. When accidents occur, they represent failures in in the way systems are designed. The main objective of systems design should be to make it difficult for accidents and errors to occur, and minimize the damage when they do (Leape, 1994).

In healthcare, there should be a certain level of base safety that continues to evolve over time as risks become known and become part of the safety requirements (Kohn et al., 2000). In IOM's report *To err is human* safety is defined as *freedom from accidental injury (Institute of Medicine, 1999: 58)*. From patient's perspective the main expectation is the prevention of accidental injuries which establishes the primary safety goal.

2.4. SYSTEM AND ACCIDENTS

According to Reason (Reason, 1990; cited by Kohn et al., 2000: 52) "*A system is a set of interdependent elements interacting to achieve a common aim. The elements may be both human and non-human (equipment, technologies, etc.).*"

Systems can be very large and complex, or they can be small yet part of another larger system such as those that exist in healthcare. Healthcare can be considered as one large, complex system consisting of many smaller systems. A multi-hospital system, having a variety of departments each having their own operating rooms are all examples of a system within a system. They all belong to the healthcare system, a large and complex system with multiple systems, not easy to analyze and understand. When there are failures in large systems, it is due to multiple faults happening at the same time in an unanticipated interaction, (Cook and Woods, 1994; Perrow, 1984; cited by Nolan, 2000: 771) creating a chain of events in which the faults grow and evolve (Gaba et al., 1987). As a result of these faulty incidents accumulating accidents happen which is a form of information about a system (Cook and Woods, 1994). Perrow defines accidents as "*An accident is an event that involves damage to a defined system that disrupts the ongoing or future output of that system "* (Perrow, 1984; cited by Kohn et al., 2000: 52).

According to Perrow, systems are characterized by two dimensions: complexity and tight or loose coupling (Perrow, 1984; cited by Kohn et al., 2000: 58). The *complexity* refers to the presence of unfamiliar or unplanned and unexpected sequences of events in a system that is either not visible or not immediately comprehensible. A *tightly coupled* system is one that is highly interdependent: Each part of the system is tightly linked to many other parts and therefore a change in one part can rapidly affect the status of other parts. Loosely coupled or decoupled systems have fewer or less tight links between parts and therefore are able to absorb failures or unplanned behavior without destabilization (Marais et al., 2004).

Systems that are more complex and tightly coupled are more prone to accidents and have to be made more reliable (Cook and Woods, 1994). Perrow considers nuclear power plants, nuclear weapons handling, and aircraft to be complex, tightly coupled systems (Perrow, 1984) as multiple processes are occurring at the same time and failure in one area can affect another dependent process easily. Dams and rail transportation are considered tightly coupled as the steps in production are closely linked, but linear because there are few unexpected

interactions. On the other hand, Universities are considered complex, but loosely coupled, since the impact of a decision in one area can likely be limited to that area (Perrow, 1984). Although Perrow did not classify healthcare as a system, others have suggested that healthcare is a complex and tightly coupled system (Cook et al., 1998) prone to accidents .

In a system although there are many parts that interact, the issue emerges when one part that have many interdependencies fail causing other dependent functions to also fail. When failures occur in a complex and large system, they are analyzed only in hindsight; however, knowing the outcome of an event influences how we assess past events (Cook et al., 1998; Reason, 1990). A *hindsight bias* occurs, meaning things that were not seen or understood at the time of the accident seem obvious in retrospect. In addition due to this hindsight bias the causes of an accident is simplified by pointing out a single element as the reason of the accident. As multiple individuals have pieces of the relevant information (Norman, 1993; cited by Kohn et al., 2000: 53), regarding an accident, hindsight bias makes it very easy and convenient to come up with a simple explanation for the accident or to blame an individual which makes it hard to determine the real causes (Kohn et al., 2000).

Although healthcare has many of the same features of systems and accidents in other industries, certain differences exist. In other industries when accidents happen, the employee, employer, worker or the company are directly affected. In healthcare this is not the case as the consequences affect a third party; the patient. The health professional or the healthcare organization is rarely affected. In addition only one patient at a time is affected by an accident, not groups of people like in other industries making the accident less visible (Kohn et al., 2000).

2.4.1. Safer Systems and Prevention of Errors

In any industry, one of the greatest contributors to accidents is human error. Perrow has estimated that, on average, 60% to 80% of accidents involve human error (Perrow, 1984). When an error occurs, to find and blame someone is the first initial reaction given though multiple factors are the reasons for accidents and errors. Blaming does not get rid of the factors contributing to the errors and same type of errors and or accidents keep happening.

Despite the fact that people working in healthcare are among the most educated and dedicated, there are still errors being made and accidents taking

place. Preventing errors and improving safety for patients require a systems approach focusing and improving on the design and the processes of the system. Certain approaches are used to make system changes in order to reduce errors and adverse events; these fall into the five categories (Leape et al., 1995; Leveson, 1995; Norman, 1988, 1993; Salvendy, 2012; cited by Nolan, 2000: 771):

- Reduce complexity
- Optimize information processing
- Automate wisely
- Use constraints
- Mitigate the unwanted side effects of change

All of these approaches can be used for error prevention, detection, and mitigation.

According to Kohn et al., design of safer systems should include specific, clear, and consistent efforts to develop a work culture that takes safety as a top priority and an ongoing effort, a working environment that encourages reporting errors and hazardous conditions, proper communication paths among staff for any safety concerns, and an effective knowledge transfer, including the systematic acquisition, dissemination, and incorporation of ideas, methods, and evidence that may have been developed elsewhere (Kohn et al., 2000).

According to them safety in healthcare processes involves a three-part strategy: 1) designing systems to prevent errors include designing jobs for safety, avoiding reliance on memory and vigilance, and simplifying and standardizing key processes using checklists and protocols. 2) designing procedures to make errors visible when they do occur, and (3) designing procedures that can mitigate the harm to patients from errors that are not detected or intercepted (Nolan, 2000: 771).

Applying TQM principles do contribute to making systems safer by preventing errors (Berwick, 1989). One of the basic principles of quality management is the pursuit of fewer variations or defects in processes, which are nothing more but errors. Errors and variations are considered not as human failures but as opportunities to improve the system by identifying and developing system modifications to eliminate the underlying failures. As in TQM, fundamental system changes to reduce errors require top management's commitment.

As safety is associated directly with how a system operates, safety considerations should be part of the design and build processes. Potential interactions among components of a system are not predictable at early stages of the design, especially when HIT is part of a larger socio-technical system. Safety

issues emerge in large complex systems due to unexpected interactions among components. To minimize these issues, safety must also be addressed during and post system implementations (Sittig and Singh, 2010).

Systems that are more complex, tightly coupled, and are more prone to accidents can reduce the likelihood of accidents by simplifying and standardizing processes, building in redundancy, developing backup systems, and so forth (Perrow, 1984). In order to prevent major incidents in these complex systems, a defence-in-depth approach also known as “Swiss Cheese” model indirectly proposed by Reason (Reason, 1990) is used incorporating controls across a series of layers.

Similarly, in healthcare delivery systems, a number of mechanisms are used to reduce the likelihood of errors and thus make the system safer. Reduced reliance on memory, improved information access, error proofing, standardization, training, and absorption of errors are among the common mechanisms. Below is a number of items presented from a case study indicating certain ways to ensure safer systems design (Kohn et al., 2000: 62);

- Redesign the devices to default to a safe mode
- Reduce the difficulties of using multiple devices simultaneously
- Minimize the variety of equipment models purchased
- Implement clear procedures for checking equipment, supplies, etc., prior to beginning surgery
- Orient and train new staff with the team(s) with which they will work
- Provide a supportive environment for identifying and communicating about errors for organizational learning and change to prevent errors.

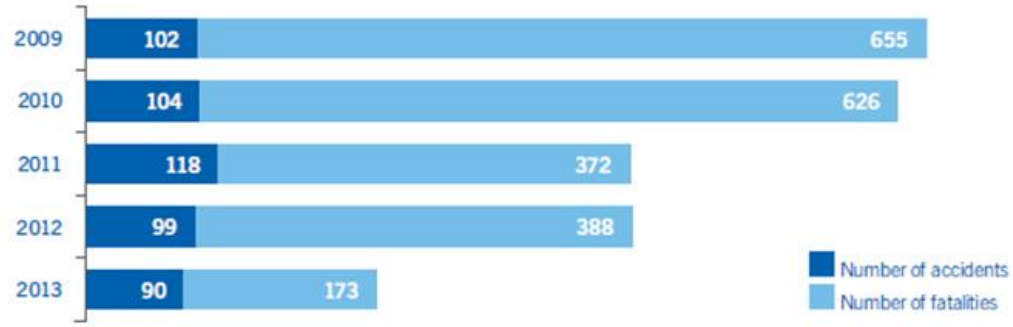
Certification and accreditation has also been identified as an important factor in promoting patient safety and error reduction in healthcare organizations (Tutuncu et al., 2007). Accreditation in healthcare, a model initially suggested by the Joint Commission on Accreditation of Healthcare Organization (Joint Commission on Accreditation of Healthcare Organizations, 2014), is probably the main ongoing international initiative aiming to foster Quality in Healthcare.

2.4.2. Safety in Aviation and Nuclear

More attention has been given to safety in aviation than healthcare even though the risk of dying as a result of a medical error is far greater than dying in an

airline accident (Kohn et al., 2000). In terms of safety, healthcare industry is a decade or more behind the other high-risk industries. Safety in aviation has been the main focus since World War II. According to Berwick and Leape, airline fatality between 1990 and 1994 was less than one-third the rate experience in mid-century (Berwick and Leape, 1999: 136). In global terms, the accident rate has been declining steadily ever since the 1950s. According to International and Civil Aviation Organization, ICAO, the year-over-year accident statistics indicate a reduction in the overall number of accidents as well as the accident rate, a positive trend for air transportation safety as shown in Figure 26 (International and Civil Aviation Organization, 2014: 5)

Figure 26: Accident Records: 2009 - 2013



Source: International and Civil Aviation Organization - ICAO, 2014: 5

Progress in aviation safety is a good example for other high risk industries such that fear, reprisal, and punishment produce not safety, but rather defensiveness, secrecy, and enormous human anguish (Berwick and Leape, 1999: 136). Scientific studies in human factors engineering, organizational psychology, operations research, and many other disciplines make it clear that, in complex systems, safety depends not on exhortation, but rather on the proper design of equipment, jobs, support systems, and organizations (Berwick and Leape, 1999: 136).

When taking safety progress in aviation certain similarities and differences between aviation and healthcare industries both of which are highly complex and risky should be kept in mind. Healthcare industry has been compared to aviation industry unfavorably due to safety records of both industries.

The key players in both industries, pilots and doctors, are highly trained and well educated professionals, determined to maintain high standards, use high

technology equipment and function as key members of a team of specialists performing difficult tasks in life-threatening environments, and exercise high level cognitive skills in a complex domain (Allnutt, 1987; cited by Leape, 1994: 1855). Despite these similarities, major differences exist between the domains. Medicine specifically has a substantial amount of uncertainty due to the number and variety of diseases as well as the unpredictability of the human organism (Leape, 1994: 1855).

Unlike doctors and physicians, pilots have their lives at stake during work and are highly motivated for doing their jobs safely. Both airlines and airplane manufacturers have very strong incentives to make flying safe as the consequences of an accident and crash might be brutal. It might affect both the airline and the manufactures to the extent that they might be out of business after a large crash or if a certain model crashes repeatedly.

Certain characteristics of a safer aviation model with suitable modifications can be applied improving safety in healthcare. In terms of design, aviation industry assumes errors and failures are part of the overall system proceeding accordingly to absorb the inevitable impact by building multiple buffers, backup systems, and automation. Though this complexity brings its own challenges for system design, these safeguards have served the safety of aviation well (Leape, 1994: 1855). Generally speaking this is not case within the medical field. With exceptions in certain areas, when errors detected a problem-solving approach is used rather than pursuing root cause analysis or identifying underlying system failures. Healthcare systems are not designed to prevent or absorb errors but designed to rely on individuals not to make errors rather than to assume they will (Leape, 1994: 1855).

Standardization in procedures is another difference between the two industries. Pilots go through a checklist before each takeoff. Certain protocols must be followed for planning flights, operations, and maintenance. In addition, training, examination, and certification is highly advanced and enforced without any flexibility. Pilots do take proficiency examinations every 6 months that focus specifically with procedures to improve safety. In healthcare standardization and task design vary widely; reliance on short term memory is an important issue especially for a busy nurse administering medications on time for the right medicine, right amount, and right patient. Education and training however exceeds that in aviation for both breadth of content and in duration. Periodic testing or certification in medicine however is not widely an accepted norm.

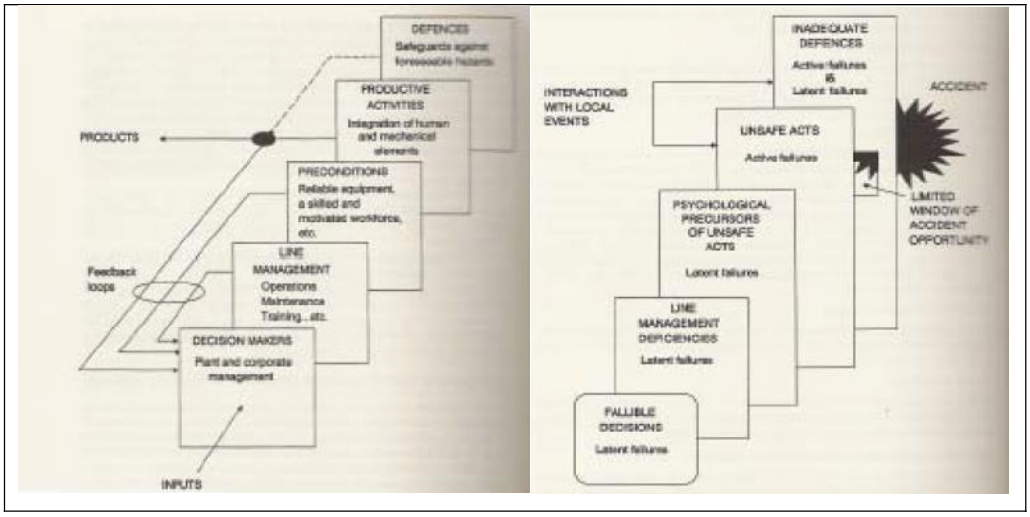
Finally, aviation safety has been institutionalized and governed by two separate independent agencies that have government-mandated responsibilities: the Federal Aviation Administration (FAA) regulates all aspects of flying and imposes safety procedures, and the National Transportation Safety Board (NTSB) investigates every accident. Recognizing that the disciplinary action did not provide any error related feedbacks, the FAA in 1975 established a confidential reporting system for safety related incidents; the Air Safety Reporting system (ASRS), which increased reporting dramatically so that potential issues related to safety, can be dealt with properly improving the overall aviation safety. The medical field in this aspect fails enormously. Though there have been certain government mandates, they are mostly about dealing with privacy and confidentiality issues such as HIPAA. Investigating accidents in depth is not realistic unless malpractice lawsuits are involved. Incident reporting perceived as individual punishment therefore not as useful and often not filed (Leape, 1994: 1856).

2.4.3. Swiss Cheese Model

The origins of the model dates back to 1988 during the writing of Human Error (Reason, 1990). "*The original intention for the book was to provide an essentially cognitive psychological account of the nature, varieties, and the mental sources of human error*" (Reason et al., 2006: 4) trying to address the question as "*What can the appearance of relatively non-random error forms tell us about the largely hidden processes that govern our thoughts and actions*?" The model refers to the examples of the gas, chemical, and nuclear plant as well as transportation disasters that happened in the late 70s such as Flixborough, Challenger, Three Mile Island, Bhopal, Chernobyl, the Herald of Free Enterprise and the King's Cross Underground fire(Reason et al., 2006: 4).

Reason identified the required elements of a production system in order to describe how and why they might fail as all of the disasters he refers exist in complex productive systems. John Wreathall and J. Reason depicted these as a sequence of five 'planes' lying one behind the other which really had nothing to do with the label Swiss-Cheese as shown in Figure 27. As a separate side note, Reason did not come up with the label Swiss-Cheese. It was probably Rob Lee, then Director of the Bureau of Air Safety Investigation (BASI) in Canberra (Reason et al., 2006: 4).

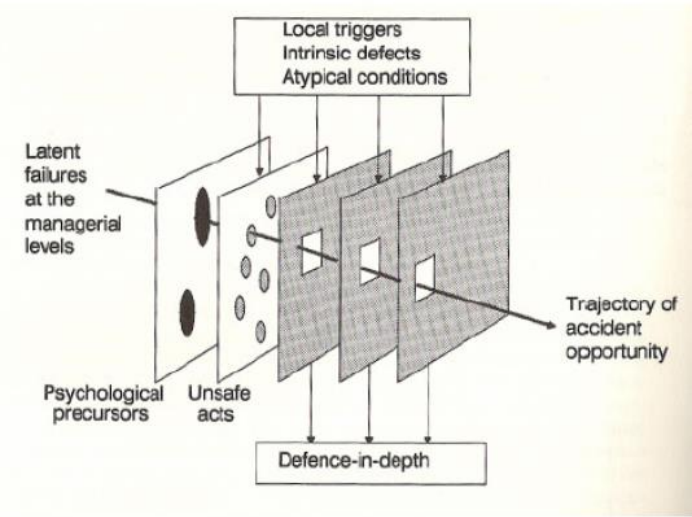
Figure 27: Original Swiss-Cheese Model



Source: J. Reason et al., 1990

Later in other chapters, Reason makes a distinction between active errors and latent errors, and includes a modified representation in Figure 28 indicating an accident trajectory passing through successive slices. The figure shows the dynamics of accident causation arising from interactions between latent failures and a variety of local triggering events. The Swiss–Cheese label probably is based on this figure.

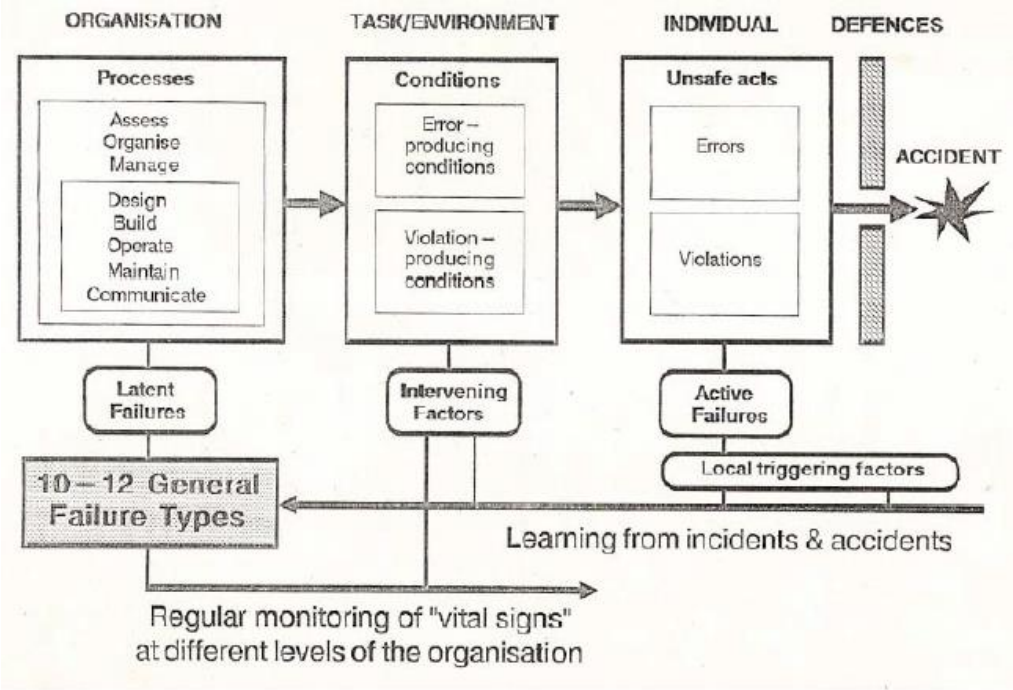
Figure 28: Latent Failures and Swiss-Cheese Model



Source: J. Reason et al., 1990

Later in the early to mid-90s the second version of the proposed Swiss-Cheese model has been introduced converting multiple phases of the production planes into organization, workplace, and person and extending the defensive layer into three layers as shown in Figure 29.

Figure 29: The Second Version of Swiss-Cheese model

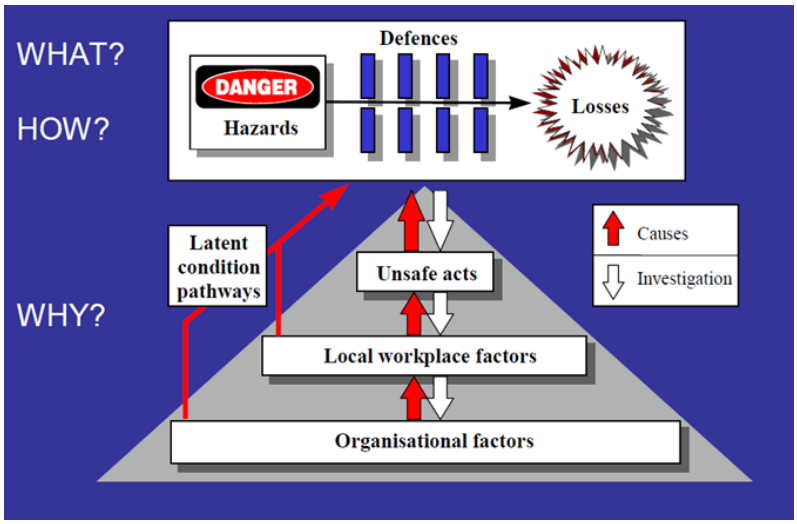


Source: J. Reason et al., 1990

The third version of the model as shown in Figure 30 appeared in *Managing the Risks of Organizational Accidents* (Reason, 1997) where a number of significant changes exist;

- Three basic elements of hazards, defenses and losses are introduced
- The planes are represented as disguised Swiss-Cheese slices
- Explanation of holes, gaps, weaknesses and the term latent conditions introduced instead of latent error or latent failure where short-term breaches may be created due to errors of front-line operators and long term and more dangerous breaches due to decisions of designers, builders, procedure writers, top-level managers and maintainers.

Figure 30: The Third Version of Swiss-Cheese Model



Source: J. T. Reason, 1997

2.5. HUMAN FACTORS

Human factor is an important component of safety and goes back to industrial engineering and psychology. It is defined as "*the study of the interrelationships between humans, the tools they use, and the environment in which they live and work"* (Weinger et al., 1998; cited by Kohn et al., 2000: 63).

Human factors approach is more effective and efficient in understanding where and why systems break, errors and failures occur by examining the causes circumstances, conditions, associated procedures and devices and other factors connected with the event. Studies in human factors can result in safer systems and fewer errors and failures. Much of the work in human factors is on improving the human–system interface by designing better systems and processes (Leape, 1994; Reason, 1990) in the form of simplifying and standardizing procedures, building redundancy, improving communications and coordination within teams.

Critical incident analysis and naturalistic decision making are among the main approaches in the study of human factors. Critical incident analysis researches a significant or pivotal occurrence to understand where the system broke down, why the incident occurred, and the circumstances surrounding the incident (Cooper et al., 1978; cited by Kohn et al., 2000: 64). It provides an understanding of the

circumstances and conditions that actually produced an error regardless of a bad outcome exists or not due to error.

Naturalistic decision making is an analytic approach (Klein, 1998;cited by Kohn et al., 2000: 64). Examining the way people make decisions in their natural work settings. It takes into account all factors that are normally controlled in a lab setting such as time, pressure, noise. The key to this approach is making observations in real life and re-visiting actions based on those observations to analyze and find out the factors affecting the decision making processes.

In human factors research two different approaches on human error and human contribution to accidents exist. One approach recognized mostly as *the old view* (Cook et al., 1998; Reason, 2000a; cited by Dekker, 2002: 372), considers human error as a cause of failure. Dekker (2002: 372) highlights the major points in the *old view* of human error as follows:

- *Human error is the cause of most accidents.*
- *The engineered systems in which people work are made to be basically safe; their success is intrinsic. The chief threat to safety comes from the inherent unreliability of people.*
- *Progress in safety can be made by protecting these systems from unreliable humans through selection, proceduralization, automation, training, and discipline.*

The second approach also called as *the new view,* sees human error as a symptom of failure, not as a cause (Cook et al., 1998; Hoffman and Woods, 2000; Rasmussen and Batstone, 1989; Reason, 2000a; Woods et al., 1994). Dekker (2002: 372) summarizes the major points of the *new view* of human error as follows:

- *Human error is a symptom of trouble deeper inside the system.*
- *Safety is not inherent in systems. The systems themselves are contradictions between multiple goals that people must pursue simultaneously. People have to create safety.*
- *Human error is systematically connected to features of people tools, tasks, and operating environment. Progress on safety comes from understanding and influencing these connections.*

The new view of human error plays an important role in human factors and organizational safety domains (Reason, 1997; Rochlin, 1999; cited by Dekker, 2002: 372) emphasizing factors that are easily lost under *human error* label such as organizational deficiencies, design and procedural issues. As Shappell and Wiegman (Shappell and Wiegmann, 2001: 60) put it ". *.simply writing off. .*

.accidents merely to (human) error is an overly simplistic, if not naive, approach ..After all, it is well established that accidents cannot be attributed to a single cause, or in most instances, even a single individual."

CHAPTER THREE
QUALITY

"*Quality means doing it right when no one is looking*." — Henry Ford

3.1. QUALITY

There are various well-known definitions of quality. According to ISO 8402 (1986) quality is defined as "*the totality of features and characteristics of a product or service that bears on its ability to meet a stated or implied need*". "*Conformance to requirement*" is how Crosby defines quality (1979). Another definition is given as "*fitness for use*" (Juran and Gryna, 1980). According to Wayne, "*user satisfaction"* is made part of the definition as the definition "*the degree of conformance to a standard*", is too narrow (Wayne, 1983). Satisfying customer's needs and expectations is common to most definitions of quality which encompasses design, price, safety, delivery, performance usability and so on.

According to Donabedian, quality in very general terms is "*the ability to achieve desirable objectives such as achievable state of health using legitimate means"* (Donabedian, 1988: 173).

3.2. QUALITY IN HEALTHCARE

Healthcare organizations deal with a variety of challenges, specifically related to effectiveness, efficiency and quality. Like in all other systems, "*in an effective and efficient healthcare system, organizational resources are used to get the best value for the money spent*" (Palmer and Torgerson, 1999: 1136). A proper and an efficient TQM implementation provides healthcare organizations to manage their resources effectively and efficiently and to provide proper service and care for their patients, to improve processes to reduce errors (Mosadeghrad, 2013: 162).

Quality care or quality in healthcare also follows certain characteristics of the definition of quality. It has multiple dimensions and criteria that encompass the concept. According to Klein et al., patient care, like morale, cannot be considered as a unitary concept and that there will never be a single comprehensive criterion by which to measure the quality of patient care (Klein et al., 1961: 140). They indicate

that the dimensions and the criteria selected to define quality influence the approaches and methods that are employed in medical care.

Quality of care given to patients is hard to measure. There have been various studies aimed at measuring quality in certain settings. Klein, et al., found in a research the 16 measurable items shown in Table 9 (Klein et al., 1961: 140).

Table 9: Measurable Criteria of Good Patient Care

1. Continuity of care
2. Follow-up procedures
3. Patient self-care
4. Family teaching
5. Patient understanding of procedures, et cetera
6. Patient understanding of condition
7. Patient teaching
8. Orientation to patients' social problems
9. Patient satisfaction
10. Case load
11. Planned program for patient
12. Availability of personnel
13. Amount of consultation
14. Privacy and confidentiality
15. Smooth processing of patient
16. Degree of medical specialization

Source: M. W. Klein et al., 1961: 140

Similarly the committee of IOM's 1990 study identified critical dimensions of quality of care and adopted the following definition which is still accepted today:

"*Quality of care is the degree to which health services for individuals and populations increase the likelihood of desired health outcomes and are consistent with current professional knowledge* " (Lohr, 1990: 4).

Among these dimensions, the first eight are explicitly incorporated in the committee's definition (Lohr, 1990: 22) as shown in Table10.

Table 10: Dimensions in Definitions of Quality

1. Scale of quality
2. Nature of entity being evaluated
3. Goal-oriented
4. Aspects of outcomes specified
5. Acceptability
6. Type of recipient identified
7. Role and responsibility of recipient asserted

8. Continuity, management, coordination
9. Professional standards
10. Technical competency of provider
11. Interpersonal skills of provider
12. Acceptability
13. Statements about use
14. Constrained by resources
15. Constrained by consumer and patient circumstances
16. Constrained by technology and state of scientific knowledge
17. Risk versus benefit tradeoffs
18. Documentation required

Source: Kathleen N. Lohr, 1990: 22

Due to adverse events taking place in healthcare, there is a need for improvement. As Leape puts it, "*when comparing patient safety and the healthcare industry to commercial aviation and the aerospace industry, healthcare's three-sigma to four-sigma quality is roughly equivalent to a three jumbo jet crashing every two days"* (Leape, 1994: 1851).

The various dimensions of healthcare, quality and patient care are grouped as a list of performance characteristics that would improve the overall system. IOM proposes six specific aims for this improvement (Institute of Medicine, 2001: 5,6). According to IOM, healthcare should be safe, effective, patient centered, timely, efficient, and equitable as explained in Table 11:

Table 11: Healthcare Quality Improvement Goals

• **Safe**—avoiding injuries to patients from the care that is intended to help them.
• **Effective**—providing services based on scientific knowledge to all who could benefit and refraining from providing services to those not likely to benefit (avoiding underuse and overuse).
• **Patient-centered**—providing care that is respectful of and responsive to individual patient preferences, needs, and values and ensuring that patient values guide all clinical decisions.
• **Timely**—reducing waits and sometimes harmful delays for both those who receive and those who give care.
• **Efficient**—avoiding waste, in particular waste of equipment, supplies, ideas, and energy.
• **Equitable**—providing care that does not vary in quality because of personal characteristics such as gender, ethnicity, geographic location, and socio-economic status.

Source: Institute of Medicine, 2001: 5, 6

Research states efforts of implementing quality management systems and patient safety are positively correlated with each other (Tutuncu, 2008). Quality

Management System is considered as an important element in implementing continuous quality improvement and total quality management in healthcare. It has also been identified as a crucial factor in enhancing patient safety and error reduction in healthcare organizations (Tutuncu and Kucukusta, 2007).

3.3. TOTAL QUALITY MANAGEMENT

Abundance of terms exists within the quality domain. Quality improvement, quality improvement process, total quality management (TQM), organization-wide quality improvement (called Total Quality Control-TQC in Japan), continuous improvement, continuous quality improvement (CQI), quality assurance are among the various terms used interchangeably. Among these terms TQM and CQI may be the most universally recognized concept (Batalden and Buchanan, 1989; Berwick, 1989) but more so in industrialized countries (Dean and Bowen, 1994; Evans and Lindsay, 1996; Garvin, 1991). The evolution of these philosophic and technical approaches have been initiated from a set of management and statistical control methods pioneered decades ago by U.S. statisticians and engineers (but implemented chiefly by post-World War II Japanese industrialists for applications in industry, primarily manufacturing (Deming, 1986; Garvin, 1986, 1988; Juran, 1988b; Juran et al., 1974). Quality efforts started with Walter Stewhart of Bell Laboratories in the 1930s. His studies focused on increasing quality by decreasing faulty elements of a process, which became the foundation of works for the other major contributors in the following decades.

Specifically Deming (1982), Crosby (1979), Ishikawa (1985) Juran (1988a) were among the key individuals who made significant contributions to the development of practical and theoretical applications. Deming with his 14 points of Management, Juran with the planning, control, improvement theme for quality and 6 steps to Quality Improvement, and Crosby with conformity to standards with his 14 steps to Quality Improvement shaped the quality related research in the early days (see Table 12) (Batalden and Stoltz, 1995; Marszalek-Gaucher and Coffey, 1993). Ishikawa was also an influential contributor with the cause and effect diagram (also called the "Ishikawa" or "fishbone" diagram).

Table 12: Three Approaches to Enacting Quality Improvement

Deming's Fourteen Points for Management	Juran's Six Steps to Quality Improvement	Crosby's Fourteen Steps to Quality Improvement
1. Create constancy of purpose for improvement of product and service. 2. Adopt the new philosophy. 3. Cease dependence on inspection to achieve quality. 4. End the practice of awarding business on the basis of price tag alone. Instead minimize total cost by working with a single supplier. 5. Improve constantly and forever every process for planning, production, and service. 6. Institute training on the job. 7. Adopt and institute leadership. 8. Drive out fear. 9. Break down barriers between staff areas. 10. Eliminate slogans, exhortations, and targets for the workforce. 11. Eliminate numerical quotas for the workforce and numerical goals for management. 12. Remove barriers that rob people of pride of workmanship. Eliminate the annual rating or merit system. 13. Institute a vigorous program of education and self-improvement for everyone. 14. Put everyone in the company to work to accomplish the transformation.	1. Identify a project. Nominate projects. Evaluate projects. Select a project. Ask: Is it quality improvement? 2. Establish a project. Prepare a mission statement. Select a team. Verify the mission. 3. Diagnose the cause. Analyze symptoms. Confirm or modify the mission. Formulate theories. Test theories. Identify root cause(s). 4. Remedy the cause. Evaluate the alternatives. Design remedy. Design controls. Design for culture. Prove effectiveness. Implement. 5. Hold the gains. Design effective quality controls. Foolproof the remedy. Audit the controls. 6. Replicate results and nominate projects. Replicate the project results. Nominate new projects.	1. Make it clear that management is committed to quality. 2. Form quality improvement teams with representatives from each department. 3. Determine where current and potential quality problems lie. 4. Evaluate the cost of quality and explain its use as a management tool. 5. Raise the quality awareness and personal concern of all employees. 6. Take actions to correct problems identified through previous steps. 7. Establish a committee for the zero defects program. 8. Train supervisors to actively carry out their part of the quality improvement program. 9. Hold a “zero defects day” to let all employees realize that there has been a change. 10. Encourage individuals to establish improvement goals for themselves and their groups. 11. Encourage employees to communicate to management the obstacles they face in attaining their improvement goals. 12. Recognize and appreciate those who participate. 13. Establish quality councils to communicate on a regular basis. 14. Do it all over again to emphasize that the quality improvement program never ends.

Source: P. B. Batalden & Stoltz, 1995; Marszalek-Gaucher & Coffey, 1993

Though TQM is a widely accepted and practiced approach to serving mainly customer needs, suppliers, and employees using reengineered processes and systems to improve products and services, there is little agreement on what it is and what the essential features are. TQM is not a specific theory and is rather an abstract concept with many vague descriptions without any commonly agreed definitions though continues improvement seems to be an exception to the rule. Mosadeghrad (2011) found 73 different definitions of TQM in the literature. Among these most recognized and accepted ones define TQM as;

- *An approach (Flynn et al., 1994)*
- *A culture (Kanji and Yui, 1997)*
- *A philosophy (Joyce et al., 2006; Saylor, 1992)*
- *A system (Hellsten and Klefsjö, 2000)*
- *A strategy (Brown and Harvey, 2011)*

- *A program (Joss and Kogan, 1995)*
- *A process (Almaraz, 1994)*
- *A technology (Camisón, 1996)*
- *A technique (Wong et al., 2010)*
- *An effort (Tobin, 1990)*
- *An impact (Feigenbaum, 1983)*

TQM is considered to be one of the leading competitive strategies (Zhu, 1999: 291) of choice during the 1990s. The main idea behind it was that the customers should be the focal point of the organizations. Therefore studies and improvements should target the customer satisfaction (Tutuncu and Kucukusta, 2007). It has been widely implemented in various firms throughout the world for either achieving greater profitability (Mosadeghrad, 2005) or for following government imposed mandates, regulations and/or incentives (Ho, 1994).

There is an increasing amount of evidence and a common perception that a successful quality improvement can translate into economic and performance success (Brah et al., 2002; Classen et al., 1997; Clemmer et al., 1999; Conrad et al., 1996; Hansson and Eriksson, 2002; Hendricks and Singhal, 2001; Jarlier and Charvet-Protat, 2000; Kaynak, 2003).

Quality improvements though lead to both substantial reductions in costs and increases in quality however these were not always as great as might have been expected (Wright et al., 1997). A study by the Agency for Healthcare Research and Quality (AHRQ) demonstrated improvements to patient safety have a positive financial benefit for hospitals based on their Medicare payment history (Zhan et al., 2006).

An effective TQM implementation provides organizations to find out their client's requirements in order to provide proper care and reduce errors. These activities lead to high quality healthcare services, patient satisfaction, and increased productivity and profitability (Alexander et al., 2006; Macinati, 2008).

Following are the main TQM factors that affect a successful implementation (Hakes, 1991; Saylor, 1992; cited by Zhu, 1999: 292).

