THE FACTORS AFFECTING INFORMATION TECHNOLOGIES RISK MANAGEMENT AT TURKEY'S STATE UNIVERSITIES

Vildan ATEŞ
Ankara Yıldırım Beyazıt University
Assist. Prof. Dr.
AYBU Business School Esenboğa/ANKARA TURKEY
vates@ybu.edu.tr

Bilal GÜNEŞ
Gazi University
Prof. Dr.
Gazi University Gazi Faculty of Education Beşeveler ANKARA TURKEY
bgunes@gazi.edu.tr

—Abstract —

The aim of this study is to identify factors affecting IT risk management in universities, to explore patterns among these factors and to reveal an IT risk management model. The research universe consists of 548 IT employees in Turkey's state universities' IT centers.

The factors effecting IT risk management success were determined based upon related literature, expert views and a theoretical model has been proposed to successful IT risk management. A quantitative research model was used and an instrument named IT Risk Management Scale (ITRM-S) was developed and used for data collection. The data analyses of this study were done by using SPSS and LISREL programs.

It is found that IT risk management process was affected by human factor, institutional, environmental and technological factors and the model for successful IT risk management have been verified. Results show that institutional, environmental and technological factors directly affect the success of IT risk management. Furthermore, it is seen that human factor affects IT risk management success through environmental factors. Results were compared with literature results and recommendations are presented to researchers and practitioners.

Key Words: *Information technology, IT risk ·management, human factor, structured equation model, Turkey*

JEL Classification: M15, D02, C39, D83.

1. INTRODUCTION

The rapid changes and developments in science and technology make organizations dependent on Information Technologies (IT). IT dependence of institutions brings along a number of IT related risks. This concern has resulted in the emergence of two constructs as Information Technologies Risks and Information Technologies Risk Management since the 1980s. Information Technologies Risks (ITR) is defined as the potential of losing the automation systems, networks or other critical IT resources that may have a negative effect upon the business processes of organizations (Savic, 2008; Teneyuca, 2001). On the other hand, Information Technologies Risk Management (ITRM) is defined as a systematic process where the IT risks are detected, analyzed and managed (Ekelhart, Fenz & Neubaueri, 2009).

Universities are among the primary institutions with the highest IT dependence using IT in the most common and active ways. It is very important to successfully detect, analyze and manage IT related risks in order to enable universities to reach their missions. A successful ITRM will result in a number of benefits to universities including a continuous service for both internal and external stakeholders, a culture with an advanced level of risk awareness, an increased social value (esteem, dignity), an advantage in the process of competition against other universities, and compliance with laws, regulations and standards.

The results of previous studies showed that the university staff and students have very low levels of ITR awareness (Rezgui & Marks, 2008). In addition the lack of sufficient number of studies on universities's IT risk management process is emphasized. Yeo et al. (2007) and Goel and Chen (2010) suggested that there is limited number of studies on the factors affecting the IT risk management and there is a need for new studies on this subject. Kotulic (2001), Saleh and Alfantookh (2011) also suggested that there is a considerable deficiency in the number of studies on security risk management. Aktaş and Soğukpınar (2010) emphasize that risk analysis and management are key concepts in information security activities and they are important to detect, analyze present risks and develop counter measures. It seems that managing IT related risks is a very important process for organizations in order to have secure and effective IT systems.

In reviewing existing studies; a need is found for additional studies that would enable researchers and practioners to determine factors affecting information

technologies risk management (ITRM) and to understand the pattern among these factors. Also there is a need to reveal a current and an integrated ITRM model to succesfully manage IT related risks for universities (Yeo, Rahim & Miri, 2007; Goel & Chen, 2010; Kotulic, 2001; Ahlan & Arshad, 2012).

The objectives of this study include:

i. determining the factors affecting the ITRM of state universities in Turkey and the indicators of these factors,
ii. examining the relationship between these factors and,
iii. reveal an integrated ITRM model involving all the factors being determined to manage IT related risks for universities.

2. PREVIOUS STUDIES ON THE FACTORS AFFECTING THE ITRM

This section examines the literature for factors affecting ITRMS, as well as studies on the indicators of these factors. Examining the relevant studies, it is determined that the primary factors affecting the ITRMS can be classified as being Institutional, Human, Environmental and Technological.

