Modern Applied Science; Vol. 10, No. 2; 2016
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

# Organizational Characteristics Role in the Implementation of Information Security in Knowledge Management with a Focus on Employee Safety Behavior

Abozar Solat Rafiee[1], Akbar Alem Tabriz[2] & Mohammadreza Babaei[3]

[1] Department of IT Management, Science and Research Branch, Islamic Azad University, Tehran, Iran

[2] Shahid Beheshti Universities, Tehran, Iran

[3] Department of Industrial Management, College of Management and Accounting, Yadegar-e-Imam Khomeini (RAH) Branch, Islamic Azad University, Tehran, Iran

Correspondence: Abozar Solat Rafiee, Department of IT Management, Science and Research Branch, Islamic Azad University, Tehran, Iran.

Received: November 25, 2015 Accepted: December 3, 2015 Online Published: December 7, 2016

doi:10.5539/mas.v10n2p123 URL: http://dx.doi.org/10.5539/mas.v10n2p123

## Abstract

Nowadays competitive advantage maintenance and organizational survival are not possible with no knowledge management. Due to the fact that the main components of the organizational knowledge transfer are human resources and this force only can produce and share knowledge content in the context of a safe system. Therefore, the implementation of the information security and safety principles observance by the personnel are essential in knowledge management. Among these factors, organizational characteristics can be an affecting factor in the implementation of information security in knowledge management. In this study, the role of organizational characteristics on the implementation of the information security in organization's knowledge management with a focus on safety behavior of the staff in the Ministry of Communications and Information Technology and its subsidiaries, is investigated. The study type is applied research and the method is descriptive method which its population consists of senior managers and experts in the Ministry of Communications and Information Technology and its subsidiary companies. The sample size of 253 people has been set. A questionnaire was used to measure the research variables. Regression analysis was used to investigate the relationships between variables and AMOS software was used in this study. The results showed a significant relationship between organizational characteristics with safety behavior and also safety behavior with information security implementation in knowledge management. The organizational characteristics significantly are associated with the implementation of information security in knowledge management.

**Keywords:** knowledge management, information security, enterprise characteristics, safety behavior of the employees, the Ministry of Communications and Information Technology

## 1. Introduction

Nowadays one of the critical infrastructures of any organization in order to achieve true knowledge management is using organizational characteristics; and aligning these characteristics is necessary in order to achieve an appropriate structure for the successful implementation of knowledge management.Acquisition and dissemination of knowledge is significantly associated with the use of proper infrastructure. These infrastructures can be in the form of culture, top management support, incentive system and appropriate organizational structure (Said et al., 2014). As for the increasing use of the internet, exchanges of information and data integration costs; the topic of management, control and transferring of information and a comprehensive system for information security management are becoming more and more important (Sango et al., 2007). Today, with increasing penetration of information systems and the increasing value of information, the importance of data protection for organizations has been more evident. Leading businesses are trying to control Intellectual property and creating value by information security implementation in knowledge management (Gerber et al., 2014).

Therefore, the implementation of the information security in knowledge management is necessary to facilitate the achievement of the objectives of the organization, which one of the affecting factors on information security implementation in knowledge management can be organization characteristics such as corporate culture, organizational structure, top management support, remuneration and etc. In another words, since one of the most important success factors for knowledge management is the organizational characteristics compatibility with knowledge management, this topic is of great importance (Johnston & Pearson, 2012).

Fundamental changes in business processes has led to one-click information transferring , and needless to say that in a complex environment with extensive connections, extensive damages threaten computer systems, information systems, and activities and critical infrastructures related to them. Finally, we can say that formulation and implementation of security measures in the face of this widespread threats, is inevitable for organizations. Appropriate measures can minimize the possibility of hazards; if any of them occurs it can keep damages minimized, and create the ability to respond quickly and effectively in order to repair damages by using predefined processes, and finally can increase information efficiency and safety so that business could continue more comfortable. (Mirdamadi, 2011)

Additionally the safety behavior should be defined in the organization in a proper way so that to be appear at all stages of the process of knowledge management. Trust is perhaps one of the most important factors influencing the development of organizational knowledge. But this confidence is the result of structural and behavioral processes in the field of information security (Haman, 2013)

According to the presented material, the need to implement information security in knowledge management increasingly has been felt in the Ministry of communication. So the present study aims to answer the question of whether organizational characteristics have impact on the information security implementation in knowledge management of the Ministry of Communications and subsidiaries?

## 2. Literature

This section presents articles on the subject of the research. For this purpose, this section has 2 subsections. The first subsection contains theoretical foundations of the research that includes organizational characteristics, implementing information security and information safety behavior of the staff and in the second subsection we refer to the other investigations in this area.

### *2.1 Theoretical Foundations*

Organizational characteristics are originating from the management model adopted by the organization, and through the structure or strategy, or through the company's culture and their relationship are embodied in the nature of the organization. According to this explanation, organizational characteristics can widely affect the organization. (Rahman Saeed et al., 2014). So in this part of the article, the studies about the role of the following variables are provided.

Culture

Senior management support

Encourage and reward

Organizational structure

#### 2.1.1 Organizational Culture

Organizational culture is an environmental variable that influences all members of the organization differently and hence proper understanding of the structure is important for managing the organization and effective work (Felin, 2014). Members of the organization teach their organizational written and unwritten culture to the new members in order to resolve issues related to external compliance (e.g. the best way to participate in the global markets) and internal integration (best way to coordinate and strengthen processes within an organization). Hence by having the capacity to transform and change organizational culture, we can change thoughts and feelings of the vast majority of members. (Lassen & Sand tones, 2002). Organizational culture has a direct impact on creating culture of information security. The effect of organizational components including collaboration, innovation, consistency, efficiency and effectiveness on the principles of information security (confidentiality, availability, integrity and accountability) were studied and the results showed that all components of organizational culture has a positive effect on the information security (Chang, 2007).