- *Leadership.*
- *Commitment.*
- *Total customer satisfaction.*
- *Continuous improvement.*
- *Total involvement.*

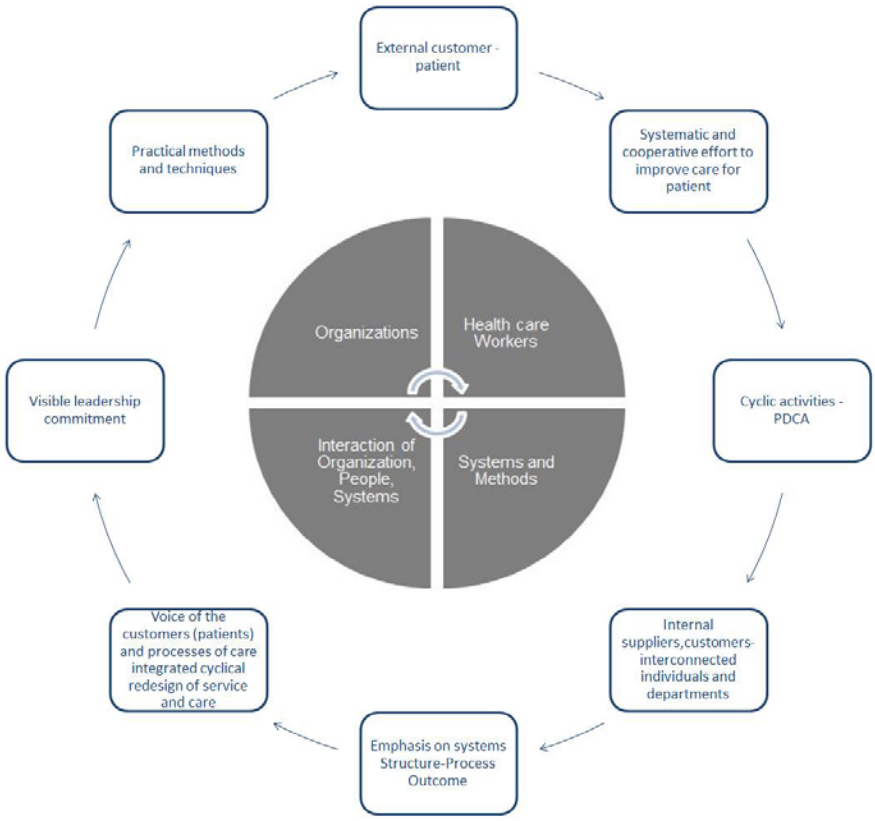
- *Training and education.*
- *Ownership.*
- *Reward and recognition.*
- *Error prevention.*
- *Co-operation and teamwork*.

3.4. CONTINUOUS QUALITY IMPROVEMENT

CQI is a philosophy that encourages all workers of an organization to always ask: "*How are we doing?"* and "*Can we do it better?*" (Edwards et al., 2007: 1).

According to Lohr, there are four core key elements part of the continuous improvement in healthcare (Lohr, 1990: 58). "*Organizations, healthcare workers, systems and methods, and interaction among these*". With the concepts of elements, eight other key constructs exist within as depicted in Figure 31.

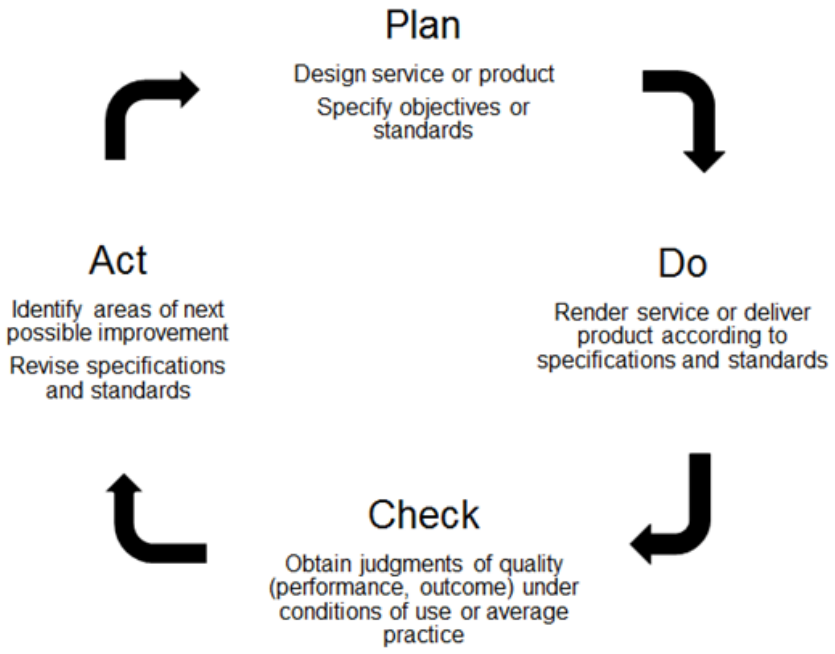
Figure 31: CQI Elements and Constructs



Source: Adapted from Kathleen N. Lohr, 1990: 58

Continuous Improvement model in healthcare shares several characteristics with those contemporary systems of quality assurance from decades ago. The bi-cycle concepts of Brown and Uhl (1970; cited by Lohr, 1990: 62) and the health accounting approach of Williamson (Williamson, 1988; Williamson and Wilson, 1978; cited by Lohr, 1990: 62) are among these contemporary systems both of which have cycles similar to Deming and Shewhart's plan-do-check-act (PDCA) approach shown in Figure 32. These also include notions of structure (organizational factors and high-level accountability), process (patient care activities), and outcomes (patient well-being or satisfaction) (Lohr, 1990: 62). Improvements in healthcare must focus on the structure (especially technology and people) and process that lead to the expected outputs and then ultimately to the desired outcomes (National Learning Consortium, 2013: 4).

Figure 32: Simplified Continuous Improvement Model



Source: Adapted from Moen and Norman, 2006: 8

The continuous improvement model mainly emphasizes ongoing efforts to enhance performance and value without any set limits. It approaches the evaluation of systems from customers' perspectives stressing on customer satisfaction. Senior management has the ultimate accountability for quality and quality improvement.

The literature shows a strong link between an explicit CQI strategy and high performance (Shortell et al., 2009; cited by National Learning Consortium, 2013: 2).

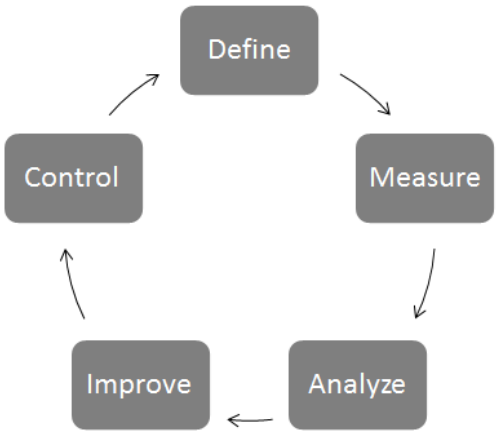
Lean is a form of a CQI process that gained acceptance after being used by Toyota. Many hospitals since then started using the key lean principles to reduce non-value added activities, mistake-proofing tasks, and waste to improve healthcare delivery. A key focus of change is on reducing or eliminating seven kinds of waste and improving efficiency (Levinson and Rerick, 2002; cited by National Learning Consortium, 2013: 7).

- Overproduction
- Waiting; time in queue
- Transportation
- Non-value-adding processes
- Inventory
- Motion
- Costs of quality, scrap, rework, and inspection

Lean CQI concepts focus on removing overburden and inconsistency while reducing waste to create a process that can deliver the required results smoothly (Holweg, 2007; cited by National Learning Consortium, 2013: 8).

Six Sigma is a business management and QI strategy that has its roots in the U.S. manufacturing industry (Bendell, 2006), specifically in Motorola and General Motors, seeking to enhance efficiency by identifying and removing the causes of defects (errors) and minimizing variability in manufacturing and business processes as shown in Figure 33.

Figure 33: Six Sigma Model



Source: Adapted from Bendell, 2006: 256

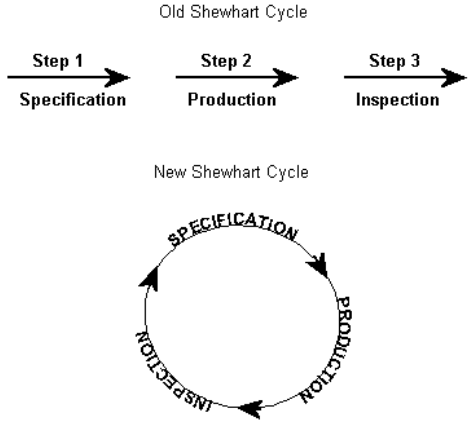
In a certain study six sigma was utilized to provide quality improvements to patients that have type 2 diabetes. Improving coordination, reducing unnecessary appointments and wait times, defining and measuring indicators, analyzing statistics and coming up with strategies based on the findings were all part of a six sigma program, which also changed certain clinical protocols and increased autonomy for staff all together providing better diabetic care to patients (Paccagnella et al., 2012; cited by National Learning Consortium, 2013: 10).

The Malcolm Baldrige Criteria (Fisher and Simmons, 2012) and Six Sigma (Christianson et al., 2005) are two modern approaches hospitals use to bolster their quality programs, to improve patient safety and to ensure alignment with their strategic goals. The balanced scorecard approach, a rational planning model to analyze volumes of quality data introduced by Kaplan and Norton (1992) also is used for improving quality and safety in a hospital environment.

3.4.1. Plan-Do-Check-Act (PDCA)

Although most people refer and relate the plan-do-check-act (PDCA) cycle to Deming, it was essentially (Shewhart, 1986; cited by Moen and Norman, 2006: 1) who first conceptualized the term. Shewhart presented the first version as shown in Figure 34 as "*Shewhart Cycle"* referring to the *Scientific Method* in his book "*Statistical Method from the Viewpoint of Quality Control"* (Shewhart and Deming, 1939; cited by Moen and Norman, 2006: 1).

Figure 34: Shewhart Cycle



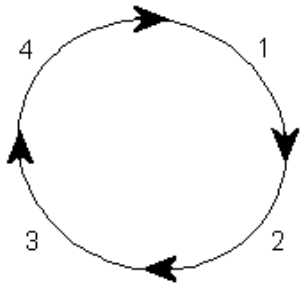
Source: Shewhart and Deming, 1939

Instead of the straight line model of specification, production, and inspection he came up with the cycle model emphasizing the model as:

> *These three steps must go in a circle instead of in a straight line, as shown . . . It may be helpful to think of the three steps in the mass production process as steps in the scientific method. In this sense, specification, production, and inspection correspond respectively to making a hypothesis, carrying out an experiment, and testing the hypothesis. The three steps constitute a dynamic scientific process of acquiring knowledge.*

W. Edwards Deming (1950) editing Shewhart model presented the modified model at a Japanese Union of Scientists and Engineers (JUSE) adding a fourth step as Redesign through marketing research to the first three steps; design, produce, sell. He emphasized the ongoing cyclic interaction among these four steps of design, production, sales, and research. This interpretation of Deming's Shewhart model with a minor modification was referred by Japanese as the *Deming Wheel* in 1951 (Moen and Norman, 2006: 6), as illustrated in Figure 35.

Figure 35: Deming's Wheel, 1951



Source: Moen and Norman, 2006: 6

According to Imai, Japanese executives later changed the term *Deming Wheel* as the Plan-Do-Check-Act (PDCA) cycle (Imai, 1986; cited by Moen and Norman, 2006: 6), which was integral part of Japanese quality improvement activities in the following decades. The PDCA cycle emphasized prevention of errors through standardization. As shown in Figure 36, the four step PDCA cycle includes:

- *Planning : definition of a problem and a hypothesis about possible causes and solutions*
- *Doing: implementing*
- *Checking: Evaluating results*
- *Acting: back to plan due to unsatisfactory results*

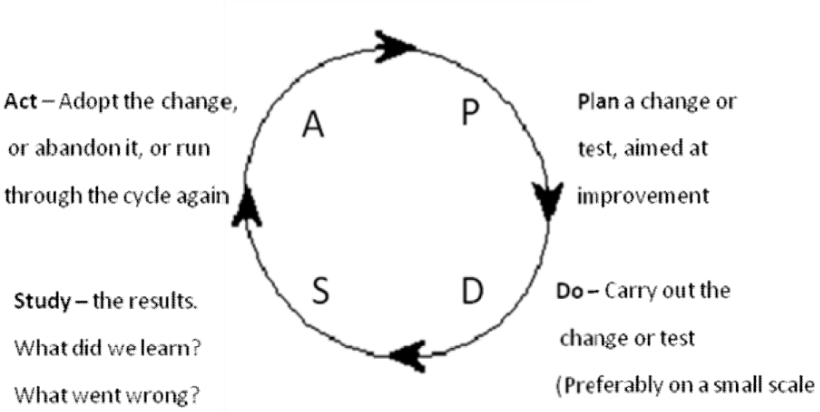
Figure 36: Japanese PDCA Cycle, 1951

Source: Moen and Norman, 2006: 7

Ishikawa (1985; cited by Moen and Norman, 2006: 8) emphasized standardization by stating *"if standards and regulations are not revised in six months, it is proof that no one is seriously using them".* He also added two more elements to the PDCA cycle; determining goals and target, methods for reaching the goals.

Deming (1986; cited by Moen and Norman, 2006: 8) presented slightly different version of the Shewhart cycle in his book *Out of the Crisis.* In his seminars he pointed out the inaccuracy of the term *Check* meaning *to hold back* in English and emphasized the term *Study* instead. Deming made this a very clear point in a personal letter to Ron Moen in 1990 (Moen and Norman, 2006: 7) as stated in Moen, Nolan, and Provost (Moen et al., 1999), *"… be sure to call it PDSA, not the corruption PDCA."* In 1993, after making a modification to the Shewhart cycle, Deming (1993) called it the *Shewhart cycle for learning and improvement- the PDSA cycle* as shown in Figure 37.

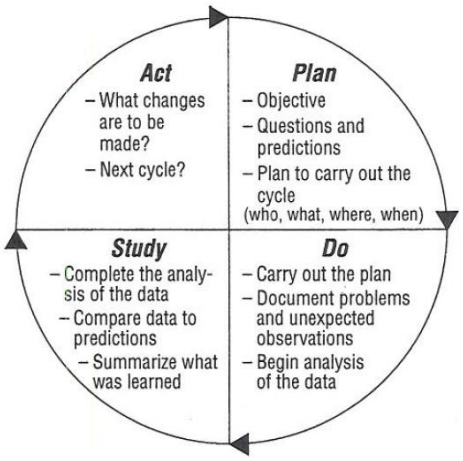
Figure 37: Shewhart Cycle for Learning and improvement - the PDCA Cycle



Source: Moen and Norman, 2006: 8

This version that Deming (1993) referred as a *flow diagram for learning, and for improvement of a product or of a process* has been further improved by Langley, Nolan, and Nolan (1994; cited by Moen and Norman, 2006: 8), which they called the PDSA Cycle as shown in Figure 38, emphasizing knowledge in the *Study* part.

Figure 38: PDSA Plan-Do-Study-Act Cycle



Source: Langley, Nolan, and Nolan, 1994: 9

As Lilrank and Kano (1989) state, the seven basic tools including cause-and-effect diagram (aka fishbone, Ishikawa diagrams), check sheet, control chart (graphs), histogram, Pareto chart, scatter diagrams, and flow chart along with the PDCA and PDSA cycles provided the proper foundation for improvement and the Japanese quality that has been well-known to-date.

3.4.2. KAIZEN

The word Kaizen in English is typically applied to measures for implementing continuous improvement. KAIZEN is defined as "*ongoing improvement involving everyone—top management, managers and workers*" (Imai, 1986: xxix).

Kaizen has often been erroneously subsumed under the terms '*Toyotism*' or TQM (Recht and Wilderom, 1998: 8). Similar methods and models influenced by American researchers (Deming) were introduced in Japan post World War II, which later evolved into TQM methods in Japan.

"*Whereas the American style stressed the suggestion's economic benefits and provided financial incentives, the Japanese style stressed the morale-boosting benefits of positive employee participation*" (Imai, 1986: 112). The traditional Western suggestion systems can be differentiated from Kaizen-oriented systems on two basic aspects: means and ends (Recht and Wilderom, 1998: 8).

Kaizen has been a successful methodology, especially in Japan. According Frank, Hofstede , and Bond, (1991), the underlying cultural factors for this success lies in values rooted in the Confucian ethic: thrift and perseverance. They indicate further that the economic growth from 1965 to 1987 is due to these cultural values. These values lead to economical behavior and to personal as well as company savings. Kaizen can be defined as "*a mindset to look for ways to achieve exactly this latter end: the lowering of costs and the achievement of greater efficiency. Grossly simplified, Kaizen in Japan is a culturally suitable means to accomplish cherished ends*" (Recht and Wilderom, 1998: 9).

3.5. QUALITY ASSURANCE

In 1974 the IOM published the following statement about quality assurance (QA) (Institute of Medicine, 1974: 1): "*The primary goal of a quality assurance system should be to make healthcare more effective in bettering the health status and satisfaction of a population, within the resources which society and individuals have chosen to spend for that care*."

Another definition puts it as "*a formal and systematic exercise in identifying problems in medical care delivery, designing activities to overcome the problems, and carrying out follow-up monitoring to ensure that no new problems have been*

introduced and that corrective steps have been effective" (Lohr and Brook, 1984: 585). Others define QA as all activities that contribute to defining, designing, assessing, monitoring, and improving the quality of healthcare (Tutuncu and Kucukusta, 2008).

QA is dependent on the principle that prevention is better than cure and it is more economical to get things right in the first place (Tang et al., 2005). Quality assurance activities do not control quality; they establish the extent to which quality will be, is being or has been controlled (Hoyle, 2001). "*Achieving error-free healthcare at all times is impossible. Therefore an effective quality assurance program is not an end in itself; rather, it is a means of maintaining and improving healthcare"* (O'Leary, 1988; cited by Lohr, 1990: 46). Lohr (1990: 46) defines Quality improvement as:

> *a set of techniques for continuous study and improvement of the processes of delivering healthcare services and products to meet the needs and expectations of the customers of those services and products. It has three basic elements: customer knowledge, a focus on processes of healthcare delivery, and statistical approaches that aim to reduce variations in those processes.*

QA is a systematic approach used by organizations to maintain and improve quality of products and services (Steeples, 1993). Prevention and control are at the center of quality assurance activities, which are an important component of continuous quality improvement. For this, strong emphasis is given to the existence of sound procedures for designing and introducing new or improved products and services as well as the design of processes that meet and exceed product and service quality requirements (Crosby, 1979; Deming, 1982, 1986; Garvin, 1983).

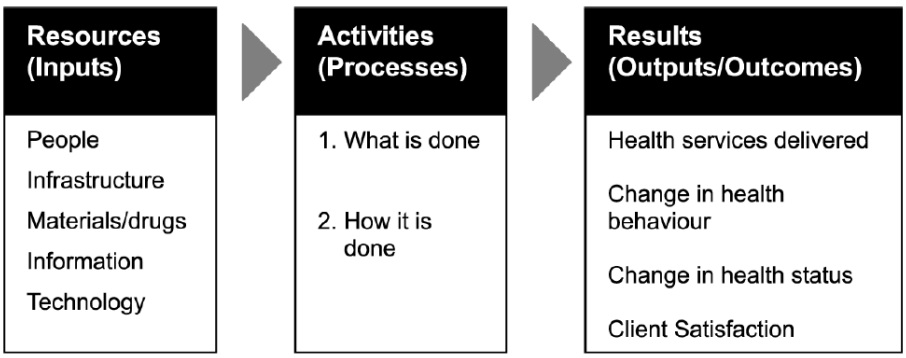
Donabedian (1988) points out that quality assurance is a misleading term as quality at best can be protected and enhanced but not assured. He emphasizes the insufficiency of the term as addressing the efforts to improve quality from monitoring of structure, process, or outcome instead of taking the effects of professional education and training, professional certification of competence, regulatory licensure, control of drugs and appliances, the methods of financing, other aspects of system design, and legal safeguards against malpractice into account.

3.6. STRUCTURE-PROCESS-OUTCOME MODEL

Donabedian has provided the conceptual framework for the well-known traditional model of quality of healthcare. He distinguished three components of the widely accepted model as structure, process, and outcome which has guided decades of research and program development (Donabedian, 1966, 1980, 1988).

According to Donabedian (1980), the functional relationships between structure (inputs) and processes, and processes and outcomes as shown in Figure 39 are key factors for determining the quality of healthcare. In other words, the structural characteristics of settings affect the process of care which in turn affects the outcome of that care. Yet, given the functional relationship of structure, process, and outcome, none of the three elements alone can adequately influence quality.

Figure 39: Inputs, Processes, and Outputs in Healthcare



Source: Donabedian, 1980

According to Lohr, (1990) structural characteristics of the resources (inputs) apply to individual practitioners, to groups of practitioners, and to organizations and agencies. These resources provide the capacity of the practitioner or provider to deliver healthcare but not the capacity of the care itself. Lohr identifies the process based on Donabedian's framework as the care of what is being done to and for the patient. Outcomes are the end results of care provided, which are the effect of the care process on the health and well-being of patients and populations. Health services delivered, change in health status,- either positive or negative-, client satisfaction are all part of the outcomes. Another outcomes list consists of "the five Ds"—death, disease, disability, discomfort, and dissatisfaction (Donabedian et al.,

1987; Lohr, 1988: 56). Lohr considers these negative outcomes as survival, states of physiologic, physical, and emotional health, and satisfaction (Lohr, 1988). More positive outcomes such as improved health status, functional ability, and perceived quality of life are also included and researched part of different health-scale –quality-measures in late 90s (Mitchell et al., 1997; Patrick, 1997).

Mitchell, Ferketich, and Jennings (1998: 43) explains Donabedian's (1966) view of structure-process-outcome as follows;

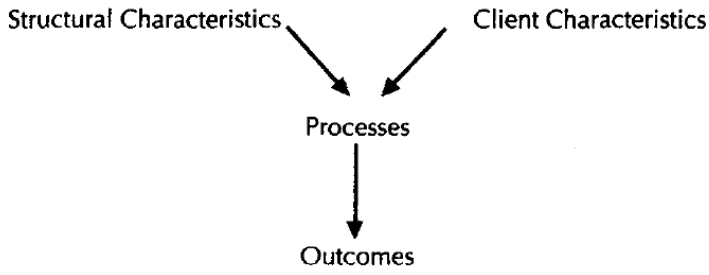
Structure – having the right things

Process – doing right things

Outcomes – having the right things happen

According to Mitchell et al., as the number of variables examined and thought to alter each of the components has increased tremendously (Mitchell et al., 1998: 43), neither structural nor process variables show consistent relationship explaining outcomes when examined alone (Mitchell and Shortell, 1997). The quality health outcomes model shown in Figure 41, with multiple feedback loops and outcomes is likely to be more sensitive to variables from structure and processes and is intended to be more closely aligned with the dynamic processes of patient care and outcomes than the traditional model (Mitchell et al., 1998: 44).

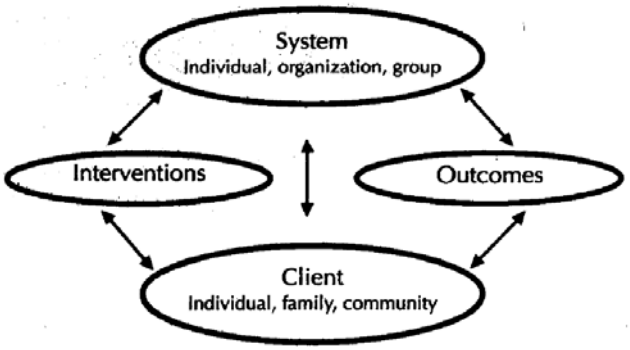
Figure 40: Linear Model Implied by Traditional Structure-Process-Outcome



Source: Mitchell, Ferketich, and Jennings, 1998: 43

The dynamic model recognizes the feedback that occurs among clients, the system, and interventions integrating the traditional structure and process elements into system characteristics.

Figure 41: Quality Health Outcome Model



Source: Mitchell et al., 1998: 44

In contrast to the traditional view that interventions or treatments directly produce expected outcomes influenced by client characteristics (Wilson and Cleary, 1995), the dynamic model does not have any direct connection linking interventions and outcomes. In the outcomes section, in addition to the five Ds, the patient-perceived dimensions of physical, social and role functioning, mental health, and overall health perceptions are included as more widely used clinical data (Patrick and Erickson, 1993; Wilson and Cleary, 1995).

Within the traditional model, more effort has been directed toward quality assessment than quality assurance (Lohr, 1990) while quality health outcomes model balances the effort between the two.

3.7. ISSUES IN QUALITY IMPROVEMENT

Quality problems can be put into three groups as overuse, underuse, and misuse (Chassin, 1991, 1997; Chassin and Galvin, 1998).

Overuse occurs when a health service is provided when its potential for harm or risk outweighs the possible benefits. Underuse is the failure to provide a healthcare service when the benefits are greater than the risks involved. Misuse occurs when the right service is provided incorrectly, and a preventable complication occurs and reduces the benefit the patient receives (Chassin, 1997). Avoidable complications of surgical and diagnostic procedures and preventable adverse events due to medication use are the two main categories of misuse.

When this suboptimal use of quality related health services is addressed properly and corrected, health outcomes are also improved and cost savings is

realized. Researchers at LDS Hospital in Salt Lake City reported a series programs aimed at reducing errors in the administration of antibiotics. The hospital reduced adverse events resulting from antibiotics by 30%, mortality of patients treated with antibiotics by 27%, overall antibiotic use by 23%, and antibiotic costs per treated patient by 58% (Pestotnik et al., 1996).

Mosadeghrad lists the categories of barriers for implementing TQM as; strategic, human resources, contextual, procedural, and structural with 39 individual items as shown in Table 13 (Mosadeghrad, 2013: 152).

Table 13: Barriers to Implementing TQM

Category	Barrier
Strategic	. poor management and leadership . lack of top management support . management turnover . middle-management resistance to change . inappropriate planning . placing a poor priority on quality improvement . unlimited demand for healthcare services
Human Resources	. lack of employees' interest in TQM . lack of employees' motivation and satisfaction . lack of employees' commitment and involvement . physicians' indifference towards TQM. . incompetent employees . employees' resistance to change . lack of good human resource management . inadequate empowerment at all levels . employee shortage, and increased work load . poor education and training . lack of recognition and reward for success.
Contextual	. inappropriate organizational culture . inter-departmental barriers . difficulties in changing organizational culture . lack of team orientation . poor communication . mindset barriers
Procedural	. lack of process focus . lack of focus on patient satisfaction . lack of customer awareness . complexity of processes . fragmentation of activities . bureaucracy and paperwork . lack of measurement, evaluation and self-assessment.
Structural	. inappropriate organizational structure . lack of physical resources . lack of information systems . lack of financial support . time shortage

Source: Mosadeghrad, 2013: 152

Dealing with the barriers to implementing quality measures should be approached through four levels of change: the individual, the group or team, the overall organization, and the larger system or environment in which individual organizations are embedded as shown in Table 14. Ferlie and Shortell (Ferlie and Shortell, 2001) indicate different methods and approaches of TQM and CQI used to address overcoming barriers to improve quality which can operate at multiple levels. They also mention that the effectiveness of the different approaches will be determined by the problem being addressed within the context of specific organizations and environments (Ferlie and Shortell, 2001: 284).

Table 14: Four Levels of Change for Improving Quality

Levels	Examples
Individual	Education Academic detailing Data feedback Benchmarking Guideline, protocol, pathway implementation Leadership development
Group/team	Team development Task redesign Clinical audits Breakthrough collaboratives Guideline, protocol, pathway implementation
Organization	Quality assurance Continuous quality improvement/total quality management Organization development Organization culture Organization learning Knowledge management/transfer
Larger system	National bodies (NICE, CHI, AHRQ) Evidence-based practice centers Accrediting/licensing agencies (NCQA,Joint Commission) Public disclosure (“report cards,” etc.) Payment policies Legal systems

Source: Ferlie & Shortell, 2001: 284

3.8. FACTORS INFLUENCING QUALITY EFFORTS

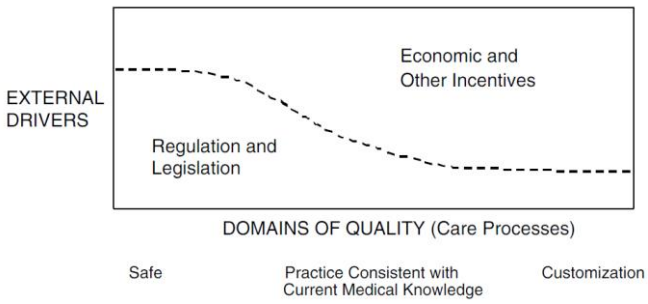
A variety of factors influence quality efforts within a healthcare organization. Culture, external environment, management, training are among the main factors.

Culture exists within the multiple levels of macro political, institutional, organizational and small group levels. Due to the wide variety professionals, subgroups, divisions, and teams operating, healthcare organizations are considered multicultural. Organizations' clinical culture and managerial culture can serve as a deterrent to quality improvements (Ferlie and Shortell, 2001: 293). Change strategies for quality are generally more complex than changes in structure. Therefore development of an organizational culture that truly value quality is an important force for change (Ferlie and Shortell, 2001: 292). In order to accomplish that, organization needs to question the way it learns best and evaluates the efforts to improve on learning practices (Argyris and Schon, 1978; Davie and Nutley, 2000; Levitt and March, 1988). In addition, in a group-oriented culture where teamwork, coordination, participation, and affiliation are emphasized, quality improvement practices are more successful (Shortell et al., 1995).

Environment also influences quality via two dimensions (Kohn et al., 2000: 18). Figure 42 shows the dimensions as well as the sub categories of the model proposed by Kohn et al. The first dimension, - domain of quality-, include safe care, practice consistent with medical knowledge, and customization. The second dimension identifies the external environment forces that can drive quality improvement in healthcare. Regulation and legislation, and economic and other incentives are the two external forces.

Safety part of the quality domain refers to "freedom from accidental injury", and it requires a larger role for regulation and oversight authority. Best practices, incorporating evidence based medicine and consistent with current medical knowledge is also part of the quality domain often showing a great deal of variability and lack of adherence to medical standards. Finally customization part of quality emphasizes customer-specific values and expectations allowing a great deal of flexibility for personalization and individual responsiveness. It requires a larger role for creative, continuous improvement and innovation within organizations and economic reward. Due to variety of individual preferences and needs, strong regulations are difficult to implement (Kohn et al., 2000).

Figure 42: Influence of the External Environment on Quality



Source: Kohn et al., 2000: 18

Part of the external forces, regulation and legislation might include any form of public policy or legal influence, such as licensing or a liability that can empower the senior management to take action internally to improve quality. It also pushes healthcare organizations to improve quality by requiring minimum investments in their systems. Economic and marketplace incentives allow more room to play for rewards more than the established industry minimum based on the performance.

As the population is aging and getting more diverse at technology, accessing health related information via Internet becomes easier (Calabretta, 2002; Frosch and Kaplan, 1999; Mansell et al., 2000), especially for more common chronic illnesses. Health professionals are not adequately prepared for this major shift. They need to have the proper skill set to respond to a variety of patient needs and expectations, to provide ongoing patient care and management, to deliver and coordinate care across teams, settings, and time frames; in short training they lack and in short supply part of clinical education settings (Calabretta, 2002). The Committee on the Health Professions Education Summit recommends to apply quality improvement as one of the responses to this issue (Greiner and Knebel, 2003).

Management involvement, especially top management is a crucial step for any quality improvement activity. Lack of top management involvement in and commitment to TQM change is the common reason for TQM failure (Hamidi and Zamanparvar, 2008; Kozak et al., 2007; Mosadeghrad, 2005). Just as managers can support TQM, they can also obstruct it. Juran (1988a) believed that most of the problems associated with quality are attributed to management. Initially, Juran and Gryna (1993) attribute the failure of the 1970s and 1980s quality initiatives in the West to lack of senior management involvement. Research also indicate low

management commitment and involvement can lead to failure in as many as 80% of organizations (Jaehn, 2000).

Another area where senior management is involved and has full responsibility for safety and quality improvements is the governance and compliance according to the imposed regulations (Conway, 2008). Ironically, maintaining compliance with regulatory requirements is frequently found to drive patient safety initiatives rather than hospitals initiating these programs for the intrinsic and real rewards due to improved quality of care (Devers et al., 2004).

One of the main reasons for a lack of top management involvement might be the diminishing concern rather than the indifference about quality issues. Senior management may be less aware of the patient safety issues than the front-line workers (Singer et al., 2003). In tall organizations as the number of levels increase, compared to flat organization, individuals tend to have a different perspective of the issues facing the front line employees (Child, 1984). In healthcare for example, board of directors perceive quality is better at their hospitals than their CEOs (Sandrick, 2007). This distance to the issues may potentially affect the level of priority senior management puts on quality and safety measures. Senior management might delegate the responsibility of quality governance to the medical staff as they have the clinical expertise for medical care evaluation. However, due to the perceived disincentives in peer review and the excessive time demands, physicians may not properly oversee a true quality improvement effort (Marren, 2004). Instead, active staff involvement in governance of quality efforts under senior management's control can significantly affect quality improvement activities (Weiner et al., 1996).

According to Wilson (2002), for an efficient and effective implementation of a quality management system, top management must:

- be the recognized leader of the QMS
- create an environment for an effective QMS
- assure compliance with a documented QMS
- supply the resources, training and support for employees implementing the QMS
- continually review the compliance performance of the organization
- recognize the successful efforts of the workforce

3.9. QUALITY MANAGEMENT SYSTEMS – ISO 9000

A variety of quality standards have been developed and adopted over the years. The ISO family of standards provided a consensus on good management practices for the purposes of ensuring organizations can deliver quality products or services. ISO 9000 standards originated in 1987 with a bulletin from the International Organization for Standardization (ISO) (Ferguson, 1996). The original series consisted of five standards: ISO 9000, 9001, 9002, 9003 and 9004, plus ISO 8402 (which was published in 1986 and it focused on terminology). The current series now has ISO 9000, 9001, 9004, 19011 (ISO, 2014).

ISO 9000 Quality Management System is a structural framework for business systems that consists of proper components aimed at imroving management practices. It earned a global reputation for establishing effective and efficient quality management best practices (ISO, 2009). The standards that are part of the ISO 9000 family are intended to be generic for quality management and assurance. They are applicable to any type of organization regardless of the size, products or services created, and the industry, private or public. The main purpose of the ISO 9000 standards is to assist and ensure organizations follow specific well-documented procedures in the making and/or delivery of their products or services (Van der Wiele et al., 2009), and identify strengths and weakness, help the evaluation of organizations, establish a basis for continuous improvement and allow and support external recognition (Oakland and Marosszeky, 2006).

Research has shown that there is a link between QA and QMS such as ISO 9000 family (Tutuncu et al., 2009: 9). The ISO 9001 which is part of the QMS family provides quality assurance to organizations allowing them implement a degree of standardization and procedural control. The quality concept and quality programs being used at present in healthcare belong to the quality assurance stage and, therefore, most institutions within this industry have not as yet implemented a QMS (Sedevich-Fons, 2013).

ISO 9001 focuses on processes rather than outcomes (Ozturk and Swiss, 2008). The standard encourages employees to demonstrate compliance with the procedures, rather than to strive for continuous improvement and focuses on doing things right, not necessarily doing the right things right from a customer point-of-view. The purpose of the standard is to ensure a quality management system exists, however it can't ensure the functionality of QMS with better performance (Curkovic

and Pagell, 1999; Martínez-Costa et al., 2009). In other word, it is quite possible to have an existing ISO 9000 system in place but still provide poor quality products or services. It alone does not provide competitive advantages (Corbett et al., 2005; Najmi and Kehoe, 2000; Sun et al., 2004). Therefore, healthcare organizations should not solely rely on the ISO quality management system. ISO 9001, through offering a set of policies and guidelines for quality management provides a foundation to TQM. It could be a starting point for TQM implementation.

CHAPTER FOUR
QUANTITATIVE RESEARCH

4.1. RESEARCH METHODS AND DESIGN

This study uses a quantitative approach to find out results for the set hypotheses exploring the collected data using survey questionnaire method. A quantitative research is defined as a process of inquiry exploring an identified issue based on checking a theory measured by numbers and analyzed with statistical techniques (Trochim, 2006). According to Creswell, examining specific instances or features of phenomena to decide if predictive generalizations regarding a theory hold true or to test causal hypotheses is the main purpose of a quantitative study (Creswell, 2013). Usually the design of quantitative studies are based on experiments (Trochim and Donnelly, 2005), however in our case it is a non-experimental study based on collected quantitative data. The use of a non-experimental survey methodology provides advantages including cause-and effect, high level of control, and most importantly the ability to replicate the study in similar circumstances (Blundell and Costa Dias, 2000).

The correlational aspect of the study explores relations among variables. Correlational studies generally are used to determine if relationships exist between variables and if so to find out the strength of the relationships and are used in hypothesis testing. The results do not provide any means for causation (Munro, 2005). Factor analysis is used to find out the interrelationships among a variety of factors in patient safety, quality, information security, and healthcare excellence and to explain these terms using the underlying dimensions. The objective is to find a way of condensing the information contained in a number of original variables into a smaller set of variables (factors) with minimal loss of information (Hair, 2009). According to Babbie (2012), exploratory studies can assist firstly better understand a new or under researched phenomenon, secondly test the feasibility of undertaking a more detailed study, and finally develop methods to be utilized in the detailed study.

Multiple regression technique is also applied to find out the impact of patient safety, quality, and information security on healthcare excellence. Hair (2009) defines multiple regression as "*a statistical technique that can be used to analyze the relationship between single dependent variable (DV) and several independent variables (IV*". Regression analysis is used to provide maximum prediction from the

IVs by weighing that is finding out the relative contributions of each IV to the overall prediction. The final set of weighted IVs form the *Regression Variate* or *Regression Equation*, or *Regression Model*.

4.1.1. Population and Sample

For this field study, Pamukkale University Training and Research Hospital has been chosen for the sample data collection. Research hospitals in general emphasize the importance of patient safety, quality, and information security related measures due to their focus on research programs and policies in order to provide new innovations, good care service, and obtain the best results through viable investment programs. Among all the research hospitals in the Aegean region in Turkey, Pamukkale Hospital along with the relevant participation of accredited standards responded and accepted our survey request regarding the topics mentioned.