Examining studies on institutional factors; it is seen that these factors involve indicators like information security policies, IT budget, communication, institutional culture and maturity, explicit objectives and goals, explicit and comprehensible missions and top management support. Kraemer, Crayon and Clem (2009) suggest that institutional factors affecting the computer and information security success involve top management support, institutional culture and information security policies. Institutional factors play an important role in making organizational decisions, and they have a strong organizational relationship with IT strategies. Accordingly, institutions are required to be in harmony with IT strategies in order to preserve and reach goals (Park, Ahmad & Ruighaver, 2010). According to Knapp and Marshall (2007) and Kankanhalli et al. (2003), the first indicator supporting and affecting the information security process is top management support, which is among the institutional factors, and other indicators could be ordered as user training, security culture, political compliance and political application.

Another factor is human factor and involves indicators including the experience and competence of IT staff, training, awareness, human mistakes, staff motivation and the number of staff members in the organization (Yıldırım, Akalp, Aytaç & Bayram, 2011; Shields et al., 2014). According to Lacey (2009:136), security is indeed a human problem and human beings irrefutably control the technology.

According to Kraemer, Carayon and Clem (2009), the human factor is a parameter that affects computer and information security gaps and it involves components like human mistakes, performance management, resource management and training.

Environmental factors consist of indicators like natural threats, compliance to standards, political environment and compliance to laws (Yıldırım et al., 2011). Norman and Yasin (2013) investigated the factors effecting information technologies security management success, and they deternined that the indicators of environmental factors involve user success, industry character, technology, infrastructure support and laws. In the study of Yaraghi and Langhe (2011), political environment is reported to be yet another indicator of environmental factors affecting risk management systems. Smith and Jamieson (2013) emphasized that one of the factors affecting the information systems security and business continuity management in e-government applications is laws.

Technological factors comprise yet another factor that may affect IT risk management success. As this study focuses on IT risk management success, the technological factor is evaluated as a separate factor different from Norman and Yasin's (2013) study, which are approached to the technological factor as one of the indicators of environmental factors. Because technological factors involve important indicators like hardware security, software security and critical infrastructure analysis. IT systems should be protected against possible attacks and security gaps. Werlinger, Kirstie and Konstantin (2009) examined the difficulties experienced by institutions in IT security applications based on human, organizational and technological factors. It is suggested that hardware and software upgrades, changes and developments in business operations cause security gaps and blanks (Taney & Costello, 2006). It is also suggested that institutions are required to know the formation possibility and frequency of threats in order to decrease the severity and effect of these threats and choose convenient and effective control methods.

3. METHODOLOGY

This section provides information about the study pattern, population and accessible population. It also includes information about the determination of external factors and indicators affecting the IT risk management of universities, structure of the theoretical model being suggested, and data collection and analysis process used in this study.

This study constitutes a part of a dissertation submitted in Department of Management Information Systems of Informatics Institute at Gazi University in Turkey. The doctoral study was conducted by using the mixed method of research. Only the quantitative section of the dissertation is reported.

3.1. Population and participants

The target population of the study consists of the staff working in the Information Technology (IT) centers in the universities of Turkey. The accessible population of the study, on the other hand, consists of the staff working in the IT centers in state universities of Turkey (N=1569). As it is aimed to reach the entire accessible population, no additional sampling was determined and 35% of the accessible population was reached (n=548 individuals, Female=105, Male=443).

3.2. Determining the external factors affecting the ITRM and their indicators

Being mentioned in the study objectives and considered to be revealed; the development process of the ITRM Model was realized in two stages. In the first stage, the factors considered to be involved in the model and the indicators of these factors were determined. The factors and their indicators were determined by using the findings presented in previous studies and the opinions of nine experts (seven department of industrial engineering and two department of business professors). The final structure of external factors, their indicators, and the theoretical model being suggested are displayed in Figures 1 and 2. In this study, the theoretical model seen in Figure 1 is expected to be explored and confirmed by using structural equation modeling (SEM).