#### 2.1.2 Senior Management Support

Senior management support is considered as one of the important potential effects in organizational knowledge (Connelly & Kelloway, 2003). The importance of information and information resources for organizations is increasing day by day. Valuable information and the importance of information security, has become the main concern of senior managers (Purser, 2004). Support and commitment of organizational senior managers is essential for success in knowledge management objectives and knowledge projects. Some examples of responsible leadership role in the successful establishment and implementation of knowledge management can be cited as follows (Watanabe, 2013):

Response to the ambiguities and gain the employees trust to changes

Stimulate the motivation of employees for knowledge sharing

Promotion of culture

Support of Knowledge-based schemes

### 2.1.3 Encourage and Reward

Encouraging knowledge management activities play an important role as an enabler among the staff. Incentives should have the ability to determine employee's stimulation or action in an organization. Reward, on the other hand, can be broadly classified as an internal or external factor. External rewards are related to the positive value of the work result which help employee to set the work, while internal rewards are the positive value of the work result which is considered as the direct result of work by the employee. Both internal and external rewards have positive impact on the performance of knowledge management in organizations (Abdel Rahman Saeed, 2014). Both external and internal rewards and encourage have positive impact on the implementation and performance of information security in the organization. (ITRC (Iran Telecom Research Center), 2009)

### 2.1.4 Organizational Structure

Appropriate structures and strategies are very effective in achieving the goals (Martinus and Marinus, 1994). Issues of human relationships and psycho-social needs of people have been entered to the field of management in general and specific design domain by the neoclassical school philosophers. The two approaches have not considered change as an important element in the management of organizations (Zach et al., 2012). Secure business environment in the early twentieth century, justifies the lack of attention to the change. Unlike the early twentieth century, today the need for flexibility to adapt to the changing world is an essential issue (Englehard & Simmons, 2002). In general, the aim of organizational structure is aligning the manpower and available resources in order to increase the efficiency and effectiveness of the organization. In fact, the structure is a process that plays an important role in achieving organizational goals. Organization structure is a framework in which the basic areas, general mission, communication system and decision-making center are determined (Anik & Medark, 2009). Organizational structures in modern organizations are periodically changing and transforming. This causes many challenges for information security authorities because resolving any of them will not be easy (ITRC, 2009). The vital Relationship between the organization systems within the framework of the organizational behavior theory and information security awareness (ISA) within the framework of information security theory was investigated and results showed a significant relationship between information security awareness and dimensions of formal organization structure, organizational culture dimensions and human resource practices and policies.

## *2.2 Information Security*

Life of the organizations is in close contact with their information systems. Information systems are always at risk of identity theft, changing information and services interruption (Thomas, 2012). In order to solve the problem of information security, the organization needs to employ a wide range of science, technology and organizational rules and at the same time has to be ensure that the organization is not focused only on technical solutions, but also other key components of information security, including processes and personnel in it is considered (Honan, 2006; Kraemer, 2006).

The tasks of Information security is protecting the information (Maiwald & Sieglen, 2002) and minimizing the risk of information disclosure in unauthorized parts (Dalton & Osmanoglo, 2001). Information security is a set of device to prevent theft, assault, murder, espionage and sabotage (Hashemian, 2000) and is the science of studying data protection methods in computers and communication systems against unauthorized access and changes (Abdullah, 1996).

So, obviously ignoring the security of the information exchange space and incorrect encounter against this category prevent the spreading of this security among people and gaining the managers trust to use the modern methods of monitoring and information management (Johnston, 2012). Creating a coherent system at national level with taking into account the specific characteristics of the exchange of information and security in this space is a necessity. Some of these features are as following:

Security of the large conceptual data exchange space and based on different field of knowledge.

Security is defined with respect to cost and efficiency and is a relative concept.

Security is set by the customs, traditions and morals of the society.

Security in the area of information exchange is affected by the rapid changes in technologies (Purmand, 2006).

### *2.3 The Safety Behavior of the Staff*

There are misinterpretations of the concept of behavioral safety. In fact, this process is focused on environmental variables that trigger and support staff activities, in a way that to not focus on the employee personality but focus on the elements of enterprise systems that encourage safety behavior or prevent unsafe behavior. Human safety has a broad application in two cases: finding and removing the barriers to the adoption of the imine behavior and strengthen support systems to promote safety behavior (Green, 2005).

Safety behavioral stresses that employees have to be caution in adopting safe behavior or unsafe behavior; when they have unsafety behavior, try to reform without punishment and when they act in a safe way, they are encouraged. Therefore, safe and unsafe behaviors can be calculated. Behavioral safety is of the opinion that what is measured, can be done and every employee can cause changes in the organizational safety. Employees are one of the resources of any attempt to change behavior (view and modify). Behavioral safety is applicable in any working condition and is a group work based on the group and at the same time based on the individual (Kila, 2006).

One of the advantages of using behavioral processes and leading companies around the world is improving safety culture and communication within the organization. Improving safety communication through the safety behavior plays a great role in creating healthy organizational safety culture that this would decrease the losses during the work (Alizadeh & Taghdisi, 2008).

### *2.4 Necessity of Information Security Implementation in Knowledge Management*

Certainly, the main ingredient in organizational knowledge transfer is human resources. This force need to be sure of protecting its data in the context of a safe system, in order to produce knowledge content and finally be able to share this content. This requires a correct safety behavior by individuals. Safety behavior shall be defined in an organization in a way that be appear at all stages of the process of knowledge management in the organization. Trust is perhaps one of the most important factors influencing the development of organizational knowledge. But this confidence is the result of structural and behavioral processes in the field of information security (Haman, 2013). It should be noted in the field of individual information security that the most important issues in information security is awareness, if we are all aware of the different aspects of information security or insecurity, we suffer less. The painful dimension of information security is when the stolen information are not personal information, but are related to a group of people in an organization and even a country that provide the possibility of sabotage with a larger scale. The simplest and most effective way to achieve awareness is training. Therefore education of information security is one of the most important issues that should be addressed at the individual, organizational and national level. This awareness must also be ongoing in the context of knowledge management (Jana, 2012). So we can say that information security has to be considered as one the most important infrastructures in the knowledge management field because it is not only effective on the facilitating the flow of knowledge but also is impressible of knowledge management (Ayako Komatsu et al. ).

### *2.5 Literature Review*

Abd Rahman Said et al. (2014) investigated the association between the organizational characteristics and implementation of information security management. The main objective of this paper is to empirically investigate the effects of organizational characteristics and its dimensions (culture, top management support, reward and incentives, and organization structure) as the knowledge management success factor on the implementation of information security. The results showed that the characteristics of the organization have created a significant positive effect. Results are in line and consistent with previous studies on the development of knowledge management. Studying empirical evidence and literature show that knowledge management is a success factor in the implementation of the information security in knowledge management.

Deepa Mani et al. (2014) in a study entitle Information security management in the real estate industry in South Australia assessed 40 real estate agencies with the aim of contributing to a better understanding of the security threats of information, awareness and risk management standards which are currently used in the real estate sector in South Australia. Results indicate that opportunities for malicious Internet activity have been expanded by the globalization and advances in information and communication technology. The findings suggest that the increased complexity of the online environment emphasize the need for regular educational programs for the public online security (including the new computer crimes) and promoting the culture of information security (for example, when using smart mobile devices to store and access sensitive data) among the employees.

