



Checking Assumptions and Requirements for the Implementation of Information Security Management System in Hospitals in Tabriz

Nahid Beirami^{1}, Naser Modiri² and Abbas Toloie Eshlaghi³*

1. Department of Management, Electronic Branch, Islamic Azad University, Tehran, Iran
beinhd@gmail.com

2. Islamic Azad University, Zanjan Branch, Department of Computer Science, Zanjan, Iran
NaserModiri@yahoo.com

3. Science and Research Branch, Islamic Azad University, Tehran, Iran
toloie@gmail.com

Original Article:

Received 19 Jan. 2015 Accepted 6 Feb. 2016 Published 26 Feb. 2016

ABSTRACT

The purpose of this study was to investigate and analyze the assumptions and requirements for the implementation of Information Security Management System (ISMS). To check assumptions security for security management system implementation, we studied the population of patients hospitals in Tabriz. Because information security is considered in most hospitals and only 8 hospitals in Tabriz cooperate, as the population of the study. Review the requirements and assumptions are based on the standard ISO / IEC 27001, ISO / IEC 27002 test target setting and ISO 27001 standard questionnaire containing 33 questions in 11 control sample. To analyze the data, descriptive and inferential statistical methods were used for implementation of information security management system. to identify factors affecting the implementation of information security management system and factor analysis, structural equation model of PLS smart software was used and according to its findings indirectly relates to impact the four dimensions of implementation effectiveness of the system were achieved. The study findings were presented.

Keyword:

Information Security Management System, ISO / IEC 27001, ISO / IEC 27002

* Corresponding author: Nahid Beirami

INTRODUCTION

from the era of mass production to the age of information and improved communication and evolutionary human life moved towards the information society and knowledge-based world, all the processes and activities economic, cultural, industrial, political and social relations in today's world not only is considered as one of the main sources of assets, but also ruled as a tool for effective management of other resources and assets of the funds, manpower was to prove so important and special value, implementation and management of factors in the country is from the vital importance factors .technology and flexibility in his everyday productivity and business prospects of correction of your heart is also in this way. Since the foundation of any type of security system, and with its presence in the system regardless to their purpose could be relevant to managers and officials who assured about all types of threats, injuries, risks and incidents to be followed based on maintaining security in the majority of other aspects of security organizations. It is therefore imperative under each condition security available and protected, because security agencies strongly supposed to have good management and systematic risk-taking . The security situation is not without risk. It was said that security can be a graduate unknown situation, uncertainty and unreliability. This type of system is the non-homogeneous distribution of shrinkage and connection. Obviously a system that is connected to other systems, is at risk in terms of security. So a more precise definition of security can be provided that the sum of all the techniques, method, procedures and activities used to maintain the system in an ideal situation among a set of rules in a heterogeneous computing systems, decentralized and interconnected systems. The purpose of rules is to determine what is legal and what is illegal.

Problem Statement:

The main source of information should be the implementation of Information Security Management and in fact, this is the shortest definition of data processing. The raw materials that are potentially significant data in order to identify and understand analyses , goods, events existence which can be found of reality or in the imagination world, through research methods, cognitive tools for language, emotions, , mind and brain and experiencing. In one hand, each system is inevitable in this type of information and tools and science and will cause business synergies; on the other hand, there are basic requirements to build information security management.

Healthcare organizations are manufacturers of health data in the context of information systems. Tasks system information preserve nature of the data in a secure environment in order to provide appropriate and high quality services for the patients. due to the importance of health data and the need of making them secure, many national and international organizations tried to develop standards such as: ISO27000, NAIC, AAMC CPRI, ASTM and HIPPA. (Moqadasi et al., 2013).

Note that an information security management system preserves information resources persistency to protection the confidentiality, integrity and availability of information organization. These three concepts associated security

information tariff patient we have the following: (karami, et al. , 2013).

- Privacy: a process ensuring that information is accessible only for authorized persons. Confidentiality is achieved through encryption of access control techniques.

Correctness and accuracy: they ensure that information is accurate and allow you to access data only when receiving exactly the same right code when you write. These features influence the patient's safety.

- Availability of information: the possibility of using on-demand information and availability of an organization or individual which is allowed. This feature is important in healthcare. The overall goal of this study is analysis requirements of the implementation of Information Security Management System for hospitals in Tabriz. to this end, assumptions and requirements for information security system based on the COBIT model which includes the criteria of organizing plans, acquisition and implementation, delivery and support, monitoring and assessment according to the standard ISO 27001 and ISO 27002 which are controlled in 11 studied areas including:

- 1-Existential security policy
- 2-Organizational information security
3. Asset Management
4. Human resources security
5. Physical and environmental security
6. Operations management and Communication
- 7- Controlling access to information.
- 8 -The development and maintenance of systems
- 9-Managing incidents related to information security
- 10-Business continuity management
- 11- Accordance with the rules

The Importance and Necessity of Research:

As one of the most valuable information assets of the organization's most sensitive task is to deliver timely and appropriate information needed, it is always a central role. Deletion and maintenance of information is a prerequisite for business continuity economic to be unauthorized. Accessing information on the disc, they turned to the problem of unauthorized use of computers and the access by employees of an organization's internet users, or by other factors organizations and companies looking to implement security. It can be only paying attention to issues, and not enough technical control also created in the proper procedures, the percentage of information security management system information security topics related to information security mandates concurrently, after the recent findings of issues, nowadays is the focus of all organizations and institutions around the world. Despite using a variety of information security management system standards, unfortunately in Iran so far no efforts has been performed to implement information security management system. There are institutions and organizations that to the current situation. Considering the conditions of regional and international political and economic aspects of comprehensive information achieved the need for extensive researching to obtain global information. It has been slowed because these opportunities using or paid to the security of information systems major obstacle facing the entrance to the community knowledge base will expand information and

communication technology using. Fortunately, this is definitely it was severely emerging. (Kazemi, 2014)

Hospitals are particularly important due to the specific types of clients, and sharing and transferring too much information. These special groups have specific types of database. Hospitals in Tabriz of the issues and problems raised HIS program and there is no exception; it is essential to investment in security information management and comprehensive planning. In this study, the analysis and assumptions and information security management system requirements and standards are examined in several hospitals in Tabriz.