3.3. Development of data collection tool

Information Technologies Risk Management Scale (ITRM-S) was developed as the data collection tool. As seen in Figure 1, items of ITRM-S were developed by using the external factors and their indicators being depicted. While developing the scale, it was aimed to perform a measurement at the interval level via 7 point Likert scale and it was scaled as 1-7 (1. Strongly disagree 7. Strongly agree). ITRM-S consists of 22 observable variables aimed at measuring four latent (Independent) variables (Institutional, Human, Environmental, Technological Factors) affecting the risk management and 6 observable variables aimed at measuring one latent (Dependent) variable (ITRM). The ITRM-S consists 28 items.

The process of generating the scale was started to check the validity of scale items. Firstly a draft scale was generated. Expert opinions were received after

preparing the draft scale. As a result of receiving expert opinions, the Content Validity Rate (CVR) was calculated for each item by using the formula CVR=(N_e-N/2)-1 for the purpose of determining the scale validity. In this study, the CVI was calculated as "1" for Institutional, technological factors and the IT risk management success and "0.97" for human factor and "0.95" for environmental factors. In conclusion, as the CVR and CVI of the entire scale were equal and "0.98" (CVI ≥ CVR), the content validity of the entire scale was observed to be statistically significant.

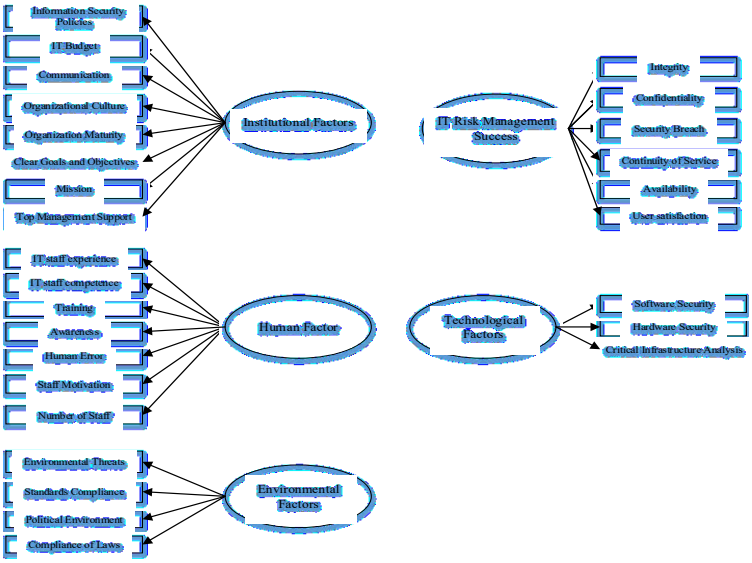

Figure 1. Factors and the indicators of these factors

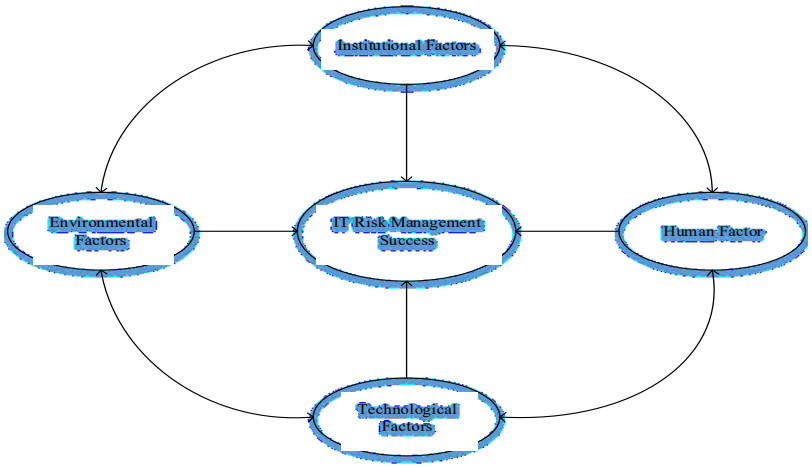

Figure 2. Theoretical model

In order to test the reliability of the ITRM-S, the internal consistency method, which is among the reliability coefficient calculation statistic was used. Cronbach alpha internal consistency method was also used. Cronbach alpha internal consistency coefficient was calculated as α=0.94 for the ITRM-S and this value shows that the scale is highly reliable. Cronbach alpha internal consistency coefficients of factors in the scale were determined as; 0.88 for institutional factors, 0.88 for human factor, 0.80 for environmental factors, 0.77 for technological factors and 0.84 for the IT risk management success. Aftter these analyses, the final form of ITRM-S is generated.