Ayako Komatsu and et al. (2013) studied the human dimensions of information security management. They did an empirical study of the actual behavior beside the intentional behavior with the aim of analyzing the behavior of individuals who have been engaged to implement information security measures.

Jana (2012) studied security information management and business continuity management in the IT organization relations. The aim of the study was to understand how IT and information security managers act in order to increase information security and manage the business continuity in the IT relationships of the organization like out sourcing, cloud computing and organizational systems. Results showed several methods, including contracts, audit and relation balance standards of the power in the organization or transition to the parties. The purpose of these methods is different in organizations. Second, the article provided a comprehensive view of security and continuity of the solutions in the IT organization relations. The findings are of practical value for IT administrators and information security experts.

Yi Hsin Lin (2012) assessed the information exchange for transfer to pilot safety behavior. The aim of the study was using organizational identification, organizational culture and safety culture as intervening variables between safety mission and safety behavior in order to check and investigate the data exchange model from the senior managers to the employees. The findings suggest that organizational identification and organizational culture are two important intervention variables between the safety mission statement (knowledge exchange) and safety behavior. Pearson correlation analysis showed that five factors are correlated with each other, particularly safety mission statement and organizational identification with organizational culture and safety culture. In addition, the safety mission statement has a direct negative effect on the safety behavior of the pilot.

Jacqueline and et al. (2011) studied the effects of organizational capabilities in information security management to assess the relationship between information security strategy, organizational performance and organizational capabilities as the most important factors influencing the successful implementation of information security strategy and organizational performance. Results showed that the organizational capabilities, including the ability to develop high-quality situational awareness of current and future threat environment, the ability to have the right tools, and the ability to coordinate the tools to respond to information security threats have a positive correlation with the effective implementation of information security strategy and consequently this would have positive effect on the organizational performance. However there was not a significant relation between decision making and the effective implementation of information security strategy.

Dan Harnesk, John Lindstrom (2011) in a study entitled shaping the security behavior through discipline and agility, investigated the implications for Information Security Management with aim to expand understanding of the safety behavior by developing security behavior based on the concepts of discipline and agility. Results suggest that security behavior can be shaped by discipline and agility and also it can exist in groups, if the fundamental and existential aspects of the management of information security (IS) are considered.

Ahmed Musa (2010) investigated the rule of information security governance in the Saudi organizations. The aim of study is to investigate the existence and implementation of information security governance (ISG) in Saudi organizations. The results show that although most organizations in Saudi Arabia are aware of importance of the information security governance as an integral factor for the success of IT and corporate governance, many of them have no clear information security strategy or written information statements that show the security policy.

Rafiee (2014) in a study entitled the relationship between safety culture and knowledge management in Iran Telecommunication Research Center has stated that human resources is one of the most important factors in accidents associated with information security. Therefore, issues related to the information security have changed their pure focus on technology towards human resources. One of the most effective fields in this area is safety culture that is affected by many factors. Results show that production, use and dissemination of the knowledge have significant relationship with safety behavior and also safety behavior and safety culture are correlated.

Ansari et al. (2013) in a study provided a conceptual model for the success of knowledge management implementation on the competitive advantage in the small and medium companies (SMEs). Results show that organizational culture and information technology have the most effect on the success of knowledge management implementation and organizational structure has the lowest effect. It is maybe because of the lack of coherent structure in Iran small and medium companies.

Matlabi et al. (2013) investigated factors affecting the implementation of knowledge management in higher education institutions using fuzzy TOPSIS method. Results of this research show that factors such as recruitment based on knowledge competencies and designing appropriate mechanisms to evaluate students with a score of 0.55 and 0.51, have the greatest impact on the implementation of knowledge management.

Heydari et al. (2013) investigated the critical success factors in the implementation of knowledge management to evaluate the effectiveness of the crucial factors in the implementation of knowledge management in the Agriculture Organization. This study is based on Hung model which is based on ten factors including organizational culture, senior management commitment, participation, training, teamwork, empowerment, information systems, performance measurement, modeling and knowledge structure. The results with a confidence level of 95% showed that all selected factors are leading to implement knowledge management. Also the Friedman test showed that the impact of all factors on knowledge management are not same and are different.

Ronaghi and Feizi (2012) studied work ethics and its relationship with information security management to evaluate the relationship between information security management and business ethics. Among the most important findings of the study is to identify positive and significant relationship between the use of the information security and business ethics in organization.

Khosrow Anjam et al. (2011) in a study entitled the role of information technology in the design and implementation of knowledge management in telecommunications using fuzzy AHP investigated the role of IT in the Implementation and designing knowledge management systems. The results indicate that communications technology and partnerships are major drivers in how to design and build knowledge management systems. Therefore, collaborate intranets and knowledge expert's transactions with knowledge users are the key indicators that affect the role of information technology for knowledge management systems.

According to the above contents, the conceptual model is presented as follows:

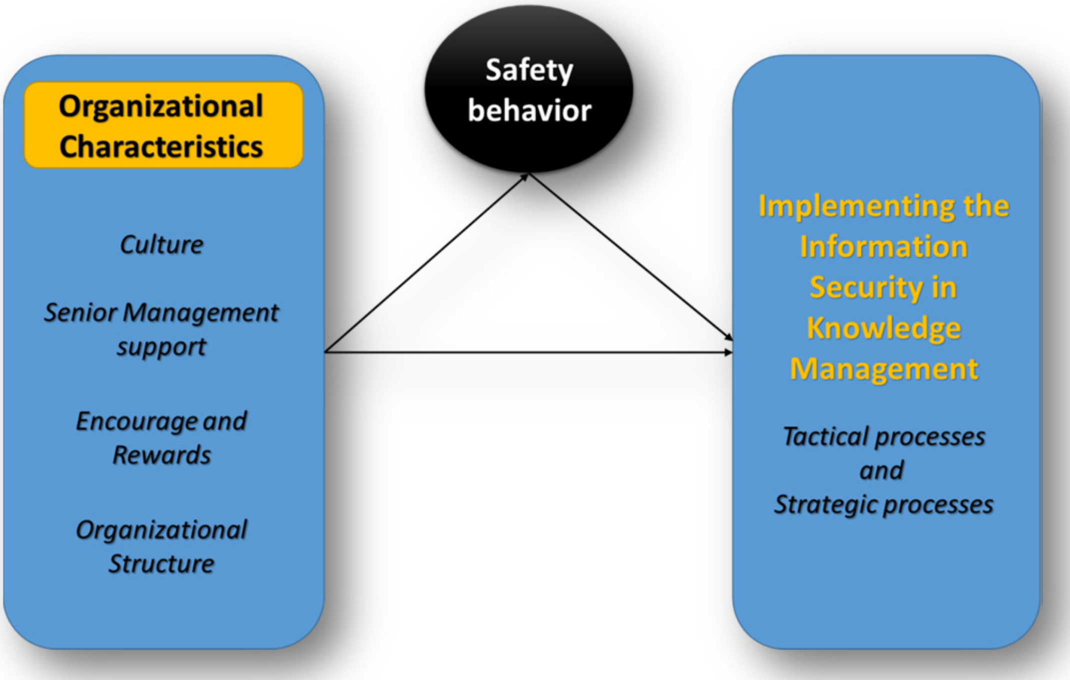

Safety behavior
Organizational Characteristics
Culture
Senior Management support
Encourage and Rewards
Organizational Structure
Implementing the Information Security in Knowledge Management
Tactical processes and Strategic processes