The Main Objectives:

The purpose of this study was to investigate and analyze the assumptions requirements of Hospitals in Tabriz for Information Security Management System implementation. To this end, the requirements of information security management system based on the COBIT model, which includes the criteria of organizing plans , providing implementation, support and supervision which are analyzed in the survey.

Detailed Objectives

1. Determining the status of hospitals in Tabriz in terms of security policy
2. Determining the status of hospitals in Tabriz in terms of organizing three information securities
3. Determining the status of hospitals in Tabriz in terms of the status of hospitals in Tabriz in terms of asset management,
4. Determining the status of hospitals in Tabriz in terms of human resources security,
5. Determining the status of hospitals in Tabriz in terms of physical security
6. Determining the status of hospitals in Tabriz in terms of Management Operations
7. Determining the status of hospitals in Tabriz in terms of control access
8. Determining the status of hospitals in Tabriz in terms of maintenance and development of information systems
9. Determining the status of hospitals in Tabriz in terms of event management of information security
10. Determining the status of hospitals in Tabriz in terms of business continuity,
11. Determining the status of hospitals in Tabriz in terms of legal match.

Framework of the Study:

The need for a framework of reference prepared for the development and management of internal control and appropriate levels of IT security is in the last priority. Most large IT organizations and institutions set it as one of their most valuable assets. Successful organizations realize that the real value of these assets is the interests of its stakeholders can use it. To ensure the accessibility of information technology, risk management and control information associated with it, they are now considered as key factors in corporate governance. This value, risk and control constitute the core of IT governance. For breakthrough management and control and management of IT monitoring and evaluation of the performance of the organization, COBIT is used as the reference framework. Activities: basis for directing the activities of the IT Based on COBIT are:

-App organizing plan

-Implementation

- Supporting-Monitoring and Evaluation

The importance and necessity of research:

As one of the most valuable information assets of the organizations most sensitive task is accessing and delivering

timely and appropriate information needed which is always a central role of the organizational status. Keeping and maintenance of information is a prerequisite for business continuity institution in economic trade processing and information from unauthorized disk accessing, unauthorized use of computers has become a problem and the accessing by employees of an organization's internet users, or by other factors in the organizations and companies need implementation of security factors. For being secure, implementation of it is only due to technical issues control and standardization are not enough, we also need to create the proper procedures. The percentage of using information security management systems information security topics are related to information security mandates concurrently, after finding the issues that, these days, regional and international political and economic conditions facet of the need for extensive research has been very high comprehensive information on the opportunities using slowed security of information systems which majorly hurdles the development of information and communication technology. Using it was the entrance to the community knowledge base of fortunately and definitely and severely emerging matter. (Kazemi, 2014)

Hospitals due to specific types of clients, sharing and transferring information are particularly important. These special groups have specific types of database. In this study, the analysis and assumptions and information security management system requirements and standards examined in several hospitals Tabriz.

Analytical model

Methodology

Methodology

In order to examine the study method, the total activities that can be done to reach the target and research are activities that researchers use them to discover rules and reality. Research methods are the means for achieving the reality. In each study, the researcher tries to select the most appropriate method and the method that is more accurate than the other methods and rules and facts of exploring the relationships between variables. The objectives, nature and case studies, theoretical framework and conceptual model, using appropriate research methods are essential. It describes, in this chapter for experimental testing, process research methods, variables, population and sample, data collection tools, reliability and validity of the tools and methods used in the paper and then we will discuss data analysis.

The present study is a cross-sectional descriptive study (survey type). It is a data collecting, research type survey. Considering the results of the research can be used in several hospitals in Tabriz subjected to testing theoretical concepts will be discussed objectively and it can also be applied.

Independent Variable:

In this study, the implementation of information security management system is considered as the independent variable. Because the model has dimensions, the original model will be considered later.

Dependent Variable:

Research study, prerequisites and requirements for the implementation of Information Security Management System consist of:

1. Despite security policy, 2. security organization 3. asset management, 4. human resources security, 5. physical and environmental security 6. managing operations for information and communication 7. control access 8- maintenance and development of information systems 9. Continuity Business Management 10- event management of information security 11. match rules as dependent variables and because the model has dimensions research should be considered.

Data were collected

Every phenomenon that makes us aware of these features depends on the nature and how to achieve it. The aim of such descriptive or explanatory researches is to access to information about the changes. The main ways to collect data include the following: the use of information and evidence, observation, interviews and questionnaires. (Arabi et al., 2011)

Data Collection:

Every phenomenon that makes us aware of these features depends on the nature and how to achieve it. The aim of such descriptive or explanatory researches is to access to information about the changes. The main ways to collect data include the following: the use of information and evidence, observation, interviews and questionnaires. (Arabi et al., 2011)

Questionnaire:

The purpose of the questionnaire is to give us information about the specified studied group or community. One of the important reasons for the use of a questionnaire is to provide the possibility of studying large samples. Qualitative and applicable questionnaire help us obtain correct information which is very important (Arabi et al., 2011).

The purpose of the questionnaire is to give us information about the specified studied group or community. One of the important reasons for the use of a questionnaire is to provide the possibility of studying large samples. Qualitative and applicable questionnaire help us obtain correct information which is very important (Arabi et al., 2011).

In this study, we have started to collect both primary and secondary data secondary data through library studies, reference books and journals, organization and using documents obtained from the Internet. Preliminary data was obtained through field studies and questionnaires.