3.4. Data collection

In the study data were collected by reaching the participants both online and directly between January and March, 2014. While collecting the data, 92 out of 108 state universities in Turkey were reached and 548 participants were included in the study. 16 state universities could not be reached.

3.5. Data analysis

The data were analyzed in three stages. During the statistical analysis and evaluation of the data the values of descriptive statistics were examined. Answers were sought to relevant questions by using the techniques of exploratory factor analysis in the second stage and the confirmatory factor analysis in the third stage. While analyzing the data to determine results of descriptive statistics and of the

exploratory factor analysis, the SPSS.17.0 package software was used. SEM was applied for the confirmatory factor analysis and the confirmatory factor analysis was conducted in the LISREL 8.72 computer software.

4. FINDINGS

This section presents findings regarding the exploratory and confirmatory factor analysis that were applied for the IT risk management success being attained via data in the study and external factors that are thought to have an effect upon this success.

4.1. Examining the assumptions

Before applying the exploratory and confirmatory factor analysis for the data set that was collected, it was tested whether or not the data set provided the necessary assumptions for these analyses. The assumptions of analyses involve the compliance of the sample size, as well as normality and linearity (Çokluk, Şekercioğlu & Büyüköztürk, 2010). As a result of the analysis, it was decided that the data set could meet the assumption.

4.2. Findings regarding the exploratory factor analysis

The technics of exploratory factor analysis were applied to the data set in order to examine the construct validity and the factor structure of the scale that was developed in this study. Exploratory factor analysis was performed by using the SPSS 17.0 (Statistical Package for the Social Science) software.

Kaiser-Meyer-Olkin (KMO) coefficient and Barlett Sphericity tests were performed for examining the compliance of the data for the factor analysis and they were determined to be significant (KMO coefficient 0.95 and significance for the Barlett test; 0.00 $p<0.001$). As this value was 0.95, the data structure was evaluated as excellent for the factor analysis. It is observed that the theoretically defined items are collected under their own factors. Examining the total variance being explained, it is observed that there are 5 factors with an eigenvalue greater than 1 in the scale. These factors explain 60% of the total variance. Accordingly, the first factor explains 15% of the total variance, the second factor 14%, the third factor 13%, the fourth factor 10% and the fifth factor 8%. As a consequence, it was observed that the construct validity of the scale was enabled via the exploratory factor analysis.

4.3. Findings regarding the confirmatory factor analysis

In addition to the exploratory factor analysis that was performed for examining the construct validity of the scale, confirmatory factor analysis (CFA) was performed by using the LISREL 8.72 software for determining the compliance of the data being observed with the five-dimensional model. In the CFA application, the correlation matrix that was acquired from 28 items was used as data. As a result of the CFA, the relationships between each latent variable (factor) in Figure 1 and their observable variables were examined by checking the error variances and the t values of observable variables. Finally, the fit indices were evaluated for testing whether or not each model was confirmed. In this study, a two-stage method was adopted and the measurement models were tested. As a result of the analyses and the fit index examinations, the one-factor structure of institutional factors, human factor, environmental factors, technological factors and IT risk management success were confirmed to be a model.

As a result of the confirmatory factor analysis, the chi-square value from the compliance indexes was examined for independent latent variables ($\chi 2$= 618,66; N=548, sd= 203, p= 0.00) and as it was significant, the $\chi 2$/sd rate was checked. The compliance indexes of independent latent variables were observed as RMSEA= 0.06, AGFI=0.88, RMR=0.06, NNFI=0.98, CFI=0.98 and RFI=0.97. As a consequence, examining the compliance indices and criteria for independent latent variables; it was determined that while AGFI had an acceptable compliance, the $\chi 2$/sd rate and RMSEA, RMR and GFI compliance indices had a good compliance. CFI, NNFI, RFI and AGFI values were observed to have an excellent compliance. Finally, the model was confirmed. It is see that there are high relationships (>0.73) between all the factors except for the relationship between the technological factors and institutional factors. The relationship between the technological factors and institutional factors is 0.69 and moderate (Büyüköztürk, 2002; Yılmaz & Çelik, 2009).