Figure 1. The conceptual model

## 3. Research Methodology

This study objective is applied because it can be used to solve scientific problems. The method of this research is descriptive; since it is describing the current statue. This research is a correlation study, as it is to investigate the correlation between the independent variable and the dependent variable and it is also a survey, because data for this study was obtained using sample surveys in order to study the distribution of community characteristics.

The study population consisted of all staff of the Ministry of Communications and Information Technology and its subsidiary companies. All the staffs composing the population are working in the research and develop and information technology sections in their organizations. The method of sampling is simple random. The number of sample is calculated according to the invention table of Morgan and as the size of the study population is 730 , by using the Morgan table , sample size of 253 people has been set.

The data collecting tool in the study is questionnaire. The questionnaire was developed in two parts. The first section includes demographic data and the second part contains detailed questions in connection with the research hypotheses. 5-item Likert answers was used in the questionnaire. The validity of this research is measured based on the validity of the content. So that by distributing questionnaires among professors and experts in different stages, reforms were done and final questionnaire was extracted. In this study, to evaluate the reliability of the tests, Cronbach's alpha was used. The results of reliability test are shown in the table below:

Table 1. Result of reliability test

| Index | The calculated coefficient | Result |
|---|---|---|
| Organizational characteristics | 0.745 | confirmed |
| Information security implementation with a focus of knowledge processes | 0.741 | confirmed |
| Safety behavior of the staff | 0.887 | confirmed |

According to the model presented by Rahman et al. (2014), In this study we sought to evaluate the following hypotheses:

According to the model, we can offer the following assumptions:

The main hypothesis: there is a significant positive relationship between the organizational characteristics and implementation of Information Security in Knowledge Management in the Ministry of Communications and its subsidiary companies.

Sub assumptions:

There is a significant positive relationship between the culture of the organization and implementation of Information Security in Knowledge Management in the Ministry of Communications and its subsidiary companies.

There is a significant positive relationship between senior management support and the implementation of Information Security in Knowledge Management in the Ministry of Communications and its subsidiary companies.

There is a significant positive relationship between organizational encourage and reward and information security implementation in knowledge management in the Ministry of Communications and its subsidiary companies.

There is a significant positive relationship between the organizational structure and implementation of Information Security in Knowledge Management in the Ministry of Communications and its subsidiary companies

Organizational characteristics and successful implementation of information security in knowledge management have a significance relationship through safety behavior.

## 4. Results

### *4.1 Assessing the Status of Variables*

#### 4.1.1 Descriptive Analysis of Research Indices

The variable descriptive analysis of the study are based on central and sprawl measures.

Table 2. Descriptive analysis of the study variables

| | | Implementing the information security in knowledge management, tactical processes and strategic processes | Safety behavior | Organizational structure | Encourage and reward | Senior management suppose | culture |
|---|---|---|---|---|---|---|---|
| **Total** | True | 253 | 253 | 253 | 253 | 253 | 253 |
| | Lost | 0 | 0 | 0 | 0 | 0 | 0 |
| Average | | 3.475 | 3.42 | 3.34 | 3.45 | 4.09 | 3.58 |
| Middle | | 3.615 | 3.50 | 3.14 | 3.50 | 4.12 | 3.50 |
| Model | | 3.785 | 4.13 | 2.71 | 3.75 | 4.13 | 3.50 |

4.1.2 Assessing the Distribution Status of Variables Using the Kolmogorov-Smirnov Test

According to the table below it can be said that significance level of the all indicators are more than the standard 0.05, the distribution of these indicators are normal.

Table 3. Assessing the distribution status of variables using the Kolmogorov-Smirnov test

| variables | Test statistics | Number | Significance level |
|---|---|---|---|
| Culture | 0.487 | 253 | 0.14 |
| Senior management support | 0.124 | 253 | 0.24 |
| Reward and encourage | 0.228 | 253 | 0.11 |
| Organizational structure | 0.486 | 253 | 0.18 |
| Safety behavior | 0.358 | 253 | 0.15 |
| Implementing the information security in knowledge management, tactical processes and strategic processes | 0.514 | 253 | 0.375 |

*4.2 Assessing the Relationships between the Variables*

Table 4. Indicators of the structural equation model and analyze of the relationships between the research's variables

| Variable | Latent and mediator and related components | Path coefficient | t Statistic | Confirm/Reject |
|---|---|---|---|---|
| Culture | Organizational characteristics | 0.41 | 6.12 | **confirm** |
| Senior management support | Organizational characteristics | 0.23 | 3.82 | **confirm** |
| Reward | Organizational characteristics | 0.24 | 3.84 | **confirm** |
| Organizational structure | Organizational characteristics | 0.22 | 3.72 | **confirm** |
| Organizational characteristics | Safety behavior | 0.32 | 5.32 | **confirm** |
| Safety behavior | Information security implementation | 0.22 | 3.87 | **confirm** |
| Organizational characteristics | Information security implementation | 0.41 | 6.324 | **confirm** |

According to the table above, all indicators were examined in order to assess the confirmatory factor model have been accepted. Due to this, it can be said that this model has been confirmed. According to the test statistic, the relationships between the main components of the research are approved.

After the assessing research model, drawing and relationships between latent variables (which are in fact the hypothesis) are discussed. In this case, first have to be ensure of fit indexes and then assumed relationships between latent variables are investigated.