Questionnaire consisted of a cover letter to explain the purpose of the study and invited people to participate in the specialized research in addition to the two general questions as follows: first, the general questions turns back to the demographic characteristics of respondents such as education, age, positions and years of service. The second specific questions is to examine the requirements have been set. In specific questions we examine prerequisites and requirements for the implementation of Information Security Management System standard including 33 items. As mentioned in the questionnaire, respondents' views (managers and professionals) about information security policy has 3 items 1-3 questionnaire), organization of information security has 3 items (questions 4-6), asset management has 3 items (questions 7-9), human resources security has 3 items (questions 10-12), physical security and environment 3 items (questions 13-15), communication management and operation of 3 items (questions 16-18), access control has 3 items (questions 19-21), use, develop and maintain systems with 3 items (questions 22-24), management of information security incidents has 3 items (questions 25-27), business continuity management 3 items (questions 28-30) and roles match 3 items (questions 31-33) Likert spectrum (from very low to very high) measures.

Validity:

The concept of validity or accreditation answer to the question that measures the extent of attribute. No knowledge of data validity can be measured accurately.

Types of validity include content validity, criterion validity and construct validity. In the narrative structures relevant to the content is a credit to check the ingredients depended on it. If the questions of the questionnaire especially attribute the skills that they have measured the researchers plan to test the validity of the content. To ensure content validity, we must act as the tool so that the question is asked from the constituent instruments of the selected content. The validity was used two forms CVR and CVI in the study.

A: index the content validity ratio (CVR): This index was designed by Lavshh ().each of the questions are asked according to the whole matter and classified in two-part Likert scale, "is it beneficial" and "not beneficial". Then, the content validity ratio is calculated based on the following formula:

$$CVR = \frac{\text{The number of experts who have chosen - benefit option}}{\text{The total number of specialists}}$$

Regarded to the number of experts who have evaluated the questions, minimum acceptable CVR should be based

on the following table. CVR value lesser than the amount calculated for the questions is asked regarding the number of

expert evaluators, should be excluded from the trial because according to content validity, content validity cannot agree.

CV minimum acceptable score based on the number of experts transition					
the amount of CVR	The number of specialists	the amount of CVR	The number of specialists	the amount of CVR	The number of specialists
0.37	25	0.59	11	0.99	5
0.33	30	0.56	12	0.99	6
0.31	35	0.54	13	0.99	7
0.29	40	0.51	14	0.75	8
		0.49	15	0.78	9
		0.42	20	0.62	10

Table 3-2 usefulness of any

$CVR_1 = \frac{9-5}{5} = 0.8$	$CVR_9 = \frac{10-5}{5} = 1$	$CVR_{17} = \frac{9-5}{5} = 0.8$	$CVR_{25} = \frac{9-5}{5} = 0.8$
$CVR_2 = \frac{9-5}{5} = 0.8$	$CVR_{10} = \frac{10-5}{5} = 1$	$CVR_{18} = \frac{9-5}{5} = 0.8$	$CVR_{26} = \frac{9-5}{5} = 0.8$
$CVR_3 = \frac{10-5}{5} = 1$	$CVR_{11} = \frac{9-5}{5} = 0.8$	$CVR_{19} = \frac{10-5}{5} = 1$	$CVR_{27} = \frac{9-5}{5} = 0.8$
$CVR_4 = \frac{9-5}{5} = 0.8$	$CVR_{12} = \frac{9-5}{5} = 0.8$	$CVR_{20} = \frac{10-5}{5} = 1$	$CVR_{28} = \frac{9-5}{5} = 0.8$
$CVR_5 = \frac{9-5}{5} = 0.8$	$CVR_{13} = \frac{9-5}{5} = 0.8$	$CVR_{21} = \frac{10-5}{5} = 1$	$CVR_{29} = \frac{9-5}{5} = 0.8$
$CVR_6 = \frac{9-5}{5} = 0.8$	$CVR_{14} = \frac{9-5}{5} = 0.8$	$CVR_{22} = \frac{9-5}{5} = 0.8$	$CVR_{30} = \frac{9-5}{5} = 0.8$
$CVR_7 = \frac{9-5}{5} = 0.8$	$CVR_{15} = \frac{9-5}{5} = 0.8$	$CVR_{23} = \frac{9-5}{5} = 0.8$	$CVR_{31} = \frac{9-5}{5} = 0.8$
$CVR_8 = \frac{9-5}{5} = 0.8$	$CVR_{16} = \frac{9-5}{5} = 0.8$	$CVR_{24} = \frac{9-5}{5} = 0.8$	$CVR_{32} = \frac{9-5}{5} = 0.8$
$CVR_{33} = \frac{9-5}{5} = 0.8$			

According to the CVR data table and the number of experts selected for this study, 10 people, CVR should be top is 0.62, so were all the questions.

B) Content validity index (CVI): Waltz and Basel evaluated the content validity index. That included specialists "relevance", "clarity" and "simplicity" of each item on a 4-point Likert scale. Experts answered each item

from 1 "not relevant", 2 "somewhat concerned", 3 "relevant" to 4 "very concerned" classifications. Simple items respectively from 1 "not easy", 2 "relatively easy", 3 "easy" to 4 "very easy" and clear the items in the order of 1 "not clear", 2 "relatively clear", 3 "obvious" to 4 "very clear" to be determined.

The number of specialists who have items 3 and 4 score

$$CVI = \frac{\text{The number of specialists who have items 3 and 4 score}}{\text{The number of specialists}}$$

The minimum acceptable value for the index equal to 79/0 CVI and CVI If the item is less than 79/0 that the items must be removed.