The total number of people working for the hospital is 2433. As one of the key areas of the study was IS, IT department at the university was our point of contact. Our population was all staff who had valid user accounts utilizing hospital information systems and applications in one form or another. The questionnaires were distributed to 700 users from various units of the University at different positions who use IT systems frequently on a daily basis. Initially there were all together 30 different job titles gathered as part of the survey. However the job titles were varying and the number of responses for majority of the positions were low. Majority of the respondents were nurses and doctors. However there were other positions such as multiple types of technicians, therapists, pharmacists, medical assistants, accountants, human resources, administrative assistants, as well as academic titles such as associate professor, lecturers, instructors and others. Due to this broad category of job positions and titles, for data processing purposes six categories were formed to represent the general participant profiles as part of the demographics. The 6 categories are as follows; 1=Nurse, 2=Doctor, 3=Secretary, 4=Clinical Staff, 5=Non-Clinical Staff, 6=IT Staff.

4.1.2. Materials - Instrumentation

The development of the instruments for the questionnaire involved in-depth literature review pertinent to patient safety, information security, and quality management systems. The list of items intended to measure the constructs have been formed referencing to prior research and formed scales.

ISO 9000 quality and ISO 27000 IS management systems as well as safety climate surveys form the underlying structure of the study. Patient safety related items were formed based on the Safety Attitudes Questionnaire (SAQ)(Sexton et al., 2006). Quality related items are finalized referencing the quantitative study of Tutuncu et al. (Tutuncu et al., 2009). Studies (Upfold and Sewry, 2005; Yeniman Yildirim et al., 2011) that use ISO/IEC 27001 Information Security Management System have been used for the IS related items on the questionnaire. The validity and the reliability of the study hence been provided via these prior studies. In order to provide sufficient coverage, the list of items for each construct was evaluated by the researchers, academic experts and practitioners in the safety, quality, and IS management fields as well. The healthcare excellence part of the study has to do with the overall satisfaction its clients experience and the level of service the organizations provide. Essentially it is a generalized term pinpointing the integrated approach for the patient safety, information security, and quality management aspects of the healthcare environment.

The survey consisted of a 2 page questionnaire. A total of 55 questions were included on the list that were based on previous studies and were also examined in detail by academicians and practitioners to make sure items are understandable and applicable. Based on the comments and feedback, certain items and/or their wordings were modified. The finalized list was the basis for the questionnaire.

The questions have been translated into Turkish by native speakers who were subject matter experts and fluent in English. Proper wording changes have been done based on the feedback received.

An extract from the survey questionnaire is shown in Figure 43. The complete list of questions as part of the questionnaire is included in Appendix 1.

Figure 43: Questionnaire Extract

	Please mark the following questions according to the frequency of occurence. PATIENT SAFETY;	Never	Rarely	Sometimes	Often	Always
1	The culture of this clinical area makes it easy to learn from the mistakes of others.	①	②	③	④	⑤
2	Medical errors are handled appropriately in this clinical area.	①	②	③	④	⑤
3	The senior leaders in my hospital listen to me and care about my concerns.	①	②	③	④	⑤
4	The physician and nurse leaders in my area listen to me and care about my concerns.	①	②	③	④	⑤
5	Management is driving us to be a safety-centered institution.	①	②	③	④	⑤

The questions were presented using a five point interval scale in the form of; 1=Never, 2=Rarely, 3=Sometimes, 4=Often, 5=Always. The list addresses the following constructs; Patient Safety, Quality management systems, Information Security Management systems, Healthcare Excellence.

4.1.3. Operational Definitions of Variables

The questionnaire consists of 55 questions with 4 sections aimed at measuring patient safety, quality, information security, and healthcare excellence. The first section with 19 (V1-V19) questions refer to the patient safety aspect and are based on the Safety Attitudes Questionnaire (SAQ), the second part consisting of 16 questions, V20 – V35, refer to the quality management systems and based on qualitative study of Tutuncu et al. (Tutuncu et al., 2009), and the final section forms the information security part with 11 questions, V36-V46 based on the ISMS, ISO 27001 standard control groups. An additional 4 questions aimed at measuring participant's general attitudes of healthcare excellence within their institution regarding general safety, quality, and information security all together.

4.1.4. Data Collection

For data collection, questionnaire methodology was preferred as it was both a reliable, economical, and a simple way. The data were obtained through structured surveys based on current standards and methodological frameworks regarding the key dimensions. The field study was conducted early January 2014. The final version of the questionnaire was distributed to the healthcare staff working at the Pamukkale University Training and Research Hospital in various clinical and service departments in Denizli Turkey, along with the proper authorization forms

indicating management's approval such that the legality of the study was ensured. For better responses and participation, questionnaires have been distributed in batches at the same time to each clinical department via their departmental supervisor or via inter-office mail. In order to ensure high participation and the accuracy of the responses, participants were asked not to provide any identification as they complete the questionnaires. A time frame of a week or so given for the returns. The finished questionnaires were collected in batches and returned to us for data processing. In our case from the 700 distributed questionnaires, 460 were returned.

4.1.5. Data Processing

Data gathered via questionnaires have been entered manually into excel sheets, and transferred to SPSS program for further analysis. The manual entry process has been checked twice by different individuals to ensure accuracy. Out of the 460 respondents, 71 have been manually eliminated due to large number of missing data, duplicate entries, incorrect entries, empty items, and inconsistent ones, providing a total of 389 records for processing that also have missing entries. Part of the analysis for factor analysis and multiple-regression, listwise method has been used for any missing values to be excluded. Imputing missing values with the variable means was not preferred in order to provide consistency. The substitution of variable mean for the missing values is recommended when the ratio is low (Bentler, 1995).

4.1.6. Data Analysis

The main purpose of the study was to find out the factors associated with patient safety, information security management systems, and quality management systems and to test the impact of information security, patient safety, quality and their subcomponents on healthcare excellence. Patient safety, quality, and IS related management practices and the proper results were required to pursue the study. The data were analyzed using SPSS 19 software. The study used validated and reliable attitudinal measures to assess the variables under investigation. In a quantitative survey method, applying proper statistical analyses is an important factor for a successful outcome (Dillman, 2000; Schonlau et al., 2002).

There were missing responses for certain questions even after the duplicates and repetitive ones were removed visually. The listwise deletion method is used for all procedures to deal with missing values. Listwise deletion although affects the statistical power of the tests conducted (Olinsky et al., 2003; Roth, 1994), is preferable to many other methods for handling missing data (Allison, 2002).

Due to the categorical distribution of the demographic variables (V51-V55) certain new variables have been formed by recoding in order to do analysis. For example variable V53 indicates the education level and has 6 categories as 1=elementary school, 2=middle school, 3=high school, 4=associate degree, 5=undergraduate, 6=graduate. We were not able to use these categories due to allocation of numbers. Hence we had to create a new variable for analysis and separated the group into two as 1=basic education level 2=advanced education level. This enabled us to use some of the comparative tests properly. The same procedure was applied to V51 that addresses the age question. We separated the group into two as 1=29yrs or younger, 2=30 yrs or older. V55 indicated the years worked. Categorizing the V55 gave us 1=5 yrs or less at work, 2=6 yrs or more at work (see Appendix 19, 20).

An exploratory factor analysis is conducted on each part of the survey consisting of 50 observed variables to identify and measure the latent constructs that are not observable directly in safety, quality security and excellence areas. The orthogonal varimax method is used as the factors stayed uncorrelated throughout the process. If they had been correlated the oblique method of promax was going to be used (Hair, 2009).

All the safety, security and quality constructs are operationalized on a five point interval scale with multiple items developed using scales developed in literature. Exploratory factor analysis (EFA) is used to find out the factors. During the EFA process 6 factors have been explored as; Unit Patient Safety, General Patient Safety, Information Security, Quality Requirements, Continuous improvement - KAIZEN, and Healthcare Excellence.

Instead of using a mean value of the variables measuring a specific construct for each respondent, the standardized values obtained based on the regression coefficients of the factor analysis performed are used. This also provided the basis for Healthcare Excellence to be analyzed as a dependent variable using multiple-regression. Within the multiple-regression, the stepwise method is performed. The

stepwise method allows a simple yet efficient solution providing a small and interpretable model containing the most important predictors in a prediction problem.

Despite the advantages of stepwise selection disadvantages also exist. Many studies (Chatfield, 2006; Harrell et al., 1996; Steyerberg et al., 1999) indicate the following disadvantages:

- The selection is unstable; adding or deleting relatively few patients may substantially change the selection.
- The statistical power of a study may be insufficient to select true predictors, whereas multiple comparisons (almost) increase the risk that noise variables are included. Failure to select true predictors leads to a loss in predictive performance.
- The variance of the estimated regression coefficients is estimated as if the selection of covariables was predetermined. This biases the calculation of confidence intervals.
- The selection is based on the fact that a covariable had a relatively extreme p-value (usually: < 5%). This biases the p-values of selected covariables to extreme values.
- Extreme p-values correspond to relatively extreme regression coefficients. The estimated regression coefficients are biased to more extreme values.

The commonly accepted criterion for the sample size for a validity test is to have at least 100 participants or five times the number of questions in the instrument (Martins, 2002). Although the preferred ratio is 1:10, 1:5 is also acceptable. In our case we had 389 valid participants for 50 variables, more than the acceptable number of 250.

4.2. DEMOGRAPHICS

The questionnaire participants represented different job levels within the hospital enviconment. Nurses formed the major category (36.5%), followed by secretaries (admin assistants) (20.4%), the doctors (18%), clinical staff (12%), non-clinical-staff (9.6%), and IT staff (3.6%).

Majority of the participants were female (69%) more than double the size of male participants (30.5%) indicating healthcare sector seems to be a good working environment for females or that females are preferred in this sector. The age profile of the participants can be considered as young. The thirty to 39 years old (43.2%) form the major group followed by the 20 to 29 years olds (42.4%), 40-49 (10.5%), 20

or younger (2.6%), 50 or over (1.3%). These figures inform us that healthcare sector in Turkey is represented generally by younger people.

Largest number of participants were the ones who had worked for the hospital between one and five years (39.9%), followed by those with six to ten years (29.9%), eleven to twenty (18.5%), less than one year (10%) and more than twenty one years (1.9%). Nearly 80% of the participant's form the one to ten years of who had been with the hosptial. Majority of them had undergrad education (42.6%) while graduate education was one-third of the under grads (16.5%).

Table 15 shows the basic profile of the distribution of the participants.

Table 15: Survey Participants' Profile

		Overall		Female		Male	
		n	%	n	%	n	%
Job class							
	Nurse	122	36.53	112	91.80	10	8.20
	Doctor	60	17.96	28	46.67	32	53.33
	Secretary	68	20.36	54	79.41	14	20.59
	Clinical Staff	40	11.98	21	52.50	19	47.50
	Non-Clinical Staff	32	9.58	14	43.75	18	56.25
	IT Staff	12	3.59	3	25.00	9	75.00
	Total	334	100.00	232	69.46	102	30.54
Age							
	<20	10	2.63	8	80.00	2	20.00
	21-29	161	42.37	115	71.43	46	28.57
	30-39	164	43.16	115	70.12	49	29.88
	40-49	40	10.53	23	57.50	17	42.50
	>50	5	1.32	1	20.00	4	80.00
	Total	380	100.00	262	68.95	118	31.05
Education							
	High School	71	18.88	47	66.20	24	33.80
	Associate	83	22.07	56	67.47	27	32.53
	Undergraduate	160	42.55	120	75.00	40	25.00
	Graduate	62	16.49	37	59.68	25	40.32
	Total	376	100.00	260	69.15	116	30.85
Yearsworked							
	<1	38	10.03	22	57.89	16	42.11
	1-5	151	39.84	102	67.55	49	32.45
	6-10	113	29.82	84	74.34	29	25.66
	11-20	70	18.47	49	70.00	21	30.00
	>21	7	1.85	4	57.14	3	42.86
	Total	379	100.00	261	68.87	118	31.13

4.3. VALIDITY AND RELIABILITY

Validity encompasses the entire experimental concept and establishes whether the results obtained meet all of the requirements of the scientific research method and basically refers to how well a test measures what it is supposed to measure. According to Trochim (2006):

> *Validity refers to the approximate truth of propositions, inferences, or conclusions. So,* external *validity refers to the approximate truth of conclusions that involve generalization. In other words, it is the extent to which the results of the study can reflect similar outcomes elsewhere, and can be generalized to other populations or situations. On the other hand, internal Validity is the approximate truth about inferences regarding cause-effect or causal relationships. Thus, internal validity is only relevant in studies that try to establish a causal relationship.*

Internal validity is a crucial measure in quantitative studies, where it ensures that a researcher's experiment design closely follows the principle of cause and effect. External validity asks the question of generalizability: "*To what populations, settings, treatment variables and measurement variables can this effect be generalized?*" (Campbell et al., 1963).

Test Validity is an indicator of how much meaning can be placed upon a set of test results. Content validity, construct validity are the types of test validity. Content Validity is the estimate of how much a measure represents every single element of a construct while construct validity defines how well a test or experiment measures up to its claims. It also includes convergent and discriminant validity. Discriminant validity indicates that measures that should not be related are indeed not related. Convergent validity is in away the opposite. Measures that should be related are indeed related.

In our case content validity has been accomplished by working with the academicians and professionals who have extensive amount of experience on the subjects, and are considered as subject matter experts (SME). In addition from a theoretical perspective, face validity was covered through the relevant literature research related to the topics. Construct validity has been provided using exploratory factor analysis. Discriminant validity was established looking at the correlation tables as well as factor loading tables.

The goal of the factor analysis is "*to explain the variance in the observed variables in terms of underlying latent factors"* (Habing, 2003). In our case, the factor analysis provides the underlying structure of our set of observed variables pertinent

to patient safety, quality, information security, and healthcare excellence domains within healthcare. The 50 attributes (V1-V50) of the study are examined in order to understand whether these responses can be grouped to better understand the bigger picture in terms of what the healthcare workers think about these concepts, as well as reduce the 50 variables maybe to a smaller size if they can similarly be represented.

In order to understand the structure of the variables, R-type factor analysis and a correlation matrix between variables are required. Sample size is one of the concerns for the development of factors. Hair (2009) provides the minimum acceptable ratio of observations to variables as 5:1. In our study a total of 50 variables for around 380 observations meets this sample requirement and considered adequate.

The starting point for the factor analysis is the judgment of the appropriateness by visual examinations of the correlations and identification of the significant ones. If there are relatively few correlations greater than .30, then factor analysis is probably inappropriate (Hair, 2009). In our case for each of the structural concept of safety, quality, security and excellence the following exist:

for Safety, 156 out of 171 correlations (91%),

for Quality, 117 out of 117 correlations (100%)

for Security, 55 out of 55 correlations (100%)

for Excellence 6 out of 6 correlations (100%)

are significant at the .01 level which provides a sufficient basis to proceed with EFA for each concept (see Appendix 4,5,6,7,8 for correlation matrix tables).

Construct validity is established via EFA. In order to determine whether EFA is suitable or not, Kaiser-Meyer-Olkin measure of sampling adequacy (MSA), which ranges from 0 to 1 and Bartlett's test of Sphericity values are used to measure the intercorrelations between items. For MSA a value of .80 or above is perfect where .60 or above can be accepted, and below 0.50 is unacceptable (Hair, 2009). Bartlett's test of Sphericity is an indication of correlation among items. If it is statistically significant, the items are suitable for factor analysis.

In our study, Bartlett's test indicates that correlations when taken as a whole are significant at the .0001 level which indicates the presence of non-zero correlations. The KMO- measure of sampling adequacy checks correlations as well as the patterns between variables. As can be seen from the Table 16, the MSA for

safety, quality, security, and excellence are all above the acceptable range of .50 (see Appendix 9 for detail).

Table 16: Bartlett and MSA Values for Safety, Quality, Security, and Excellence

Factor	KMO – Kaiser-Meyer-Olkin Measure of Sampling Adequacy	Bartlett's Test of Sphericity	Sig.
Safety	.936	3028.339	.000
Quality	.958	4990.266	.000
Security	.957	3510.381	.000
Excellence	.858	1299.733	.000

Looking at each variable for the MSA values, only in safety dimension, V18 has a value of .413 (see Appendix 10 for detail). The V18 is excluded in order to meet the minimum acceptable level of .05. The deletion of V18 in safety provides a 100% correlation in safety among 153 correlations. The reduced set of safety items shows an overall MSA of .941 and the Bartlett value of 2989.499 still significant at .0001 level.

The results all indicated that the final set of variables for all safety, quality, security, and excellence are appropriate for factor analysis procedures (see Appendix 11, 12, 13, 14).

According to Hair (2009), in order to determine the number of factors to be retained for interpretation, either a subjective method of selecting a number of factors a priori or specifying the percentage of variance extracted, or an objective method of latent root criterion or scree test can be used. Table 17 shows the information regarding all the constructs and the components and their relative explanatory power explaining the variances in the total unrotated model. Only components where the eigenvalues above "1.0" are included for each construct using the latent root criterion as well as the scree test (see Appendix 15 for detail). According to Table 17, safety and quality have two factors to analyze, where IS and healthcare excellence have one.

Table 17: Extraction of Component Factors Based on Eigenvalues

Total Variance Explained

	Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
		Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
Patient Safety	1	8.797	48.870	48.870	8.797	48.870	48.870
	2	1.304	7.243	56.113	1.304	7.243	56.113
	3	.991	5.507	61.621			
	4	.923	5.129	66.749			
	…..	…..	…..	…..			
Quality Management	1	10.128	63.302	63.302	10.128	63.302	63.302
	2	1.115	6.966	70.268	1.115	6.966	70.268
	3	.745	4.657	74.925			
	4	.571	3.569	78.494			
	…..	…..	…..	…..			
Information Security	1	7.681	69.827	69.827	7.681	69.827	69.827
	2	.639	5.806	75.633			
	3	.449	4.083	79.716			
	…..	…..	…..	…..			
Healthcare Excellence	1	3.354	83.853	83.853	3.354	83.853	83.853
	2	.253	6.318	90.171			
	3	.218	5.457	95.628			
	…..	…..	…..	…..			

Extraction Method: Principal Component Analysis.

In order to interpret the factors within each construct the factor matrix of loadings can be used. The process compares the unrotated and the rotated factor matrices looking for the significant loadings and sufficient commonalities. The Factor loadings in factor matrices represent the degree of correlation between each variable and the factor (Hair, 2009), where the main objective is to associate each variable with a single factor as much as possible.

Tables 18, 19, 20, and 21 show the varimax rotated factor analysis for each of the constructs. Each table consists of the variables, the factors extracted, factor loadings, eigenvalues, and the variance explained. Details of the factor structure including communalities are included in Appendix 3. Communalities can be seen as a continuation of factor loadings. In our case, communalities and correlations are used to address the convergent validity as evident by the factor loadings. The communality column indicates the values are over the accepted value 0.5 (Campbell et al., 1963).

The Eigenvalues (sum of squared factor loadings) show the relative importance of each factor taking the variance associated with the set of variables as well as % of the total variance it contributes (Hair, 2009). Table 18 shows the two factors and loadings as well as the eigenvalues, and the total variance explained. Factor1 named General Patient Safety with a value of 5.915 accounts for most of the variance (32.86%). Similarly factor 2, Unit patient Safety has an eigenvalue of 4.19 and accounts for 23.25% of the total variance.

The factor loading patterns give us an idea of the overall factors associated with the constructs. Depending on the set value of the loading factor, certain entries can be excluded or hidden. So items with loadings of .40 and above are kept and below .40 are suppressed in the model (see Appendix 3 for all the loadings for each construct). The variables are also sorted based on the highest loading value for each factor. The communalities indicate the amount of variance in a particular variable is accounted for by the factors. For example for quality construct in Appendix 3, V27 has a communality of .757 which indicates it has more in common with the other variables included than V24 with a communality value of .427.

The patient safety construct has some variables (V5, V15, V14, V9, V19, and V8) that cross load on both factors of general and unit patient safety. For these variables the possible solutions include ignoring the cross-loading, deleting the variables, using another rotation technique or decreasing the number of factors. Using an oblique rotation such as promax instead of orthogonal varimax would eliminate this issue without changing the factor structure. Looking at the variables, the effect would be insignificant. Similarly in quality construct V23 cross-loads onto both factors. Promax rotation removes the cross-loading without changing the factor structure as well.

Power is defined by Hair as "*the probability of correctly rejecting the null hypothesis when it is false; that is , correctly finding a hypothesized relationship when it exists*" Hair (2009). He indicates to obtain a power level of 80 percent at a .05 significance level with 350 observations, a factor loading of .30 is required. He also suggests that practical significance of the decision to include variables is important. Loadings of .50 or greater are of great significance compared to those at 0.30.

Compared to Table 17 unrotated model, varimax rotation doesn't change the total amount of variance extracted. The variance is redistributed so that the factor loading pattern and the percentage of variance for each of the factors are slightly different and evenly distributed. Checking Table 18, General Patient Safety now has a 5.915 eigenvalue a reduction from the previous 8.797, explaining 32.86% instead of 48.870% of total variance. Other factors also change accordingly as shown.

Table 18: Patient Safety Factor Analysis Results

	Factor Loading	Eigen-Value	Variance Explained
F1 - General Patient Safety		5.915	32.86
My suggestions about safety would be acted upon if I expressed them to management	.80		
Briefings regarding patient safety are common here	.75		
The senior leaders in my hospital listen to me and care about my concerns	.71		
I receive appropriate feedback about my performance	.71		
Management is driving us to be a safety-centered institution	.70		
İ would feel safe being treated here as a patient	.69		
The physician and nurse leaders in my area listen to me and care about my concerns	.65		
This institution is doing more for patient safety now, than it did one year ago	.62		
I am satisfied with the availability of clinical leadership	.60		
Management does not knowingly compromise safety concerns for productivity	.59		
In our unit, system failures are not attributable to one individual's actions	.55		
I know the proper channels to direct questions regarding patient safety	.52		
F2 - Unit Safety		4.19	23.25
The culture of this clinical area makes it easy to learn from the mistakes of others	.79		
Briefing personnel before the start of a shift is an important part of patient safety	.75		
Patient safety is a priority in this clinical area	.67		
Medical errors are handled appropriately in this clinical area	.61		
I am encouraged by my colleagues to report any patient safety concerns I may have	.58		
The personnel would not mind taking additional responsibility for patient safety	.57		

Table 19: Quality Management Factor Analysis Results

	Factor Loading	Eigenvalue	Variance Explained
F1 - KAIZEN (Continous Quality Improvement)		7.59	47.41
Proper infrastructure is provided for quality service	.83		
Services are improved based on the findings	.81		
Services are delivered according to plans	.81		
Proper working conditions are provided for quality service	.81		
Management is able to plan for future and take the proper actions	.79		
Services and procedures are provided in coordination	.78		
Services provided are evaluated	.77		
Experienced staff exists for a quality service	.74		
Services provided are sufficient	.73		
Management provides the settings for authorithy, responsibility, and communication	.72		
Outcomes are controlled and analyzed	.71		
Management fulfills their responsibilities	.60		
Management is patient centric	.55		
F2 - General Quality Requirements		3.66	22.86
Appropriate records are maintained properly for our services	.88		
Definitions for care services are documented	.82		
Quality requirements are determined towards our services	.78		

Table 20: Information Security Factor Analysis Results

	Factor Loading	Eigenvalue	Variance Explained
F1 - Information Security		7.68	69.83
IS related incidents are handled according to the specific.....	.87		
Communications and operations mgmt. related proced...well defined	.87		
Physical and environmental security measures of the IS are in place	.86		
Access control policy ensures auth. access and prevents unauth..	.85		
In our institution, organization of IS is coordinated and .. handled	.85		
IT acquisitions, development, and maint. .handled according.. policies	.84		
IT security policies comply according to the standards and legal reqmt..	.84		
In our institution Inventory, ownership,... use of assets are managed ...	.83		
Business continuity plans are developed and.. to avoid interruptions....	.82		
Personnel fulfill their responsibilities according to the IS policies...	.81		
In our institution, work is handled.. to a documented uptodate IS policy	.78		

Table 21: Healthcare Excellence Factor Analysis Results

	Factor Loading	Eigenvalue	Variance Explained
F1 - Healthcare Excellence		3.35	83.85
In our institution, a complete patient safety is provided	.92		
In our institution, health care quality is ensured	.91		
İn our institution, a complete information security is provided	.91		
In our institution, quality service is provided	.91		

The reliability of a study tells us that the results are repeatable so that others can test them and verify the acceptance of the hypothesis based on the statistically significant results. Cronbach alpha values are used for each construct to determine the reliability based on internal consistency. Reliability has to do with the extent to which measurements are repeatable when conducted on various occasions by different researchers (Nunally and Bernstein, 1978). In addition, correlations among each construct is also provided and reliability testing has been done for the sample using Cronbach alpha value. Overall internal consistency and the reliability of all the items on the questionnaire taken as a whole is represented by the Cronbach alpha value of .979 indicating a very high level.

The final factor structure is shown in Table 22 including the reliability analysis of the solution as presented in terms of Cronbach's alpha covering each dimension, with values all exceeding 0.8. Higher values of alpha indicate higher reliability. For the reliability, though Cronbach alphas of .70 - .80 are acceptable, in top educational journals a value above .80 is used (Nunally and Bernstein, 1978; Osborne et al., 2001).

Examining the factor correlation matrix gives us some information regarding discriminant validity. Factor 3 is highly correlated with factors 1, 5, and 6. In addition factor 5 is with factor 6. This indicates majority of variance is being shared. However the factors are from theoretical perspective separate.

Table 22: Descriptive Statistics and Factor Correlations

Variables	1	2	3	4	5	6
1. General Patient Safety	1					
2. Unit Patient Safety	0.735*	1				
3. KAIZEN	0.763*	0.674*	1			
4. General Quality Requirement	0.568*	0.668*	0.701*	1		
5. Information Security	0.710*	0.638*	0.848*	0.721*	1	
6. Healthcare Excellence	0.713*	0.641*	0.801*	0.658*	0.803*	1
Means	3.455	4.036	3.663	4.047	3.800	3.776
Standard Deviation	0.27	0.19	0.13	0	0.05	0
Cronbach's Alpha	0.923	0.818	0.959	0.876	0.957	0.936

*. Correlation is significant at the 0.01 level (2-tailed)

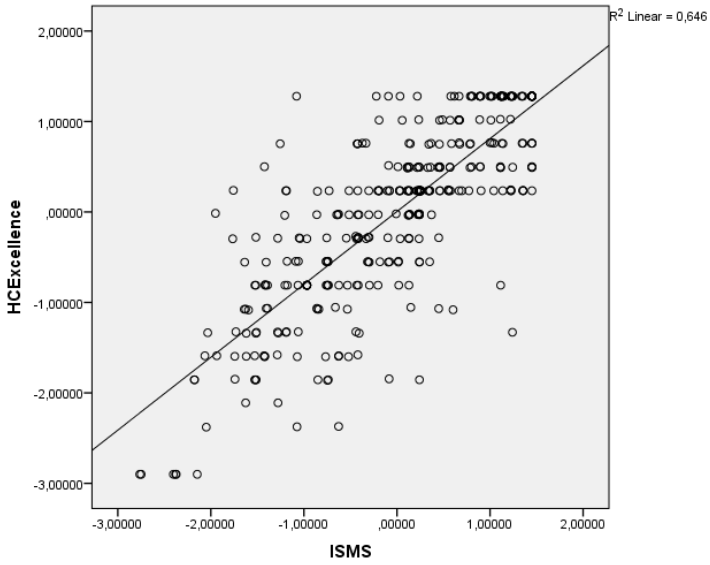
**. p value is significant at 0.01 level

The second phase of the study involved predicting the Healthcare Excellence dependent variable using the independent variables (IV) of General Patient Safety, Unit Patient Safety, General Quality Requirements, Kaizen, and Information Security. In order to proceed with the multiple-regression certain requirements needed to be established.

According to (Osborne and Waters, 2002), in order to proceed with a multiple regression study; (1) Variables need to be normally distributed. (2) A linear relationship between IVs and DV should exist. (3) Variables should be measured reliably. (4) Homoscedasticity, the variance of errors being the same across all levels of the IV, needs to be confirmed. In addition, multiple independent variables are needed for the multiple-regression. Multicollinearity is also another factor that needs to be analyzed. It is the situation where the correlations among IVs are very strong and the standard errors are incorrectly inflated causing statistical insignificance of variables when they should be significant.

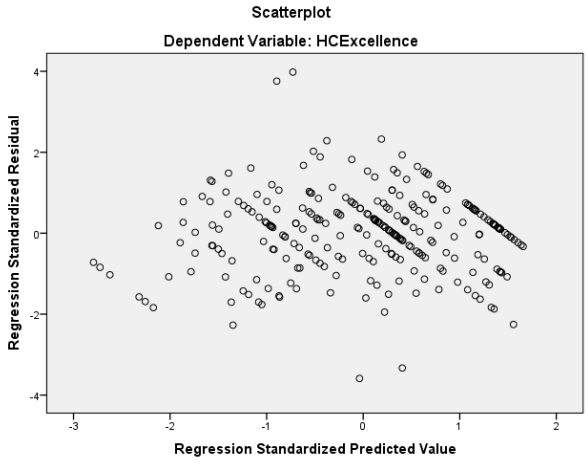
In our case, P-P plots and histograms are used to determine the normality aspect of the data, along with the scatter plots indicating the linear relationship among variables (see Appendix 16, 17, 18). Figure 44 shows the plot for Information security and healthcare excellence indicating a linear relationship.

Figure 44: Scatter Plot -Linearity for Regression



The Homoscedasticity assumption is confirmed checking at the plot of the standardized residuals as shown in Figure 45. The figure might present a very little bit of heteroscedasticity, but slight heteroscedasticity has little effect on significance tests and is not an issue (Berry and Feldman, 1985; Tabachnick and Fidell, 2001).

Figure 45: Plot of the Standardized Residuals



The Pearson correlations of the independent variables also indicate multicollinearity is not an issue as the absolute values are all less than 0.8 (see Appendix 21). The VIF values in Table 26 are also a good indicator of the nonexistence of multicollinearity.

Table 23 shows the model summary done using a stepwise method which indicates the value of *R*, the *multiple correlation coefficient, as .877 a good level of prediction for Healthcare Excellence.* The coefficient of determination, R^2 is the proportion of variance in the dependent variable *Healthcare Excellence* that can be explained by the independent variables. Here a value of .769 indicates that the independent variables together explain 77% of the variability of the dependent variable Healthcare Excellence. This is an overall measure of the strength of association and does not reflect the extent to which any particular independent variable is associated with the dependent variable (Nardi, 2006).

Table 23: Multiple Regression Model Summary

	R	R^2	*B*	SE	*β*	*t*
	0.877	0.769				
KAIZEN			0.365	0.58	0.353*	6.25
Information Security			0.331	0.061	0.319*	5.436
General Patient Safety			0.19	0.042	0.187*	4.495
General Quality			0.184	0.049	0.18*	3.754
Requirement						
Unit Patient			0.135	0.042	0.1328	3.246

Statistical significance : p<0.001

The detail model in Table 24 indicates values get better as each IV is added. All the IV are part of the model and none of them are excluded. Durbin Watson value informs us about whether the assumption of independent errors is tenable. A value closer to 2 is better, as Field (2013) suggests that values less than 1 or greater than 3 are cause for concern. In our case the value of 2.085 is acceptable.

Table 24: Detailed Model Summary for Multiple Regression

Model Summary[f]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.818[a]	.670	.668	.58808547	
2	.844[b]	.713	.711	.54945799	
3	.865[c]	.749	.746	.51479418	
4	.871[d]	.759	.756	.50474701	
5	.877[e]	.769	.764	.49580406	2.085

a. Predictors: (Constant), ISMS
b. Predictors: (Constant), ISMS, Kaizen
c. Predictors: (Constant), ISMS, Kaizen, GeneralQR
d. Predictors: (Constant), ISMS, Kaizen, GeneralQR, GeneralPS
e. Predictors: (Constant), ISMS, Kaizen, GeneralQR, GeneralPS, UnitPS
f. Dependent Variable: HCExcellence

The F-ratio in the ANOVA as shown in Table 25 tests whether the overall regression model is a good fit for the data or not. According to the model, the IVs; (constant), ISMS-Information security, Kaizen, GeneralQR-General quality requirements, GeneralPS-General patient safety, UnitPS-Unit patient safety, statistically significantly predict the dependent variable of HCExcellence-Healthcare Excellence therefore it is a good fit of the data. All five variables added statistically significantly to the prediction.

Table 25: ANOVA for the Multiple-Regression

ANOVA[f]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	185.842	1	185.842	537.356	.000[a]
	Residual	91.649	265	.346		
	Total	277.490	266			
2	Regression	197.788	2	98.894	327.567	.000[b]
	Residual	79.703	264	.302		
	Total	277.490	266			
3	Regression	207.792	3	69.264	261.361	.000[c]
	Residual	69.698	263	.265		
	Total	277.490	266			
4	Regression	210.741	4	52.685	206.796	.000[d]
	Residual	66.750	262	.255		
	Total	277.490	266			
5	Regression	213.331	5	42.666	173.566	.000[e]
	Residual	64.159	261	.246		
	Total	277.490	266			

a. Predictors: (Constant), ISMS
b. Predictors: (Constant), ISMS, Kaizen
c. Predictors: (Constant), ISMS, Kaizen, GeneralQR
d. Predictors: (Constant), ISMS, Kaizen, GeneralQR, GeneralPS
e. Predictors: (Constant), ISMS, Kaizen, GeneralQR, GeneralPS, UnitPS
f. Dependent Variable: HCExcellence

Table 26 shows unstandardized coefficients, standardized coefficients, significance and the collinearity statistics. According to the coefficients table, all independent variable coefficients are statistically significantly different from 0 (zero) in model 5. The coefficients (standardized or unstandardized) tell us the weight and the direction (positive or inverse) of the relationship of each IV with DP. The standardized coefficients (beta) compared to unstandardized are better as values are measured in standard deviation units. Therefore regardless of the different unit measures they can provide better insight to the model. The VIF values are less than 5 and the Tolerance values are over .20 indicating multicollinearity does not exist. Condition index of 4.507 shown in Table 27 also indicates multicollinearity is not an issue and that it is a good fit as it is much less than the accepted value of 30. (O'brien, 2007).

The regression model can be expressed as;

Healthcare Excellence = .319xISMS + .353*Kaizen + .180*GeneralQR + .187*GeneralPS + .132*UnitPS

The model indicates information and quality have more effect in predicting healthcare excellence.

Table 26: Coefficients - Multiple-Regression

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	-.042	.036		-1.177	.240		
	ISMS	.847	.037	.818	23.181	.000	1.000	1.000
2	(Constant)	-.048	.034		-1.413	.159		
	ISMS	.638	.048	.616	13.379	.000	.513	1.950
	Kaizen	.300	.048	.290	6.290	.000	.513	1.950
3	(Constant)	-.048	.032		-1.533	.127		
	ISMS	.372	.062	.359	5.974	.000	.264	3.783
	Kaizen	.488	.054	.472	9.013	.000	.349	2.869
	GeneralQR	.270	.044	.265	6.144	.000	.515	1.941
4	(Constant)	-.049	.031		-1.601	.111		
	ISMS	.336	.062	.324	5.419	.000	.257	3.898
	Kaizen	.435	.055	.421	7.868	.000	.321	3.114
	GeneralQR	.263	.043	.257	6.087	.000	.514	1.946
	GeneralPS	.134	.039	.131	3.402	.001	.617	1.621
5	(Constant)	-.051	.030		-1.694	.091		
	ISMS	.331	.061	.319	5.436	.000	.256	3.900
	Kaizen	.365	.058	.353	6.250	.000	.278	3.603
	GeneralQR	.184	.049	.180	3.754	.000	.386	2.589
	GeneralPS	.190	.042	.187	4.495	.000	.512	1.954
	UnitPS	.135	.042	.132	3.246	.001	.532	1.879

a. Dependent Variable: HCExcellence

Table 27: Collinearity Diagnostics for Multiple Regression

Collinearity Diagnostics[a]

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions					
				Constant	ISMS	Kaizen	GeneralQR	GeneralPS	UnitPS
1	1	1.001	1.000	.50	.50				
	2	.999	1.001	.50	.50				
2	1	1.698	1.000	.00	.15	.15			
	2	1.000	1.303	1.00	.00	.00			
	3	.302	2.371	.00	.85	.85			
3	1	1.849	1.000	.00	.07	.06	.05		
	2	1.023	1.345	.36	.00	.07	.21		
	3	.987	1.369	.64	.00	.04	.13		
	4	.142	3.614	.00	.93	.82	.61		
4	1	2.342	1.000	.00	.04	.04	.02	.07	
	2	1.053	1.491	.10	.01	.05	.33	.02	
	3	.994	1.535	.90	.00	.01	.04	.00	
	4	.470	2.232	.00	.07	.12	.00	.90	
	5	.141	4.069	.00	.89	.78	.61	.00	
5	1	2.567	1.000	.00	.03	.02	.02	.04	.03
	2	1.323	1.393	.00	.00	.03	.10	.08	.12
	3	1.000	1.602	1.00	.00	.00	.00	.00	.00
	4	.692	1.926	.00	.00	.08	.16	.17	.20
	5	.292	2.966	.00	.29	.02	.03	.64	.49
	6	.126	4.507	.00	.68	.84	.69	.07	.16

a. Dependent Variable: HCExcellence

CONCLUSION

a. Discussion

Regression analysis as expressed in the equation below indicates that there is a statistically significant relationship between information security and healthcare excellence, which was one of the hypotheses set. Due to the contribution of information security as indicated with beta coefficient of .319 predicting the overall Healthcare excellence we do not reject the $H11_a$ hypothesis.

Healthcare Excellence = .353*Kaizen + .319*Information Security + .187*General Patient Safety + .180*General Quality Requirements + .132*Unit Patient Safety

Similarly the analysis shows that there is a statistically significant relationship between general patient safety and healthcare excellence, as well as between unit patient safety and healthcare excellence. Thus, we do not reject the $H21_a$ and $H22_{a,}$ which also show that there is a statistically significant relationship between patient safety and healthcare excellence and therefore, we do not reject the $H2_a$ hypothesis.