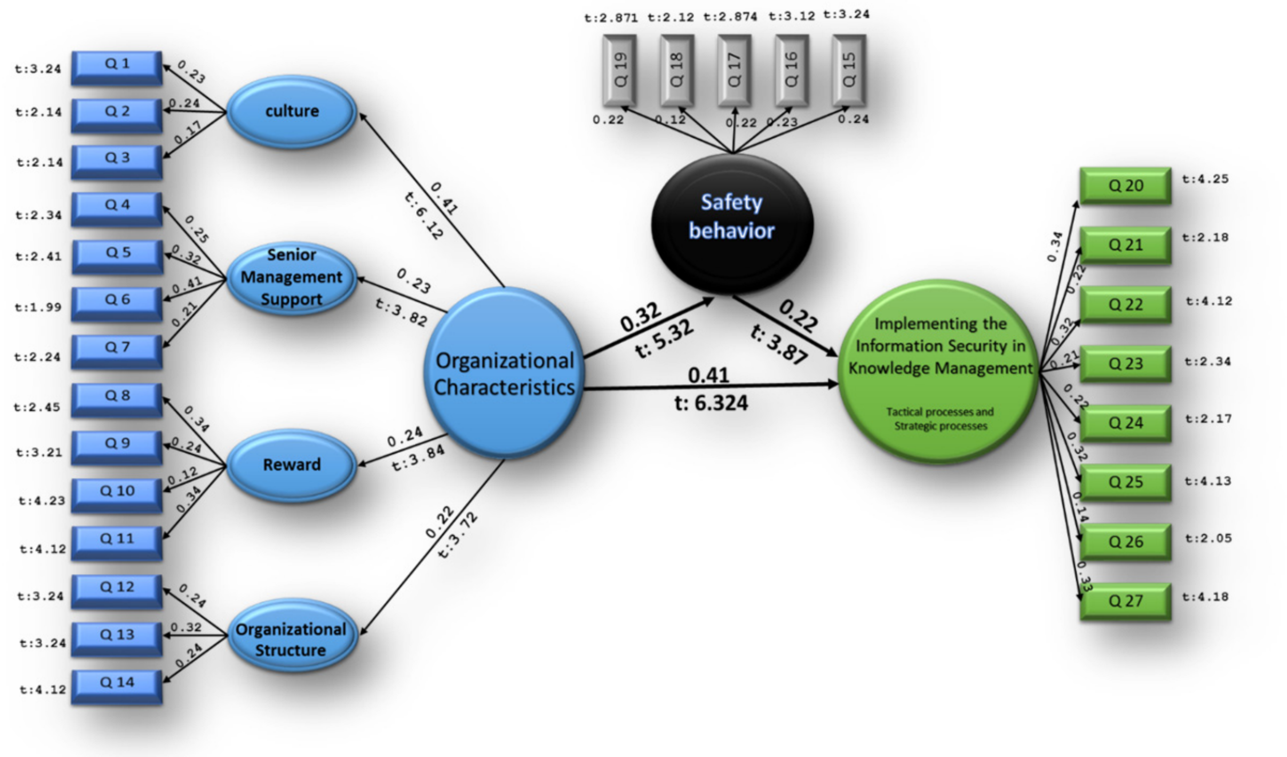


Figure 2. Structural equation modeling

The first hypothesis result (There is a significant positive relationship between the culture of the organization and implementation of Information Security in Knowledge Management in the Ministry of Communications and its subsidiary companies): examining the association between dependent and independent variables of the hypothesis test showed that test statistic is 3.15. The amount is more than standard value of 1.96, so the relationship between the two variables is confirmed. Moreover the correlation coefficient of this relation is 0.23 which indicates that the status of the connection is weak.

The second hypothesis result (There is a significant positive relationship between senior management support and the implementation of Information Security in Knowledge Management in the Ministry of Communications and its subsidiary companies): examining the association between dependent and independent variables of the hypothesis test showed that test statistic is 6.32. The amount is more than standard value of 1.96, so the relationship between the two variables is confirmed. Moreover the correlation coefficient of this relation is 0.41 which indicates that the status of the connection is weak.

The third hypothesis result (There is a significant positive relationship between organizational encourage and reward and information security implementation in knowledge management in the Ministry of Communications and its subsidiary companies): examining the association between dependent and independent variables of the hypothesis test showed that test statistic is 3.12. The amount is more than standard value of 1.96, so the relationship between the two variables is confirmed. Moreover the correlation coefficient of this relation is 0.22 which indicates that the status of the connection is weak.

The fourth hypothesis result (There is a significant positive relationship between the organizational structure and implementation of Information Security in Knowledge Management in the Ministry of Communications and its subsidiary companies): examining the association between dependent and independent variables of the hypothesis test showed that test statistic is 2.32. The amount is more than standard value of 1.96, so the relationship between the two variables is confirmed. Moreover the correlation coefficient of this relation is 0.12 which indicates that the status of the connection is weak.

### *4.3 Assessment of the Relationship between the Organizational Characteristics Dimensions and Successful Implementation of Information Security in Knowledge Management*

In this section, after calculating the dimension average of the organizational characteristics, the relationship between these dimensions and the successful implementation of information security were examined:

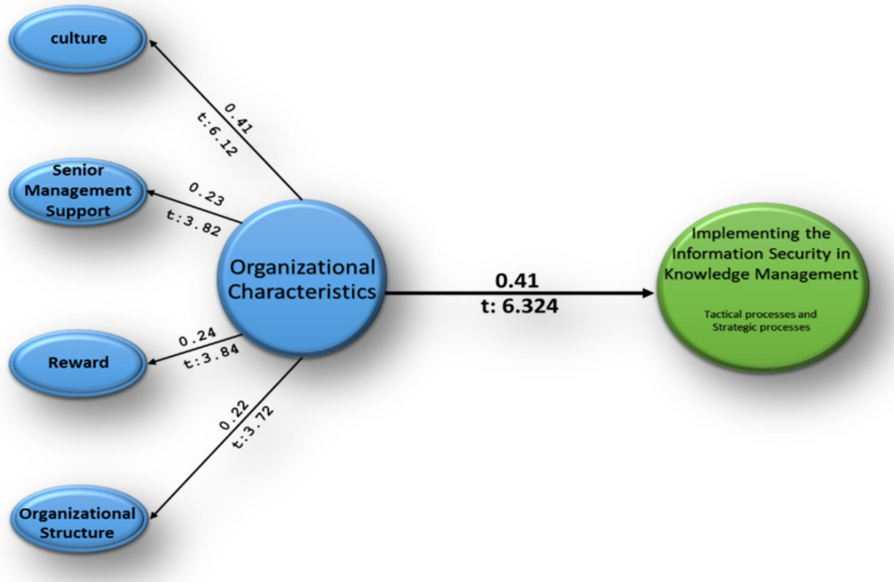

culture
0.41
t:6.12
Senior Management Support
0.23
t:3.82
Organizational Characteristics
0.41
t: 6.324
Implementing the Information Security in Knowledge Management
Tactical processes and Strategic processes
Reward
0.24
t:3.84
0.22
t:3.72
Organizational Structure

Figure 3. Relationship between the organizational characteristics dimensions and successful implementation of information security in knowledge management

#### 4.3.1 Assessing the relationship between organizational characteristics and information security with and without safety behaviour

Employee safety behavior act as mediator in the relationship between the organizational characteristics and implementation of information security in knowledge management.