The latent and observable variables being suggested in this study were analyzed as a whole. As a result of the confirmatory factor analysis, it was observed that the human factor did not give a significant t value. Accordingly, the human factor was excluded from the model and some modifications were made in the observable variables of K1 and K2 and B2 and B3. The t values were observed to be statistically significant at the level of 0,01 and the error variances varied between 0.36 and 0.72. The compliance indexes of the theoretical model are as; $\chi 2$=878.25 ($\chi 2$/sd=2.5), RMSEA= 0.05, AGFI=0.88, RMR=0.06, NNFI=0.98, CFI=0.98 and RFI=0.97 and while AGFI has an acceptable compliance, $\chi 2$/sd and RMR have a good compliance and RMSEA, NNFI and CFI have an excellent compliance. As a

consequence, the theoretical model will be confirmed in the event of excluding the human factor.

In the event of excluding a factor like the human factor in the model in SEM, it is recommended to carry the analyses a step forward. When dependent and independent variables become the primary question in this stage, the effect caused by multiple independent variables is considered and the indirect (total) effect is acquired from all the factors being obtained. In the second stage, it is required to zero (0) the correlations between the independent variables and obtain the direct effect of all independent variables upon the dependent variable. If the analysis is repeated by setting up the correlation coefficients to zero between the independent variables, a model called direct effect model will be obtained.

After repeating the analyses by setting up the correlation coefficients between all the independent variables to zero, the following results were obtained. Examining the t values of all items in the direct effect model, they were observed to be significant at the level of 0.01. While the rates of observable variables being defined to explain the latent variable varied between 0.75 and 0.95; the error variances of observable variables varied between 0.38 and 0.77. The compliance indexes of the direct effect model were as $\chi 2$ =2032 ($\chi 2$/sd=5.9*)*, (2032/343), which signified an acceptable compliance. The AGFI value was 0.75 and the RMR value was 0.28, which signified an unacceptable compliance. On the other hand, other values were as; RMSEA 0.09 NNFI 0.94 and CFI 0.95, which signified an acceptable compliance, whereas RFI 0.93 showed a good compliance. As a consequence, the model was confirmed. It was concluded that the t values between all the independent latent variables (structural model) in the IT risk management model were significant at the level of 0.01 and as the human factor did not give a significant t value in the theoretical model, the human factor was mediated by one of the three other factors (institutional, environmental and technological factors).

In order to determine which independent latent variable mediated the human factor, analyses were repeated via each of the institutional, technological and environmental factors in the LISREL software. As a result of the three analyses, as the lowest t value (0.03) was obtained when the human factor was mediated by environmental factors, it was decided that the human factor was mediated by environmental factors and the analyses were repeated. Examining the compliance indexes for the mediator variable IT risk management model; AGFI was 0.86, which signified an acceptable compliance, whereas RMSEA was 0.06 and RMR

0.06, which signified a good compliance. Additionally, RFI was 0.96, NNFI 0.98, CFI 0.98 and RFI 0.96, which signified an excellent compliance. As a consequence, the mediator variable IT risk management model being built was confirmed (Figure 3).

Table 1. Regressional relationships among models' variables

Model name	Dependent variable	Independent variables				
		Institutional factors	Human factor	Environmental factors	Technological factors	R^2
Theoretical model	ITRM success	0,20	-	0,31	0,33	0,57
Direct effect model	ITRM success	0,28	0,22	0,31	0,35	0,35
Mediator variable model	ITRM success	0,20	-	0,30	0,35	0,56

Table 1 shows the causal relationships between four independent variables (institutional factors, human factor, environmental and technological factors) and the dependent variable (IT risk management success) of theoretical, direct effect and mediator variable models. Accordingly, regarding the theoretical model, the variable with the greatest effect upon the IT risk management success is technological factors (33%), which is followed by environmental factors (31%) and institutional factors (20%). In the direct effect IT risk management model, the variable with the greatest effect upon the IT risk management success is technological factors (35%), which is followed by environmental factors (31%), institutional factors (28%) and the human factor (22%). In the mediator variable IT risk management model, on the other hand, the variable with the greatest effect upon the IT risk management success is technological factors (35%), which is followed by environmental factors (30%) and institutional factors (20%).