Furthermore quality is also significant and the analysis shows that there is a statistically significant relationship between KAIZEN and healthcare excellence, as well as between general quality requirements and healthcare excellence. Thus, we do not reject the $H31_a$ and $H32_{a,}$ which also show that there is a statistically significant relationship between quality and healthcare excellence and therefore we do not reject the $H3_a$ hypothesis either.

The interesting outcome of this study, based on the model above is that Quality Management with KAIZEN and General Quality Requirements combined provides the highest explanation for the variances in Healthcare Excellence with the combined beta coefficient being 0.533, followed by Information Security with a beta coefficient of 0.319, and by Patient Safety with a total beta coefficient of 0.312 combined for General Patient Safety and Unit Patient Safety. These results indicate all three constructs have meaningful impact on explaining the healthcare excellence.

The results of the study are consistent with the findings of the previous studies taken as references for the scale constructions for each of the 3 dimensions; patient safety, information security, and quality management.

As a result of the analysis, from the patient safety items we ended up excluding the variable 18, which was a reverse question. The final dimensions and

the results for patient safety comply with and confirm the findings of the previous studies (Tutuncu, 2008) done in Turkey. These results also match and confirm the findings of the original study of Sexton (Sexton et al., 2006) on which the patient safety items were based with the exception of the reverse item 18 being excluded.

The findings related to the information security dimension provide new insight to the studies done previously in this area. Where the previous studies (Upfold and Sewry, 2005; Yeniman Yildirim et al., 2011) use ISO/IEC 17999 on a detail level of 10 items to find out the information security concerns of SMEs, our study approaches the information security issue in healthcare from a top, summary level and utilizes the new standard of ISO 27001 with minor changes.

As far as the quality management section of the study, the results of our study showed no differences compared to the previous studies of Tutuncu (Tutuncu, 2008; Tutuncu et al., 2009; Tutuncu and Erbil, 2006). As the items used on our study were based on the quality scale of Tutuncu, the two dimensions discovered confirmed the original quality scale of Tutuncu (Tutuncu et al., 2009) as well.

The important point to keep in mind is that all the three domains of information security, patient safety, and quality explain the healthcare excellence very well. For future work, if and when a scale for healthcare excellence is considered, these three dimensions should be considered and taken together. They should be made part of the new scale due to their high beta coefficients of the final regression model discovered in this study explaining the healthcare excellence.

b. Implications

The healthcare environment is a complex system highly interdependent on other systems but especially on technology and the people that exist within this system. As technology advances rapidly it is not easy to stay up-to-date and utilize the full benefits. Information part of a technological platform is a vital asset that knows no boundaries if not managed properly, and brings security issues for the most sensitive private data. Confidentiality, integrity and availability of data are concern for most people. Healthcare similar to financial sector is among the few institutions where protection of information is very crucial and most of the time is regulated by governmental policies in the developed countries. Information security is a crucial factor for a healthcare system running in harmony and providing excellent healthcare services.

Due to the complex “tightly coupled” nature of healthcare, the system is prone to errors, failures, and accidents affected by a variety of internal and external factors such as environment, technology, humans, training, organizational, and cultural issues. Proper working of the system full of these risks is the ultimate goal. So is safety as it is of immense importance especially when human lives are at stake. Adverse events causing negative impact on the overall system can be minimized making safety as an integral part of the system. Improvements in general patient safety as well as safety within departmental units in healthcare institutions and reduction of adverse medical events improve the overall system and provide a better, excellent healthcare. The degree of patient safety measures taken affects the overall healthcare excellence.

One of the main goals of the healthcare system is to provide good care and services using the available resources effectively and efficiently in order to minimize the impact on consumers. Quality standards can improve the processes, minimizing waste, allowing better, efficient, and effective working environments contributing to a high quality healthcare. Overall, information security and quality standards, in addition to patient safety measures do contribute and affect the overall state of healthcare excellence.

Healthcare organizations in private sector can utilize standards, frameworks, and methodologies in regards to information security and quality systems along with safety measures to improve and enhance the overall quality of care they provide to their clients. Obviously existence of standards, policies and regulations differ from country to country as well as their consequences. Still following and implementing best practices in regards to information security, quality, and patient safety provide a competitive edge as well as satisfaction to consumers for the care services they receive.

As our study indicates, quality and information security, along with safety play crucial roles in healthcare. Information security is a critical issue due to the privacy related regulations and the legal and governmental consequences. Security breaches in all forms cause big damages to organizations, and the reputation they worked so hard for. In addition to the monetary damages, non-monetary damages are very difficult to overcome. Management can utilize the safety, security, and quality components as the main building blocks of the system in such an integrated manner to develop strategic plans that would positively impact the overall healthcare excellence. Quality aspect is valued more in the eyes of consumers for any type of

product or service. Healthcare is not an exception. Patient safety is a concern most people as the consequences of not being healthy is a big concern. In order to improve quality of care and provide excellent service all these main building blocks need to exist in an integrated framework.

c. Recommendations

The study has a couple of limitations. The first and most important limitation is that the research has been carried out in a single hospital in Turkey. Therefore the study is limited with certain characteristics of the working environment in Denizli and of those people living in Denizli, Turkey. The applicability of the type of questions designed in western countries and the cultural differences might be considered as a limitation of the study as well. The responses given are probably affected by the environment, existing regulations, policies, and culture in Turkey. In addition the study references legal actions imposed by governments in other countries when there are information security related breaches in healthcare institutions regarding private data. There is a major gap between the consequences of these types of security incidents in Turkey and other developed countries; especially where governmental regulations are imposed and privacy of people are protected to the extreme. In general, there is a great benefit of conducting the study in other hospitals, in different cities in Turkey as well as in other countries. Comparative analysis then can be conducted further findings can be obtained that would assist our understanding of these topics and their use in practice.

Another area the study has limitations is the lack of certain statistical models which need to be pursued regarding this study. Especially the statistical technique of Structural Equation Modeling (SEM) along with Confirmatory Factor Analysis (CFA) should be deployed in future research to confirm the factors and design a better model of healthcare excellence, as well as to indicate the relationships among components. The model then can be compared with the existing theoretical frameworks and confirm the results, providing better understanding of the concepts.

REFERENCES

Adler-Milstein, J. and Cohen, G. R. (2013). Better Measurements for Realizing the Full Potential of Health Information Technologies. *The Global Information Technology Report 2013 (*pp. 81-91). Geneva: SRO-Kundig.

Advisory Committee for Safety in Nuclear Installations. (1993). Third Report: Organising for Safety, Study Group on Human Factors. Sheffield: ACSNI.

Aleccia, J. (2011). Nurse's suicide highlights twin tragedies of medical errors. *NBC News.* http://www.nbcnews.com/id/43529641/ns/health-health_care/t/nurses-suicide-highlights-twin-tragedies-medical-errors/#.VCG6yl-xWUk, (22.08.2013).

Alexander, J. A., Weiner, B. J., and Griffith, J. (2006). Quality improvement and hospital financial performance. *Journal of Organizational Behavior*. 27(7): 1003-1029.

Allison, P. D. (2002). Missing data: Quantitative applications in the social sciences. *British Journal of Mathematical and Statistical Psychology*. 55(1): 193-196.

Allnutt, M. (1987). Human factors in accidents. *British Journal of Anaesthesia*. 59(7): 856-864. Cited by Leape, (1994).

Almaraz, J. (1994). Quality management and the process of change. *Journal of Organizational Change Management*. 7(2): 06-14.

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*. 22(4): 308-313.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., . . . Savage, S. (2012). *Measuring the Cost of Cybercrime*. Paper presented at the 11th Annual Workshop on the Economics of Information Security (WEIS). Berlin,Germany. 25-26 June 2012.

Anderson, R., Böhme, R., Clayton, R., and Moore, T. (2009). Security economics and european policy. *Managing Information Risk and the Economics of Security* (pp. 55-80). New York: Springer.

Appari, A., Anthony, D. L., and Johnson, M. E. (2009). *HIPAA Compliance: An Examination of Institutional and Market Forces*. Paper presented at the 8th Annual

Workshop on the Economics of Information Security (WEIS). London,UK. 24-25 June 2009.

Appari, A. and Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management*. 6(4): 279-314.

Argyris, C. and Schon, D. (1978). *Organizational Learning: A Theory of Action Perspective*. Reading, MA: Addision Wesley.

Armijo, D., McDonnell, C., and Werner, K. (2009). Electronic health record usability: evaluation and use case framework. 09(10)-0091-1-EF. Rockville, MD: Agency for Healthcare Research and Quality. October 2009.

Ash, J. (1997). Organizational factors that influence information technology diffusion in academic health sciences centers. *Journal of the American Medical Informatics Association*. 4(2): 102-111.

Ash, J. S., Berg, M., and Coiera, E. (2004). Some unintended consequences of information technology in health care: the nature of patient care information system-related errors. *Journal of the American Medical Informatics Association*. 11(2): 104-112.

Ash, J. S., Sittig, D. F., Dykstra, R., Campbell, E., and Guappone, K. (2009). The unintended consequences of computerized provider order entry: findings from a mixed methods exploration. *Int J Med Inform*. 78(Supp 1): S69-S76.

Aspden, P., Corrigan, J. M., Wolcott, J., and Erickson, S. M. (2004). *Patient Safety: Achieving a New Standard for Care*. Washington, D.C.: The National Academies Press.

Aspden, P., Wolcott, J., Bootman, J. L., and Cronenwett, L. R. (2006). *Preventing medication errors: quality chasm series*. Washington, D.C.: The National Academies Press.

Aven, T. (2014). What is safety science? *Safety Science*. 67(0): 15-20.

Aven, T. and Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of risk research*. 12(1): 1-11.

Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics.* http://www.crcpress.com/product/isbn/9781466518254, (25.06.2013).

Babbie, E. (2012). *The practice of social research*. Belmonth, CA: Cengage Learning.

Bagian, J. P. (2006). Patient safety: lessons learned. *Pediatric radiology*. 36(4): 287-290.

Barley, S. R. (1986). Technology as an occasion for structuring: Evidence from observations of CT scanners and the social order of radiology departments. *Administrative science quarterly*. 31(1): 78-108.

Barley, S. R. (1990). The alignment of technology and structure through roles and networks. *Administrative science quarterly*. 35(1): 61-103.

Baskerville, R. (1988). *Designing information systems security*. New York, NY, USA: John Wiley & Sons, Inc.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR)*. 25(4): 375-414.

Batalden, P. and Buchanan, E. (1989). Industrial models of quality improvement. *Providing quality care: The challenge to clinicians*: 133-159.

Batalden, P. B. and Stoltz, P. K. (1995). Quality management and continual improvement of health care: a framework. *Journal of Continuing Education in the Health Professions*. 15(3): 146-164.

Bates, D. W. and Gawande, A. A. (2003). Improving safety with information technology. *New England Journal of Medicine*. 348(25): 2526-2534.

Bates, D. W., Leape, L. L., Cullen, D. J., Laird, N., Petersen, L. A., Teich, J. M., . . . Shea, B. (1998). Effect of computerized physician order entry and a team intervention on prevention of serious medication errors. *JAMA: the journal of the American Medical Association*. 280(15): 1311-1316.

Begun, J. W., Zimmerman, B., and Dooley, K. (2003). Health Care Organizations as Complex Adaptive Systems. *Advances in health care organization theory* (pp. 253-288). San Francisco, CA: Jossey-Bass.

Belden, J. L., Grayson, R., and Barnes, J. (2009). Defining and testing EMR usability: Principles and proposed methods of EMR usability evaluation and rating. *HIMSS EHR Usability Task Force*. Healthcare Information and Management Systems Society (HIMSS). https://himssconference.org/files/HIMSSorg/content/files/HIMSS_DefiningandTestingEMRUsability.pdf, (10.08.2013).

Belsis, P., Kokolakis, S., and Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. *Information Management & Computer Security*. 13(3): 189-202.

Bendell, T. (2006). A review and comparison of six sigma and the lean organisations. *The TQM Magazine*. 18(3): 255-262.

Bentler, P. M. (1995). *EQS structural equations program manual*. Encino,CA: Multivariate Software Inc.

Berner, E. S., Maisiak, R. S., Cobbs, C. G., and Taunton, O. D. (1999). Effects of a decision support system on physicians' diagnostic performance. *Journal of the American Medical Informatics Association*. 6(5): 420-427.

Berry, W. D. and Feldman, S. (1985). *Multiple regression in practice*. Thousand Oaks, CA: SAGE Publications.

Bertino, E. and Sandhu, R. (2005). Database security-concepts, approaches, and challenges. *Dependable and Secure Computing, IEEE Transactions on*. 2(1): 2-19.

Berwick, D. M. (1989). Continuous improvement as an ideal in health care. *The New England journal of medicine*. 320(1): 53.

Berwick, D. M. and Leape, L. L. (1999). Reducing errors in medicine: It's time to take this more seriously. *BMJ: British Medical Journal*. 319(7203): 136.

Bess, D. A. (2012). *Understanding Information Security Culture in an Organization: An Interpretive Case Study.* (3526079 Ph.D.), Nova Southeastern University, Ann Arbor. http://search.proquest.com/docview/1039269451, (22.07.2014).

Bilbao-Osorio, B., Dutta, S., and Lanvin, B. (2013). The Global Information Technology Report 2013. *Growth and Jobs in a Hyperconnected World*. Geneva: SRO-Kundig.

Bishop, T. F., Ryan, A. M., and Casalino, L. P. (2011). Paid malpractice claims for adverse events in inpatient and outpatient settings. *JAMA*. 305(23): 2427-2431.

Björck, F. (2004). *Institutional Theory: A New Perspective for Research into IS/IT Security in Organisations.* Paper presented at the 37th Hawaii International Conference on System Sciences (HICSS). Hawaii. 5-8 January 2004. Cited by Coles-Kemp, (2009).

Black, A. D., Car, J., Pagliari, C., Anandan, C., Cresswell, K., Bokun, T., . . . Sheikh, A. (2011). The impact of eHealth on the quality and safety of health care: a systematic overview. *PLoS medicine*. 8(1): e1000387.

Blakley, B., McDermott, E., and Geer, D. (2001). *Information security is information risk management.* Paper presented at the 2001 workshop on New security paradigms. Cloudcroft, New Mexico. 11-13 September 2001.

Blobel, B. (2002). *Analysis, design and implementation of secure and interoperable distributed health information systems* (Vol. 89). Amsterdam, The Netherlands: IOS Press. Cited by Orel, (2013).

Blumenthal, D. and Kilo, C. M. (1998). A report card on continuous quality improvement. *Milbank Quarterly*. 76(4): 625-648.

Blundell, R. and Costa Dias, M. (2000). Evaluation methods for non-experimental data. *Fiscal studies*. 21(4): 427-468.

Bogner, M. S. E. (1994). *Human error in medicine*. Hillsdale, NJ, England: Lawrence Erlbaum Associates, Inc.

Bower, M. (1966). *The will to manage*: McGraw-Hill. Cited by Smit and Dellemijn, (2011).

Boynton, B. C. (2007). *Identification of process improvement methodologies with application in information security.* Paper presented at the 4th annual conference on Information security curriculum development Kennesaw, Georgia, USA. 28-29 September 2007.

Brady, J. W. (2011). *Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers.* Paper presented at the 44th Hawaii International Conference on System Sciences (HICSS). Hawaii. 4-7 January 2011.

Brah, S. A., Tee, S. S., and Rao, B. M. (2002). Relationship between TQM and performance of Singapore companies. *International Journal of Quality & Reliability Management*. 19(4): 356-379.

Brennan, T. A., Gawande, A., Thomas, E., and Studdert, D. (2005). Accidental deaths, saved lives, and improved quality. *New England Journal of Medicine*. 353(13): 1405.

Brennan, T. A., Leape, L. L., Laird, N. M., Hebert, L., Localio, A. R., Lawthers, A. G., . . . Hiatt, H. H. (1991). Incidence of adverse events and negligence in hospitalized patients: results of the Harvard Medical Practice Study I. *New England Journal of Medicine*. 324(6): 370-376. Cited by Kohn et al., (2000).

Brenner, B. (2009). Heartland CEO on Data Breach: QSAs Let Us Down. http://www.csoonline.com/article/2124260/privacy/heartland-ceo-on-data-breach--qsas-let-us-down.html, (09.04.2014).

Breslow, L. (1972). A quantitative approach to the World Health Organization definition of health: physical, mental and social well-being. *International journal of Epidemiology*. 1(4): 347-355.

British Assessment Bureau. (2013). ISO 27001 update is around the corner. http://www.british-assessment.co.uk/news/iso-27001-update-is-around-the-corner, (23.08.2014).

Brown, D. R. and Harvey, D. F. (2011). *An experiential approach to organization development*. Upper Saddle River, NJ: Prentice Hall.

Brown Jr, C. R. and Uhl, H. S. (1970). Mandatory continuing education. *JAMA: the journal of the American Medical Association*. 213(10): 1660-1668. Cited by Lohr, (1990).

Burger, C. S. (1997). The use of problem knowledge couplers in a primary care practice. *Healthcare information management: journal of the Healthcare Information and Management Systems Society of the American Hospital Association*. 11(4): 13.

Burrell, G. and Morgan, G. (1979). *Sociological paradigms and organisational analysis* (Vol. 248). London: Ashgate Publishing. Cited by Scott et al., (2003).

BusinessDictionary.com. (2014). Business Dictionary. http://www.businessdictionary.com/definition/safety.html, (20.7.2014).

Cain, M. M., Mittman, R., Sarasohn-Kahn, J., and Wayne, J. C. (2000). Health e-people: the online consumer experience. *Institute for the Future*. http://www.chcf.org/publications/2000/08/health-epeople-the-online-consumer-experience, (23.12.2013).

Calabretta, N. (2002). Consumer-driven, patient-centered health care in the age of electronic information. *Journal of the Medical Library Association*. 90(1): 32.

Callahan, D. (1973). The WHO definition of'health'. *Hastings Center Studies*. 1(3): 77-87.

Camisón, C. (1996). Total quality management in hospitality: an application of the EFQM model. *Tourism management*. 17(3): 191-201.

Campbell, D. T., Stanley, J. C., and Gage, N. L. (1963). *Experimental and quasi-experimental designs for research*. Boston: Houghton Mifflin.

Carayon, P., Alvarado, C., and Hundt, A. S. (2003). *Reducing workload and increasing patient safety through work and workspace design*. Washington, D.C.: Institute of Medicine.

Carlisle, K. E. (1986). *Analyzing jobs and tasks*. Englewood Cliffs, NJ: Educational Technology Publications Inc. Cited by Palmieri et al., (2010).

Chan, M., Woon, I., and Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security*. 1(3): 18-41. Cited by Brady, (2011).

Chan, Y. E., Huff, S. L., Barclay, D. W., and Copeland, D. G. (1997). Business strategic orientation, information systems strategic orientation, and strategic alignment. *Information Systems Research*. 8(2): 125-150.

Chang, A. J.-T. and Yeh, Q.-J. (2006). On security preparations against possible IS threats across industries. *Information Management & Computer Security*. 14(4): 343-360.

Chang, S. E. and Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*. 106(3): 345-361.

Chang, S. E. and Lin, C.-S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*. 107(3): 438-458. Cited by Bess, (2012).

Chassin, M. R. (1991). Quality of care: time to act. *JAMA*. 266(24): 3472-3473.

Chassin, M. R. (1997). Assessing strategies for quality improvement. *Health Aff (Millwood)*. 16(3): 151-161.

Chassin, M. R. and Galvin, R. W. (1998). The urgent need to improve health care quality: Institute of Medicine National Roundtable on Health Care Quality. *JAMA*. 280(11): 1000-1005.

Chatfield, C. (2006). *Model uncertainty. Encyclopedia of Environmetrics.* http://onlinelibrary.wiley.com/doi/10.1002/9780470057339.vam030/pdf, (18.03.2014).

Child, J. (1984). *Organization: A guide to problems and practice*. London: Harper & Row Ltd.

Christianson, J. B., Warrick, L. H., Howard, R., and Vollum, J. (2005). Deploying Six Sigma in a health care system as a work in progress. *Joint Commission Journal on Quality and Patient Safety*. 31(11): 603-613.

Clark, B. R. (1970). *The distinctive college: Reed, Antioch, and Swarthmore*. Chicago: Aldine.

Classen, D. C. (1998). Clinical decision support systems to improve clinical practice and quality of care. *JAMA*. 280(15): 1360-1361.

Classen, D. C., Pestotnik, S. L., Evans, R. S., Lloyd, J. F., and Burke, J. P. (1997). Adverse drug events in hospitalized patients. Excess length of stay, extra costs, and attributable mortality. *JAMA*. 277(4): 301-306.

Classen, D. C., Resar, R., Griffin, F., Federico, F., Frankel, T., Kimmel, N., . . . James, B. C. (2011). 'Global trigger tool'shows that adverse events in hospitals may be ten times greater than previously measured. *Health Aff (Millwood)*. 30(4): 581-589.

Clemmer, T. P., Spuhler, V. J., Oniki, T. A., and Horn, S. D. (1999). Results of a collaborative quality improvement program on outcomes and costs in a tertiary critical care unit. *Critical care medicine*. 27(9): 1768-1774.

Coiera, E. (2003). Interaction design theory. *Int J Med Inform*. 69(2): 205-222.

Coiera, E., Aarts, J., and Kulikowski, C. (2012). The dangerous decade. *Journal of the American Medical Informatics Association*. 19(1): 2-5.

Coles-Kemp, L. (2009). Information security management: An entangled research challenge. *Information Security Technical Report*. 14(4): 181-185.

Computer History Museum. (2006). Timeline of Computer History. http://www.computerhistory.org/timeline/?year=1971, (14.04.2014).

Conrad, D., Wickizer, T., Maynard, C., Klastorin, T., Lessler, D., Ross, A., . . . Travis, K. (1996). Managing care, incentives, and information: an exploratory look inside the" black box" of hospital efficiency. *Health services research*. 31(3): 235.

Conway, M. (2008). Getting boards on board: engaging governing boards in quality and safety. *Joint Commission Journal on Quality and Patient Safety*. 34(4): 214-220.

Cook, R. I. and Woods, D. D. (1994). Operating at the sharp end: the complexity of human error. *Human error in medicine* (pp. 255-310). Hillsdale, NJ: Lawrence Erlbaum Associates. Cited by Kohn et al., (2000).

Cook, R. I., Woods, D. D., and Miller, C. (1998). *A tale of two stories: contrasting views of patient safety*. Chicago, IL: National Patient Safety Foundation. Cited by Kohn et al., (2000).

Cooke, R. A. and Rousseau, D. M. (1988). Behavioral Norms and Expectations A Quantitative Approach To the Assessment of Organizational Culture. *Group & Organization Management*. 13(3): 245-273.

Cooper, J. B., Newbower, R. S., Long, C. D., and McPeek, B. (1978). Preventable anesthesia mishaps: a study of human factors. *Anesthesiology*. 49(6): 399-406.

Cooper, M. D. and Phillips, R. A. (2004). Exploratory analysis of the safety climate and safety behavior relationship. *Journal of safety research*. 35(5): 497-512.

Corbett, C. J., Montes-Sancho, M. J., and Kirsch, D. A. (2005). The financial impact of ISO 9000 certification in the United States: An empirical analysis. *Management science*. 51(7): 1046-1059.

Cox, S. and Flin, R. (1998). Safety culture: philosopher's stone or man of straw? *Work & Stress*. 12(3): 189-201.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. London: Sage.

Crosby, P. B. (1979). *Quality is free: The art of making quality certain* (Vol. 94). New York, NY: McGraw-Hill

Croteau, A.-M. and Bergeron, F. (2001). An information technology trilogy: business strategy, technological deployment and organizational performance. *The Journal of Strategic Information Systems*. 10(2): 77-99.

Curkovic, S. and Pagell, M. (1999). A critical examination of the ability of ISO 9000 certification to lead to a competitive advantage. *Journal of quality management*. 4(1): 51-67.

D'Arcy, J. and Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics*. 89(1): 59-71. Cited by Brady, (2011).

Da Veiga, A. and Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*. 24(4): 361-372.

Da Veiga, A. and Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*. 29(2): 196-207.

Da Veiga, A., Martins, N., and Eloff, J. H. (2007). Information security culture-validation of an assessment instrument. *Southern African Business Review*. 11(1): 147-166.

Davenport, D. L., Henderson, W. G., Mosca, C. L., Khuri, S. F., and Mentzer Jr, R. M. (2007). Risk-adjusted morbidity in teaching hospitals correlates with reported levels of communication and collaboration on surgical teams but not with scale measures of teamwork climate, safety climate, or working conditions. *Journal of the American College of Surgeons*. 205(6): 778-784.

Davie, H. T. and Nutley, S. M. (2000). Developing learning organisations in the new NHS. *Bmj*. 320(7240): 998-1001.

Davies, H. T., Nutley, S. M., and Mannion, R. (2000). Organisational culture and quality of health care. *Quality in Health Care*. 9(2): 111-119.

Davis, R. E., Jacklin, R., Sevdalis, N., and Vincent, C. A. (2007). Patient involvement in patient safety: what factors influence patient participation and engagement? *Health Expectations*. 10(3): 259-267.

Dean, J. W. and Bowen, D. E. (1994). Management theory and total quality: improving research and practice through theory development. *Academy of management review*. 19(3): 392-418.

Dekker, S. W. (2002). Reconstructing human contributions to accidents: the new view on error and performance. *Journal of safety research*. 33(3): 371-385.

Delaney, B. C., Fitzmaurice, D. A., Riaz, A., and Hobbs, F. R. (1999). Can computerised decision support systems deliver improved quality in primary care? *BMJ: British Medical Journal*. 319(7220): 1281.

Deming, W. E. (1950). *Elementary Principles of the Statistical Control of Quality, JUSE*. Paper presented at the Japanese Union of Scientists and Engineers. Tokyo.

Deming, W. E. (1982). *Quality, productivity, and competitive position* (Vol. 183). Cambridge, MA: MIT-Center for Advanced Engineering Study (CAES).

Deming, W. E. (1986). *Out of the crisis*. Cambridge, MA: MIT-Center for Advanced Engineering Study (CAES). Cited by Moen and Norman, (2006).

Deming, W. E. (1993). *The new economics*. Cambridge, MA: MIT-Center for Advanced Engineering Study (CAES).

Dennis, A. (2002). *Networking in the internet age*. New York, NY: John Wiley & Sons, Inc. Cited by Williams, (2006).

DesRoches, C. M., Campbell, E. G., Rao, S. R., Donelan, K., Ferris, T. G., Jha, A., . . . Shields, A. E. (2008). Electronic health records in ambulatory care—a national survey of physicians. *New England Journal of Medicine*. 359(1): 50-60.

Detmer, D. (2000). Counterpoint. Your privacy or your health-will medical privacy legislation stop quality health care? *International Journal for Quality in Health Care*. 12(1): 1-3.

Devers, K. J., Pham, H. H., and Liu, G. (2004). What is driving hospitals' patient-safety efforts? *Health Aff (Millwood)*. 23(2): 103-115.

Dhillon, G. and Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*. 43(7): 125-128.

Dhillon, G. and Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*. 11(2): 127-153.

Dillman, D. A. (2000). *Mail and internet surveys: The tailored design method* (Vol. 2). Hoboken, NJ: John Wiley & Sons, Inc.

Dionach. (2011). Update to ISO 27001 Planned for 2013. http://www.dionach.com/blog/update-to-iso-27001-planned-for-2013, (23.08.2014).

Doherty, N. F. and Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security*. 25(1): 55-63.

Donabedian, A. (1966). Evaluating the quality of medical care. *The Milbank memorial fund quarterly*. 44(3): 166-206.

Donabedian, A. (1980). *Explorations in quality assessment and monitoring*. Ann Arbor, Michigan: Health Administration Press.

Donabedian, A. (1988). Quality assessment and assurance: unity of purpose, diversity of means. *Inquiry*. 25(1): 173-192.

Donabedian, A., Elinson, J., Spitzer, W., and Tarlov, A. (1987). Advances in health assessment conference discussion panel. *Journal of Chronic Diseases*. 40(Supplement 1): 183S-191S.

Donaldson, L. (1995). *American anti-management theories of organization: A critique of paradigm proliferation* (Vol. 25). Cambridge, Great Britain: Cambridge University Press.

Donaldson, M. S. and Lohr, K. N. (1994). *Health data in the information age: use, disclosure, and privacy*. Washington, D.C.: National Academies Press.

Dorr, D., Bonner, L. M., Cohen, A. N., Shoai, R. S., Perrin, R., Chaney, E., and Young, A. S. (2007). Informatics systems to promote improved care for chronic illness: a literature review. *Journal of the American Medical Informatics Association*. 14(2): 156-163.

dos Santos Moreira, E., Martimiano, L. A. F., dos Santos Brandão, A. J., and Bernardes, M. C. (2008). Ontologies for information security management and governance. *Information Management & Computer Security*. 16(2): 150-165.

Dourish, P. and Anderson, K. (2006). Collective information practice: emploring privacy and security as social and cultural phenomena. *Human-computer interaction*. 21(3): 319-342.

Dragovic, B. and Crowcroft, J. (2004). *Information exposure control through data manipulation for ubiquitous computing.* Paper presented at the 2004 workshop on New security paradigms. Nova Scotia, Canada. 20-23 September 2004.

Dranove, D. and Ludwick, R. (1999). Competition and pricing by nonprofit hospitals: a reassessment of Lynk's analysis. *J Health Econ*. 18(1): 87-98. Cited by Hassan and Kanji, (2007).

Drevin, L., Kruger, H., and Steyn, T. (2006). Value-Focused Assessment of Information Communication and Technology Security Awareness in an Academic Environment. *Computers & Security*. 26: 36-43.

Dunkerley, K. D. (2011). *Developing an Information Systems Security Success Model for Organizational Context.* (3456547 Ph.D.), Nova Southeastern University, Ann Arbor. http://search.proquest.com/docview/871586432, (12.03.2014).

Dutta, A. and McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review*. 45(1): 67-87.

Dwyer, C. (1999). Ideas and trends: medical informatics and health care computing. *Annals of internal medicine*. 130(2): 170-172.

Edwards, P., Huang, D., Metcalfe, L., and Sainfort, F. (2007). Maximizing your investment in EHR. Utilizing EHRs to inform continuous quality improvement. *Journal of healthcare information management: JHIM*. 22(1): 32-37.

Eisenberg, J. M., Bowman, C. C., and Foster, N. E. (2001). Does a healthy health care workplace produce higher-quality care? *Joint Commission Journal on Quality and Patient Safety*. 27(9): 444-457. Cited by Yassi and Hancock, (2005).

El-Jardali, F. and Lagace, M. (2004). Making hospital care safer and better: the structure-process connection leading to adverse events. *Healthcare quarterly (Toronto, Ont.)*. 8(2): 40-48. Cited by Yassi and Hancock, (2005).

Elkin, N. (2008). How America searches: Health and Wellness. http://www.icrossing.com/sites/default/files/how-america-searches-health-and-wellness.pdf, (02.12.2013).

Eloff, J. H. and Eloff, M. (2003). *Information security management: a new paradigm.* Paper presented at the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology.

Eloff, J. H. P. and Eloff, M. M. (2005). Information security architecture. *Computer Fraud & Security*. 2005(11): 10-16.

Evans, J. R. and Lindsay, W. M. (1996). *The management and control of quality*. Mason, OH: South-Western.

Evans, R. S., Pestotnik, S. L., Classen, D. C., and Burke, J. P. (1999). Evaluation of a computer-assisted antibiotic-dose monitor. *Annals of Pharmacotherapy*. 33(10): 1026-1031.

Evans, R. S., Pestotnik, S. L., Classen, D. C., Clemmer, T. P., Weaver, L. K., Orme Jr, J. F., . . . Burke, J. P. (1998). A computer-assisted management program for antibiotics and other antiinfective agents. *New England Journal of Medicine*. 338(4): 232-238.

Feigenbaum, A. (1983). Total quality control. New York, NY: McGraw-Hill.

Ferguson, W. (1996). Impact of the ISO 9000 series standards on industrial marketing. *Industrial Marketing Management*. 25(4): 305-310.

Ferlie, E. B. and Shortell, S. M. (2001). Improving the Quality of Health Care in the United Kingdom and the United States: A Framework for Change. *Milbank Quarterly*. 79(2): 281-315.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. London: Sage.

Fisher, D. C. and Simmons, B. P. (2012). *The Baldrige workbook for healthcare*. New York, NY: Quality Resources.

Flanagan, J. C. (1954). The critical incident technique. *Psychological bulletin*. 51(4): 327. Cited by Palmieri et al., (2010).

Flin, R. (2007). Measuring safety culture in healthcare: A case for accurate diagnosis. *Safety Science*. 45(6): 653-667.

Flin, R., Mearns, K., O'Connor, P., and Bryden, R. (2000). Measuring safety climate: identifying the common features. *Safety Science*. 34(1–3): 177-192.

Flynn, B. B., Schroeder, R. G., and Sakakibara, S. (1994). A framework for quality management research and an associated measurement instrument. *Journal of Operations management*. 11(4): 339-366.

Flynn, N. (2001). *The E-policy handbook: designing and implementing effective E-mail, Internet, and software policies*. New York, NY: AMACOM Div American Mgmt Assn.

Fox, S. and Duggan, M. (2012). Mobile Health 2012. http://www.pewinternet.org/2012/11/08/mobile-health-2012/, (24.06.2014).

Fox, S. and Jones, S. (2009). The Social Life of Health Information. http://www.pewinternet.org/Reports/2009/8-The-Social-Life-of-Health-Information.aspx, (16.04.2014).

Fox, S. and Rainie, L. (2014). The Web at 25 in the U.S. *Internet Project*. http://www.pewinternet.org/2014/02/27/the-web-at-25-in-the-u-s/, (04.04.2014).

Franke, R. H., Hofstede, G., and Bond, M. H. (1991). Cultural roots of economic performance: A research noteA. *Strategic management journal*. 12(S1): 165-173.

Franqueira, V. N., Lopes, R. H., and van Eck, P. (2009). *Multi-step attack modelling and simulation (MsAMS) framework based on mobile ambients.* Paper presented at the 2009 ACM symposium on Applied Computing. Honolulu, Hawaii, U.S.A. 8-12 March 2009.

Frosch, D. L. and Kaplan, R. M. (1999). Shared decision making in clinical medicine: past research and future directions. *American journal of preventive medicine*. 17(4): 285-294.

Fulford, H. and Doherty, N. F. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security*. 11(3): 106-114.

Gaba, D. M., Maxwell, M., and DeAnda, A. (1987). Anesthetic mishaps: breaking the chain of accident evolution. *Anesthesiology*. 66(5): 670-676.

Gaba, D. M., Singer, S. J., Sinaiko, A. D., Bowen, J. D., and Ciavarelli, A. P. (2003). Differences in safety climate between hospital personnel and naval aviators. *Human Factors: The Journal of the Human Factors and Ergonomics Society*. 45(2): 173-185.

Gamma. (2013). The new versions of ISO/IEC 27001 and 27002 are now International Standards. http://www.gammassl.co.uk/27001/revision.php, (23.08.2014).

Gandhi, T. K. and Lee, T. H. (2010). Patient safety beyond the hospital. *New England Journal of Medicine*. 363(11): 1001-1003.

Garg, A. X., Adhikari, N. K., McDonald, H., Rosas-Arellano, M. P., Devereaux, P., Beyene, J., . . . Haynes, R. B. (2005). Effects of computerized clinical decision support systems on practitioner performance and patient outcomes: a systematic review. *JAMA*. 293(10): 1223-1238.

Garvin, D. A. (1983). Quality on the line. *Harvard business review*. 61(5): 65-75.

Garvin, D. A. (1986). *A Note on Quality: The Views of Deming, Juran, and Crosby.* http://hbr.org/product/recommended/an/687011-HCB-ENG?referral=02153&cm_vc=rr_item_page.horizontal, (20.05.2014).

Garvin, D. A. (1988). *Managing quality: The strategic and competitive edge*. New York, NY: The Free Press.

Garvin, D. A. (1991). How the Baldrige Awar Really Works. *Harvard business review*.

Gerber, M. and von Solms, R. (2005). Management of risk in the information age. *Computers & Security*. 24(1): 16-30.

Gerber, M. and von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security*. 27(5–6): 124-135.

Gershon, R. R., Karkashian, C. D., Grosch, J. W., Murphy, L. R., Escamilla-Cejudo, A., Flanagan, P. A., . . . Martin, L. (2000). Hospital safety climate and its relationship with safe work practices and workplace exposure incidents. *Am J Infect Control*. 28(3): 211-221.

Goedert, J. (2011). Tackling the health IT workforce shortage. *Health Data Manag*. 19(2): 40-47.

Goldman, J. (1998). Protecting privacy to improve health care. *Health Aff (Millwood)*. 17(6): 47-60.

Gosling, A. S., Westbrook, J. I., and Braithwaite, J. (2003). Clinical team functioning and IT innovation: a study of the diffusion of a point-of-care online evidence system. *Journal of the American Medical Informatics Association*. 10(3): 244-251.

Gregorich, S. E., Helmreich, R. L., and Wilhelm, J. A. (1990). The structure of cockpit management attitudes. *Journal of Applied Psychology*. 75(6): 682.

Greiner, A. C. and Knebel, E. (2003). *Health Professions Education: A Bridge to Quality*. Washington, D.C.: The National Academies Press.

Guldenmund, F. W. (2000). The nature of safety culture: a review of theory and research. *Safety Science*. 34(1): 215-257.

Guzman, I. R., Stam, K. R., and Stanton, J. M. (2008). The occupational culture of IS/IT personnel within organizations. *ACM SIGMIS Database*. 39(1): 33-50.