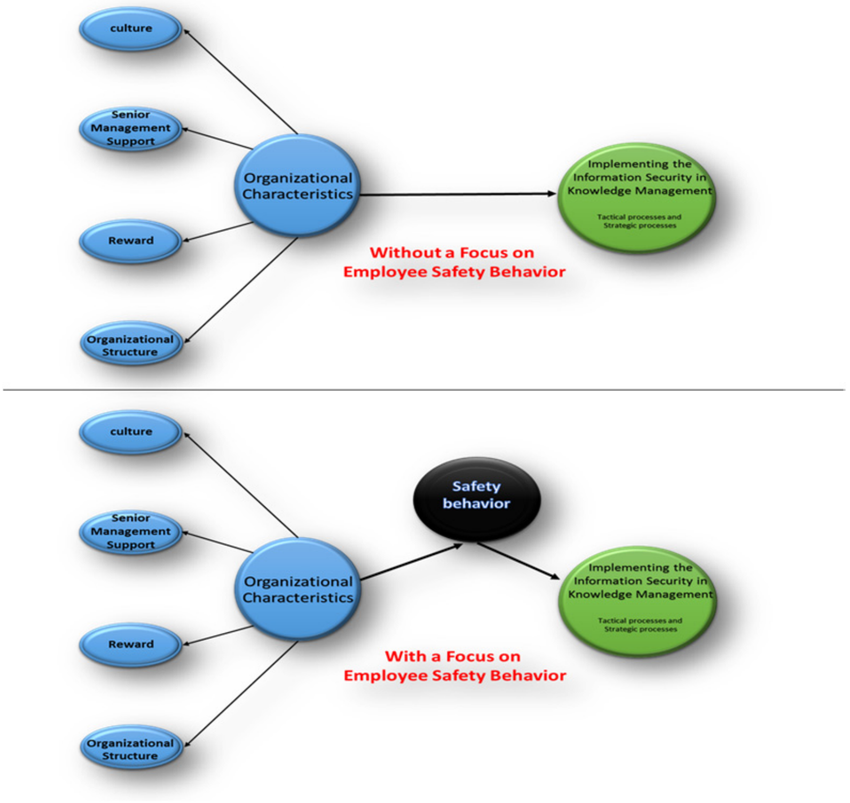

culture
Senior Management Support
Organizational Characteristics
Reward
Organizational Structure
Implementing the Information Security in Knowledge Management
Tactical processes and Strategic processes
Without a Focus on Employee Safety Behavior
culture
Safety behavior
Senior Management Support
Organizational Characteristics
Implementing the Information Security in Knowledge Management
Tactical processes and Strategic processes
Reward
With a Focus on Employee Safety Behavior
Organizational Structure

Table 5. Regression test of the relationship between the safety behavior of staff, organizational characteristics implementing information security

| Independent variable | Dependent variable | Significance level | Beta coefficient |
|---|---|---|---|
| organizational characteristics | implementing information security | 0.000 | **0.41** |
| organizational characteristics | implementing information security | 0.000 | **0.63** |
| safety behavior | | 0.003 | **0.324** |

According to the above table the level of significance in all cases shows that there is a connection. While without safety behavior factor the correlation coefficient of the relationship between the organizational characteristics and implementation of information security is calculated 0.41 and with the safety behavior factor the correlation coefficient increased to 0.63. So with the arrival of safety behavior to the organizational characteristics, the influence of this index and implementing information security has risen. So the arrival of safety behavior to the organizational characteristics exacerbates this relationship and this variable can be considered as the intervent variable with positive effect.

Table 6. The results of the hypotheses

| **Hypothesis** | **Result** |
|---|---|
| There is a significant positive relationship between the organizational characteristics and implementation of Information Security in Knowledge Management in the Ministry of Communications and its subsidiary companies. | Confirmed |
| There is a significant positive relationship between the culture of the organization and implementation of Information Security in Knowledge Management in the Ministry of Communications and its subsidiary companies. | Confirmed |
| There is a significant positive relationship between senior management support and the implementation of Information Security in Knowledge Management in the Ministry of Communications and its subsidiary companies. | Confirmed |

| | |
|---|---|
| There is a significant positive relationship between organizational encourage and reward and information security implementation in knowledge management in the Ministry of Communications and its subsidiary companies. | Confirmed |
| There is a significant positive relationship between the organizational structure and implementation of Information Security in Knowledge Management in the Ministry of Communications and its subsidiary companies | Confirmed |
| Organizational characteristics and successful implementation of information security in knowledge management have a significance relationship through safety behavior. | Confirmed |

## 5. Conclusions and Suggestions

The results of this study confirmed the relationship between the dimensions of knowledge management practices and the safety behavior of people and the results showed that the safety behavior is effective on the organizational culture. According to the results, it can be said that correct knowledge management by correct production, protection and diffusion via using different hardware and software can develop the safety behavior of the staff. On the one hand, by trial and empower employees to provide proper safety behaviors in the organization, we can improve the overall safety culture of the organization. On another hand, these behaviors have to be observed in general among all members, especially senior managers to finally achieve the desired culture. Because according to Robbins (2009) one of the most important cultural origins of corporate is senior managers and founders of it.

The results showed that there is a significant positive relationship between the organizational characteristics and implementation of Information Security Knowledge Management in the Ministry of Communications and its subsidiary companies. This result is in line with research of Rahman (2014), which showed that the implementation of information security and personnel safety is essential in knowledge management. Meanwhile, one of the most important factors affecting the implementation of information security in knowledge management apart from technical issues are organizational characteristics and human behavior.

The relationship between organizational culture and implement information security in knowledge management in the Ministry of Communications and subsidiaries was confirmed as the research of Chang (2007), in which the organization has a direct impact on creating information security culture. Results showed that all factors of organizational culture have a positive impact on the information security components. The relationship between senior management support and the implementation of Information Security in Knowledge Management in the Ministry of Communications and subsidiaries was approved as Pestimus (2004) in which the support, involvement and commitment of senior management to information security program are useful and effective in information security. In the research of Salmez (2006) motivational strategies, loyalty, commitment and accountability of staff were cited which is in line with present research, since the relationship between reward and encourage with information security was confirmed in this research. Cheng (2005) found that organizational factors, including the size of the organization and the kind of industry, significantly affect the application of information security management. This relation also was confirmed by the fourth hypothesis. Kerager and Cerny (2010) studied the awareness of information security through a test carried out in the knowledge and behavior of users. They concluded that increasing employees' awareness of information security by concepts and vocabulary test is very useful and there is significant correlation between information security learning and change in user safety behavior. Present study also demonstrated that Organizational characteristics and successful implementation of information security in knowledge management have a significance relationship through safety behavior.