Table 3 -3 relevance of each item

$CVI_1 = \frac{10}{10}$	$CVI_8 = \frac{9}{10}$	$CVI_{15} = \frac{8}{10}$	$CVI_{22} = \frac{9}{10}$	$CVI_{29} = \frac{9}{10}$
$CVI_2 = \frac{9}{10}$	$CVI_9 = \frac{8}{10}$	$CVI_{16} = \frac{8}{10}$	$CVI_{23} = \frac{9}{10}$	$CVI_{30} = \frac{9}{10}$
$CVI_3 = \frac{9}{10}$	$CVI_{10} = \frac{9}{10}$	$CVI_{17} = \frac{8}{10}$	$CVI_{24} = \frac{10}{10}$	$CVI_{31} = \frac{10}{10}$
$CVI_4 = \frac{8}{10}$	$CVI_{11} = \frac{8}{10}$	$CVI_{18} = \frac{9}{10}$	$CVI_{25} = \frac{9}{10}$	$CVI_{32} = \frac{9}{10}$
$CVI_5 = \frac{9}{10}$	$CVI_{12} = \frac{9}{10}$	$CVI_{19} = \frac{8}{10}$	$CVI_{26} = \frac{8}{10}$	$CVI_{33} = \frac{8}{10}$
$CVI_6 = \frac{9}{10}$	$CVI_{13} = \frac{10}{10}$	$CVI_{20} = \frac{8}{10}$	$CVI_{27} = \frac{9}{10}$	
$CVI_7 = \frac{9}{10}$	$CVI_{14} = \frac{9}{10}$	$CVI_{21} = \frac{8}{10}$	$CVI_{28} = \frac{8}{10}$	

According to Jdv13-3 all the items on 79/0 CVI indicators have relevance for later.

Table 3-4 simplicity of any

$CVI_1 = \frac{9}{10}$	$CVI_8 = \frac{9}{10}$	$CVI_{15} = \frac{9}{10}$	$CVI_{22} = \frac{9}{10}$	$CVI_{29} = \frac{8}{10}$
$CVI_2 = \frac{9}{10}$	$CVI_9 = \frac{8}{10}$	$CVI_{16} = \frac{9}{10}$	$CVI_{23} = \frac{9}{10}$	$CVI_{30} = \frac{9}{10}$
$CVI_3 = \frac{9}{10}$	$CVI_{10} = \frac{9}{10}$	$CVI_{17} = \frac{8}{10}$	$CVI_{24} = \frac{9}{10}$	$CVI_{31} = \frac{9}{10}$
$CVI_4 = \frac{9}{10}$	$CVI_{11} = \frac{9}{10}$	$CVI_{18} = \frac{9}{10}$	$CVI_{25} = \frac{9}{10}$	$CVI_{32} = \frac{9}{10}$
$CVI_5 = \frac{9}{10}$	$CVI_{12} = \frac{10}{10}$	$CVI_{19} = \frac{9}{10}$	$CVI_{26} = \frac{10}{10}$	$CVI_{33} = \frac{9}{10}$
$CVI_6 = \frac{9}{10}$	$CVI_{13} = \frac{9}{10}$	$CVI_{20} = \frac{8}{10}$	$CVI_{27} = \frac{9}{10}$	
$CVI_7 = \frac{8}{10}$	$CVI_{14} = \frac{9}{10}$	$CVI_{21} = \frac{8}{10}$	$CVI_{28} = \frac{8}{10}$	

Table 3-5 clear of any

$CVI_1 = \frac{8}{10}$	$CVI_8 = \frac{9}{10}$	$CVI_{15} = \frac{9}{10}$	$CVI_{22} = \frac{9}{10}$	$CVI_{29} = \frac{9}{10}$
$CVI_2 = \frac{9}{10}$	$CVI_9 = \frac{8}{10}$	$CVI_{16} = \frac{8}{10}$	$CVI_{23} = \frac{9}{10}$	$CVI_{30} = \frac{9}{10}$
$CVI_3 = \frac{9}{10}$	$CVI_{10} = \frac{9}{10}$	$CVI_{17} = \frac{8}{10}$	$CVI_{24} = \frac{8}{10}$	$CVI_{31} = \frac{10}{10}$
$CVI_4 = \frac{8}{10}$	$CVI_{11} = \frac{8}{10}$	$CVI_{18} = \frac{9}{10}$	$CVI_{25} = \frac{9}{10}$	$CVI_{32} = \frac{9}{10}$
$CVI_5 = \frac{9}{10}$	$CVI_{12} = \frac{9}{10}$	$CVI_{19} = \frac{9}{10}$	$CVI_{26} = \frac{9}{10}$	$CVI_{33} = \frac{9}{10}$
$CVI_6 = \frac{9}{10}$	$CVI_{13} = \frac{10}{10}$	$CVI_{20} = \frac{8}{10}$	$CVI_{27} = \frac{9}{10}$	
$CVI_7 = \frac{8}{10}$	$CVI_{14} = \frac{9}{10}$	$CVI_{21} = \frac{9}{10}$	$CVI_{28} = \frac{8}{10}$	

According to the findings of validity indicators CVI and CVR, it is concluded that this study has content validity. For the validity of structures, we used confirmatory factor analysis. Researchers are preparing a model which relatively assumes little empirical data based on several parameters, describing explanation or justification. This information is a pre-experimental model data structure that can be used in the form of a theory or hypothesis, or a classification in

compliance form and content of objective, empirically determined conditions or knowledge gained from previous studies. Verifications procedures determine that the data is synchronized or is not a given factor structure. Confirmatory factor analysis uses PLS software for the structural prerequisites for the implementation of ISMS.