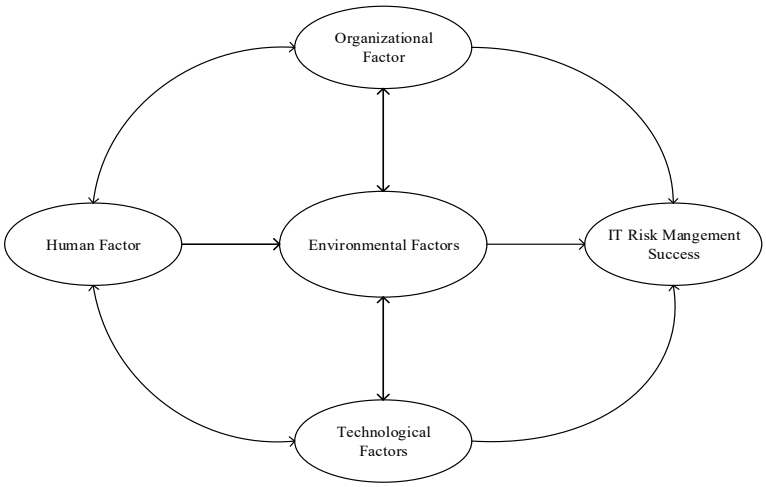

Figure 3. Reached model

As is seen in Table 1, the coefficient of determination in this study (R^2) is 0.57 for the theoretical model, 0.35 for the direct effect model and 0.56 for the mediator variable IT risk management model. It is observed that the external factors (institutional, human, environmental and technological factors) affecting the IT risk management in state universities in Turkey explain 57% of the IT risk management in the theoretical model, 56% in the mediator variable model and 35% in the direct effect model.

5. CONCLUSION AND SUGGESTIONS

This section involves the study results and the relevant suggestions. This study is aimed at determining the external factors affecting the IT risk management success of universities and their indicators, as well as the pattern between the factors and presenting an IT risk management model.

There is a pattern between the external factors affecting the IT risk management success, which include institutional factors, human factor, environmental and technological factors. According to the program outputs, three different models were confirmed (theoretical model, direct effect model and mediator variable IT risk management model) and the IT risk management model was attained.

Institutional factors are observed to have an effect upon the IT risk management model. The studies being conducted emphasize that institutional factors play a determinant role in the IT risk management success (Al-awadi & Renaud, 2007; Chang & Ho, 2006; Knapp & Marshall, 2007; Tohidi, 2011).

Human factor apparently has no effect upon the theoretical IT risk management model and the mediator variable IT risk management model. However, it has a significant effect upon the direct effect model. In the mediator variable model, the human factor affects the IT risk management via environmental factors (Figure 3). Studies from the literature also emphasize that the human factor affects the IT risk management and plays a role in information security and risk management (Kraemer, Carayon & Clem, 2009; Landoll, 2006). According to Lacey (2009), security is actually a human problem. Individuals control the technology; otherwise is unimaginable. In another study, the researchers suggest that the human factor is one of the two critical components required for the success of security programs being applied in institutions (Ang et al., 2006). In their study, Jahner and Kremar (2005) suggest that as well as technological factors; the top management support, human factor, IT infrastructure of institutions and the structure of institutions are effective upon the IT risk management. In their study, Yıldırım et al. (2011) emphasize that the processes of information security and IT risk management consist of complex processes that are affected by a number of factors like human factor, education and technology, and it is required to manage them under a single roof. According to Kairab (2005), if the institution staff are not aware of the information security policies and are unable to receive the convenient training, the workers will probably fail to follow the security policies and the risk management processes.

Environmental factors are observed to have an effect upon the IT risk management model Findings from this study support the view in literature suggesting that environmental factors have an effect upon the IT risk management model (Norman & Yasin, 2013; Kvavik, Robert & Voloudakis, 2006). Technological factors are observed to have an effect upon the IT risk management model. Similarly, the study results in the literature also emphasize that technological factors have an effect upon the IT risk management model. Accordingly, in their study, Werlinger et al. (2009) state that technological factors have an effect upon the IT risk management process and they separate the technological factors into three sub-factors of mobility, gaps and the support of security devices. According to Vellani and Owles (2007), it is required to collect information about the important technological factors in the IT risk evaluation process like network topology, system security infrastructure, identity validation and use them in the IT risk evaluation process.