Habing, B. (2003). Exploratory Factor Analysis. http://www.stat.sc.edu/~habing/courses/530EFA.pdf, (24.08.2014).

Hair, J. F. (2009). *Multivariate data analysis*. New York, NY: Prentice Hall.

Hakes, C. (1991). *Total quality management: the key to business improvement*. Suffolk, Great Britain: St Edmundsbury Press Ltd. Cited by Zhu, (1999).

Halbesleben, J. R., Wakefield, B. J., Wakefield, D. S., and Cooper, L. B. (2008). Nurse Burnout and Patient Safety Outcomes Nurse Safety Perception Versus Reporting Behavior. *Western Journal of Nursing Research*. 30(5): 560-577.

Hamidi, Y. and Zamanparvar, A. (2008). Quality management in health systems of developed and developing countries: which approaches and models are appropriate? *Journal of research in health sciences*. 8(2): 40-50.

Hammons, T., Piland, N., Small, S., Hatlie, M., and Burstin, H. (2001). An Agenda for Research in Ambulatory Patient Safety: Conference Synthesis. Rockville, MD: Agency for Healthcare Research and Quality.

Hansson, J. and Eriksson, H. (2002). The impact of TQM on financial performance. *Measuring Business Excellence*. 6(4): 44-54.

Hanuscak, T. L., Szeinbach, S. L., Seoane-Vazquez, E., Reichert, B. J., and McCluskey, C. F. (2009). Evaluation of causes and frequency of medication errors during information technology downtime. *American Journal of Health-System Pharmacy*. 66(12): 1119-1124.

Harms-Ringdahl, L. (2003). *Safety analysis: principles and practice in occupational safety*. New York, NY: Taylor & Francis.

Harrell, F., Lee, K. L., and Mark, D. B. (1996). Tutorial in biostatistics multivariable prognostic models: issues in developing models, evaluating assumptions and adequacy, and measuring and reducing errors. *Statistics in medicine*. 15(4): 361-387.

Harris, J. and Cummings, M. (2007). Compliance issues and IS degree programs. *Journal of Computing Sciences in Colleges*. 23(1): 14-20.

Harrison, M. I., Koppel, R., and Bar-Lev, S. (2007). Unintended consequences of information technologies in health care—an interactive sociotechnical analysis. *Journal of the American Medical Informatics Association*. 14(5): 542-549.

Hassan, D. K. and Kanji, G. K. (2007). *Measuring Quality Performance in Health Care: The Effect of Joint Commission International Standards on Quality Performance*. West Sussex, UK: Kingsham Press.

Häyrinen, K., Saranto, K., and Nykänen, P. (2008). Definition, structure, content, use and impacts of electronic health records: a review of the research literature. *Int J Med Inform*. 77(5): 291-304.

Hazlehurst, B., McMullen, C., Gorman, P., and Sittig, D. (2003). *How the ICU follows orders: care delivery as a complex activity system.* Paper presented at the AMIA 2003 Annual Symposium. Washington, D.C. 8-12 November 2003.

Healthcare Information and Management Systems Society. (2009). 2009 HIMSS Security Survey. https://www.himss.org/files/HIMSSorg/content/files/HIMSS2009SecuritySurveyReport.pdf, (12.03.2014).

Hellriegel, D., Slocum Jr, J., and Woodman, R. (2001). *Organizational Behavior*. Mason, OH: Thomson Learning, South-Western College Publishing.

Hellsten, U. and Klefsjö, B. (2000). TQM as a management system consisting of values, techniques and tools. *The TQM Magazine*. 12(4): 238-244.

Helmreich, R., Merritt, A., Sherman, P., Gregorich, S., and Wiener, E. (1993). The flight management attitudes questionnaire (FMAQ). *(*pp. 93-95). Austin, TX: University of Texas.

Helmreich, R. L. and Merritt, A. C. (1998). *Culture at work in aviation and medicine: National, organizational, and professional influences*. Brookfield, VT: Ashgate.

Helmreich, R. L. and Wilhelm, J. A. (1991). Outcomes of crew resource management training. *The International Journal of Aviation Psychology*. 1(4): 287-300. Cited by Palmieri et al., (2010).

Hemmelgarn, A. L., Glisson, C., and Dukes, D. (2001). Emergency room culture and the emotional support component of family-centered care. *Children's Health Care*. 30(2): 93-110.

Hendricks, K. B. and Singhal, V. R. (2001). Firm characteristics, total quality management, and financial performance. *Journal of Operations management*. 19(3): 269-285.

Herold, R. (2009). HIPAA enforcement getting stronger. http://searchcompliance.techtarget.com/tip/HIPAA-enforcement-getting-stronger, (14.04.2014).

Hewitt, M. and Simone, J. V. (2000). *Enhancing data systems to improve the quality of cancer care*. Washington, D.C.: The National Academies Press.

Higgs, E. (1997). Health informatics blueprint: business needs. *Information Management & Computer Security*. 5(2): 58-62.

Ho, S. K. (1994). Is the ISO 9000 series for total quality management? *International Journal of Quality & Reliability Management*. 11(9): 74-89.

Hodge Jr, J. G., Gostin, L. O., and Jacobson, P. D. (1999). Legal issues concerning electronic health information: privacy, quality, and liability. *JAMA*. 282(15): 1466-1471.

Hoffer, J. A. and Straub, D. W. (1989). The 9 to 5 Underground-Are You Policing computer Crimes. *Sloan management review*. 30(4): 35-43.

Hoffman, R. R. and Woods, D. D. (2000). Studying cognitive systems in context: Preface to the special section. *Human Factors: The Journal of the Human Factors and Ergonomics Society*. 42(1): 1-7.

Holden, R. J. and Karsh, B.-T. (2010). The technology acceptance model: its past and its future in health care. *Journal of biomedical informatics*. 43(1): 159-172.

Holweg, M. (2007). The genealogy of lean production. *Journal of Operations management*. 25(2): 420-437. Cited by National Learning Consortium, (2013).

Hong, K.-S., Chi, Y.-P., Chao, L. R., and Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*. 11(5): 243-248.

Hoyle, D. (2001). *ISO 9000: quality systems handbook*. Woburn, MA: Butterworth-Heinemann.

Hsiao, C.-J. and Hing, E. (2012). *Use and Characteristics of Electronic Health Record Systems Among Office-based Physician Practices, United States, 2001-2012*: US Department of Health and Human Services, Centers for Disease Control and Prevention, National Center for Health Statistics.

Huang, L., Bai, X., and Nair, S. (2008). *Developing a SSE-CMM-based security risk assessment process for patient-centered healthcare systems.* Paper presented at the 6th international workshop on Software quality. Leipzig, Germany. 10 May 2008.

Humphreys, T. (2006). State-of-the-art information security management systems with ISO/IEC 27001: 2005. *ISO Management Systems*. 6(1): 15-18.

Hunt, D. L., Haynes, R. B., Hanna, S. E., and Smith, K. (1998). Effects of computer-based clinical decision support systems on physician performance and patient outcomes: a systematic review. *JAMA*. 280(15): 1339-1346.

Hutchins, E. (1995). *Cognition in the Wild* (Vol. 262082314). Cambridge, MA: MIT press

Hutt, A. E., Hoyt, D. B., and Bosworth, S. (1995). *Computer Security Handbook*. New York, NY: John Wiley & Sons, Inc. .

Iivari, J. and Hirschheim, R. (1996). Analyzing information systems development: A comparison and analysis of eight IS development approaches. *Information Systems*. 21(7): 551-575.

Imai, M. (1986). *Kaizen: The key to Japan's competitive success*. New York, NY: McGraw-Hill. Cited by Moen and Norman, (2006).

Institute of Medicine. (1974). *Advancing The Quality of Health Care: A Policy Statement*. Washington, D.C.: The National Academies Press.

Institute of Medicine. (1999). To Err is Human: Building a Safer Health System. Washington, D.C.: The National Academy Press.

Institute of Medicine. (2000). *Networking Health: Prescriptions for the Internet*. Washington, D.C.: The National Academies Press.

Institute of Medicine. (2001). *Crossing the quality chasm: A new health system for the 21st century*. Washington, D.C.: The National Academies Press.

Institute of Medicine. (2004). Keeping Patients Safe: Transforming the Work Environment of Nurses. Washington, D.C.: The National Academies Press.

Institute of Medicine. (2012). *Health IT and Patient Safety: Building Safer Systems for Better Care*. Washington, D.C.: The National Academies Press.

International and Civil Aviation Organization. (2014). Safety Report. http://www.skybrary.aero/bookshelf/books/2698.pdf, (07.06.2014).

International Nuclear Safety Advisory Group. (1991). Summary report on the post accident review meeting on the chernobyl accident (75-insag-1). Vienna: IAEA. Cited by Palmieri et al., (2010).

Ishikawa, K. (1985). *What Is Total Quality Control: The Japanese Way.* Englewood Cliffs, NJ: Prentice-Hall. Cited by Moen and Norman, (2006).

ISO-27001. (2005). ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements: ISO.

ISO-IEC. (2004). ISO-IEC Guide 2:2004(E/F/R), ISO/IEC. Geneva.

ISO 8402. (1986). Quality Vocabulary. Geneva: The International Organization for Standardization.

ISO. (2009). Selection and use of the ISO 9000 family of standards. http://www.iso.org/iso/iso_9000_selection_and_use-2009.pdf, (04.06.2014).

ISO. (2014). ISO 9000 - Quality management. http://www.iso.org/iso/iso_9000, (18.07.2014).

ISO/IEC-27000. (2014). ISO/IEC 27000:2014 Overview and Vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en, (04.06.2014).

Ives, B. and Olson, M. H. (1984). User involvement and MIS success: a review of research. *Management science*. 30(5): 586-603.

Jackson, D., Thomas, M., and Millett, L. I. (2007). *Software for Dependable Systems: Sufficient Evidence?* Washington, D.C.: National Academies Press.

Jaehn, A. (2000). Requirements for total quality leadership. *Intercom*. 47(10): 38-39.

James, J. T. (2013). A new, evidence-based estimate of patient harms associated with hospital care. *Journal of Patient Safety*. 9(3): 122-128.

Jaques, E. (1951). *The Changing Culture of a Factory*. London: Tavistock Publication Ltd. Cited by Scott et al., (2003).

Jarlier, A. and Charvet-Protat, S. (2000). Can improving quality decrease hospital costs? *International Journal for Quality in Health Care*. 12(2): 125-131.

Jha, A. K., DesRoches, C. M., Campbell, E. G., Donelan, K., Rao, S. R., Ferris, T. G., . . . Blumenthal, D. (2009). Use of electronic health records in US hospitals. *New England Journal of Medicine*. 360(16): 1628-1638.

Jha, A. K., Ferris, T. G., Donelan, K., DesRoches, C., Shields, A., Rosenbaum, S., and Blumenthal, D. (2006). How common are electronic health records in the United States? A summary of the evidence. *Health Aff (Millwood)*. 25(6): w496-w507.

Johnston, D., Pan, E., and Walker, J. (2004). The value of CPOE in ambulatory settings. *J Healthc Inf Manag*. 18(1): 5-8.

Joint Commission on Accreditation of Healthcare Organizations. (2014). 2014 National Patient Safety Goals. http://www.jointcommission.org/standards_information/npsgs.aspx, (16.08.2014).

Jones, S. S., Koppel, R., Ridgely, M. S., Palen, T. E., Wu, S.-Y., and Harrison, M. I. (2011). Guide to Reducing Unintended Consequences of Electronic Health Records. 11-0105-EF. Rockville, MD: Agency for Healthcare Research and Quality.

Joss, R. and Kogan, M. (1995). *Advancing quality: Total quality management in the National Health Service*: Open University Press Buckingham.

Joyce, P., Green, R., and Winch, G. (2006). A new construct for visualising and designing e-fulfilment systems for quality healthcare delivery. *The TQM Magazine*. 18(6): 638-651.

Juran, J. M. (1988a). *Juran on planning for quality*. New York, NY: Free Press.

Juran, J. M. (1988b). Juran's quality control handbook. New York, NY: McGraw-Hill.

Juran, J. M., Gryna, F., and Bingham, R. (1974). *Quality Control Handbook* (Vol.). McGraw-Hill.

Juran, J. M. and Gryna, F. M. (1980). Quality planning and analysis.

Juran, J. M. and Gryna, F. M. (1993). Quality planning and analysis: from product development through use. *McGraw-Hill series in industrial engineering and management science*.

Kabay, M. E. (1996). *The NCSA Guide to Enterprise Security*. New York, NY: McGraw-Hill.

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review*. 50(4): 1193-1294.

Kanjanarat, P., Winterstein, A. G., Johns, T. E., Hatton, R. C., Gonzaler-Rothi, R., and Segal, R. (2003). Nature of preventable adverse drug events in hospitals: a literature review. *American Journal of Health-System Pharmacy*. 60(17): 1750-1759.

Kanji, G. K. and Yui, H. (1997). Total quality culture. *Total Quality Management*. 8(6): 417-428.

Kankanhalli, A., Teo, H.-H., Tan, B. C., and Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*. 23(2): 139-154.

Kaplan, R. S. and Norton, D. P. (1992). The balanced scorecard—measures that drive performance *Harvard business review*. 70(1): 71-79.

Karjoth, G., Schunter, M., and Waidner, M. (2003). Platform for enterprise privacy practices: Privacy-enabled management of customer dataPrivacy Enhancing Technologies (pp. 69-84). Zurich, Switzerland: Springer.

Karlene, H. and Martha, G. (1995). Organization, Technology and Structuring. *Handbook of Organization Studies* (pp. 409-423). London: SAGE Publications.

Katz-Navon, T., Naveh, E., and Stern, Z. (2005). Safety climate in health care organizations: a multidimensional approach. *Academy of Management Journal*. 48(6): 1075-1089.

Katz, D. and Kahn, R. L. (1978). *The social psychology of organizations*. New York, NY: John Wiley & Sons.

Kaushal, R. and Bates, D. W. (2001). Computerized Physician Order Entry (CPOE) with Clinical Decision Support Systems (CDSSs). *Making Health Care Safer: A Critical Analysis of Patient Safety Practices* (pp. 59-70): Agency for Healthcare Research and Quality.

Kaushal, R., Shojania, K. G., and Bates, D. W. (2003). Effects of computerized physician order entry and clinical decision support systems on medication safety: a systematic review. *Arch Intern Med*. 163(12): 1409-1416.

Kaynak, H. (2003). The relationship between total quality management practices and their effects on firm performance. *Journal of Operations management*. 21(4): 405-435.

Kijsanayotin, B., Pannarunothai, S., and Speedie, S. M. (2009). Factors influencing health information technology adoption in Thailand's community health centers: Applying the UTAUT model. *Int J Med Inform*. 78(6): 404-416.

Klein, G. A. (1998). *Sources of power: How people make decisions*. Cambridge, MA: MIT press. Cited by Kohn et al., (2000).

Klein, G. A., Calderwood, R., and Macgregor, D. (1989). Critical decision method for eliciting knowledge. *Systems, Man and Cybernetics, IEEE Transactions on*. 19(3): 462-472.

Klein, M. W., Malone, M. F., Bennis, W. G., and Berkowitz, N. H. (1961). Problems of measuring patient care in the out-patient department. *Journal of health and human behavior*. 2(2): 138-144.

Kleinke, J. (1998). Release 0.0: clinical information technology in the real world. *Health Aff (Millwood)*. 17(6): 23-38.

Knapp, K. J., Franklin Morris Jr, R., Marshall, T. E., and Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*. 28(7): 493-508.

Knapp, K. J., Marshall, T. E., Rainer Jr, R. K., and Ford, F. N. (2007). Information security effectiveness: conceptualization and validation of a theory. *International Journal of Information Security and Privacy (IJISP)*. 1(2): 37-60.

Koehoorn, M., Lowe, G. S., Rondeau, K. V., Schellenberg, G., and Wagar, T. H. (2002). Creating High-Quality Health Care Workplaces. Ottawa, Ontario: October 29 2001. http://www.cprn.org/documents/8984_en.PDF, (19.04.2014).

Kohn, L. T., Corrigan, J. M., and Donaldson, M. S. (2000). *To Err Is Human: Building a Safer Health System*. Washington, D.C.: The National Academies Press.

Koppel, R., Metlay, J. P., Cohen, A., Abaluck, B., Localio, A. R., Kimmel, S. E., and Strom, B. L. (2005). Role of computerized physician order entry systems in facilitating medication errors. *JAMA*. 293(10): 1197-1203.

Kozak, M., Asunakutlu, T., and Safran, B. (2007). TQM implementation at public hospitals: a study in Turkey. *International Journal of Productivity and Quality Management*. 2(2): 193-207.

Kreitner, R. and Kinicki, A. (1992). *Organizational Behavior* New York, NY: McGraw-Hill. Cited by Da Veiga and Eloff, (2010).

Kroll Advisory Solutions. (2012). HIMSS Analytics Report: Security of Patient Data. New York, NY:

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*. 18(1): 4-13. Cited by Bess, (2012).

Lampson, B. W. (2004). Computer security in the real world. *Computer*. 37(6): 37-46.

Landrigan, C. P., Parry, G. J., Bones, C. B., Hackbarth, A. D., Goldmann, D. A., and Sharek, P. J. (2010). Temporal trends in rates of patient harm resulting from medical care. *New England Journal of Medicine*. 363(22): 2124-2134.

Langley, G. J., Nolan, K. M., and Nolan, T. W. (1994). The foundation of improvement. *Quality Progress*. 27(6): 81-86. Cited by Moen and Norman, (2006).

Leape, L. L. (1994). Error in medicine. *JAMA-Journal of the American Medical Association-US Edition*. 272(23): 1851-1856.

Leape, L. L., Bates, D. W., Cullen, D. J., Cooper, J., Demonaco, H. J., Gallivan, T., . . . Laffel, G. (1995). Systems analysis of adverse drug events. *JAMA*. 274(1): 35-43. Cited by Nolan, (2000).

Leape, L. L. and Berwick, D. M. (2005). Five years after to err is human. *JAMA: the journal of the American Medical Association*. 293(19): 2384-2390.

Leape, L. L., Brennan, T. A., Laird, N., Lawthers, A. G., Localio, A. R., Barnes, B. A., . . . Hiatt, H. (1991). The nature of adverse events in hospitalized patients: results of the Harvard Medical Practice Study II. *New England Journal of Medicine*. 324(6): 377-384. Cited by Kohn et al., (2000).

Leape, L. L., Lawthers, A. G., Brennan, T. A., and Johnson, W. G. (1993). Preventing medical injury. *QRB. Quality review bulletin*. 19(5): 144. Cited by Kohn et al., (2000).

Lederman, R. (2004). *The medical privacy rule: can hospitals comply using current health information systems?* Paper presented at the 17th IEEE Symposium on Computer-Based Medical Systems, CBMS. Bethesda, MD.

Lederman, R. and Parkes, C. (2005). Systems Failure in Hospitals—Using Reason's Model to Predict Problems in a Prescribing Information System. *Journal of medical systems*. 29(1): 33-43.

Lending, D. and Dillon, T. W. (2007). The effects of confidentiality on nursing self-efficacy with information systems. *International Journal of Healthcare Information Systems and Informatics (IJHISI)*. 2(3): 49-64. Cited by Brady, (2011).

Lesar, T. S., Lomaestro, B. M., and Pohl, H. (1997). Medication-prescribing errors in a teaching hospital: a 9-year experience. *Arch Intern Med*. 157(14): 1569.

Leveson, N. G. (1995). *Safeware: system safety and computers* (Vol. 680). Reading, MA: Addison-Wesley. Cited by Leveson, (2011).

Leveson, N. G. (2011). *Engineering a safer world: Systems thinking applied to safety*. Cambridge, MA: Mit Press.

Levinson, W. A. and Rerick, R. A. (2002). *Lean enterprise: A synergistic approach to minimizing waste*. Milwaukee, WI ASQ Quality Press. Cited by National Learning Consortium, (2013).

Levitt, B. and March, J. G. (1988). Organizational learning. *Annual Review of Sociology*: 319-340.

Lewis, J. A. and Baker, S. (2013). The Economic Impact of Cybercrime and Cyber Espionage. http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf, (02.24.2014).

Lillrank, P. and Kano, N. (1989). *Continuous improvement: quality control circles in Japanese industry*: Center for Japanese Studies, The University of Michigan.

Lindqvist, U. and Jonsson, E. (1997). *How to systematically classify computer security intrusions.* Paper presented at the 1997 IEEE Symposium on Security and Privacy. Oakland, CA. 4-7 May 1997.

Liotta, P. H. (2002). Boomerang effect: The convergence of national and human security. *Security Dialogue*. 33(4): 473-488.

Localio, A. R., Lawthers, A. G., Brennan, T. A., Laird, N. M., Hebert, L. E., Peterson, L. M., . . . Hiatt, H. H. (1991). Relation between malpractice claims and adverse events due to negligence: results of the Harvard Medical Practice Study III. *New England Journal of Medicine*. 325(4): 245-251.

Loch, K. D., Carr, H. H., and Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS quarterly*. 16(2): 173-186.

Logan, P. Y. and Noles, D. (2008). Protecting Patient Information in Outsourced Telehealth Services: Bolting on Security When it Cannot be Baked in. *International*

Journal of Information Security and Privacy (IJISP). 2(3): 55-70. Cited by Brady, (2011).

Lohr, K. N. (1988). Outcome measurement: concepts and questions. *Inquiry*. 25(1): 37-50.

Lohr, K. N. (1990). *Medicare:A Strategy for Quality Assurance, Volume I*. Washington, D.C.: The National Academies Press.

Lohr, K. N. and Brook, R. H. (1984). *Quality assurance in medicine*. Santa Monica,CA: Rand Corporation.

Longhurst, C. A. and Landa, H. M. (2012). Health information technology and patient safety. *Bmj*. 344(1): 1-2.

Lorincz, C., Drazen, E., Sokol, P., Neerukonda, K., Metzger, J., Toepp, M., . . . Wynia, M. (2011). Research in Ambulatory Patient Safety 2000–2010: a 10-year review. *Our Children: The National PTA Magazine*. http://psnet.ahrq.gov/resource.aspx?resourceID=23742, (08.12.2013).

Lowrance, W. W. (1976). *Of Acceptable Risk: Science and the Determination of Safety*. Los Altos, CA: Kaufmann, William, Incorporated.

Ma, Q., Johnston, A. C., and Pearson, J. M. (2008). Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security*. 16(3): 251-270. Cited by Brady, (2011).

Macinati, M. S. (2008). The relationship between quality management systems and organizational performance in the Italian National Health Service. *Health Policy*. 85(2): 228-241.

MacPherson, J., Kochman, S., and McCullough, J. (2009). Regulating blood manufacturing software: report of a conference. *Transfusion*. 49(11): 2490-2494.

Mader, A. and Srinivasan, S. (2005). *Curriculum development related to information security policies and procedures.* Paper presented at the 2nd annual conference on Information security curriculum development. Kennesaw, GA. 23-24 September 2005.

Magrabi, F., Li, S. Y., Day, R. O., and Coiera, E. (2010). Errors and electronic prescribing: a controlled laboratory study to examine task complexity and interruption effects. *Journal of the American Medical Informatics Association*. 17(5): 575-583.

Magrabi, F., Ong, M.-S., Runciman, W., and Coiera, E. (2010). An analysis of computer-related patient safety incidents to inform the development of a classification. *Journal of the American Medical Informatics Association*. 17(6): 663-670.

Magrabi, F., Ong, M.-S., Runciman, W., and Coiera, E. (2012). Using FDA reports to inform a classification for health information technology safety problems. *Journal of the American Medical Informatics Association*. 19(1): 45-53.

Magrabi, F., Ong, M. S., Runciman, W., and Coiera, E. (2011). Patient safety problems associated with heathcare information technology: an analysis of adverse events reported to the US Food and Drug Administration. *AMIA Annu Symp Proc*. 2011: 853-857.

Mak, S. (2001). A model of information management for construction using information technology. *Automation in Construction*. 10(2): 257-263.

Malhotra, S., Jordan, D., Shortliffe, E., and Patel, V. L. (2007). Workflow modeling in critical care: piecing together your own puzzle. *Journal of biomedical informatics*. 40(2): 81-92.

Mansell, D., Poses, R. M., Kazis, L., and Duefield, C. A. (2000). CLinical factors that influence patients' desire for participation in decisions about illness. *Arch Intern Med*. 160(19): 2991-2996.

Manuele, F. A. (2003). *On the Practice of Safety*. Hoboken, NJ: John Wiley & Sons.

Manuele, F. A. (2013). *On the practice of safety*. Hoboken, NJ: John Wiley & Sons.

Marais, K., Dulac, N., and Leveson, N. (2004). *Beyond normal accidents and high reliability organizations: The need for an alternative approach to safety in complex systems.* Paper presented at the Engineering Systems Division Symposium. Cambridge, MA. 29-31 March 2004.

MarketsandMarkets. (2014). Health IT Spending. http://www.marketsandmarkets.com, (14.07.2014).

Marren, J. (2004). The trustee's responsibility for quality care. *Trustee: the journal for hospital governing boards*. 57(7): 26, 28.

Marszalek-Gaucher, E. and Coffey, R. J. (1993). *Total quality in healthcare: from theory to practice*. San Francisco, CA: Jossey-Bass Publishers.

Martínez-Costa, M., Choi, T. Y., Martínez, J. A., and Martínez-Lorente, A. R. (2009). ISO 9000/1994, ISO 9001/2000 and TQM: the performance debate revisited. *Journal of Operations management*. 27(6): 495-511.

Martins, E. C. (2002). An Organizational Culture Model to Promote Creativity and innovation. *Journal of Industrial Psychology*. 28(4): 58-65.

McGlynn, E. A., Asch, S. M., Adams, J., Keesey, J., Hicks, J., DeCristofaro, A., and Kerr, E. A. (2003). The quality of health care delivered to adults in the United States. *New England Journal of Medicine*. 348(26): 2635-2645.

McKeon, L. M., Oswaks, J. D., and Cunningham, P. D. (2006). Safeguarding patients: complexity science, high reliability organizations, and implications for team training in healthcare. *Clinical Nurse Specialist*. 20(6): 298-304.

Mearns, K., Whitaker, S. M., and Flin, R. (2003). Safety climate, safety management practice and safety performance in offshore environments. *Safety Science*. 41(8): 641-680.

Mearns, K. J. and Flin, R. (1999). Assessing the state of organizational safety—culture or climate? *Current Psychology*. 18(1): 5-17. Cited by Palmieri et al., (2010).

Medlin, B. D. and Cazier, J. A. (2007). An empirical investigation: Health care employee passwords and their crack times in relationship to hipaa security standards. *International Journal of Healthcare Information Systems and Informatics (IJHISI)*. 2(3): 39-48. Cited by Brady, (2011).

Merriam-Webster.com. (2012). Merriam Webster Dictionary. http://www.merriam-webster.com/dictionary/safety, (20.07.2014).

Mesjasz, C. (2004). *Security as an analytical concept.* Paper presented at the 5th Pan-European conference on International Relations. Cracow, Poland. 9-11 September 2004.

Meta Security Group. (2000). Information Security Policy Framework. http://lazarusalliance.com/horsewiki/images/1/18/Information-Security-Policy-Framework-Research-Report.pdf, (10.04.2014). Cited by Eloff and Eloff, (2005).

Miles, R. E., Snow, C. C., Meyer, A. D., and Coleman, H. J. (1978). Organizational strategy, structure, and process. *Academy of management review*. 3(3): 546-562. Cited by Croteau and Bergeron, (2001).

Misumi, Y. and Sato, Y. (1999). Estimation of average hazardous-event-frequency for allocation of safety-integrity levels. *Reliability Engineering and System Safety*. 66(2): 135-144.

Mitchell, P. H., Ferketich, S., and Jennings, B. M. (1998). Quality health outcomes model. *Image: The Journal of Nursing Scholarship*. 30(1): 43-46.

Mitchell, P. H., Heinrich, J., Moritz, P., and Hinshaw, A. S. (1997). Outcome measures and care delivery systems: Introduction and purposes of conference. *Medical care*. 35(11): NS1-NS5.

Mitchell, P. H. and Shortell, S. M. (1997). Adverse outcomes and variations in organization of care delivery. *Medical care*. 35(11): NS19-NS32.

Moen, R. and Norman, C. (2006). Evolution of the PDCA cycle. http://pkpinc.com/files/NA01MoenNormanFullpaper.pdf, (20.06.2014)

Moen, R. D., Nolan, T. W., and Provost, L. P. (1999). *Quality improvement through planned experimentation*. New York, NY: McGraw-Hill.

Møller, B. (2000). *National, Societal and Human Security: A General Discussion with a Case Study from the Balkans*: Copenhagen Peace Research Institute.

Moody, R. F. (2006). *Safety culture on hospital nursing units: Human performance and organizational system factors that make a difference*: ProQuest.

Mosadeghrad, A. M. (2005). A survey of total quality management in Iran: Barriers to successful implementation in health care organizations. *Leadership in Health Services*. 18(3): 12-34.

Mosadeghrad, A. M. (2011). *Developing and testing a quality management model for healthcare organisations.* (PhD dissertation), University of London, London, Unpublished Thesis

Mosadeghrad, A. M. (2013). Obstacles to TQM success in health care systems. *International Journal of Health Care Quality Assurance*. 26(2): 147-173.

Möller, N., Hansson, S. O., and Peterson, M. (2006). Safety is more than the antonym of risk. *Journal of Applied Philosophy*. 23(4): 419-432.

Munro, B. H. (2005). *Statistical methods for health care research*. Newyork, NY: Lippincott Williams & Wilkins.

Myler, E. and Broadbent, G. (2006). ISO 17799: Standard for security. *Information Management Journal*. 40(6): 43.

Nadzam, D. M. (1991). Development of medication-use indicators by the Joint Commission on Accreditation of Healthcare Organizations. *American Journal of Health-System Pharmacy*. 48(9): 1925-1930.

Najmi, M. and Kehoe, D. F. (2000). An integrated framework for post-ISO 9000 quality development. *International Journal of Quality & Reliability Management*. 17(3): 226-258.

Nanji, K. C., Rothschild, J. M., Salzberg, C., Keohane, C. A., Zigmont, K., Devita, J., . . . Poon, E. G. (2011). Errors associated with outpatient computerized prescribing systems. *Journal of the American Medical Informatics Association*. 18(6): 767-773.

Nardi, P. M. (2006). *Interpreting data: A guide to understanding research*. New York, NY: Pearson.

National Learning Consortium. (2013). Continuous Quality Improvement (CQI) Strategies to Optimize your Practice. http://www.healthit.gov/sites/default/files/tools/nlc_continuousqualityimprovementprimer.pdf, (24.07.2014).

National Patient Safety Agency. (2014). Patient Safety. http://www.nrls.npsa.nhs.uk/, (16.08.2014).

National Patient Safety Foundation. (2014). Patient Safety Dictionary. http://www.npsf.org/for-healthcare-professionals/resource-center/definitions-and-hot-topics/patient-safety-dictionary-n-z/, (20.07.2014).

National Research Council Board on Biology. (1998). *Privacy Issues in Biomedical and Clinical Research.* http://www.nap.edu/catalog/6326.html, (12.6.2014).

National Telecommunications and Information Administration. (2013). Exploring the Digital Nation: America's Emerging Online Experience. http://www.ntia.doc.gov/report/2013/exploring-digital-nation-americas-emerging-online-experience, (24.06.2014).

Netschert, B. M. (2008). *Information security readiness and compliance in the healthcare industry.* (3317887 Ph.D.), Stevens Institute of Technology, Ann Arbor. http://search.proquest.com/docview/304371765, (14.04.2014).

Niazkhani, Z., Pirnejad, H., Berg, M., and Aarts, J. (2009). The impact of computerized provider order entry systems on inpatient clinical workflow: a literature review. *Journal of the American Medical Informatics Association*. 16(4): 539-549.

Nieva, V. and Sorra, J. (2003). Safety culture assessment: a tool for improving patient safety in healthcare organizations. *Quality and Safety in Health Care*. 12(suppl 2): ii17-ii23.

Nnolim, A. L. (2007). *A framework and methodology for information security management.* (3296872 D.Mgt.), Lawrence Technological University, Ann Arbor. http://search.proquest.com/docview/304792663, (16.03.2014).

Nolan, T. W. (2000). System changes to improve patient safety. *BMJ: British Medical Journal*. 320(7237): 771.

Norman, D. A. (1988). *The psychology of everyday things*. New York, NY: Basic books. Cited by Nolan, (2000).

Norman, D. A. (1993). *Things that make us smart: Defending human attributes in the age of the machine*. New York, NY: Basic Books. Cited by Kohn et al., (2000).

Norman, D. A. (2002). *The design of everyday things*. New York, NY: Basic books.

Nunally, J. C. and Bernstein, I. H. (1978). Psychometric theory. New York, NY: McGraw-Hill.

O'Leary, D. S. (1988). Quality Assessment Moving From Theory to Practice. *JAMA: the journal of the American Medical Association*. 260(12): 1760-1760. Cited by Lohr, (1990).

O'brien, R. M. (2007). A caution regarding rules of thumb for variance inflation factors. *Quality & Quantity*. 41(5): 673-690.

Oakland, J. S. and Marosszeky, M. (2006). *Total quality in the construction supply chain*. Burlington,MA: Routledge.

Olinsky, A., Chen, S., and Harlow, L. (2003). The comparative efficacy of imputation methods for missing data in structural equation modeling. *European Journal of operational research*. 151(1): 53-79.

Orel, A. and Bernik, I. (2013). Implementing healthcare information security: standards can help. *Stud Health Technol Inform*. 186: 195-199.

Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization science*. 3(3): 398-427.

Osborne, J., Christensen, W., and Gunter, J. (2001). *Educational psychology from a statistician's perspective: A review of the power and goodness of educational psychology research.* Paper presented at the National meeting of the American Education Research Association (AERA). Seattle, WA.

Osborne, J. and Waters, E. (2002). Four assumptions of multiple regression that researchers should always test. *Practical assessment, research & evaluation*. 8(2): 1-9.

Ott, J. S. (1989). *The organizational culture perspective*. Chicago: Dorsey Press.

Ozturk, A. O. and Swiss, J. E. (2008). Implementing management tools in Turkish public hospitals: the impact of culture, politics and role status. *Public Administration and Development*. 28(2): 138-148.

Paccagnella, A., Mauri, A., and Spinella, N. (2012). Quality improvement for integrated management of patients with type 2 diabetes (PRIHTA project stage 1). *Quality Management in Healthcare*. 21(3): 146-159. Cited by National Learning Consortium, (2013).

Page, A. (2004). *Keeping patients safe: Transforming the work environment of nurses*. Washington, D.C.: National Academies Press.

Palmer, S. and Torgerson, D. J. (1999). Economics notes: Definitions of efficiency. *BMJ: British Medical Journal*. 318(7191): 1136.

Palmieri, P. A., Peterson, L. T., Pesta, B. J., Flit, M. A., and Saettone, D. M. (2010). Safety culture as a contemporary healthcare construct: theoretical review, research assessment, and translation to human resource management. *Advances in Health Care Management*. 9: 97-133.

Parsons, T. (1977). *Social systems and the evolution of action theory* (Vol.). New York, NY: Free Press. Cited by Scott et al., (2003).

Patel, V. L., Zhang, J., Yoskowitz, N. A., Green, R., and Sayan, O. R. (2008). Translational cognition for decision support in critical care environments: a review. *Journal of biomedical informatics*. 41(3): 413-431.

Patrick, D. L. (1997). Finding health-related quality of life outcomes sensitive to health-care organization and delivery. *Medical care*. 35(11): NS49-NS57.

Patrick, D. L. and Erickson, P. (1993). *Health status and health policy*. New York, NY: Oxford University Press.

Peltier, T. R. (2003). Preparing for ISO 17799. *Information systems security*. 11(6): 21-28.

Peltier, T. R. (2005). *Information security risk analysis*. Boca Raton, FL: CRC press.

Perks, C. and Beveridge, T. (2003). *Guide to enterprise IT architecture*. New York, NY: Springer.

Perlroth, N. (12.31.2012). Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt. *New York Times*.

http://www.nytimes.com/2013/01/01/technology/antivirus-makers-work-on-software-to-catch-malware-more-effectively.html?pagewanted=all&_r=0, (20.06.2014).

Perrow, C. (1984). *Normal accidents: Living with high risk systems*. New York, NY: Basic Books. Cited by Palmieri et al., (2010).

Perrow, C. (1994). The limits of safety: the enhancement of a theory of accidents. *Journal of contingencies and crisis management*. 2(4): 212-220.

Perrow, C. (1999). *Normal accidents: Living with high risk technologies*. Princeton, NJ: Princeton University Press.

Perry, S. J., Wears, R. L., and Cook, R. I. (2005). The role of automation in complex system failures. *Journal of Patient Safety*. 1(1): 56-61.

Pestotnik, S. L., Classen, D. C., Evans, R. S., and Burke, J. P. (1996). Implementing antibiotic practice guidelines through computer-assisted decision support: clinical and financial outcomes. *Annals of internal medicine*. 124(10): 884-890.

Pettigrew, A. M. (1979). On studying organizational cultures. *Administrative science quarterly*. 24(4): 570-581.

Pfleeger, C. P. (1997). *Security in computing*. Upper Saddle, NJ: Prentice Hall.

Pieters, W. (2011). The (Social) Construction of Information Security. *The Information Society*. 27(5): 326-335.

Porter, M. E. (2008). *Competitive strategy: Techniques for analyzing industries and competitors*. New York, NY: Simon and Schuster.

Porter, M. E. and Millar, V. E. (1985). How information gives you competitive advantage. 63(4): 149-160.

Potter, C. and Beard, A. (2010). Information security breaches survey 2010. Earl's Court, London:

Press, G. (2013). A Very Short History of Information Technology (IT) http://www.forbes.com/sites/gilpress/2013/04/08/a-very-short-history-of-information-technology-it/, (14.04.2014).