CV minimum acceptable score based on the number of experts transition					
the amount of CVR	The number of specialists	the amount of CVR	The number of specialists	the amount of CVR	The number of specialists
0.37	25	0.59	11	0.99	5
0.33	30	0.56	12	0.99	6
0.31	35	0.54	13	0.99	7
0.29	40	0.51	14	0.75	8
		0.49	15	0.78	9
		0.42	20	0.62	10

Table 6-3 Outer Loadings Load factor

	develope.c	k.access	legaly	m.business	m.daraei	m.event	m.operation	policy	s.human	s.physical	sazmandehi
bc1_1				0.554160							
bc2_1				0.550386							
bc3_1				0.790180							
ca1_1		0.506628									
ca2_1		0.838499									
ca3_1		0.863216									
dms1_1	0.559943										
dms2_1	0.848968										
dms3_1	0.872949										
il_1			0.814123								
il2_1			0.896947								
il3_1			0.841914								
ma1_1					0.797405						
ma2_1					0.815671						
ma3_1					0.774589						
macl1_1						0.506971					
macl2_1						0.536870					
macl3_1						0.503993					
mec1_1							0.838696				
mec2_1							0.848851				
mec3_1							0.869376				
sa1_1											0.840833
sa2_1											0.882303
sa3_1											0.787405
p1_1								0.828107			
p2_1								0.843002			
p3_1								0.813563			
sh1_1									0.798717		
sh2_1									0.864975		
sh3_1									0.780866		
spk1_1										0.854389	
spk2_1										0.787176	
spk3_1										0.809724	

As the results of outer loading table indicate, all factor loadings are larger than 0.3. So, all items have a positive impact on the implementation of information security management systems and are desirable; therefore, their validity in estimating the factors and requirements in their information security management system implementation. Reliability or credibility is the measurement tool of the technical reliability. This decision deals with the measurement tool concept mentioned that remains up to what extent the same conditions gives the same results. The reliability coefficient is confidence of zero (no relation) to

+1 (a perfect relationship). Reliability coefficient indicates the extent measures stable characteristics or features of the variable subjects and its temporary measurements. For calculating the reliability of the instrument we used to measured it in various ways. (Bazargan et al., 2008) There are two ways of reliability: Cronbach's alpha and composite reliability (reliability structure) the study used them to measure the reliability of composite reliability.

Table 3-7 reliability research

	Composite Reliability		Composite Reliability
develope.c	0.895524	s.human	0.855165
isms	0.950966	s.physical	0.857969
k.access	0.874720	sazmandehi	0.866674
legaly	0.887780	tamin	0.848010
m.business	0.879789	tarahi	0.903945
m.daraei	0.838401	policy	0.867651
m.event	0.856727	poshtibani	0.904305
m.operation	0.887654	nezarat	0.881047

0.7 indicates high levels of internal consistency are reflective measurement models.

0.6 <CR> 0.7 is sufficient for exploratory research
0.9> CR> 0.7 for the stage of maturity.

According to the results table CR: Because the amount is more than 0.7, then the reliability of the questionnaire used in the study, is confirmed. In other words, the model has internal consistency.

Society Sample

Models, Structural Equation Modeling
-Model Measure

Structural –Model

Structural model: a model in which the relationships between latent variables are considered and measured is called internal model.

Measurement model: a model in which the relationships between observable and latent variables are considered and measured.

Structural equation model, i.e. the measurement model: first, the role of confirmatory factor analysis, second, its role in the structural model and discovering hidden relationships between variables and testing criteria for measuring the reflection.

- Reliability Test (Validity Test)

The validity of the tests (Reliability Test): Measures quality test reflection
Measures reliability test reflection: alpha is the, composition

the population of individuals who have at least one common trait. In case that the number of population is restricted to a limited population. society sample of in this study, includes all managers and information security and IT experts and users of hospitals in Tabriz information system, which includes 101 individuals of the reliability and validity of the test

Measuring Validity Reflection:

validity or reliability of the statements or question the same concept used in the questionnaire that measures the plans.

Reflective assessment of validity of the measurement model consists of the following:

- 1) Convergent validity (AVE)
- 2) Divergent validity (cross loading test,)

To test the reliability and validity as well as reflective quality test model, tests should be performed in 3 steps.

If reflective measurement model, and homogeneous model's factor was the absolute time of any observable variables corresponding it, it has a minimum of 0.7. Some have suggested eliminating the reflective visible variables of measurement models that are meaningful in the factor loadings under significance level of 0.4.