The results of the assessing the relationship between research variables has shown that there is a significant relationship between the organizational characteristics and the dependent variables of safety behavior and information security. Thus, by increasing and improving organizational characteristics can improve the dependent variables. This improvement can be achieved through the following strategies:

Offered to all employees at all levels, to share their knowledge with specific security protocols and try to use the knowledge and experience of other staff.

Recommended that in the implementation of information security in knowledge management, all organization managers should be participated in the process of process of production and dissemination of knowledge. This should be implemented from planning to implementation.

Use continuing bonuses to develop the willingness of employees to secure release of knowledge and experience in various fields and also special attention of the staff to the topic of information security can be effective.

It is essential to use a punitive system to prevent destructive behaviors in Knowledge Management and safety behavior of employees in the organization.

Using a flexible organizational structure can accelerate the implementation and application of information security in knowledge management.

The organizational structure should be designed in such way that ultimately could lead to improving secure sharing of knowledge in the organization.

**References**

Abd, R. S., Haslinda, A., Jegak, U., & Zainal, A. M. (2014). Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation. *Social and Behavioral Sciences, 123*(20), 433–443.

Ahmad, A. M. (2010). Information security governance in Saudi organizations: an empirical study. *Information Management & Computer Security, 18*(4), 226–276.

Akhavan, P., Jafari, M., & Behazin, F. (2006). Critical SuccessFactors of Knowledge Management System: A Multi-case Analysis. *European BusinessReview Journal, 18*(2), 97-113.

Alavi, M., & Lidner, D. (2001). Review: KM and KMS: conceptual foundations and research issues. *MIS quarterly, 25*(1), 107–136.

Alizadeh, A., & Taghdisi, M. H. (2008). Behavioral safety. *Journal of healthy work, 3*, 3.

Anjam, D., Elahi, S. C., & Shayan, A. (2011). The role of information technology in the design and implementation of knowledge management in telecommunications using fuzzy AHP Technique. *Industrial Management, 6*(17), 59-71.

Annick, W., Marc, B., & Ives, D. J. (2007). Impact of organizational structure on nurses' job satisfaction: A questionnaire survey. *International Journal of Nursing Studies, 44*, 1011–1020.

Ansari, M., Rahmani, Y. H., Rahmani, K., Pasbani, M., & Asgari, M. (2013). Proposing a Conception model of effect of successful implementation of knowledge management on competitive advantage in the small and medium-sized companies (SMEs). *Business Management, 5*(1), 21-40.

Ayako, K., Daisuke, T., & Toshihiko, T. (2013). Human aspects of information security: An empirical study of intentional versus actual behavior. *Information Management & Computer Security, 21*(1), 5–15.

Bennet, A. D. (2003). The Partnership between Organizational Learning and Knowledge Management. *Handbook on Knowledge Management, 1*, 439-456.

Bodur, S., & Filiz, E. (2009). A survey on patient safety culture in primary healthcare services in Turkey. *Int J Qual Health Care, 21*, 348-55.

Bose, R., & Sugumaran, V. (2003). Application of Knowledge Management Techniques in Customer Relationship Management. *Journal of Knowledge and ProcessManagement, 10*(1), 3–17.

Cardoso, R. C., & Freire, M. M. (2005). Security vulnerabilities and exposures in internet systems and services. In M. Pagani (Ed.), *Encyclopedia of multimedia technology and networking* (pp. 910-916). Hershey, Pennsylvania, IDEA GROUP REFERENCE.

Chait, L. P. (2000). Creating a Successful KM System. *IEEE Engineering Management, Review, 28*(2), 92-95.

Chung Hung, Y., Ming Huang, S., Pin Lin, Q., & Tsai, M. (2005). Critical factor in adopting a knowledge management system for the pharmaceutical industry. *Industrial management & Data systems, 105*(2), 164-183.

Conti, B., & Kleiner, B. (1997). How to increase teamwork in organizational. *Training for Quality, 5*(1), 26–29.

Dan, H., & John, L. (2011). Shaping security behaviour through discipline and agility: Implications for information security management. *Information Management & Computer Security, 19*(4), 262–276.

Davenport, T. H., & Prusak, L. (1998). *Kennismanagement in de praktijk*. Amsterdam: Contact.

Deepa, M., Kim Kwang, R. C., & Sameera, M. (2014). Information security in the South Australian real estate industry: A study of 40 real estate organisations. *Information Management & Computer Security, 22*(1), 24–41.

Heidari, M. H., & Ali, A. F. (2007). The relationship between safety climate and safety behavior in a production line of metal industry workers in Arak. *Iran Occupational Health Journal, 4*(4-3), 1-9.

Iran Telecommunication Research Center (ITRC). (2009). Extracted from the project: The theoretical and practical explain of models and implementation strategies of Information security management in organizations.

Marquardt, M. J. (2006). *Creating a learning organization: development of 5 elements for organizational learning, translation of Zali*. Tehran, Tehran University Entrepreneurship Center.

Matlabi, A., Alipour, A., & Nasri, F. (2013). Identification of factors affecting the implementation of knowledge management in higher education institutions and ranking them using TOPSIS. *Journal of Educational Management, 5*(1), 133-153.

Mirdamadi, M. (2010). Necessity of paying attention to information security. *Information age analysts monthly journal*.

NazEmi, Sh. D., Mortazavi, S., & Razavi, A. (2011). Investigating the effect of organizational characteristics on admission process in Customer Relationship Management-A Case Study of imported cars in Mashhad. *Public management reserach, 13*, 25-48.

Olfat, L., Jafarian, A., & Hassan, Z. A. (2011). The role of the implementation of information security management in the reduction of strengthening of orders in supply chains. *Industrial management perspective, 2*, 259.

Proust, G. et al. (2006). *Knowledge management*. A. Hosseini, Tehran, Seitaron publication.