PricewaterhouseCoopers. (2013a). 2013 US State of Cyber Crime Survey. http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-state-of-cybercrime.jhtml, (08.04.2014).

PricewaterhouseCoopers. (2013b). The Global State of Information Security® Survey 2014. http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml, (28.03.2014).

Probst, C. W., Hansen, R. R., and Nielson, F. (2007). Where can an insider attack? *Formal Aspects in Security and Trust* (pp. 127-142). New York, NY: Springer.

Quality Services Limited. (2013). More changes ahead…..ISO 27001:2005 Information Security Management Standard. http://www.isoqsltd.com/ahead-iso-270012005-information-security-management-standard/, (23.08.2014).

Raghupathi, W. (1997). Health care information systems. *Communications of the ACM*. 40(8): 80-82.

Rannenberg, K., Pfitzmann, A., and Müller, G. (1999). IT security and multilateral security. *Multilateral Security in Communications*. 3(1): 21-29.

Rasmussen, J. and Batstone, R. (1989). Why do complex organizational systems fail?

Reason, J. (1990). *Human error*. Cambridge, MA: Cambridge university press. Cited by Kohn et al., (2000).

Reason, J. (1998). Achieving a safe culture: theory and practice. *Work & Stress*. 12(3): 293-306.

Reason, J. (2000a). *Grace under fire: Compensating for adverse events in cardiothoracic surgery.* Paper presented at the 5th conference on naturalistic decision making. Cited by Dekker, (2002).

Reason, J. (2000b). Human error: models and management. *BMJ: British Medical Journal*. 320(7237): 768.

Reason, J., Hollnagel, E., and Paries, J. (2006). Revisiting the «Swiss cheese» model of accidents. *Our Children: The National PTA Magazine*. Brussels:

http://www.eurocontrol.int/eec/public/standard_page/DOC_Report_2006_017.html, (24.06.2014).

Reason, J. T. (1997). *Managing the risks of organizational accidents* (Vol. 6): Ashgate Aldershot. Cited by Dekker, (2002).

Recht, R. and Wilderom, C. (1998). Kaizen and culture: on the transferability of Japanese suggestion systems. *International Business Review*. 7(1): 7-22.

Reckmann, M. H., Westbrook, J. I., Koh, Y., Lo, C., and Day, R. O. (2009). Does computerized provider order entry reduce prescribing errors for hospital inpatients? A systematic review. *Journal of the American Medical Informatics Association*. 16(5): 613-623.

Rees, J., Bandyopadhyay, S., and Spafford, E. H. (2003). PFIRES: a policy framework for information security. *Communications of the ACM*. 46(7): 101-106.

Reich, B. H. and Benbasat, I. (2000). Factors that influence the social dimension of alignment between business and information technology objectives. *MIS quarterly*. 24(1): 81-113.

Reis, D. W. (2012). *An Examination of an Information Security Framework Implementation Based on Agile Values to Achieve Health Insurance Portability and Accountability Act Security Rule Compliance in an Academic Medical Center: The Thomas Jefferson University Case Study.* (3507943 Ph.D.), Nova Southeastern University, Ann Arbor. http://search.proquest.com/docview/1017870699, (20.04.2014).

Richardson, R. (2011). 2010 / 2011 CSI Computer Crime and Security Survey. http://reports.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html, (08.04.2014).

Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the ACM*. 40(8): 92-100.

Robbins, S. P. (2001). *Organizational Behavior 9th ed.* Upper Saddle River, NJ: Prentice Hall. Cited by Da Veiga and Eloff, (2010).

Robbins, S. P., Odendaal, A., and Roodt, G. (2003). *Organisational behaviour: global and Southern African perspectives*. Pinelands, CapeTown: Pearson South Africa.

Roberts, K. (1999). *Risk, Regulation, Litigation and Organizational Issues in Safety High-Hazard Industries.* Paper presented at the Workshop on Organizational Analysis in High Hazard Production Systems: An Academy/Industry Dialogue.

Roberts, K. H. (1990). Some characteristics of one type of high reliability organization. *Organization science*. 1(2): 160-176.

Rochlin, G. I. (1999). Safe operation as a social construct. *Ergonomics*. 42(11): 1549-1560. Cited by Dekker, (2002).

Roethlisberger, F. and Dickson, W. (1939). *Management and the worker*. Cambridge, MA: Harvard University Press. Cited by Scott et al., (2003).

Rogers, E. M. (2010). *Diffusion of innovations*. New York, NY: Simon and Schuster.

Rogers, M. K. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study.* University of Manitoba

Rosa, E. A. (1998). Metatheoretical foundations for post-normal risk. *Journal of risk research*. 1(1): 15-44. Cited by Aven and Renn, (2009).

Rosa, E. A. (2003). *The logical structure of the social amplification of risk framework (SARF): Aferatheoretical foundations and policy implications. The social amplification of risk* http://ebooks.cambridge.org/chapter.jsf?bid=CBO9780511550461&cid=CBO9780511550461A014, (24.07.2014).

Roth, P. L. (1994). Missing data: A conceptual review for applied psychologists. *Personnel psychology*. 47(3): 537-560.

Rotvold, G. (2008). How to create a security culture in your organization. *Information Management Journal*. 42(6): 32-38.

Rouse, W. B. (2003). Engineering complex systems: Implications for research in systems engineering. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*. 33(2): 154-156.

Rouse, W. B. (2008). Health care as a complex adaptive system: implications for design and management. *NAE Annual Meeting Technical Symposium (*pp. 17). 1. Washington, D.C.: 1 October 2007.

Ruighaver, A. B. and Maynard, S. B. (2006). Organizational Security Culture: More Than Just an End-User Phenomenon. *Security and Privacy in Dynamic Environments* (pp. 425-430). Boston: Springer.

Ruighaver, A. B., Maynard, S. B., and Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*. 26(1): 56-62.

Rungta, S., Raman, A., Kohlenberg, T., Li, H., Dave, M., and Kime, G. (2004). Bringing Security Proactively Into the Enterprise. *Intel Technology Journal*. 8(4): 303-311.

Sagan, S. D. (1993). *The limits of safety* (Vol.). Princeton: Princeton University Press

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal*. 39(4): 60-66.

Salvendy, G. (2012). *Handbook of human factors and ergonomics*. New York, NY: John Wiley & Sons. Cited by Nolan, (2000).

Sandrick, K. (2007). Enhancing the board's role in quality. *Trustee: the journal for hospital governing boards*. 60(1): 20-24.

Saylor, J. H. (1992). *TQM field manual*. New York, NY: McGraw-Hill. Cited by Zhu, (1999).

Schein, E. H. (1984). Coming to a new awareness of organizational culture. *Sloan management review*. 25(2): 3-16.

Schein, E. H. (1985). *Organisational culture and leadership: A dynamic view*. San Francisco, CA: Jossey-Bass.

Schein, E. H. (1988). Organizational culture. http://dspace.mit.edu/handle/1721.1/2224, (24.05.2014)

Schein, E. H. (1990). Organizational culture. 45(2): 109-119.

Schlienger, T. and Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. *14th International Workshop on Database and Expert Systems Applications, 2003* (pp. 405-409): IEEE.

Schneider, B. (1975). Organizational climate: Individual preferences and organizational realities revisited. *Journal of Applied Psychology*. 60(4): 459.

Schneider, E. C., Riehl, V., Courte-Wienecke, S., Eddy, D. M., and Sennett, C. (1999). Enhancing performance measurement: NCQA's road map for a health information framework. *JAMA*. 282(12): 1184-1190.

Schonlau, M., Ronald Jr, D., and Elliott, M. N. (2002). *Conducting research surveys via e-mail and the web*. Santa Monica, CA: Rand Corporation.

Schultz, E. E., Proctor, R. W., Lien, M.-C., and Salvendy, G. (2001). Usability and security an appraisal of usability issues in information security methods. *Computers & Security*. 20(7): 620-634.

Schweitzer, J. A. (1987). How security fits in—a management view: Security is an essential for quality information. *Computers & Security*. 6(2): 129-132.

Scott, D. J. (2004). Abstracting application-level security policy for ubiquitous computing. UCAM-CL-TR-613. Cambridge, UK: January 2005.

Scott, T., Mannion, R., Davies, H., and Marshall, M. (2003). The quantitative measurement of organizational culture in health care: a review of the available instruments. *Health services research*. 38(3): 923-945.

Sedevich-Fons, L. (2013). Healthcare quality costs based on an ISO 9000 model. *Leadership in Health Services*. 26(3): 184-195.

Selznick, P. (1957). Leadership in administration: A sociological interpretation. Berkeley. *Cal*.

Sexton, J. B., Helmreich, R. L., Neilands, T. B., Rowan, K., Vella, K., Boyden, J., . . . Thomas, E. J. (2006). The Safety Attitudes Questionnaire: psychometric properties, benchmarking data, and emerging research. *BMC Health Serv Res*. 6(1): 44.

Sexton, J. B., Thomas, E. J., and Helmreich, R. L. (2000). Error, stress, and teamwork in medicine and aviation: cross sectional surveys. *BMJ: British Medical Journal*. 320(7237): 745.

Shah, N. R., Seger, A. C., Seger, D. L., Fiskio, J. M., Kuperman, G. J., Blumenfeld, B., . . . Gandhi, T. K. (2006). Improving acceptance of computerized prescribing alerts in ambulatory care. *Journal of the American Medical Informatics Association*. 13(1): 5-11.

Shamliyan, T. A., Duval, S., Du, J., and Kane, R. L. (2008). Just what the doctor ordered. Review of the evidence of the impact of computerized physician order entry system on medication errors. *Health services research*. 43(1p1): 32-53.

Shappell, S. A. and Wiegmann, D. A. (2001). Applying reason: The human factors analysis and classification system (HFACS). *Human Factors and Aerospace Safety*. DOT/FAA/AM-00/7. Washington, D.C.: Office of Aviation Medicine. https://www.nifc.gov/fireInfo/fireInfo_documents/humanfactors_classAnly.pdf, (24.06.2014).

Shea, S., DuMouchel, W., and Bahamonde, L. (1996). A meta-analysis of 16 randomized controlled trials to evaluate computer-based clinical reminder systems for preventive care in the ambulatory setting. *Journal of the American Medical Informatics Association*. 3(6): 399-409.

Shewhart, W. A. (1986). *Statistical method from the viewpoint of quality control*. New York, NY: Courier Dover Publications. Cited by Moen and Norman, (2006).

Shewhart, W. A. and Deming, W. E. (1939). Statistical method from the viewpoint of quality control. Cited by Moen and Norman, (2006).

Shortell, S. M., Gillies, R., Siddique, J., Casalino, L. P., Rittenhouse, D., Robinson, J. C., and McCurdy, R. K. (2009). Improving chronic illness care: a longitudinal cohort analysis of large physician organizations. *Medical care*. 47(9): 932-939. Cited by National Learning Consortium, (2013).

Shortell, S. M., O'Brien, J. L., Carman, J. M., Foster, R. W., Hughes, E., Boerstler, H., and O'Connor, E. J. (1995). Assessing the impact of continuous quality improvement/total quality management: concept versus implementation. *Health services research*. 30(2): 377.

Singer, S. J., Gaba, D., Geppert, J., Sinaiko, A., Howard, S., and Park, K. (2003). The culture of safety: results of an organization-wide survey in 15 California hospitals. *Quality and Safety in Health Care*. 12(2): 112-118.

Singer, S. J., Gaba, D. M., Falwell, A., Lin, S., Hayes, J., and Baker, L. (2009). Patient safety climate in 92 US hospitals: differences by work area and discipline. *Medical care*. 47(1): 23-31.

Singer, S. J., Lin, S., Falwell, A., Gaba, D., and Baker, L. (2009). Relationship of safety climate and safety performance in hospitals. *Health services research*. 44(2 Pt 1): 399-421.

Singh, H., Classen, D. C., and Sittig, D. F. (2011). Creating an oversight infrastructure for electronic health record-related patient safety hazards. *Journal of Patient Safety*. 7(4): 169.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*. 49(8): 97-100. Cited by Coles-Kemp, (2009).

Siponen, M. and Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*. 46(5): 267-270.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*. 8(1): 31-41.

Siponen, M. T. (2005). An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems*. 14(3): 303-315.

Sittig, D. F. and Singh, H. (2010). A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *Quality and Safety in Health Care*. 19(Suppl 3): i68-i74.

Sittig, D. F. and Singh, H. (2011). Defining health information technology–related errors: New developments since To Err Is Human. *Arch Intern Med*. 171(14): 1281-1284.

Slewe, T. and Hoogenboom, M. (2004). Who will rob you on the digital highway? *Communications of the ACM*. 47(5): 56-60.

Smit, J. and Dellemijn, M. (2011). The Relationship Between Information Systems Management and Organizational Culture. *Communications of the IIMA*. 11(3): 21-33.

Smith, M. (1989). Computer security-threats, vulnerabilities and countermeasures. *Information Age*. 11(4): 205-210.

Sorra, J. and Nieva, V. (2004). Hospital Survey on Patient Safety Culture.(Prepared by Westat, under Contract No. 290-96-0004). AHRQ Publication No. 04-0041. *Rockville, MD: Agency for Healthcare Research and Quality*.

Söderström, E. (2004). B2B standards implementation: issues and solutions. http://su.diva-portal.org/smash/record.jsf?pid=diva2:191723, (20.05.2014)

Steeples, M. M. (1993). *Corporate Guide to the Malcolm Baldrige National Quality Award*. Milwaukee: ASQC Quality Press.

Steyerberg, E. W., Eijkemans, M. J., and Habbema, J. D. F. (1999). Stepwise selection in small data sets: a simulation study of bias in logistic regression analysis. *Journal of clinical epidemiology*. 52(10): 935-942.

Stone, P. W., Larson, E. L., Mooney-Kane, C., Smolowitz, J., Lin, S. X., and Dick, A. W. (2006). Organizational climate and intensive care unit nurses' intention to leave. *Critical care medicine*. 34(7): 1907-1912.

Stone, P. W., Mooney-Kane, C., Larson, E. L., Horan, T., Glance, L. G., Zwanziger, J., and Dick, A. W. (2007). Nurse working conditions and patient safety outcomes. *Medical care*. 45(6): 571-578.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*. 1(3): 255-276. Cited by Brady, (2011).

Straub, D. W. and Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS quarterly*. 22(4): 441-469.

Sun, H., Li, S., Ho, K., Gertsen, F., Hansen, P., and Frick, J. (2004). The trajectory of implementing ISO 9000 standards versus total quality management in Western Europe. *International Journal of Quality & Reliability Management*. 21(2): 131-153.

Tabachnick, B. G. and Fidell, L. S. (2001). *Using multivariate statistics*. Boston: Pearson.

Tang, J. (2008). The Implementation of Deming's System Model to improve Security Management: A Case Study. *International Journal of Management*. 25(1): 54.

Tang, S.-l., Ahmed, S. M., Aoieong, R. T., and Poon, S. (2005). *Construction quality management*. Hong Kong Special Administrative Region, China: Hong Kong University Press

Technology Business Research. (2013). SourceIT Healthcare Report http://tbri.com/, (12.05.2014).

The American Heritage Dictionary. (2014) Our Children: The National PTA Magazine (fifth ed.). Boston, MA: Houghton Mifflin Harcourt Publishing Company.

The Open Group. (2011). Open Group Standard TOGAF Version 9.1. San Francisco, California: The Open Group.

The Pragmatic Auditor. (2013). ISO 27001:2013 - Understanding the New Standard. https://www.brightline.com/2013/04/iso-270012013-understanding-the-new-standard-2/, (23.08.2014).

Theodorakis, Y. (1994). Planned behavior, attitude strength, role identity, and the prediction of exercise behavior. *Sport Psychologist*. 8(2): 149.

Thomas, E. J., Sexton, J. B., and Helmreich, R. L. (2003). Discrepant attitudes about teamwork among critical care nurses and physicians*. *Critical care medicine*. 31(3): 956-959.

Thomas, G. and Botha, R. A. (2007). Secure mobile device use in healthcare guidance from HIPAA and ISO17799. *Information Systems Management*. 24(4): 333-342.

Thompson, E. D. and Kaarst-Brown, M. L. (2005). Sensitive information: A review and research agenda. *Journal of the American Society for Information Science and Technology*. 56(3): 245-257.

Thompson, J. D. (2011). *Organizations in action: Social science bases of administrative theory* (Vol.). New Brunswick, NJ: Transaction Publishers.

Thompson, T. G. (2002). Reducing Medical Errors and Improving Patient Safety. http://www.hhs.gov/asl/testify/t020910a.html, (27.07.2014).

Tippett, P. (2002). Is IT Overspending on Security? November 20, 2002, CNET Networks, INC. http://news.com.eom/2010-1071-966448.html, .

TNS Opinion & Social. (2012). Special Eurobarometer 390 on Cybersecurity. Wave EB77.2. Special Eurobarometer 390 on Cybersecurity, (18.05.2014).

Tobin, L. M. (1990). The New Quality Landscape-Total Quality Management. *Journal of Systems Management*. 41(11): 10-14.

Torres, J. M., Sarriegi, J. M., Santos, J., and Serrano, N. (2006). Managing information systems security: critical success factors and indicators to measure effectiveness. *Information Security* (pp. 530-545): Springer.

Trček, D. (2003). An integral framework for information systems security management. *Computers & Security*. 22(4): 337-360.

Trochim, W. M. and Donnelly, J. (2005). *Research methods: The concise knowledge base*. Mason, OH: Atomic Dog Pub.

Trochim, W. M. K. (2006). The research methods knowledge base. http://www.socialresearchmethods.net/kb/survtype.php, (25.08.2014).

Tucker, S. and Mohamed, S. (1996). Introducing information technology in construction: Pains and gainsThe Organization and Management of Construction: Shaping Theory and Practice (Vol. 3, pp. 348-356): E & FN Spon.

Tudor, K. J. (2002). *Information security architecture: an integrated approach to security in the organization*. Boca Raton, FL: CRC Press.

Turner, B., Pidgeon, N., Blockley, D., and Toft, B. (1989). *Safety culture: its importance in future risk management.* Paper presented at the Position paper for the second World Bank workshop on safety control and risk management, . Karlstad, Sweden.

Tutuncu, O. (2008). *Relationship Between Patient Safety and Quality Management System: A Comparative Analysis Among ISO 9000 Certified and Non-Certified*

Hospitals in Turkey. Paper presented at the The 6th Asia Network for Quality Congress 2008. Bangkok, Thailand. 28-31 October 2008.

Tutuncu, O., Camsari, T., Cavdar, C., and Kiremitci, I. (2009). *Evaluating the Perceptions of Nephrology Physicians on Quality Management System in Turkey*. Paper presented at the International Symposium of Quality Management. Taipei.

Tutuncu, O. and Erbil, H. (2006). *The Role of Quality Management System in Patient Safety Culture for Central Sterilization Units.* Paper presented at the Norway: Annual European Forum for Hospital Sterile Supply Conference, Lillehammer.

Tutuncu, O. and Kucukusta, D. (2007). Relationship between organizational commitment and EFQM business excellence model: A study on Turkish quality award winners. *Total Quality Management*. 18(10): 1083-1096.

Tutuncu, O. and Kucukusta, D. (2008). *Evaluating the Effects of Quality Assurance: A Comparative Analysis between ISO 9001 Certified and Non-Certified Hospitals in Turkey*. Paper presented at the Asia-Pacific Quality Network 2008 Conference and Annual General Meeting. Tokyo, Japan.

Tutuncu, O., Kucukusta, D., Akman, A., Baykan, A., Kiremitci, I., and Nizamoglu, G. (2007). *The Role of Patient Safety Climate on ISO 9001 Quality Management System, 51st European Organization for Quality Annual Congress, Prague, Czech Republic*.

U.S. Department of Health and Human Services. (2014). Understanding Health Information Privacy. http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html, (23.08.2014).

Upfold, C. T. and Sewry, D. A. (2005). *An investigation of information security in small and medium enterprises (SME's) in the Eastern Cape.* Rhodes University. http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/082_Article.pdf, (12.03.2014).

Van Der Sijs, H., Aarts, J., Vulto, A., and Berg, M. (2006). Overriding of drug safety alerts in computerized physician order entry. *Journal of the American Medical Informatics Association*. 13(2): 138-147.

Van der Wiele, T., van Iwaarden, J., Brown, A., Steimle, U., and Zink, K. J. (2009). An international comparison of the perceptions about the revised ISO 9000 quality system standards. *Total Quality Management*. 20(4): 393-408.

Van Niekerk, J. F. and Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*. 29(4): 476-486. Cited by Bess, (2012).

Venkatesh, V. and Davis, F. D. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management science*. 46(2): 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*. 27(3): 425-478.

Venkatraman, N., Henderson, J. C., and Oldach, S. (1993). Continuous strategic alignment: Exploiting information technology capabilities for competitive success. *European Management Journal*. 11(2): 139-149.

Vermeulen, C. and Von Solms, R. (2002). The information security management toolbox–taking the pain out of security management. *Information Management & Computer Security*. 10(3): 119-125.

von Solms, B. (2001). Information Security — A Multidimensional Discipline. *Computers & Security*. 20(6): 504-508.

von Solms, B. (2006). Information Security – The Fourth Wave. *Computers & Security*. 25(3): 165-168.

von Solms, B. and von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*. 23(5): 371-376.

Von Solms, R. (1998). Information security management (1): why information security is so important. *Information Management & Computer Security*. 6(4): 174-177.

von Thaden, T. L. and Gibbons, A. M. (2008). The safety culture indicator scale measurement system (SCISMS). *National Technical Information Service Final Report (*pp. 1-57). HFD-08-03/FAA-08-2. Illinois: HFDIA.

http://www.aviation.illinois.edu/avimain/papers/research/pub_pdfs/techreports/08-03.pdf, (14.02.2014).

Vroom, C. and von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*. 23(3): 191-198.

Wagner, C., van Merode, G. G., and van Oort, M. (2003). Costs of Quality Management Systems in Long-Term Care Organizations: An Exploration. *Quality Management in Healthcare*. 12(2): 106-114. Cited by Hassan and Kanji, (2007).

Walker, J. M., Carayon, P., Leveson, N., Paulus, R. A., Tooker, J., Chin, H., . . . Stewart, W. F. (2008). EHR safety: the way forward to safe and effective systems. *Journal of the American Medical Informatics Association*. 15(3): 272-277.

Walker, S. (2012). Economics and the cyber challenge. *Information Security Technical Report*. 17(1–2): 9-18.

Walker, S. T. (1985). *Network security overview.* Paper presented at the 1985 IEEE Symposium on Security and Privacy. 1985.

Waly, N., Tassabehji, R., and Kamala, M. (2012). *Measures for improving information security management in organisations: the impact of training and awareness programmes.* Paper presented at the UK Academy for Information Systems Conference Proceedings 2012.

Wang, S. J., Middleton, B., Prosser, L. A., Bardon, C. G., Spurr, C. D., Carchidi, P. J., . . . Sussman, A. J. (2003). A cost-benefit analysis of electronic medical records in primary care. *The American Journal of Medicine*. 114(5): 397-403.

Wayne, S. R. (1983). Quality Control Circle and Company Wide Quality Control. *Quality Progress*. 16(10): 14-17.

Wears, R. L. and Perry, S. J. (2002). Human factors and ergonomics in the emergency department. *Annals of emergency medicine*. 40(2): 206-212.

Weed, L. L. and Weed, L. (1999). Opening the black box of clinical judgment—an overview. *BMJ: British Medical Journal*. 319(7220): 1279.

Weeda, D. and O'Flaherty, N. (1998). Food and Drug Administration regulation of blood bank software: the new regulatory landscape for blood establishments and their vendors. *Transfusion*. 38(1): 86-89.

Weick, K. and Sutcliffe, K. (2001). Managing the unexpected: Assuring high performance in an age of uncertainty. *San Francisco: Wiley*. 1(3): 5.

Weick, K. E. and Roberts, K. H. (1993). Collective mind in organizations: Heedful interrelating on flight decks. *Administrative science quarterly*. 38(3): 357-381. Cited by Palmieri et al., (2010).

Weick, K. E. and Sutcliffe, K. M. (2006). Mindfulness and the quality of organizational attention. *Organization science*. 17(4): 514-524.

Weiner, B. J., Alexander, J. A., and Shortell, S. M. (1996). Leadership for quality improvement in health care: Empirical evidence on hospital boards, managers, and physicians. *Medical Care Research and Review*. 53(4): 397-416.

Weiner, J. P., Kfuri, T., Chan, K., and Fowles, J. B. (2007). "e-Iatrogenesis": The most critical unintended consequence of CPOE and other HIT. *Journal of the American Medical Informatics Association*. 14(3): 387-388.

Weinger, M. B., Pantiskas, C., Wiklund, M. E., and Carstensen, P. (1998). Incorporating human factors into the design of medical devices. *JAMA: the journal of the American Medical Association*. 280(17): 1484-1484. Cited by Kohn et al., (2000).

Werlinger, R., Hawkey, K., and Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*. 17(1): 4-19.

Wetterneck, T. B., Walker, J. M., Blosky, M. A., Cartmill, R. S., Hoonakker, P., Johnson, M. A., . . . Carayon, P. (2011). Factors contributing to an increase in duplicate medication order errors after CPOE implementation. *Journal of the American Medical Informatics Association*. 18(6): 774-782.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management*. 24(1): 43-57.

Wiegmann, D. A., Zhang, H., Von Thaden, T. L., Sharma, G., and Gibbons, A. M. (2004). Safety culture: An integrative review. *The International Journal of Aviation Psychology*. 14(2): 117-134.

Williams, P. (2008). A practical application of CMM to medical security capability. *Information Management & Computer Security*. 16(1): 58-73.

Williams, P. A. (2006). *The Role of Standards in Medical Information Security: An Opportunity for Improvement.* Paper presented at the 2006 International Conference on Security and Management Las Vegas, Nevada.

Williamson, J. W. (1988). Future Policy Directions for Quality Assurance: Lessons From the Health Accounting Experience. *Inquiry*. 25(1): 67-77. Cited by Lohr, (1990).

Williamson, J. W. and Wilson, R. (1978). *Assessing and improving health care outcomes: the health accounting approach to quality assurance*. Pensacola, FL Ballinger Publishing Company. Cited by Lohr, (1990).

Wilson, I. B. and Cleary, P. D. (1995). Linking clinical variables with health-related quality of life: a conceptual model of patient outcomes. *JAMA*. 273(1): 59-65.

Wilson, L. A. (2002). *The quality management system* (Vol. The ASQ ISO 9000-2000 Handbook). Milwaukee: ASQ Quality Press.

Winkel, O. (2007). Electronic government and network security: a viewpoint. *Transforming Government: People, Process and Policy*. 1(3): 220-229.

Wolfers, A. (1960). *National Security as an ambiguous symbol*. Discord and Collaboration: Essays on International Politics. Cited by Mesjasz, (2004).

Wolfstadt, J. I., Gurwitz, J. H., Field, T. S., Lee, M., Kalkar, S., Wu, W., and Rochon, P. A. (2008). The effect of computerized physician order entry with clinical decision support on the rates of adverse drug events: a systematic review. *J Gen Intern Med*. 23(4): 451-458.

Womble, J. C. (2007). *E-learning: the relationship among learner satisfaction, self-efficacy, and usefulness*. San Diego, CA: Alliant International University.

Wong, C.-H., Sim, J.-J., Lam, C.-H., and Loke, S.-P. (2010). A linear structural equation modelling of TQM principles and its influence on quality performance. *International Journal of Modelling in Operations Management*. 1(1): 107-124.

Wong, Y. K. and Thite, M. (2009). Information security and privacy in HRIS.

Woods, D. D. (2010). *Behind human error*. Farnham, UK: Ashgate Publishing, Ltd.

Woods, D. D., Johannesen, L. J., Cook, R. I., and Sarter, N. B. (1994). Behind human error: Cognitive systems, computers and hindsight. CSERIAC SOAR 94-01. Dayton, OH: U. o. D. R. Institute. December 1994. http://www.dtic.mil/dtic/tr/fulltext/u2/a492127.pdf, (16.06.20140.

Woods, D. D. and Shattuck, L. G. (2000). Distant supervision–local action given the potential for surprise. *Cognition, Technology & Work*. 2(4): 242-245. Cited by Palmieri et al., (2010).

Woodward, J., Dawson, S., and Wedderburn, D. (1965). *Industrial organization: Theory and practice* (Vol.). London: Oxford University Press. Cited by Donaldson, (1995).

Workman, M., Bommer, W. H., and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*. 24(6): 2799-2816.

World Health Organization. (1948, 19-22 June, 1946). WHO definition of Health. *International Health Conference.* http://www.who.int/about/definition/en/print.html, (18.04.2014).

Worthen, B. (20.01.2009). Card Data Breached, Firm Says. http://online.wsj.com/news/articles/SB123249174099899837, (16.06.2014).

Wright, C. D., Wain, J. C., Grillo, H. C., Moncure, A. C., Macaluso, S. M., and Mathisen, D. J. (1997). Pulmonary lobectomy patient care pathway: a model to control cost and maintain quality. *The Annals of thoracic surgery*. 64(2): 299-302.

Wu, S., Chaudhry, B., Wang, J., Maglione, M., Mojica, W., Roth, E., . . . Shekelle, P. G. (2006). Systematic review: impact of health information technology on quality, efficiency, and costs of medical care. *Annals of internal medicine*. 144(10): 742-752.

Yassi, A. and Hancock, T. (2005). Patient safety–worker safety: Building a culture of safety to improve healthcare worker and patient well-being. *Healthc Q*. 8: 32-38.

Yeniman Yildirim, E., Akalp, G., Aytac, S., and Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*. 31(4): 360-365.

Yin, R. K. (2009). *Case study research: Design and methods* (Vol.). Thousand Oaks: sage.

Young, F. E. (1987). Validation of medical software: present policy of the Food and Drug Administration. *Annals of internal medicine*. 106(4): 628-629.

Zhan, C., Friedman, B., Mosso, A., and Pronovost, P. (2006). Medicare payment for selected adverse events: building the business case for investing in patient safety. *Health Aff (Millwood)*. 25(5): 1386-1393.

Zhu, Z. (1999). A comparison of quality programmes: total quality management and ISO 9000. *Total Quality Management*. 10(2): 291-297.

Zohar, D. (1980). Safety climate in industrial organizations: theoretical and applied implications. *Journal of Applied Psychology*. 65(1): 96.

Zohar, D. (2002). Modifying supervisory practices to improve subunit safety: a leadership-based intervention model. *Journal of Applied Psychology*. 87(1): 156. Cited by Palmieri et al., (2010).

Zohar, D. (2003). Safety climate: Conceptual and measurement issues. *Handbook of occupational health psychology* (pp. 123-142). Washington, D.C.: American Psychological Association.

Zohar, D., Livne, Y., Tenne-Gazit, O., Admi, H., and Donchin, Y. (2007). Healthcare climate: A framework for measuring and improving patient safety. *Critical care medicine*. 35(5): 1312-1317.

Zohar, D. and Luria, G. (2005). A multilevel model of safety climate: cross-level relationships between organization and group-level climates. *Journal of Applied Psychology*. 90(4): 616.

Zviran, M. and Haga, W. J. (1999). Password security: an empirical study. *Journal of Management Information Systems*. 15: 161-186.

Zwass, V. (1997). *Foundations of information systems*. Irwin, CA: McGraw Hill.

APPENDICES

APPENDIX 1. Question Forms (English)

This research is conducted for an academic purpose and analyzes the relationships among information security, patient safety, and quality. It will not take much of your time and the results of the survey will be used for educational purposes. Thanks for your interest, Yours Sincerely.

	Please mark the following questions according to the frequency of occurence. **PATIENT SAFETY;**	**Never**	**Rarely**	**Sometimes**	**Often**	**Always**
1	The culture of this clinical area makes it easy to learn from the mistakes of others.	①	②	③	④	⑤
2	Medical errors are handled appropriately in this clinical area.	①	②	③	④	⑤
3	The senior leaders in my hospital listen to me and care about my concerns.	①	②	③	④	⑤
4	The physician and nurse leaders in my area listen to me and care about my concerns.	①	②	③	④	⑤
5	Management is driving us to be a safety-centered institution.	①	②	③	④	⑤
6	My suggestions about safety would be acted upon if I expressed them to management.	①	②	③	④	⑤
7	Management does not knowingly compromise safety concerns for productivity.	①	②	③	④	⑤
8	I am encouraged by my colleagues to report any patient safety concerns I may have.	①	②	③	④	⑤
9	I know the proper channels to direct questions regarding patient safety.	①	②	③	④	⑤
10	I receive appropriate feedback about my performance.	①	②	③	④	⑤
11	İ would feel safe being treated here as a patient.	①	②	③	④	⑤
12	Briefing personnel before the start of a shift is an important part of patient safety.	①	②	③	④	⑤
13	Briefings regarding patient safety are common here.	①	②	③	④	⑤
14	I am satisfied with the availability of clinical leadership.	①	②	③	④	⑤
15	This institution is doing more for patient safety now, than it did one year ago.	①	②	③	④	⑤
16	In our unit, system failures are not attributable to one individual's actions.	①	②	③	④	⑤
17	The personnel would not mind taking additional responsibility for patient safety.	①	②	③	④	⑤
18	Personnel frequently disregard rules or guidelines int this clinical area .	①	②	③	④	⑤
19	Patient safety is a priority in this clinical area.	①	②	③	④	⑤
	QUALITY SYSTEM;					
20	Quality requirements are determined towards our services.	①	②	③	④	⑤
21	Appropriate records are maintained properly for our services.	①	②	③	④	⑤
22	Definitions for care services are documented.	①	②	③	④	⑤
23	Management fulfills their responsibilities.	①	②	③	④	⑤
24	Management is patient centric.	①	②	③	④	⑤
25	Management provides the settings for authorithy, responsibility, and communication.	①	②	③	④	⑤
26	Management is able to plan for future and take the proper actions.	①	②	③	④	⑤
27	Proper infrastructure is provided for quality service.	①	②	③	④	⑤
28	Experienced staff exists for a quality service.	①	②	③	④	⑤
29	Proper working conditions are provided for quality service.	①	②	③	④	⑤
30	Services are delivered according to plans.	①	②	③	④	⑤
31	Services and procedures are provided in coordination.	①	②	③	④	⑤
32	Services provided are sufficient.	①	②	③	④	⑤
33	Services provided are evaluated.	①	②	③	④	⑤
34	Outcomes are controlled and analyzed.	①	②	③	④	⑤
35	Services are improved based on the findings.	①	②	③	④	⑤

	INFORMATION SECURITY;	Never	Rarely	Sometimes	Often	Always
36	In our institution, work is handled according to a documented up-to-date information security policy.	①	②	③	④	⑤
37	In our institution, organization of information security is coordinated and properly handled.	①	②	③	④	⑤
38	In our institution, inventory, ownership, and acceptable use of assets are managed according to policies.	①	②	③	④	⑤
39	Personnel fulfill their responsibilities according to the information security policies and procedures.	①	②	③	④	⑤
40	Physical and environmental security measures of the information systems are in place.	①	②	③	④	⑤
41	Communications and operations management related procedures and responsibilities are well defined.	①	②	③	④	⑤
42	Access control policy ensures authorized access and prevents unauthorized access to information systems.	①	②	③	④	⑤
43	Information systems acquisitions, development, and maintenance are handled according to policies.	①	②	③	④	⑤
44	Information security related incidents are handled according to the specific responsibilities and procedures.	①	②	③	④	⑤
45	Business continuity plans are developed and implemented to avoid interruptions to business activities.	①	②	③	④	⑤
46	Information systems security policies comply according to the standards and legal requirements.	①	②	③	④	⑤
	IN GENERAL;					
47	In our institution, health care quality is ensured	①	②	③	④	⑤
48	In our institution, a complete patient safety is provided.	①	②	③	④	⑤
49	İn our institution, a complete information security is provided	①	②	③	④	⑤
50	In our institution, quality service is provided	①	②	③	④	⑤

BACKGROUND INFORMATION

51	**Age:**					
	a) 20 or younger	**b)** 20-29	**c)** 30-39	**d)** 40-49	**e)** 50 or over	
52	**Gender:**					
	a) Female	**b)** Male				
53	**Education:**					
	a) Elementary Sc.	**b)** Middle School	**c)** High School	**d)** Associate	**e)** Undergrad.	**f)** Graduate
54	**Job position:** _____					
55	**Experience in position in years:**					
	a) Less than 1	**b)** 1-5	**c)** 6-10	**d)** 11-20	**e)** 21 or overi	

Thanks For Your Participation...

APPENDIX 2. Question Forms (Turkish)

Sayın Katılımcı,

Akademik bir çalışma doğrultusunda, hasta güvenliği, bilgi güvenliği ve kalite arasındaki ilişkiler araştırılmaktadır. Anketin doldurulması fazla vaktinizi almayacaktır. Çalışmanın sonuçları eğitim amaçlı kullanılacaktır. İlginize çok teşekkür eder, saygılarımızı sunarız.