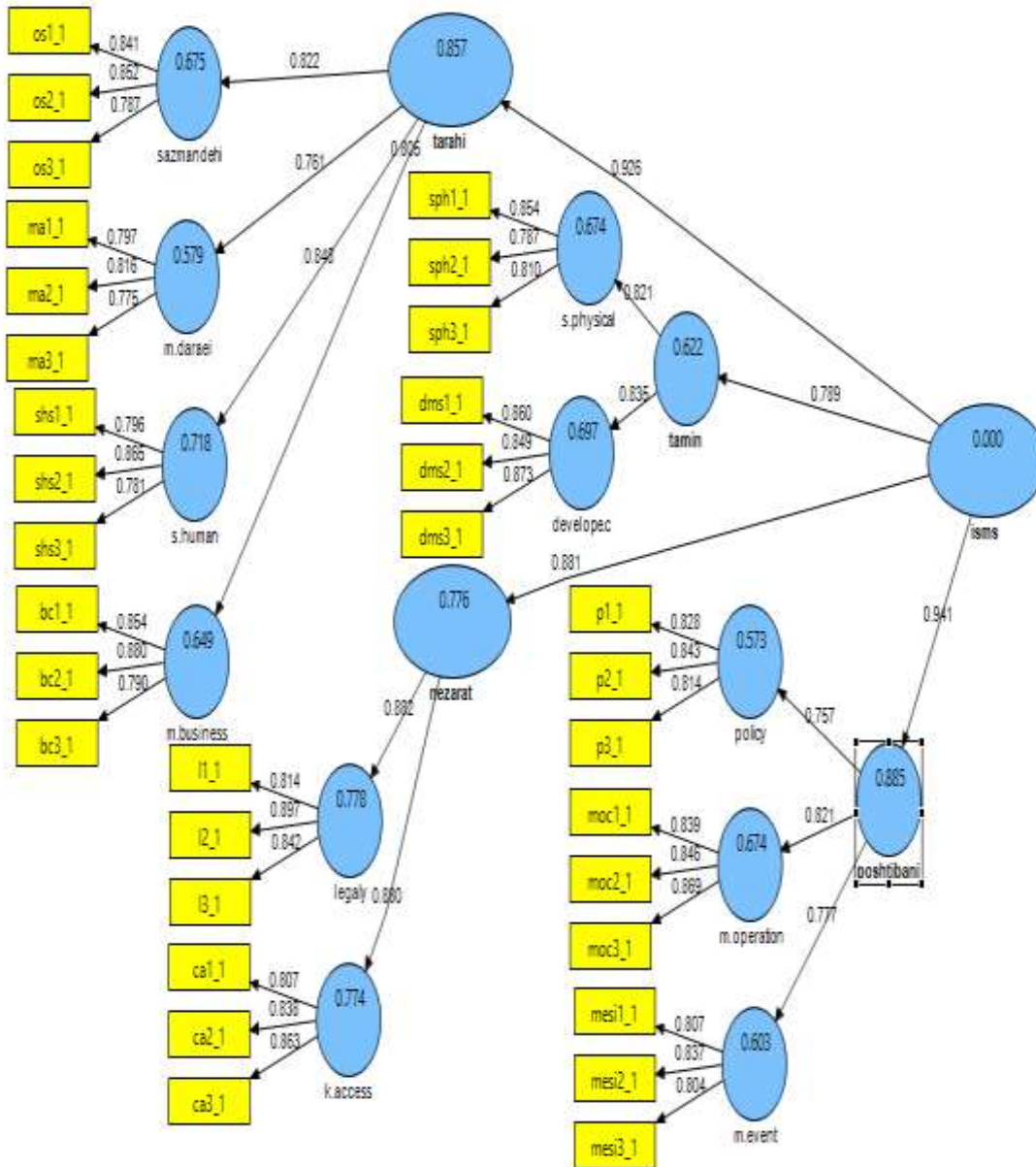


Figure 1, external loads

According to Figure 4-2, the numbers shown between latent variables (circles) and observable variables (rectangles) external loads or external weights according to the model that represents these two variable becomes visible and hidden they called measurement model. Coefficients between latent variables are called regression coefficients or weight path and model that contains only variables are hidden and observable variables which are removed, according to the structural model.