In this study, the technological factors were observed to have the greatest effect upon the IT risk management in state universities in Turkey. The second factor

with the greatest effect upon the IT risk management process of state universities in Turkey is environmental factors and they have prominent indicators like compliance with standards and laws and the attitude of political environment. In this study, the third factor with the greatest effect upon the IT risk management is institutional factors. Human factors affect IT risk management success via environmental factors and they are required to efficiently apply the IT risk management process. Failure to address human factors may pose an important obstacle for universities in pursuing their missions. Accordingly, it is important that university staff members become aware of threats to security and trained in the field of IT. The IT staff should be specifically trained about current IT threats and risks and become competent in these subjects. In addition to this, the entire university staff should receive basic training in using IT. These steps reduce usage errors made by the institution staff.

In the future, the studies can be done to examine the effectivenes of the proposed models to manage IT related risks for universities. In addition, this study could be advanced to include all universities or other institutions in Turkey. Further, it may be recommended that possible contributions of implementing this model in other locations be determined.

BIBLIOGRAPHY

Ahlan, Abd Rahman and Arshad, Yusri (2012), "Information Technology Risk Management: The Case Of The International Islamic University Malaysia", *Journal Of Research And Innovation In Information Systems,* No: 1, pp. 58-67.

Aktaş, F.Özden and Soğukpınar, İbrahim (2010), "Bilgi Güvenliğinde Uygun Risk Analizi ve Yönetimi Yönteminin Seçimi İçin Bir Yaklaşım", *TBV Bilgisayar Bilimleri ve Mühendisliği Dergisi*, Vol. 3, pp. 53-62.

Al-Awadi, Maryam and Renaud, Karen (2009), "Success factors in information security implementation in organizations", *IADIS International Conference e-Society*.

Ang, Wee Horng; Lee Yang W; Madnick Stuart E.; Mistress Dinsha and And Siegel, M. (2006, August). "House of security: Locale, roles and resources for ensuring information security". *Conference on Information Systems*, Acapulco, Mexico.

Büyüköztürk, Şener (2002), "Faktör Analizi: Temel Kavramlar ve Ölçek Geliştirmede Kullanımı", *Kuram ve Uygulamada Eğitim Yönetimi,* Vol. 32, pp. 470-483.

Chang Shuchih. E. and Ho Chienta B. (2006), "Organizational factors to the effectiveness of implementing information security management", *Industrial Management & Data Systems*, Vol. 106, pp.345-61.

Çokluk Ömer, Şekercioğlu Güçlü and Büyüköztürk Şener (2010), *Sosyal bilimler için çok değişkenli istatistik SPSS ve LISREL uygulamaları* (First Edition). Ankara: Pegem Publishing.

Ekelhart, Andreas; Stefan, Fenz and Neubauer, Thomas (2009, January), "AURUM: A Framework for Information Security Risk Management" *42nd International Conference on System Sciences*, Hawaii, pp.1-10.

Giles, David C. (2002), "Qualitative research in psychology", Advanced research methods in psychology. London: Routledge.

Goel, Sanjay and Chen, Vicki. (2010), "Information Security Risk Analysis–A Matrix-Based Approach". *Information Resources Management Journal*, Vol.23, No.2, pp.33-52.

Jahner, Stefanie and Krcmar, Helmut (2005), "Beyond Technical Aspects of Information Security: Risk Culture as a Success Factor for IT Risk Management", The *Americas Conference on Information Systems,* pp. 462.

Kairab, Sudhanshu (2005), *A practical guide to security assessments (*First Edition). Boca Raton, FL: Auerbach Publications, pp. 23.

Kankanhalli, Atreyi; Teo, Hack-Hoi; Tan, Bernard C. Y.and Wei, K-K. (2003), "An Integrative Study of Information Systems Security Effectiveness", *International Journal of Information Management*, Vol. 23, No: 2, pp.139-154.