	Lütfen aşağıdaki soruları karşılaşma düzeyinize göre işaretleyiniz. HASTA GÜVENLİĞİ;	Asla	Nadiren	Ara sıra	Çoğu Zaman	Her zaman
1	Birimimizde yapılan tıbbi hatalardan ders çıkarırız.	①	②	③	④	⑤
2	Birimimizde tıbbi hatalar bilimsel şekilde değerlendirilir.	①	②	③	④	⑤
3	Hastanemizdeki yöneticiler hasta güvenliğiyle ilgili fikirlerimi dikkate alır.	①	②	③	④	⑤
4	Hekim arkadaşlarım hasta güvenliğiyle ilgili fikirlerimi dikkate alır.	①	②	③	④	⑤
5	Yönetim bizi güvenli bir kurum olmaya doğru yönlendirir.	①	②	③	④	⑤
6	Güvenlik hakkındaki önerilerimi, yöneticiler dikkate alır.	①	②	③	④	⑤
7	Yönetim herhangi bir çıkar için güvenliği tehlikeye atmaz.	①	②	③	④	⑤
8	Hasta güvenliğini tehdit edici bir olayı rahatça rapor edebilirim.	①	②	③	④	⑤
9	Hasta güvenliği ile ilgili başvuracağımız yerler belirlidir.	①	②	③	④	⑤
10	Performansımla ilgili geribildirimler alırım.	①	②	③	④	⑤
11	Hasta olsaydım, hastanemizde kendimi güvende hissederdim.	①	②	③	④	⑤
12	Vardiya değişimlerinde, hasta güvenliği açısından bilgi paylaşırız.	①	②	③	④	⑤
13	Hastanemizde sıkça güvenlikle ilgili bilgilendirme toplantıları yapılır.	①	②	③	④	⑤
14	Birim yöneticilerime hasta güvenliği konusunda rahatça ulaşabilirim.	①	②	③	④	⑤
15	Kurumumuz hasta güvenliğinde, geçen yıla göre daha iyidir.	①	②	③	④	⑤
16	Birimimizde sistemden kaynaklanan hatalar, kişiye mal edilmez.	①	②	③	④	⑤
17	Hasta güvenliğinde artı sorumluluk almaktan kaçınmayız.	①	②	③	④	⑤
18	Çalışanlar tıbbi kurallara ve yönergelere aldırmaz.	①	②	③	④	⑤
19	Birimimizde hasta güvenliği önceliklidir.	①	②	③	④	⑤
	KALİTE SİSTEMİ;					
20	Sağlık hizmetlerimize yönelik genel kalite şartları belirlenir.	①	②	③	④	⑤
21	Sağlık hizmetlerimize yönelik gerekli kayıtlar eksiksiz tutulur.	①	②	③	④	⑤
22	Sağlık hizmetlerimize yönelik tanımlamalar yazılı hale getirilir.	①	②	③	④	⑤
23	Yönetim taahhütlerini yerine getirir.	①	②	③	④	⑤
24	Yönetim hasta odaklıdır.	①	②	③	④	⑤
25	Yönetim yetki, sorumluluk ve iletişim olanaklarını sağlar.	①	②	③	④	⑤
26	Yönetimin planlama ve geleceği görme yeteneği vardır.	①	②	③	④	⑤
27	İyi bir hizmet sunmak için uygun altyapı sağlanır.	①	②	③	④	⑤
28	İyi bir hizmet sunmak için gerekli olan yetkin çalışanlar vardır.	①	②	③	④	⑤
29	İyi bir hizmet sunmak için çalışma ortamımızın uygunluğu sağlanır.	①	②	③	④	⑤
30	Hizmetler planlı bir şekilde sunulur.	①	②	③	④	⑤
31	Hizmetler (süreçler) koordinasyonlu bir şekilde sunulur.	①	②	③	④	⑤
32	Sunulan hizmetler yeterlidir.	①	②	③	④	⑤
33	Verilen hizmetler değerlendirilmektedir.	①	②	③	④	⑤
34	Elde edilen bulgu ve veriler kontrol ve analiz edilmektedir.	①	②	③	④	⑤
35	Elde edilen veriler ışığında, hizmetler iyileştirilmektedir.	①	②	③	④	⑤

Lütfen Arka Sayfaya Geçiniz...

	BİLGİ GÜVENLİĞİ;	Asla	Nadiren	Ara sıra	Çoğu Zaman	Her zaman
36	Hastanemizde, yazılı ve güncel bir bilgi güvenliği politikası doğrultusunda çalışılmaktadır.	①	②	③	④	⑤
37	Hastanemizde bilgi güvenliğinin organizasyonu sağlıklı bir şekilde yürütülür.	①	②	③	④	⑤
38	Hastanemizde bilgi işlemle ilgili yazılım, donanım gibi varlıklar iyi bir şekilde yönetilmektedir	①	②	③	④	⑤
39	Çalışanlar, bilgi güvenliği politika ve prosedürleri doğrultusunda sorumluluklarını yerine getirirler.	①	②	③	④	⑤
40	Bilgi sistemlerinin fiziksel ve çevresel güvenliği sağlıklı bir şekilde sağlanmaktadır.	①	②	③	④	⑤
41	Bilgi sistemleri ile ilgili iletişim ve operasyon yönetimi sağlıklı bir şekilde gerçekleştirilir.	①	②	③	④	⑤
42	Verilere yetkili kişilerin güvenli bir şekilde ulaşmaları için, erişim kontrolü sağlanmaktadır.	①	②	③	④	⑤
43	Bilgi sistemleri sağlıklı bir şekilde kurulmakta, geliştirilmekte ve bakımı sağlanmaktadır.	①	②	③	④	⑤
44	Hastanemizde, bilgi güvenliği açıklarında, belirlenen sorumluluk ve prosedürler çerçevesinde hareket edilir	①	②	③	④	⑤
45	Kesintisiz hizmet sunumu için olağanüstü durumlara yönelik planlamalar yapılmaktadır.	①	②	③	④	⑤
46	Hastanemizdeki bilgi sistemlerinin güvenliği, standartlara göre yönetilir.	①	②	③	④	⑤
	GENEL OLARAK;					
47	Hastanemizde sağlık kalitesi güvence altındadır.	①	②	③	④	⑤
48	Hastalarımızın tıbbi güvenliği eksiksiz sağlanmaktadır.	①	②	③	④	⑤
49	Hastanemizde bilgi güvenliği eksiksi sağlanmaktadır.	①	②	③	④	⑤
50	Hastanemizde kaliteli bir hizmet sunulmaktadır.	①	②	③	④	⑤

DEMOGRAFİK DEĞERLENDİRMELER;

51 **Yaşınız:**
a) 20' den küçük b) 20-29 c) 30-39 d) 40-49 e) 50 ve üzeri

52 **Cinsiyetiniz:**
a) Kadın b) Erkek

53 **Eğitim durumunuz:**
a) İlkokul b) Ortaokul/İlköğretim c) Lise d) Ön lisans e) Lisans f) Lisansüstü

54 **Kaç yıldır bu görevde çalışıyorsunuz:**
a) 1'den az b) 1-5 c) 6-10 d) 11-20 e) 21 ve üzeri

55 **Lütfen görevinizi yan tarafa yazınız:** _____

İLGİNİZE ÇOK TEŞEKKÜR EDERİZ...

APPENDIX 3. Varimax Rotated Factor Structure

Patient Safety				Quality				Information Security			Healthcare Excellence		
	General	Unit			General			Information			Healthcare		
Variable	Safety	Safety	communalities	Variable	KAIZEN	Quality Req	communalities	Variable	Security	communalities	Variable	Excellence	communalities
V6	**.805**	.219	.695	V27	**.826**	.275	.757	V44	**.866**	.750	V48	**.925**	.855
V13	**.749**	.229	.613	V35	**.811**	.307	.752	V41	**.866**	.749	V47	**.914**	.835
V3	**.715**	.294	.598	V30	**.811**	.287	.740	V40	**.855**	.731	V49	**.913**	.833
V10	**.713**	.107	.520	V29	**.808**	.202	.694	V42	**.849**	.721	V50	**.912**	.831
V5	**.702**	**.475**	.718	V26	**.794**	.330	.740	V37	**.848**	.718			
V11	**.692**	.195	.517	V31	**.785**	.387	.765	V43	**.839**	.704			
V4	**.652**	.322	.529	V33	**.765**	.372	.724	V46	**.837**	.700			
V15	**.620**	**.485**	.619	V28	**.743**	.315	.652	V38	**.829**	.687			
V14	**.604**	**.542**	.658	V32	**.730**	.329	.641	V45	**.816**	.667			
V7	**.594**	.320	.456	V25	**.718**	.395	.672	V39	**.807**	.652			
V16	**.551**	.298	.393	V34	**.715**	.397	.668	V36	**.775**	.601			
V9	**.518**	**.484**	.503	V23	**.597**	.511	.618						
V1	.086	**.790**	.631	V24	**.555**	.345	.427						
V12	.195	**.750**	.600	V21	.235	**.885**	.838						
V19	**.405**	**.668**	.610	V22	.346	**.822**	.795						
V2	.335	**.608**	.483	V20	.390	**.780**	.761						
V8	**.496**	**.578**	.580										
V17	.216	**.575**	.377										
Eigenvalue	5.915	4.186	10.100		7.585	3.658	11.243		7.681	7.681		3.354	3.354
% of total Variance	32.86	23.25	**56.11**		47.41	22.86	**70.27**		69.83	**69.83**		83.85	**83.85**

APPENDIX 4. Patient Safety Items Correlation Matrix

Correlations

		V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V18	V19
V1	Pearson Correlation	1	.536**	.336**	.342**	.386**	.248**	.289**	.379**	.430**	.247**	.219**	.425**	.228**	.402**	.370**	.264**	.332**	.092	.395**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.074	.000
	N	387	380	379	371	381	380	378	384	380	377	384	381	378	381	373	378	380	381	380
V2	Pearson Correlation	.536**	1	.481**	.504**	.510**	.384**	.326**	.435**	.399**	.374**	.340**	.446**	.379**	.426**	.388**	.325**	.313**	.051	.374**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.321	.000
	N	380	380	373	365	374	373	371	377	374	371	378	356	371	374	368	371	373	374	373
V3	Pearson Correlation	.336**	.401**	1	.667**	.635**	.731**	.425**	.474**	.365**	.465**	.490**	.405**	.524**	.501**	.477**	.419**	.328**	-.027	.400**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.607	.000
	N	379	373	379	365	373	373	371	376	372	370	376	355	370	373	366	370	372	373	372
V4	Pearson Correlation	.342**	.504**	.667**	1	.549**	.570**	.421**	.494**	.349**	.454**	.385**	.349**	.458**	.461**	.428**	.399**	.362**	.022	.371**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.673	.000
	N	371	365	365	371	365	364	364	368	364	362	368	350	363	366	358	362	364	365	364
V5	Pearson Correlation	.386**	.510**	.635**	.549**	1	.636**	.545**	.601**	.596**	.441**	.512**	.402**	.559**	.631**	.600**	.422**	.397**	.042	.517**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.419	.000
	N	381	374	373	365	383	376	375	380	376	373	380	358	374	376	369	374	377	377	376
V6	Pearson Correlation	.248**	.384**	.731**	.570**	.636**	1	.561**	.497**	.376**	.508**	.517**	.366**	.565**	.531**	.477**	.413**	.300**	-.023	.389**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.657	.000
	N	380	373	373	364	376	382	373	380	375	375	380	358	374	377	370	375	377	377	376
V7	Pearson Correlation	.289**	.326**	.425**	.421**	.545**	.561**	1	.536**	.431**	.327**	.374**	.316**	.433**	.469**	.401**	.443**	.348**	.093	.439**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.111	.000
	N	378	371	371	364	375	373	380	377	373	370	377	357	372	374	367	373	373	374	373
V8	Pearson Correlation	.379**	.435**	.474**	.494**	.601**	.497**	.536**	1	.578**	.375**	.410**	.466**	.472**	.588**	.495**	.337**	.396**	.101	.578**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.050	.000
	N	384	377	376	368	380	380	377	386	379	377	383	360	377	379	373	378	379	380	379
V9	Pearson Correlation	.430**	.399**	.365**	.349**	.596**	.376**	.431**	.578**	1	.443**	.415**	.388**	.430**	.509**	.528**	.356**	.294**	.153**	.477**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.003	.000
	N	380	374	372	364	376	375	373	379	382	372	379	356	373	376	368	373	375	377	376
V10	Pearson Correlation	.247**	.374**	.465**	.454**	.441**	.508**	.327**	.375**	.443**	1	.462**	.311**	.503**	.438**	.361**	.342**	.225**	-.037	.279**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.471	.000
	N	377	371	370	362	373	375	370	377	372	379	378	357	370	373	367	371	373	373	372
V11	Pearson Correlation	.219**	.340**	.490**	.385**	.512**	.517**	.374**	.410**	.415**	.462**	1	.310**	.521**	.522**	.498**	.360**	.286**	-.006	.401**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.915	.000
	N	384	378	376	368	380	380	377	383	379	378	386	362	377	380	374	378	380	380	379
V12	Pearson Correlation	.425**	.446**	.405**	.349**	.402**	.366**	.316**	.466**	.388**	.311**	.310**	1	.340**	.549**	.432**	.255**	.312**	.160**	.473**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.002	.000
	N	361	356	355	350	358	358	357	360	356	357	362	363	358	360	355	357	361	359	357
V13	Pearson Correlation	.228**	.379**	.524**	.458**	.559**	.565**	.433**	.472**	.430**	.503**	.521**	.348**	1	.636**	.571**	.388**	.257**	-.023	.376**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.653	.000
	N	378	371	370	363	374	374	372	377	373	370	377	358	380	376	369	373	375	375	374
V14	Pearson Correlation	.402**	.426**	.501**	.461**	.631**	.531**	.469**	.589**	.509**	.438**	.522**	.549**	.636**	1	.651**	.415**	.406**	.059	.467**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.253	.000
	N	381	374	373	366	376	377	374	379	376	373	380	360	376	382	372	376	378	377	376
V15	Pearson Correlation	.370**	.388**	.477**	.428**	.600**	.477**	.481**	.495**	.528**	.361**	.498**	.432**	.571**	.651**	1	.465**	.334**	.025	.477**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.631	.000
	N	373	368	366	358	369	370	367	373	368	367	374	355	369	372	375	369	371	370	369
V16	Pearson Correlation	.264**	.325**	.419**	.399**	.422**	.413**	.443**	.337**	.356**	.342**	.360**	.255**	.388**	.415**	.465**	1	.388**	-.096	.397**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.063	.000
	N	378	371	370	362	374	375	373	378	373	371	378	357	373	376	369	380	375	375	374
V17	Pearson Correlation	.332**	.313**	.328**	.362**	.397**	.300**	.348**	.396**	.294**	.225**	.286**	.312**	.257**	.406**	.334**	.388**	1	.109*	.477**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.034	.000
	N	380	373	372	364	377	377	373	379	375	373	380	361	375	378	371	375	382	378	376
V18	Pearson Correlation	.092	.051	-.027	.022	.042	-.023	.093	.101	.153**	-.037	-.006	.160**	-.023	.059	.025	-.096	.109*	1	.220**
	Sig. (2-tailed)	.074	.321	.607	.673	.419	.657	.111	.050	.003	.471	.915	.002	.653	.253	.631	.063	.034		.000
	N	381	374	373	365	377	377	374	380	377	373	380	359	375	377	370	375	378	383	378
V19	Pearson Correlation	.395**	.374**	.400**	.371**	.517**	.389**	.439**	.578**	.477**	.279**	.401**	.473**	.376**	.467**	.477**	.397**	.477**	.220**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	
	N	380	373	372	364	376	376	373	379	376	372	379	357	374	376	369	374	376	378	382

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

APPENDIX 5. Patient Safety Items Correlation Matrix –V18 excluded

Correlations

		V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V19
V1	Pearson Correlation	1	.536**	.336**	.342**	.386**	.248**	.289**	.379**	.430**	.247**	.219**	.425**	.228**	.402**	.370**	.264**	.332**	.395**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	387	380	379	371	381	380	378	384	380	377	384	361	378	381	373	378	380	380
V2	Pearson Correlation	.536**	1	.481**	.504**	.510**	.384**	.326**	.435**	.399**	.374**	.340**	.446**	.379**	.426**	.388**	.325**	.313**	.374**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	380	380	373	365	374	373	371	377	374	371	378	356	371	374	368	371	373	373
V3	Pearson Correlation	.336**	.481**	1	.667**	.635**	.731**	.425**	.474**	.365**	.465**	.490**	.405**	.524**	.501**	.477**	.419**	.328**	.400**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	379	373	379	365	373	373	371	376	372	370	376	355	370	373	366	370	372	372
V4	Pearson Correlation	.342**	.504**	.667**	1	.549**	.570**	.421**	.494**	.349**	.454**	.385**	.349**	.458**	.461**	.428**	.399**	.362**	.371**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	371	365	365	371	365	364	364	368	364	362	368	350	363	366	358	362	364	364
V5	Pearson Correlation	.386**	.510**	.635**	.549**	1	.636**	.545**	.601**	.596**	.441**	.512**	.402**	.559**	.631**	.600**	.422**	.397**	.517**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	381	374	373	365	383	376	375	380	376	373	380	358	374	376	369	374	377	376
V6	Pearson Correlation	.248**	.384**	.731**	.570**	.636**	1	.561**	.497**	.376**	.508**	.517**	.366**	.565**	.531**	.477**	.413**	.300**	.389**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	380	373	373	364	376	382	373	380	375	375	380	358	374	377	370	375	377	376
V7	Pearson Correlation	.289**	.326**	.425**	.421**	.545**	.561**	1	.536**	.431**	.327**	.374**	.316**	.433**	.469**	.481**	.443**	.348**	.439**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	378	371	371	364	375	373	380	377	373	370	377	357	372	374	367	373	373	373
V8	Pearson Correlation	.379**	.435**	.474**	.494**	.601**	.497**	.536**	1	.578**	.375**	.410**	.466**	.472**	.588**	.495**	.337**	.396**	.578**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	384	377	376	368	380	380	377	386	379	377	383	360	377	379	373	378	379	379
V9	Pearson Correlation	.430**	.399**	.365**	.349**	.596**	.376**	.431**	.578**	1	.443**	.415**	.300**	.430**	.509**	.520**	.356**	.294**	.477**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	380	374	372	364	376	375	373	379	382	372	379	356	373	376	368	373	375	376
V10	Pearson Correlation	.247**	.374**	.465**	.454**	.441**	.508**	.327**	.375**	.443**	1	.462**	.311**	.503**	.438**	.361**	.342**	.225**	.279**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000
	N	377	371	370	362	373	375	370	377	372	379	378	357	370	373	367	371	373	372
V11	Pearson Correlation	.219**	.340**	.490**	.395**	.512**	.517**	.374**	.410**	.415**	.462**	1	.310**	.521**	.522**	.498**	.360**	.286**	.401**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000
	N	384	378	376	368	380	380	377	383	379	378	386	362	377	380	374	378	380	379
V12	Pearson Correlation	.425**	.446**	.405**	.349**	.402**	.366**	.316**	.466**	.388**	.311**	.310**	1	.348**	.549**	.432**	.255**	.312**	.473**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000
	N	361	356	355	350	358	358	357	360	356	357	362	363	358	360	355	357	361	357
V13	Pearson Correlation	.229**	.379**	.524**	.458**	.559**	.565**	.433**	.472**	.430**	.503**	.521**	.349**	1	.636**	.571**	.398**	.257**	.376**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000
	N	378	371	370	363	374	374	372	377	373	370	377	358	380	376	369	373	375	374
V14	Pearson Correlation	.402**	.426**	.501**	.461**	.631**	.531**	.469**	.588**	.509**	.438**	.522**	.549**	.636**	1	.651**	.415**	.406**	.467**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000
	N	381	374	373	366	376	377	374	379	376	373	380	360	376	382	372	376	378	376
V15	Pearson Correlation	.370**	.388**	.477**	.428**	.600**	.477**	.481**	.495**	.520**	.361**	.498**	.432**	.571**	.651**	1	.465**	.334**	.477**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000
	N	373	368	366	358	369	370	367	373	369	367	374	355	369	372	375	369	371	369
V16	Pearson Correlation	.264**	.325**	.419**	.399**	.422**	.413**	.443**	.337**	.356**	.342**	.360**	.255**	.388**	.415**	.465**	1	.388**	.397**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000
	N	378	371	370	362	374	375	373	378	373	371	378	357	373	376	369	380	375	374
V17	Pearson Correlation	.332**	.313**	.328**	.362**	.397**	.300**	.348**	.396**	.294**	.225**	.286**	.312**	.257**	.406**	.334**	.388**	1	.477**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000
	N	380	373	372	364	377	377	373	379	375	373	380	361	375	378	371	375	382	376
V19	Pearson Correlation	.395**	.374**	.400**	.371**	.517**	.389**	.439**	.578**	.477**	.279**	.401**	.473**	.376**	.467**	.477**	.397**	.477**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	
	N	380	373	372	364	376	376	373	379	376	372	379	357	374	376	369	374	376	382

**. Correlation is significant at the 0.01 level (2-tailed).

APPENDIX 6. Quality Items Correlation Matrix

Correlations

		V20	V21	V22	V23	V24	V25	V26	V27	V28	V29	V30	V31	V32	V33	V34	V35
V20	Pearson Correlation	1	.723**	.650**	.566**	.454**	.578**	.567**	.533**	.553**	.464**	.547**	.598**	.543**	.569**	.562**	.571**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	387	385	383	386	385	383	385	382	384	385	387	383	386	386	385	385
V21	Pearson Correlation	.723**	1	.738**	.513**	.383**	.486**	.494**	.454**	.469**	.419**	.477**	.511**	.469**	.513**	.499**	.490**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	385	387	384	386	384	384	385	383	384	386	387	383	386	386	384	385
V22	Pearson Correlation	.650**	.738**	1	.597**	.448**	.565**	.534**	.540**	.533**	.470**	.518**	.601**	.530**	.562**	.570**	.516**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	383	384	385	385	382	382	383	381	382	384	385	381	384	384	382	383
V23	Pearson Correlation	.566**	.513**	.597**	1	.539**	.638**	.649**	.606**	.567**	.563**	.576**	.632**	.588**	.619**	.609**	.618**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	386	386	385	388	385	384	386	383	385	386	388	383	387	387	385	385
V24	Pearson Correlation	.454**	.383**	.448**	.539**	1	.585**	.556**	.549**	.386**	.469**	.494**	.533**	.439**	.511**	.506**	.494**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	385	384	382	385	386	382	384	381	383	384	386	382	385	385	384	384
V25	Pearson Correlation	.578**	.486**	.565**	.638**	.585**	1	.760**	.718**	.633**	.621**	.626**	.695**	.542**	.618**	.588**	.659**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	383	384	382	384	382	385	383	381	382	384	385	381	384	384	382	383
V26	Pearson Correlation	.567**	.494**	.534**	.649**	.556**	.760**	1	.794**	.678**	.668**	.701**	.670**	.624**	.646**	.608**	.709**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	385	385	383	386	384	383	387	382	384	385	387	382	386	386	384	384
V27	Pearson Correlation	.533**	.454**	.540**	.606**	.549**	.718**	.794**	1	.725**	.702**	.704**	.685**	.629**	.653**	.622**	.715**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000
	N	382	383	381	383	381	381	382	384	381	383	384	380	383	383	381	382
V28	Pearson Correlation	.553**	.469**	.533**	.567**	.386**	.633**	.678**	.725**	1	.626**	.658**	.692**	.603**	.651**	.620**	.700**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000
	N	384	384	382	385	383	382	384	381	386	384	386	381	385	385	383	383
V29	Pearson Correlation	.464**	.419**	.470**	.563**	.469**	.621**	.668**	.702**	.626**	1	.712**	.682**	.622**	.680**	.604**	.662**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000
	N	385	386	384	386	384	384	385	383	384	387	387	383	386	386	384	385
V30	Pearson Correlation	.547**	.477**	.518**	.576**	.494**	.626**	.701**	.704**	.658**	.712**	1	.804**	.687**	.686**	.664**	.661**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000
	N	387	387	385	388	386	385	387	384	386	387	389	384	388	388	386	386
V31	Pearson Correlation	.598**	.511**	.601**	.632**	.533**	.695**	.670**	.685**	.692**	.682**	.804**	1	.718**	.730**	.695**	.712**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000
	N	383	383	381	383	382	381	382	380	381	383	384	384	383	383	382	383
V32	Pearson Correlation	.543**	.469**	.530**	.588**	.439**	.542**	.624**	.629**	.603**	.622**	.687**	.718**	1	.722**	.645**	.682**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000
	N	386	386	384	387	385	384	386	383	385	386	388	383	388	388	385	385
V33	Pearson Correlation	.569**	.513**	.562**	.619**	.511**	.618**	.646**	.653**	.651**	.680**	.686**	.730**	.722**	1	.750**	.740**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000
	N	386	386	384	387	385	384	386	383	385	386	388	383	388	388	385	385
V34	Pearson Correlation	.562**	.499**	.570**	.609**	.506**	.588**	.608**	.622**	.620**	.604**	.664**	.695**	.645**	.750**	1	.753**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000
	N	385	384	382	385	384	382	384	381	383	384	386	382	385	385	386	385
V35	Pearson Correlation	.571**	.490**	.516**	.618**	.494**	.659**	.709**	.715**	.700**	.662**	.661**	.712**	.682**	.740**	.753**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	
	N	385	385	383	385	384	383	384	382	383	385	386	383	385	385	385	386

**. Correlation is significant at the 0.01 level (2-tailed).

APPENDIX 7. Information Security Items Correlation Matrix

Correlations

		V36	V37	V38	V39	V40	V41	V42	V43	V44	V45	V46
V36	Pearson Correlation	1	.744**	.664**	.550**	.620**	.590**	.591**	.573**	.594**	.538**	.602**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	388	387	386	385	386	385	386	383	384	381	385
V37	Pearson Correlation	.744**	1	.729**	.681**	.679**	.719**	.666**	.647**	.641**	.617**	.636**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000	.000	.000	.000	.000
	N	387	388	386	385	386	385	386	383	384	381	385
V38	Pearson Correlation	.664**	.729**	1	.615**	.695**	.690**	.689**	.643**	.661**	.597**	.650**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000	.000	.000	.000	.000
	N	386	386	387	384	385	384	385	382	383	380	384
V39	Pearson Correlation	.550**	.681**	.615**	1	.671**	.684**	.653**	.642**	.647**	.625**	.668**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000	.000	.000	.000	.000
	N	385	385	384	386	384	383	384	381	382	379	383
V40	Pearson Correlation	.620**	.679**	.695**	.671**	1	.736**	.692**	.622**	.701**	.623**	.698**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000	.000	.000	.000	.000
	N	386	386	385	384	387	384	386	382	383	381	384
V41	Pearson Correlation	.590**	.719**	.690**	.684**	.736**	1	.725**	.724**	.697**	.643**	.654**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000	.000	.000	.000	.000
	N	385	385	384	383	384	386	384	382	382	379	383
V42	Pearson Correlation	.591**	.666**	.689**	.653**	.692**	.725**	1	.717**	.708**	.611**	.655**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000		.000	.000	.000	.000
	N	386	386	385	384	386	384	387	382	383	380	384
V43	Pearson Correlation	.573**	.647**	.643**	.642**	.622**	.724**	.717**	1	.736**	.653**	.680**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000		.000	.000	.000
	N	383	383	382	381	382	382	382	384	382	379	383
V44	Pearson Correlation	.594**	.641**	.661**	.647**	.701**	.697**	.708**	.736**	1	.735**	.708**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000		.000	.000
	N	384	384	383	382	383	382	383	382	385	381	384
V45	Pearson Correlation	.538**	.617**	.597**	.625**	.623**	.643**	.611**	.653**	.735**	1	.729**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000		.000
	N	381	381	380	379	381	379	380	379	381	382	382
V46	Pearson Correlation	.602**	.636**	.650**	.668**	.698**	.654**	.655**	.680**	.708**	.729**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	
	N	385	385	384	383	384	383	384	383	384	382	386

**. Correlation is significant at the 0.01 level (2-tailed).

APPENDIX 8. Healthcare Excellence Items Correlation Matrix

Correlations

		V47	V48	V49	V50
V47	Pearson Correlation	1	.797**	.754**	.788**
	Sig. (2-tailed)		.000	.000	.000
	N	384	383	383	384
V48	Pearson Correlation	.797**	1	.812**	.776**
	Sig. (2-tailed)	.000		.000	.000
	N	383	383	382	383
V49	Pearson Correlation	.754**	.812**	1	.774**
	Sig. (2-tailed)	.000	.000		.000
	N	383	382	383	383
V50	Pearson Correlation	.788**	.776**	.774**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	384	383	383	384

**. Correlation is significant at the 0.01 level (2-tailed).

APPENDIX 9. Bartlett Test and Measure of Sampling Adequacy for Safety,Quality, Security,Excellence

KMO and Bartlett's Test for Safety Items

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.936
Bartlett's Test of Sphericity	Approx. Chi-Square	3028.339
	df	171
	Sig.	.000

KMO and Bartlett's Test for Quality Items

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.958
Bartlett's Test of Sphericity	Approx. Chi-Square	4990.266
	df	120
	Sig.	.000

KMO and Bartlett's Test for Information Security Items

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.957
Bartlett's Test of Sphericity	Approx. Chi-Square	3510.381
	df	55
	Sig.	.000

KMO and Bartlett's Test for Healthcare Excellence

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.858
Bartlett's Test of Sphericity	Approx. Chi-Square	1299.733
	df	6
	Sig.	.000

APPENDIX 10. MSA and Partial Correlations for Safety

Note: Measures of sampling adequacy are on the diagonal, partial correlations are off-diagonal in Anti-image Correlation section

Anti-image Matrices

		V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V18	V19
Anti-image Covariance	V1	.569	-.184	-.003	-.003	-.012	.021	-.003	.008	-.069	.017	.044	-.086	.053	-.037	-.052	.028	-.056	-.004	-.027
	V2	-.184	.521	-.043	-.059	-.062	.013	.031	-.015	.012	-.026	-.006	-.080	-.014	-.003	.007	-.005	.004	.032	.011
	V3	-.003	-.043	.343	-.149	-.039	-.124	.050	.036	-.010	-.026	-.052	-.030	.029	-.024	.013	-.004	-.025	.006	-.030
	V4	-.003	-.059	-.149	.421	-.019	-.025	-.006	-.092	.053	-.033	.025	.013	-.024	.008	-.014	-.057	-.048	-.058	.042
	V5	-.012	-.062	-.039	-.019	.311	-.042	-.071	-.026	-.076	-.011	-.024	.028	-.011	-.039	-.026	-.011	.009	-.015	-.037
	V6	.021	.013	-.124	-.025	-.042	.336	-.131	-.028	.026	-.059	-.044	-.002	-.049	-.021	.013	.031	.000	.022	.013
	V7	-.003	.031	.050	-.006	-.071	-.131	.515	-.045	-.031	.037	.006	.014	.011	.011	-.045	-.075	-.014	-.013	-.028
	V8	.008	-.015	.036	-.092	-.026	-.028	-.045	.408	-.116	.014	.020	-.038	.008	-.054	-.003	-.076	-.007	.075	-.111
	V9	-.069	.012	-.010	.053	-.076	.026	-.031	-.116	.455	-.116	-.028	-.008	-.006	-.003	-.056	-.014	.013	-.099	.021
	V10	.017	-.026	-.026	-.033	-.011	-.059	.037	.014	-.116	.542	-.064	-.016	-.113	.005	.031	-.030	.021	.043	.020
	V11	.044	-.006	-.052	.025	-.024	-.044	.006	.020	-.028	-.064	.557	.036	-.046	-.049	-.030	.017	-.035	.027	-.061
	V12	-.086	-.080	-.030	.013	.028	-.002	.014	-.038	-.008	-.016	.036	.531	.008	-.107	.022	.037	-.046	-.038	-.104
	V13	.053	-.014	.029	-.024	-.011	-.049	.011	.008	-.006	-.113	-.046	.008	.414	-.102	-.081	-.024	.035	.029	-.018
	V14	-.037	-.003	.013	.008	-.039	-.021	.011	-.054	-.003	.005	-.049	-.107	-.102	.333	-.079	-.031	-.030	-.003	.026
	V15	-.052	.007	-.004	-.014	-.026	.013	-.045	-.003	-.056	.031	-.030	.022	-.081	-.079	.368	-.089	.027	-.010	-.053
	V16	.028	-.005	-.025	-.057	-.011	.031	-.075	.076	-.014	-.030	.017	.037	-.024	-.031	-.089	.537	-.144	-.028	-.065
	V17	-.056	.004	.006	-.048	.009	.000	-.014	-.007	.013	.021	-.035	-.046	.035	-.030	.027	-.144	.661	-.104	-.104
	V18	-.004	.032	.052	-.058	-.015	.022	-.013	.075	-.099	.043	.027	-.038	.029	-.003	-.010	.157	-.028	.816	-.143
	V19	-.027	.011	-.030	.042	-.037	.013	-.028	-.111	.021	.020	-.061	-.104	-.018	.026	-.053	-.065	-.104	-.143	.393
Anti-image Correlation	V1	.917[a]	-.338	-.007	-.006	-.029	.048	-.006	.016	-.135	.030	.079	-.156	-.018	-.085	-.114	.051	-.091	-.006	-.057
	V2	-.338	.940[a]	-.102	-.127	-.154	.032	.060	-.032	.024	-.049	-.012	-.153	-.029	-.008	.017	-.010	.007	.049	.023
	V3	-.007	-.102	.915[a]	-.393	-.121	-.365	.120	.096	-.026	-.060	-.119	-.071	.078	.040	-.012	-.058	.014	.098	-.083
	V4	-.006	-.127	-.393	.927[a]	-.054	-.066	-.014	-.222	.121	-.069	.051	.028	-.059	.022	-.036	-.120	-.092	-.099	.103
	V5	-.029	-.154	-.121	-.054	.968[a]	-.129	-.179	-.073	-.203	-.027	-.059	.069	-.031	-.122	-.078	-.026	.021	-.029	-.106
	V6	.048	.032	-.365	-.066	-.129	.932[a]	-.316	-.075	.067	-.138	-.102	-.005	-.131	-.062	.037	.072	.000	.042	.037
	V7	-.006	.060	.120	-.014	-.179	-.316	.940[a]	-.099	-.065	.071	.011	.026	.024	.026	-.103	-.143	-.023	-.020	-.062
	V8	.016	-.032	.096	-.222	-.073	-.075	-.099	.932[a]	-.269	.029	.041	-.081	.020	-.146	-.008	.162	-.014	.130	-.278
	V9	-.135	.024	-.026	.121	-.203	.067	-.065	-.269	.934[a]	-.234	-.055	-.017	-.013	-.009	-.136	-.029	.023	-.162	.049
	V10	.030	-.049	-.060	-.069	-.027	-.138	.071	.029	-.234	.944[a]	-.117	-.030	-.238	.012	.069	-.056	.035	.065	.043
	V11	.079	-.012	-.119	.051	-.059	-.102	.011	.041	-.055	-.117	.967[a]	.067	-.097	-.113	-.065	.031	-.058	.040	-.131
	V12	-.156	-.153	-.071	.028	.069	-.005	.026	-.081	-.017	-.030	.067	.934[a]	.018	-.254	.050	.069	-.077	-.057	-.228
	V13	.110	-.029	.078	-.059	-.031	-.131	.024	.020	-.013	-.238	-.097	.018	.944[a]	-.275	-.207	-.052	.066	.050	-.044
	V14	-.085	-.008	.040	.022	-.122	-.062	.026	-.146	-.009	.012	-.113	-.254	-.275	.948[a]	-.227	-.073	-.065	-.005	.071
	V15	-.114	.017	-.012	-.036	-.078	.037	-.103	-.008	-.136	.069	-.065	.050	-.207	-.227	.955[a]	-.199	.056	-.019	-.139
	V16	.051	-.010	-.058	-.120	-.026	.072	-.143	.162	-.029	-.056	.031	.069	-.052	-.073	-.199	.915[a]	-.242	.237	-.141
	V17	-.091	.007	.014	-.092	.021	.000	-.023	-.014	.023	.035	-.058	-.077	.066	-.065	.056	-.242	.935[a]	-.039	-.204
	V18	-.006	.049	.098	-.099	-.029	.042	-.020	.130	-.162	.065	.040	-.057	.050	-.005	-.019	.237	-.039	.413[a]	-.252
	V19	-.057	.023	-.083	.103	-.106	.037	-.062	-.278	.049	.043	-.131	-.228	-.044	.071	-.139	-.141	-.204	-.252	.923[a]

a. Measures of Sampling Adequacy(MSA)

APPENDIX 11. MSA and Partial Correlations for Safety - V18 excluded

Note: Measures of sampling adequacy are on the diagonal, partial correlations are off-diagonal in Anti-image Correlation section