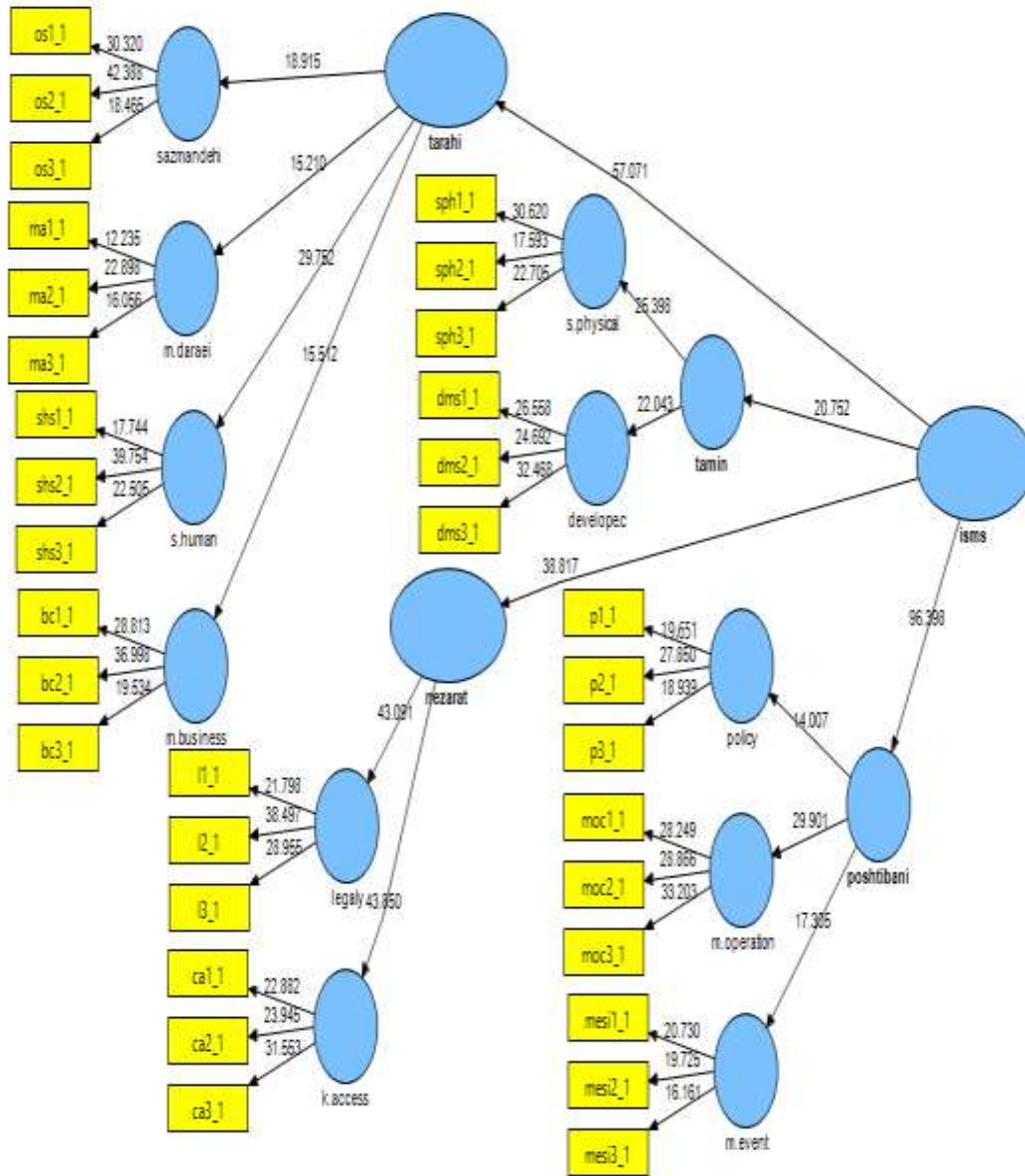


Figure 2 is a significant factor loadings

According to Figure 4-3, the values of T or significant coefficients on the model graphics software on the arrows in the main view will be created. T values should be at 90 percent larger than 64/1, greater than 96/1 95% confidence level and a confidence level of 99% is larger than 56/2.

According to the results of Shk14-3, t values are greater than 56/2 at 99% significance of each factor loadings have been met.

Diagnostic validity or divergent

	develope.c	isns	k.access	legaly	m.business	m.daraei	m.event	m.operation	necarat	policy	poshtibani	s.human	s.physical	sazmandehi	tamin	tarahi
bc1_1	0.384944	0.650637	0.539406	0.492933	0.854148	0.412175	0.500822	0.388810	0.583858	0.267367	0.473963	0.495768	0.386967	0.493808	0.468379	0.702618
bc2_1	0.225487	0.586896	0.477615	0.366815	0.880386	0.359961	0.479054	0.369312	0.479049	0.212331	0.434756	0.502809	0.368375	0.490183	0.357569	0.696313
bc3_1	0.290941	0.572769	0.479882	0.426309	0.790192	0.346021	0.514311	0.411928	0.514221	0.189805	0.459027	0.505442	0.332017	0.391994	0.320652	0.633854
ca1_1	0.478852	0.643121	0.806629	0.449835	0.471300	0.473462	0.446994	0.451167	0.711808	0.366758	0.518107	0.454327	0.380470	0.375779	0.520361	0.546714
ca2_1	0.428733	0.666836	0.838504	0.460475	0.542295	0.429595	0.478836	0.428941	0.736200	0.321253	0.503314	0.488329	0.452474	0.484814	0.531879	0.602548
ca3_1	0.499223	0.709907	0.863210	0.473193	0.473761	0.468595	0.540362	0.468238	0.758104	0.373947	0.565944	0.416641	0.540494	0.559023	0.627795	0.592649
dms1_1	0.859944	0.520838	0.513957	0.397565	0.340368	0.444951	0.330232	0.187129	0.517199	0.321826	0.337832	0.258012	0.342122	0.262045	0.732332	0.398378
dms2_1	0.849956	0.416033	0.423306	0.280100	0.154033	0.186801	0.305917	0.194689	0.399030	0.327899	0.333675	0.229038	0.255776	0.213835	0.671153	0.240067
dms3_1	0.872969	0.541181	0.505611	0.316862	0.329486	0.303469	0.424341	0.333275	0.466504	0.392498	0.466901	0.304016	0.353172	0.268404	0.747206	0.372573
l1_1	0.439532	0.617197	0.477888	0.814101	0.417328	0.397409	0.537731	0.345295	0.734362	0.404474	0.521734	0.378886	0.287970	0.453138	0.441443	0.509908
l2_1	0.348770	0.666522	0.472296	0.896951	0.462782	0.446196	0.557404	0.510546	0.778797	0.371792	0.590013	0.423465	0.400579	0.450105	0.452122	0.550382
l3_1	0.199405	0.615626	0.459073	0.841930	0.418347	0.473202	0.417746	0.453558	0.739437	0.311697	0.486620	0.445492	0.336027	0.553130	0.322262	0.583301
ma1_1	0.311714	0.567181	0.444865	0.392192	0.440812	0.797403	0.315166	0.435879	0.475092	0.315907	0.439882	0.356238	0.387553	0.412775	0.422922	0.606332
ma2_1	0.250572	0.572997	0.432352	0.364914	0.328949	0.815675	0.355044	0.464783	0.452334	0.317103	0.468570	0.500587	0.390788	0.441472	0.385959	0.630944
ma3_1	0.153312	0.579412	0.428095	0.479820	0.287003	0.774587	0.373815	0.442201	0.515453	0.306024	0.462181	0.471099	0.426579	0.376858	0.447257	0.577748
ms1_1	0.361839	0.660596	0.486011	0.579771	0.490573	0.353136	0.804652	0.464054	0.605484	0.399031	0.678565	0.487035	0.395643	0.475742	0.457080	0.561625
ms2_1	0.299923	0.606254	0.471535	0.465062	0.424587	0.423176	0.838063	0.372211	0.531911	0.345200	0.630034	0.417718	0.353550	0.458341	0.394874	0.523731
ms3_1	0.345404	0.619648	0.473868	0.403274	0.525193	0.295507	0.805243	0.416223	0.497813	0.428834	0.667620	0.504753	0.362173	0.441815	0.427148	0.551478
mac1_1	0.163923	0.651229	0.441301	0.473730	0.351188	0.509228	0.410776	0.841158	0.519619	0.399535	0.688813	0.562400	0.539655	0.507865	0.421312	0.594607
mac2_1	0.257290	0.660216	0.436953	0.439357	0.400435	0.401044	0.447689	0.847819	0.497495	0.477166	0.735434	0.550924	0.521376	0.518878	0.467383	0.580145
mac3_1	0.287975	0.704634	0.494127	0.401644	0.425887	0.529294	0.451383	0.865018	0.508371	0.408275	0.719435	0.573145	0.602879	0.587969	0.535175	0.656299
os1_1	0.186463	0.672823	0.472775	0.517337	0.501722	0.420780	0.421287	0.582951	0.562116	0.434740	0.582887	0.548615	0.464711	0.840835	0.390498	0.719701
os2_1	0.418866	0.714513	0.559945	0.489216	0.431029	0.500303	0.572963	0.531644	0.595609	0.401436	0.617352	0.480542	0.494229	0.852290	0.550547	0.702381
os3_1	0.097054	0.547886	0.365405	0.397970	0.420617	0.353320	0.396328	0.457209	0.433485	0.343181	0.491574	0.403587	0.380187	0.787421	0.285277	0.611332
p1_1	0.385568	0.527627	0.348161	0.414518	0.198458	0.337229	0.396069	0.423597	0.433220	0.832344	0.665266	0.405148	0.239290	0.334141	0.379477	0.392664
p2_1	0.282508	0.574967	0.393988	0.347018	0.268036	0.361307	0.382608	0.455504	0.420602	0.838345	0.677461	0.402167	0.464856	0.488861	0.449248	0.469975
p3_1	0.338364	0.491531	0.307316	0.294928	0.192975	0.276339	0.416607	0.371263	0.341804	0.814201	0.642641	0.360947	0.313941	0.360619	0.393932	0.368159
she1_1	0.287183	0.591268	0.412080	0.435225	0.409299	0.435637	0.458675	0.498345	0.480929	0.377242	0.539304	0.795724	0.299754	0.382911	0.354360	0.627095
she2_1	0.311172	0.669182	0.403986	0.436748	0.557031	0.474973	0.516470	0.497050	0.477211	0.439814	0.594281	0.864974	0.420572	0.496970	0.440837	0.743209
she3_1	0.145803	0.640712	0.507624	0.323354	0.475583	0.446895	0.451377	0.619906	0.471149	0.329508	0.580030	0.780561	0.522805	0.531269	0.400127	0.693812
sph1_1	0.345309	0.637475	0.464110	0.333426	0.389562	0.401287	0.364224	0.607314	0.452687	0.353476	0.549798	0.493543	0.854386	0.526977	0.719204	0.560862
sph2_1	0.296368	0.577817	0.433916	0.415762	0.330531	0.444770	0.397729	0.492401	0.482430	0.329307	0.502702	0.360777	0.787170	0.359739	0.649832	0.459931
sph3_1	0.282986	0.555550	0.448722	0.236834	0.336214	0.391254	0.355407	0.491367	0.388744	0.324046	0.483055	0.396580	0.809733	0.436009	0.641575	0.481244