Knapp, Kenneth. J. and Marshall, Thomas E. (2007), "Top Management Support Essential for Effective Information Security" In Tipton, H. F. & Krause, M. (Eds.), *Information security management handbook* (6th edition), Boca Raton, FL: Auerbach Publications, pp. 51-58.

Kotulic, Andrew G. (2001), *The Security Of The IT Resource And Management Support: Security Risk Management Program Effectiveness*, Unpublished Doctora Thesis, The University Of Texas At Arlington, USA.

Kraemer, Sara; Carayon, Pascale and Clem, John. (2009), "Human and organizational factors in computer and information security: Pathways to vulnerabilities", *Computers & Security*, Vol. 28, pp. 509–520.

Kvavik, Robert B and John Voloudakis (2006), "Safeguarding the Tower: IT Security in Higher Education", *Educase Center For Applied Research (ECAR),* Vol. 6, pp. 21-43.

Lacey, David (2009), *Managing the Human Factor in information security: How to win over staff and influence business managers* (First Edition). England: Wiley & Sons, pp.134-137.

Norman, Anir A. and Yasin, Mord N. (2013), "Information systems security management (ISSM) success factor: Retrospection from the scholars". *African Journal of Business Management*, Vol: 7, No. 27, pp. 2646-2656.

Park, Sangseo; Ahmad, Atif and Ruighaver, Anthonie B. (2010, April), "Factors Influencing the Implementation of Information Systems Security Strategies in Organizations", *International Information Science and Applications Conference*, Seoul, Korea, pp. 1-6.

Rezgui, Yacine and Marks, Adam (2008), "Information security awareness in higher education: An exploratory study", *Computers&Security*, Vol. 27, No. 7-8, pp. 241-253.

Saleh, Mohamed.S and Alfantookh, Abdulkader (2011), "A new comprehensive framework for enterprise information security risk management", *Applied Computing and Informatics*, Vol. 9, No. 2, pp. 107–118.

Savic, Ana (2008), "Managing It-Related Operational Risks", *Ekonomski Annals,* Vol. 53, No. 176, pp. 88-109.

Shields, Tyler; Balaouras, Stephanie; Johnson, David K. and Frechette, Thayer (2014), "Raise The Security Bar With Human-Factor-Friendly Design Concepts", Forrester Research Report.

Taney, Francis. X. Jr and Costello, Thomas (2006), "Securing the whole enterprise: Business and legal issues", *IT Professional*, Vol. 8, No. 1, pp. 37-42.

Teneyuca, David (2001), "Organizational Leader's Use of Risk Management for İnformation Technology", *Information Security Technical Report*, Vol. 6, No. 3, pp. 54-59.

Tohidi, Hamid (2011), "The Role of Risk Management in IT systems of organizations", *Computer Science*, Vol. 3, pp. 881–887.

Vellani, Karim H. and Robert E. Owles (2007),"Vulnerability and Risk Assessments in the Environment of Care", *Journal of Healthcare Protection Management*, Vol. 23, No. 2, pp. 67-77.

Werlinger, Rodrigo; Hawkey, Kirstie and Beznosov, Konstantin (2009), "An integrated view of human, organizational, and technological challenges of IT security management", *Information Management & Computer Security*, Vol. 17, No. 1, pp. 4-19.

Yaraghi, Niam and Langhe, Roland G. (2011), "Critical success factors for risk management systems*", Journal of Risk Research*, Vol.14, No:5, pp. 551-581.

Yeo, Ai. C; Rahim, Mahbubur. M. And Miri, Leon (2007, April), "Understanding factors affecting success of information security risk assessment: The case of an Australian higher education institution*", 11th Pacific Asia Conference on Information Systems*, University of Auckland, Auckland New Zealand, pp.1-12.

Yıldırım, Ebru Y; Akalp, Gizem; Aytaç, Serpil and Bayram, Nuran (2011), "Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey*". International Journal of Information Management*, Vol.31, No. 4, pp. 360-365.

Yılmaz, Veysel and Çelik, Eray H. (2009), *LISREL ile Yapısal Eşitlik Modellemesi–1* (First Edition). Ankara: Pegem Academy, pp.29.