Anti-image Matrices

		V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V19
Anti-image Covariance	V1	.572	-.182	-.005	-.002	-.013	.019	-.002	.009	-.076	.025	.043	-.086	.054	-.037	-.051	.027	-.057	-.030
	V2	-.182	.528	-.042	-.062	-.063	.017	.028	-.020	.023	-.041	-.005	-.082	-.016	-.002	.006	-.005	.008	.020
	V3	-.005	-.042	.346	-.148	-.039	-.129	.053	.033	-.006	-.026	-.055	-.028	.028	.013	-.003	-.039	.008	-.024
	V4	-.002	-.062	-.148	.424	-.021	-.023	-.009	-.090	.048	-.031	.027	.011	-.023	.009	-.015	-.048	-.050	.036
	V5	-.013	-.063	-.039	-.021	.310	-.041	-.072	-.025	-.081	-.010	-.024	.028	-.011	-.039	-.026	-.009	.009	-.042
	V6	.019	.017	-.129	-.023	-.041	.337	-.130	-.030	.028	-.058	-.046	-.001	-.050	-.021	.014	.026	.000	.018
	V7	-.002	.028	.053	-.009	-.072	-.130	.514	-.046	-.033	.037	.007	.013	.011	.011	-.045	-.075	-.013	-.031
	V8	.009	-.020	.033	-.080	-.025	-.030	-.046	.415	-.112	.010	.018	-.035	.005	-.054	-.002	.067	-.004	-.106
	V9	-.076	.023	-.006	.048	-.081	.028	-.033	-.112	.468	-.109	-.027	-.012	-.002	-.004	-.057	.001	.009	.004
	V10	.025	-.041	-.026	-.031	-.010	-.058	.037	.010	-.109	.554	-.064	-.017	-.117	.005	.029	-.035	.024	.029
	V11	.043	-.005	-.055	.027	-.024	-.046	.007	.018	-.027	-.064	.557	.038	-.048	-.049	-.029	.011	-.035	-.060
	V12	-.086	-.082	-.028	.011	.028	-.001	.013	-.035	-.012	-.017	.038	.534	.010	-.108	.021	.048	-.047	-.120
	V13	.054	-.016	.028	-.023	-.011	-.050	.011	.005	-.002	-.117	-.048	.010	.414	-.102	-.080	-.032	.036	-.013
	V14	-.037	-.002	.013	.009	-.039	-.021	.011	-.054	-.004	.005	-.049	-.108	.333	-.080	-.032	-.031	.026	
	V15	-.051	.006	-.003	-.015	-.026	.014	-.045	-.002	-.057	.029	-.029	.021	-.080	-.080	.368	-.091	.027	-.059
	V16	.027	-.005	-.039	-.048	-.009	.026	-.075	.067	.001	-.035	.011	.048	-.032	-.032	-.091	.569	-.149	-.043
	V17	-.057	.008	.008	-.050	.009	.000	-.013	-.004	.009	.024	-.035	-.047	.036	-.031	.027	-.149	.660	-.117
	V19	-.030	.020	-.024	.036	-.042	.018	-.031	-.106	.004	.029	-.060	-.120	-.013	.026	-.059	-.043	-.117	.421
Anti-image Correlation	V1	.917[a]	-.331	-.011	-.005	-.030	.043	-.003	.018	-.147	.044	-.077	-.156	.110	-.086	-.112	.048	-.093	-.062
	V2	-.331	.938[a]	-.098	-.132	-.156	.041	.053	-.043	.047	-.077	-.010	-.154	-.034	-.005	.014	-.010	.013	.042
	V3	-.011	-.098	.916[a]	-.386	-.118	-.377	.126	.086	-.015	-.059	-.125	-.065	.074	.039	-.009	-.089	.016	-.062
	V4	-.005	-.132	-.386	.933[a]	-.059	-.060	-.019	-.215	.109	-.065	.055	.024	-.056	.024	-.038	-.098	-.095	.085
	V5	-.030	-.156	-.118	-.059	.967[a]	-.127	-.181	-.071	-.213	-.023	-.059	.069	-.031	-.121	-.077	-.020	.020	-.116
	V6	.043	.041	-.377	-.060	-.127	.930[a]	-.313	-.080	.071	-.135	-.106	-.002	-.133	-.063	.040	.060	.001	.047
	V7	-.003	.053	.126	-.019	-.181	-.313	.941[a]	-.099	-.067	.069	.013	.025	.024	.027	-.104	-.139	-.023	-.067
	V8	.018	-.043	.086	-.215	-.071	-.080	-.099	.943[a]	-.254	.020	.037	-.074	.012	-.145	-.005	.138	-.008	-.254
	V9	-.147	.047	-.015	.109	-.213	.071	-.067	-.254	.943[a]	-.215	-.053	-.024	-.005	-.010	-.138	.003	.016	.009
	V10	.044	-.077	-.059	-.065	-.023	-.135	.069	.020	-.215	.944[a]	-.116	-.031	-.244	.013	.064	-.062	.040	.061
	V11	.077	-.010	-.125	.055	-.059	-.106	.013	.037	-.053	-.116	.968[a]	.070	-.100	-.113	-.063	.019	-.057	-.125
	V12	-.156	-.154	-.065	.024	.069	-.002	.025	-.074	-.024	-.031	.070	.930[a]	.021	-.255	.048	.087	-.080	-.252
	V13	.110	-.034	.074	-.056	-.031	-.133	.024	.012	-.005	-.244	-.100	.021	.943[a]	-.275	-.206	-.066	.069	-.031
	V14	-.086	-.005	.039	.024	-.121	-.063	.027	-.145	-.010	.013	-.113	-.255	-.275	.948[a]	-.228	-.075	-.066	.070
	V15	-.112	.014	-.009	-.038	-.077	.040	-.104	-.005	-.138	.064	-.063	.048	-.206	-.228	.955[a]	-.199	.055	-.150
	V16	.048	-.010	-.089	-.098	-.020	.060	-.139	.138	.003	-.062	.019	.087	-.066	-.075	-.199	.937[a]	-.242	-.088
	V17	-.093	.013	.016	-.095	.020	.001	-.023	-.008	.016	.040	-.057	-.080	.069	-.066	.055	-.242	.931[a]	-.222
	V19	-.062	.042	-.062	.085	-.116	.047	-.067	-.254	.009	.061	-.125	-.252	-.031	.070	-.150	-.088	-.222	.937[a]

a. Measures of Sampling Adequacy(MSA)

APPENDIX 12. MSA and Partial Correlations for Quality

Note: Measures of sampling adequacy are on the diagonal, partial correlations are off-diagonal in Anti-image Correlation section

Anti-image Matrices

		V20	V21	V22	V23	V24	V25	V26	V27	V28	V29	V30	V31	V32	V33	V34	V35
Anti-image Covariance	V20	.368	-.148	-.032	-.024	-.037	-.035	-.005	.008	-.025	.039	-.012	-.009	-.030	-.001	-.017	-.011
	V21	-.148	.351	-.168	-.006	.014	.016	-.017	.017	.007	-.013	-.013	.020	.014	-.021	.006	-.011
	V22	-.032	-.168	.340	-.059	-.007	-.028	.011	-.022	-.021	.005	.026	-.040	-.020	.004	-.036	.042
	V23	-.024	-.006	-.059	.424	-.074	-.029	-.032	.003	-.013	-.012	.016	-.018	-.027	-.008	-.025	-.023
	V24	-.037	.014	-.007	-.074	.543	-.065	-.029	-.053	.093	-.012	-.005	-.023	.032	-.030	-.025	.013
	V25	-.035	.016	-.028	-.029	-.065	.305	-.081	-.032	-.019	-.021	.024	-.060	.048	-.002	.011	-.021
	V26	-.005	-.017	.011	-.032	-.029	-.081	.248	-.079	-.018	-.003	-.046	.026	-.023	-.005	.021	-.038
	V27	.008	.017	-.022	.003	-.053	-.032	-.079	.250	-.073	-.056	-.032	.009	-.014	.007	.010	-.025
	V28	-.025	.007	-.021	-.013	-.012	-.021	-.003	-.056	.360	-.008	-.018	-.031	.007	-.027	-.007	-.044
	V29	.039	-.013	.005	-.012	-.012	-.021	-.046	-.032	-.018	.366	-.066	-.006	-.019	-.052	.003	-.027
	V30	-.012	-.013	.026	.016	-.005	.024	-.046	-.032	-.018	-.066	.260	-.098	-.036	.012	-.048	.024
	V31	-.009	.020	-.040	-.018	-.023	-.060	.026	.009	-.031	-.006	-.098	.230	-.051	-.026	-.012	-.018
	V32	-.030	.014	-.020	-.027	.032	.048	-.023	-.014	.007	-.019	-.036	-.051	.358	-.081	.009	-.038
	V33	-.001	-.021	.004	-.008	-.030	-.002	-.005	.007	-.027	-.052	.012	-.026	-.081	.274	-.085	-.034
	V34	-.017	.006	-.036	-.025	-.025	.011	.021	.010	-.007	.003	-.048	-.012	.009	-.085	.309	-.092
	V35	-.011	-.011	.042	-.023	.013	-.021	-.038	-.025	-.044	-.027	.024	-.018	-.038	-.034	-.092	.263
Anti-image Correlation	V20	.955[a]	-.413	-.089	-.061	-.083	-.105	-.017	.027	-.068	.107	-.039	-.033	-.082	-.002	-.051	-.036
	V21	-.413	.902[a]	-.488	-.015	.033	.048	-.059	.058	.021	-.037	-.043	.071	.039	-.068	.017	-.035
	V22	-.089	-.488	.931[a]	-.157	-.017	-.086	.038	-.076	-.059	.013	.088	-.142	-.058	.014	-.111	.141
	V23	-.061	-.015	-.157	.983[a]	-.154	-.080	-.098	.010	-.032	-.031	.048	-.057	-.069	-.022	-.070	-.068
	V24	-.083	.033	-.017	-.154	.961[a]	-.160	-.079	-.143	.211	-.026	-.013	-.065	.073	-.079	-.061	.036
	V25	-.105	.048	-.086	-.080	-.160	.960[a]	-.295	-.116	-.059	-.063	.086	-.227	.146	-.006	.036	-.075
	V26	-.017	-.059	.038	-.098	-.079	-.295	.957[a]	-.315	-.059	-.010	-.183	.111	-.079	-.017	.074	-.150
	V27	.027	.058	-.076	.010	-.143	-.116	-.315	.960[a]	-.242	-.184	-.126	.037	-.046	.028	.036	-.098
	V28	-.068	.021	-.059	-.032	.211	-.059	-.059	-.242	.972[a]	-.021	-.058	-.109	.020	-.086	-.021	-.141
	V29	.107	-.037	.013	-.031	-.026	-.063	-.010	-.184	-.021	.976[a]	-.214	-.022	-.051	-.165	.009	-.087
	V30	-.039	-.043	.088	.048	-.013	.086	-.183	-.126	-.058	-.214	.949[a]	-.401	-.119	.044	-.169	.092
	V31	-.033	.071	-.142	-.057	-.065	-.227	.111	.037	-.109	-.022	-.401	.954[a]	-.177	-.104	-.045	-.075
	V32	-.082	.039	-.058	-.069	.073	.146	-.079	-.046	.020	-.051	-.119	-.177	.968[a]	-.259	.028	-.123
	V33	-.002	-.068	.014	-.022	-.079	-.006	-.017	.028	-.086	-.165	.044	-.104	-.259	.965[a]	-.291	-.125
	V34	-.051	.017	-.111	-.070	-.061	.036	.074	.036	-.021	.009	-.169	-.045	.028	-.291	.959[a]	-.323
	V35	-.036	-.035	.141	-.068	.036	-.075	-.150	-.098	-.141	-.087	.092	-.075	-.123	-.125	-.323	.964[a]

a. Measures of Sampling Adequacy(MSA)

APPENDIX 13. MSA and Partial Correlations for Information Security

Note: Measures of sampling adequacy are on the diagonal, partial correlations are off-diagonal in Anti-image Correlation section

Anti-image Matrices

		V36	V37	V38	V39	V40	V41	V42	V43	V44	V45	V46
Anti-image Covariance	V36	.385	-.142	-.054	.022	-.019	.011	-.019	-.004	-.020	-.002	-.027
	V37	-.142	.277	-.065	-.056	-.017	-.049	-.009	-.017	.010	-.017	.008
	V38	-.054	-.065	.349	.008	-.048	-.029	-.046	-.011	-.019	.008	-.029
	V39	.022	-.056	.008	.392	-.061	-.041	-.021	-.019	-.012	-.027	-.056
	V40	-.019	-.017	-.048	-.061	.296	-.068	-.054	.049	-.029	-.013	-.058
	V41	.011	-.049	-.029	-.041	-.068	.278	-.045	-.079	-.016	-.008	.017
	V42	-.019	-.009	-.046	-.021	-.054	-.045	.322	-.053	-.048	.006	-.007
	V43	-.004	-.017	-.011	-.019	.049	-.079	-.053	.309	-.071	-.026	-.057
	V44	-.020	.010	-.019	-.012	-.029	-.016	-.048	-.071	.268	-.101	-.023
	V45	-.002	-.017	.008	-.027	-.013	-.008	.006	-.026	-.101	.338	-.094
	V46	-.027	.008	-.029	-.056	-.058	.017	-.007	-.057	-.023	-.094	.325
Anti-image Correlation	V36	.943[a]	-.435	-.147	.057	-.057	.033	-.054	-.011	-.062	-.006	-.076
	V37	-.435	.938[a]	-.210	-.171	-.058	-.177	-.031	-.057	.036	-.056	.026
	V38	-.147	-.210	.971[a]	.023	-.149	-.093	-.138	-.034	-.064	.022	-.087
	V39	.057	-.171	.023	.972[a]	-.178	-.124	-.060	-.053	-.037	-.075	-.156
	V40	-.057	-.058	-.149	-.178	.955[a]	-.235	-.174	.163	-.104	-.042	-.187
	V41	.033	-.177	-.093	-.124	-.235	.958[a]	-.149	-.269	-.058	-.026	.057
	V42	-.054	-.031	-.138	-.060	-.174	-.149	.972[a]	-.167	-.162	.019	-.022
	V43	-.011	-.057	-.034	-.053	.163	-.269	-.167	.951[a]	-.248	-.080	-.180
	V44	-.062	.036	-.064	-.037	-.104	-.058	-.162	-.248	.954[a]	-.337	-.077
	V45	-.006	-.056	.022	-.075	-.042	-.026	.019	-.080	-.337	.953[a]	-.283
	V46	-.076	.026	-.087	-.156	-.187	.057	-.022	-.180	-.077	-.283	.958[a]

a. Measures of Sampling Adequacy(MSA)

APPENDIX 14. MSA and Partial Correlations for Healthcare Excellence

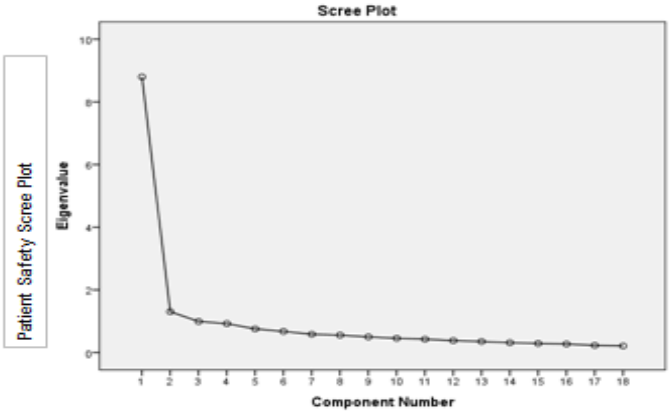
Note: Measures of sampling adequacy are on the diagonal, partial correlations are off-diagonal in Anti-image Correlation section

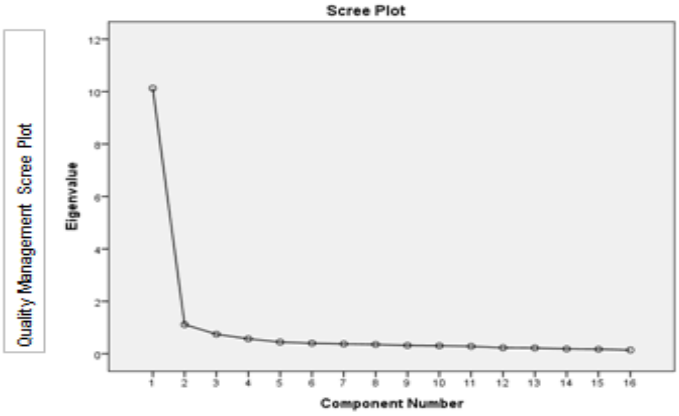
Anti-image Matrices

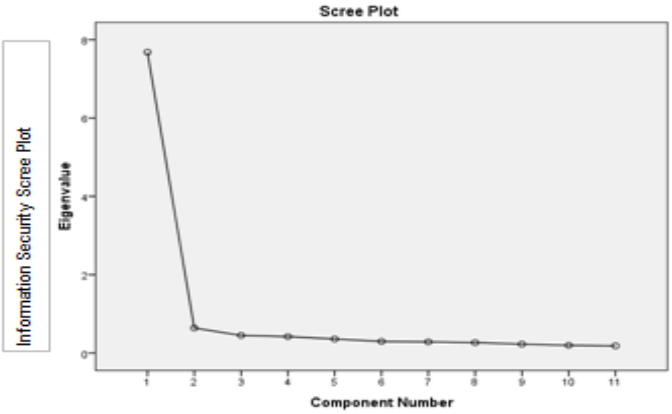
		V47	V48	V49	V50
Anti-image Covariance	V47	.281	-.093	-.047	-.108
	V48	-.093	.252	-.114	-.057
	V49	-.047	-.114	.281	-.083
	V50	-.108	-.057	-.083	.289
Anti-image Correlation	V47	.862[a]	-.349	-.169	-.380
	V48	-.349	.843[a]	-.430	-.213
	V49	-.169	-.430	.860[a]	-.292
	V50	-.380	-.213	-.292	.869[a]

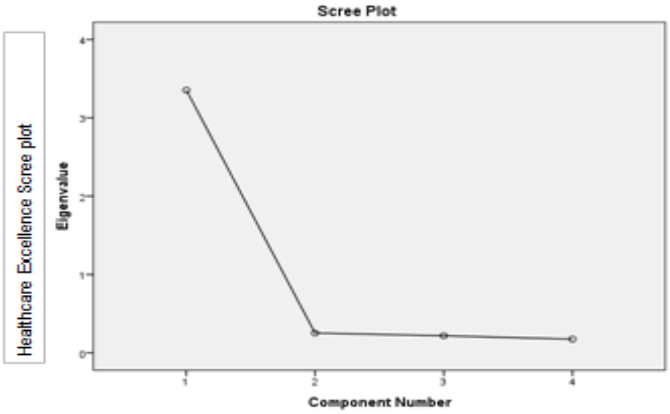
a. Measures of Sampling Adequacy(MSA)

APPENDIX 15. Scree Plots

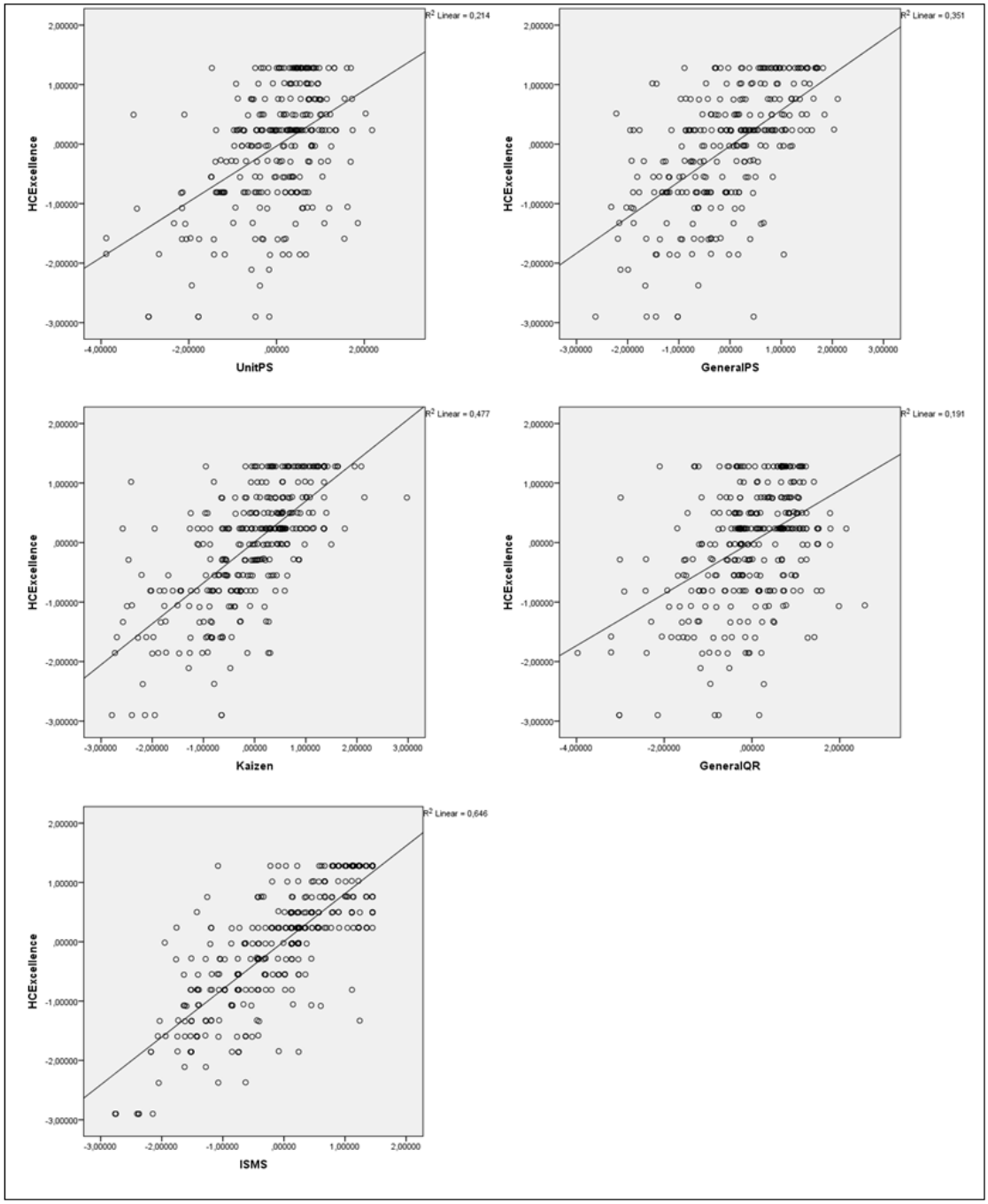




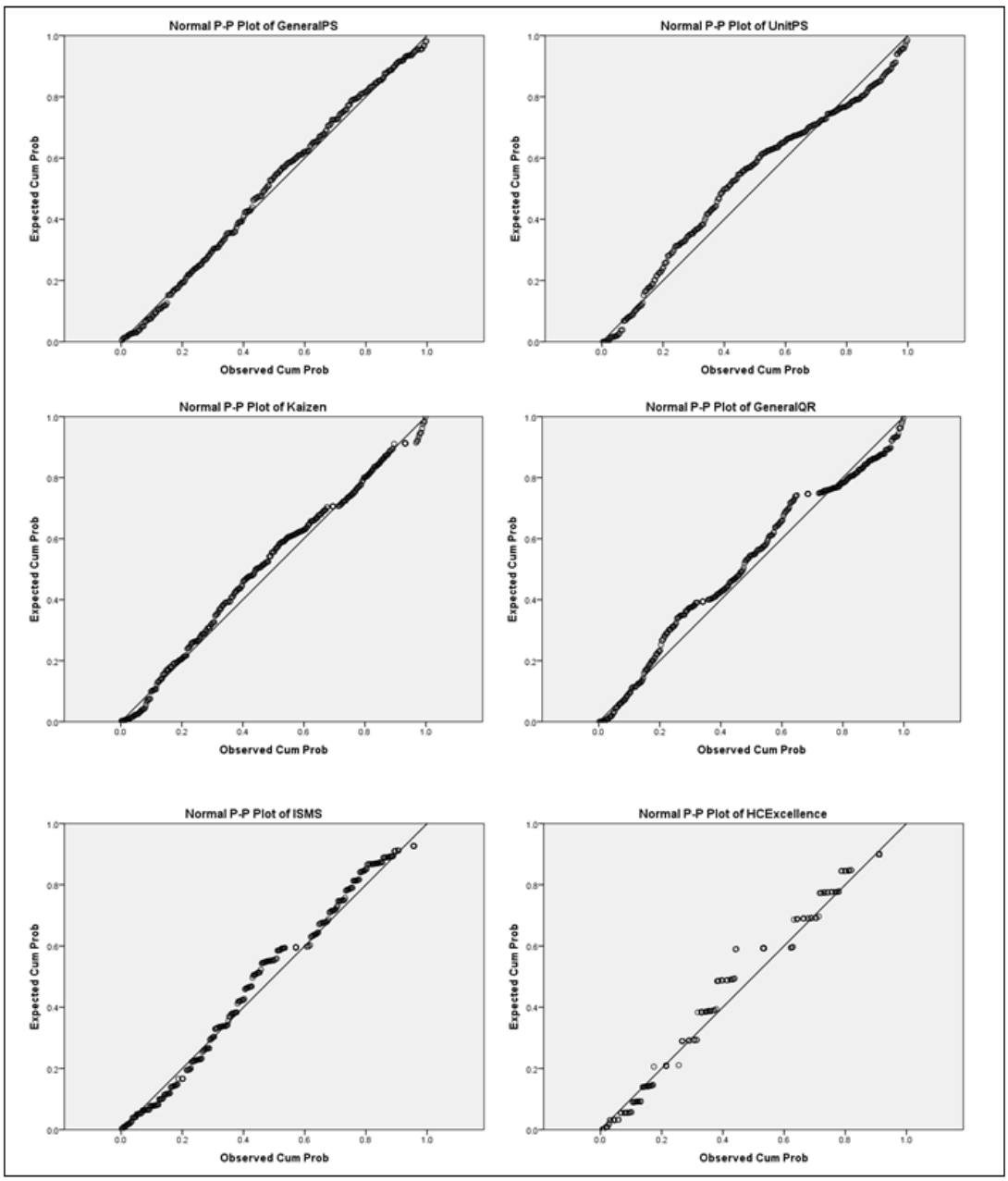




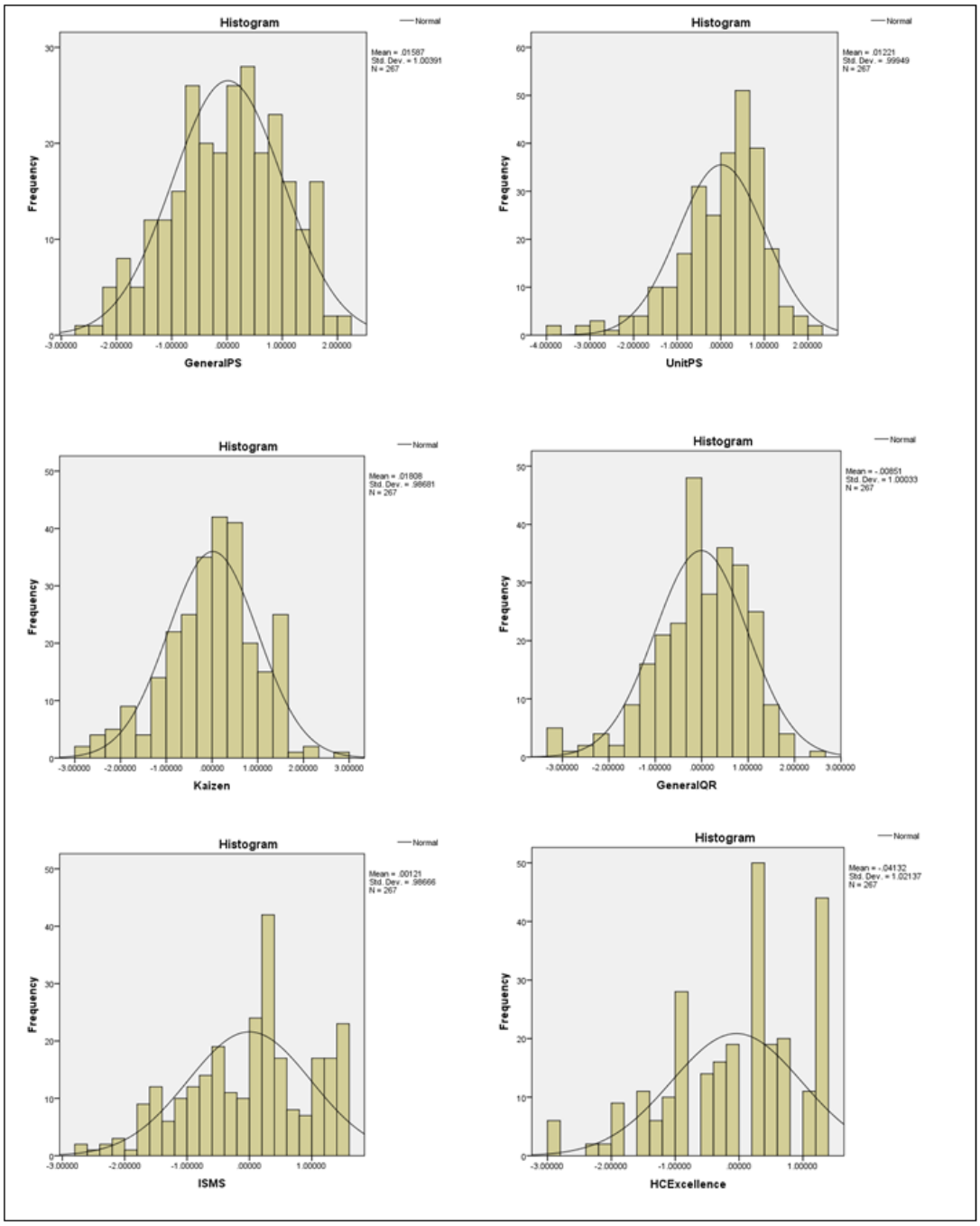
APPENDIX 16. Scatter/Dot Chart for Healthcare Excellence Dependent Variable and Other Independent Variables;



APPENDIX 17. P-P Plots for Healthcare Excellence Dependent Variable and Other Independent Variables;



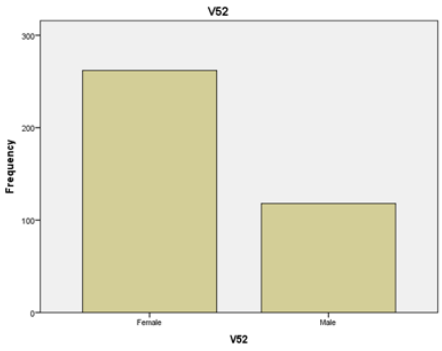
APPENDIX 18. Normal Distribution Graph - Histogram for Healthcare Excellence Dependent Variable and Other Independent Variables;



APPENDIX 19. V52/Gender -- V54/Job Position -- V51 –> Recoded into Age

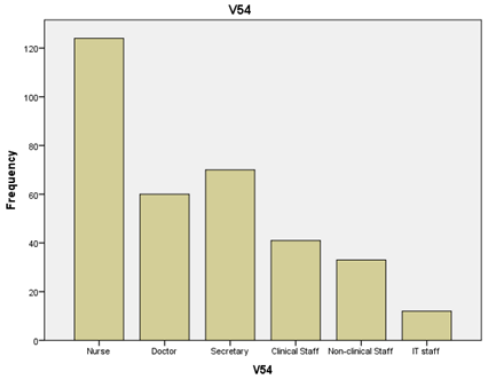
V52 = Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	262	67,4	68,9	68,9
	Male	118	30,3	31,1	100,0
	Total	380	97,7	100,0	
Missing	System	9	2,3		
Total		389	100,0		



V54 = Job Position

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nurse	124	31,9	36,5	36,5
	Doctor	60	15,4	17,6	54,1
	Secretary	70	18,0	20,6	74,7
	Clinical Staff	41	10,5	12,1	86,8
	Non-clinical Staff	33	8,5	9,7	96,5
	IT staff	12	3,1	3,5	100,0
	Total	340	87,4	100,0	
Missing	System	49	12,6		
Total		389	100,0		

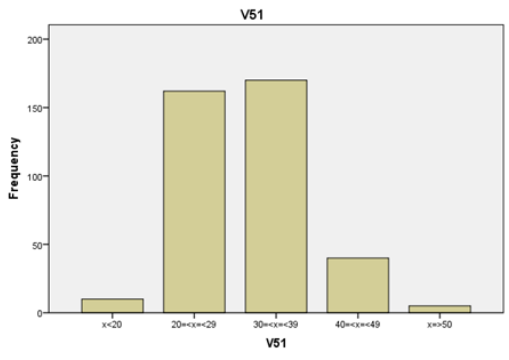


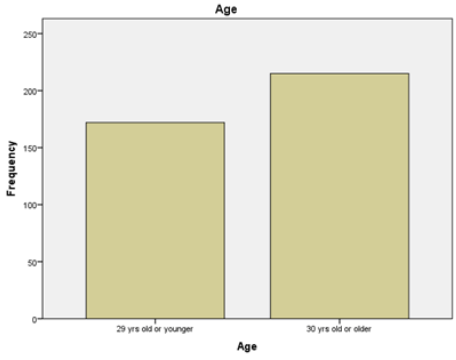
V51 = Original Variable for Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	x<20	10	2,6	2,6	2,6
	20=<x=<29	162	41,6	41,9	44,4
	30=<x=<39	170	43,7	43,9	88,4
	40=<x=<49	40	10,3	10,3	98,7
	x=>50	5	1,3	1,3	100,0
	Total	387	99,5	100,0	
Missing	System	2	,5		
Total		389	100,0		

Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	29 yrs old or younger	172	44,2	44,4	44,4
	30 yrs old or older	215	55,3	55,6	100,0
	Total	387	99,5	100,0	
Missing	System	2	,5		
Total		389	100,0		





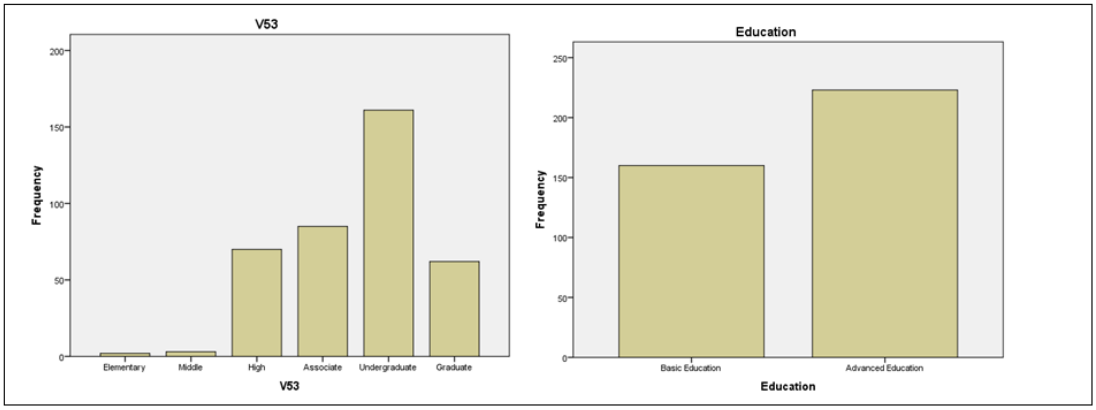
APPENDIX 20. V53, Recoded into Education -- V55, Recoded into Years Worked

V53 = Original Variable for Education Level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Elementary	2	,5	,5	,5
	Middle	3	,8	,8	1,3
	High	70	18,0	18,3	19,6
	Associate	85	21,9	22,2	41,8
	Undergraduate	161	41,4	42,0	83,8
	Graduate	62	15,9	16,2	100,0
	Total	383	98,5	100,0	
Missing	System	6	1,5		
Total		389	100,0		

Education

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Basic Education	160	41,1	41,8	41,8
	Advanced Education	223	57,3	58,2	100,0
	Total	383	98,5	100,0	
Missing	System	6	1,5		
Total		389	100,0		

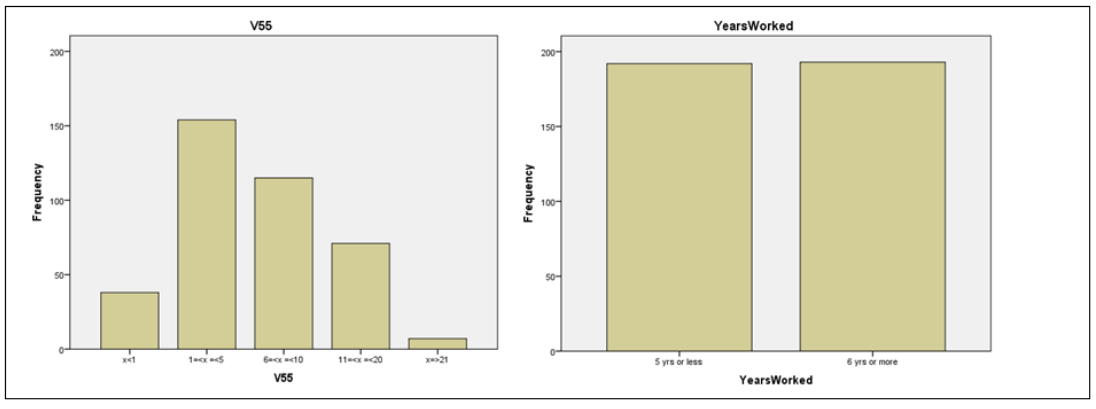


V55 = Original variable for years at Work

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	x<1	38	9,8	9,9	9,9
	1=<x=<5	154	39,6	40,0	49,9
	6=<x=<10	115	29,6	29,9	79,7
	11=<x=<20	71	18,3	18,4	98,2
	x=>21	7	1,8	1,8	100,0
	Total	385	99,0	100,0	
Missing	System	4	1,0		
Total		389	100,0		

YearsWorked

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	5 yrs or less	192	49,4	49,9	49,9
	6 yrs or more	193	49,6	50,1	100,0
	Total	385	99,0	100,0	
Missing	System	4	1,0		
Total		389	100,0		



APPENDIX 21. Pearson Correlations for Regression Variables

Correlations

		HCExcellence	GeneralPS	UnitPS	Kaizen	GeneralQR	ISMS
Pearson Correlation	HCExcellence	1.000	.602	.468	.720	.436	.818
	GeneralPS	.602	1.000	-.002	.574	.182	.564
	UnitPS	.468	-.002	1.000	.288	.521	.442
	Kaizen	.720	.574	.288	1.000	-.010	.698
	GeneralQR	.436	.182	.521	-.010	1.000	.492
	ISMS	.818	.564	.442	.698	.492	1.000
Sig. (1-tailed)	HCExcellence	.	.000	.000	.000	.000	.000
	GeneralPS	.000	.	.489	.000	.001	.000
	UnitPS	.000	.489	.	.000	.000	.000
	Kaizen	.000	.000	.000	.	.437	.000
	GeneralQR	.000	.001	.000	.437	.	.000
	ISMS	.000	.000	.000	.000	.000	.
N	HCExcellence	267	267	267	267	267	267
	GeneralPS	267	267	267	267	267	267
	UnitPS	267	267	267	267	267	267
	Kaizen	267	267	267	267	267	267
	GeneralQR	267	267	267	267	267	267
	ISMS	267	267	267	267	267	267