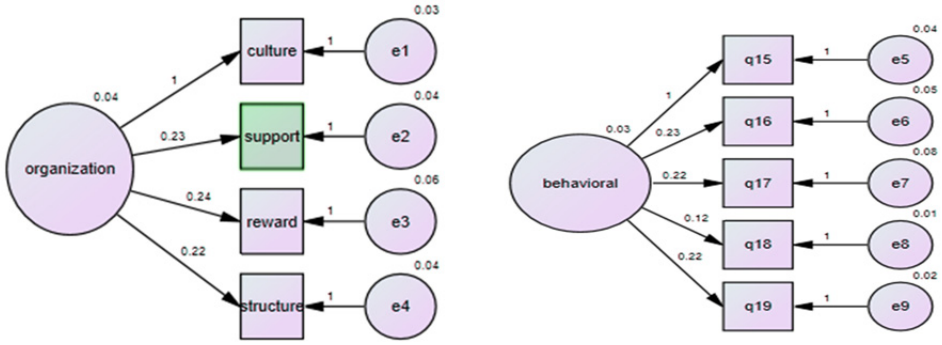
Robbins, A. P. (2012). *Management of Organizational Behavior (thirty-third edition)*. (A. Parsaeian, & S. M. Arabi, Translator) Tehran: the Institute of Business Studies and Research.

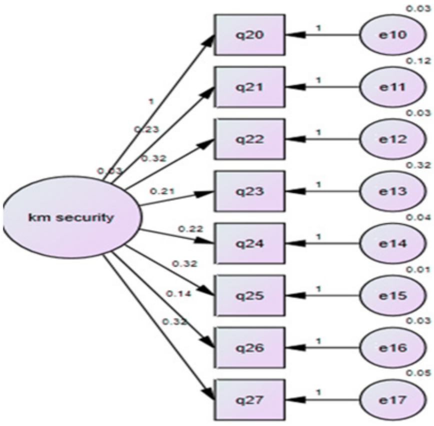
Roonaghi, M. H., & Feizi, K. (2012). Work ethics and its relationship with information security management. *Moral knowledge, 3*(11), 95-105.

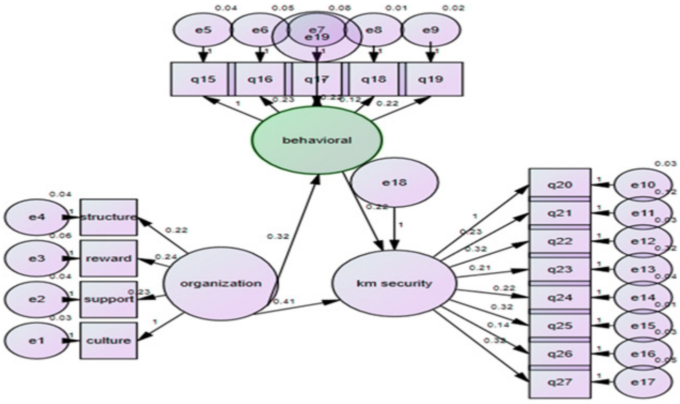
Vaezi, R., & Motavali Habibi, M. (2006). A Knowledgeable insight to Knowledge Management. *Management magazine, 113*.

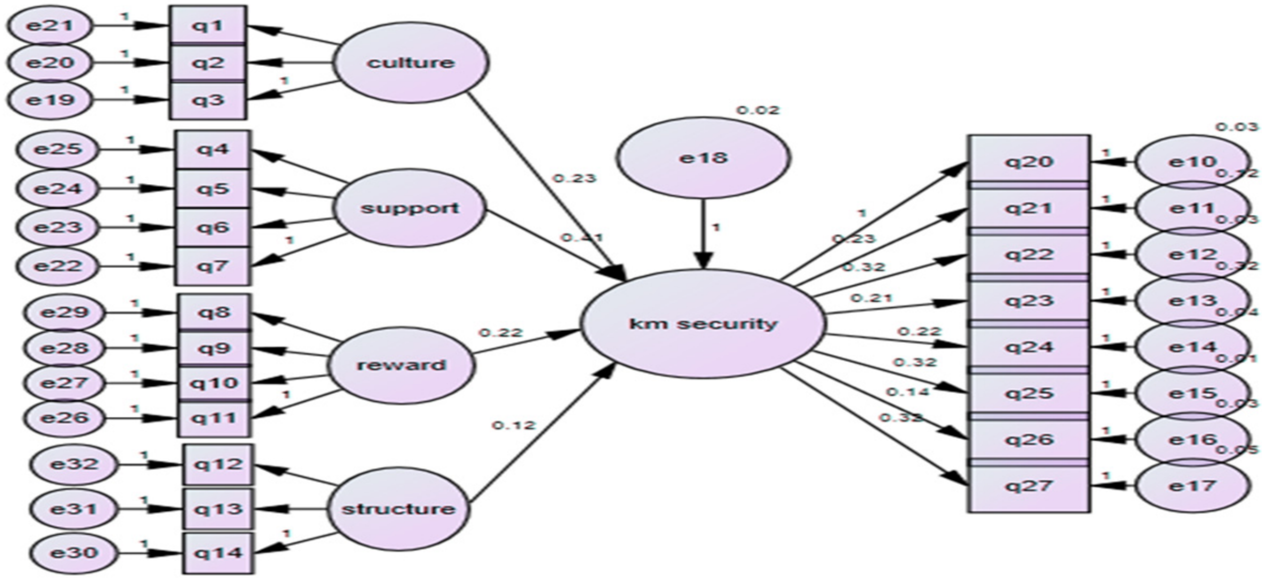
## Appendix

O Applications AMOS




km security
q20
q21
q22
q23
q24
q25
q26
q27
e10
e11
e12
e13
e14
e15
e16
e17
1
0.23
0.32
0.21
0.22
0.32
0.14
0.32
0.03
0.12
0.03
0.32
0.04
0.01
0.03
0.05


e5
e6
e7
e19
e8
e9
q15
q16
q17
q18
q19
behavioral
e18
organization
km security
structure
reward
support
culture
e4
e3
e2
e1
q20
q21
q22
q23
q24
q25
q26
q27
e10
e11
e12
e13
e14
e15
e16
e17
0.32
0.41
0.22
0.24
0.23
1


e21
e20
e19
e25
e24
e23
e22
e29
e28
e27
e26
e32
e31
e30
q1
q2
q3
q4
q5
q6
q7
q8
q9
q10
q11
q12
q13
q14
culture
support
reward
structure
e18
0.02
km security
0.23
0.41
0.22
0.12
1
q20
q21
q22
q23
q24
q25
q26
q27
e10
e11
e12
e13
e14
e15
e16
e17
0.23
0.32
0.21
0.22
0.32
0.14
0.32
0.03
0.12
0.03
0.32
0.04
0.01
0.03
0.05

## Copyrights