Diagnostic validity represents the wide Yabar

Table divergent 4-30Rvayy

According to the results presented in Table 4-30 loading any observable variables on the latent variable related to the variable loadings at least 1/0 more visible the hidden Brmtghyrah Dygrast after the diagnostic validity of its structural level.

Conclusion:

in order to evaluate the questionnaire validity, and content validity, we used the form CVI, and CVR and narratives about the structure and reliability combined with optimum reliability.

In this study, society included all managers and information security and IT experts and users of information system of hospitals in Tabriz which may ultimately include 101 persons .Hence, the nature of this analytical study is from the survey applicable type,. Based on field studies and analysis of questionnaire respondents, it included 56 males, and 45 female. 8 of the respondents were under 25 years old, 48 respondents were between 25-35 years old, 32 respondents were between 35-45 years old and 13 of them were older than 45 years old. Also, 3 of respondents have PhD degrees, 25 M.A, 57 B.A and 16 of them were with A.D. A Security of Manager project, 4 Director / Head of IT, IT

expert 29, an information security management consular, 66 users hospital information system. 5 respondents less than 5 years, 32 between 5 - 10 years, 13 between 10 - 15 years and 21 for more than 15 years of service with 73 respondents lesser than 2 years, 23 patients between 2 - 5 years, 5 patients between 5 - 8 years project implementation experience with information security management system. 72 persons respondents in low volume projects, 26 medium-size projects, three people who attended in ISMS project were old. Using the software, smart-PLS software and using structural equation modeling confirmatory factor analysis, we measured the results of test of convergent validity, divergent validity, reliability Security and reliability of observable variables and quality test and measurement model of 101 comments of experts, all about the prerequisites and requirements, including information security policy, the organization of information security, asset management, human resources in terms of security, physical and environmental security, communications and operations management, access control, use, development and maintenance, incident management information security, business continuity management and compliance with laws in secure level at %99 forecasted in hospitals in Tabriz are effective information security management system. According to prioritization of the factors affecting information security management system, operating (after

the most monitors and agents (after) the supply and implementation of information security management system at least affected hospitals in Tabriz.

Suggestions for Future Research

1. Given that in this study, only 8 hospitals were studied in Tabriz. Next, the researchers are recommended to perform such reviews in both public and private hospitals in order to compare the results with the results of several studies in terms of reliability and confidence in using of the results achieved.

2. Comparative study of organizations, including hospitals that have attempted to establish information security management system and review results prior to the implementation of the deployment and provide suggestions to improve performance 3. According to the study, structural equation modeling and analysis of PLS is used for factors like the other researchers' suggested techniques such as AHP, TOPSIS and other software use and structural equation such as LISREL, AMOS, etc.

References

1. Arabi, S.M., Dehqan. N. (2011). Research Methods in Strategic Management Research Center, No. 20(60).
2. Bazrgan, et al. (2008) Behavioral Science Research Methods. Tehran: Agah publications
3. Kazmi, M. (2014) .Survey and Assessing the Implementation of Information Security Management , mayor of Tabriz, M.D of executive management ,Faculty of Humanities. Islamic Azad University. Bonab branch.
4. Karami et al, (2013). Patients' Rights Guidelines for Electronic Information Security Environment. Medical Ethics.
5. Moqaddasi, H. Ayani. Sh. (2013). Data Security of Health Information Systems. Protective Research -Security: University of Imam Hussein.