American Journal of Theoretical and Applied Business
2016; 2(4): 28-37
http://www.sciencepublishinggroup.com/j/ajtab
doi: 10.11648/j.ajtab.20160204.11
ISSN: 2469-7834 (Print); ISSN: 2469-7842 (Online)

Identifying Key Success Factors in the Implementation of Information Security Systems on Service Businesses: A Case Study of the Private Banks of Tehran

Reihaneh Amel Sadeghi

Economy Department, Ferdowsi University, Mashad, Iran

Email address:
Amel_sadeghi_r@yahoo.com

To cite this article:
Reihaneh Amel Sadeghi. Identifying Key Success Factors in the Implementation of Information Security Systems on Service Businesses: A Case Study of the Private Banks of Tehran. *American Journal of Theoretical and Applied Business.* Vol. 2, No. 4, 2016, pp. 28-37.
doi: 10.11648/j.ajtab.20160204.11

Received: October 17, 2016; **Accepted**: November 26, 2016; **Published**: December 20, 2016

Abstract: Nowadays, the critical role of information in global markets is inevitable. This importance is much stronger especially in the fields of finance and credit. Because of the expansion of private banks and ceding the shares of many state banks to the private sector, and due to the hasty deployment of electronic systems in these banks, the health of financial activities in the market, to a great extent, depends on the correct performance of information security systems in electronic sections. Launching information security systems is a costly activity which is associated with financial resources and information security. Hence, the factors that lead to higher effectiveness in this process should be identified. This study is an attempt to identify such factors. The reviews resulted in identification of 39 preliminary variables in the form of a questionnaire which was distributed to 131 branch managers of private banks in Tehran, Iran. Convergent validity and composite reliability combined with Cronbach's alpha coefficient were used to evaluate the questionnaire, which all supported the validity and reliability of the questionnaire. The results indicated that these factors had the highest priority: presence of regulatory and appropriate processes, availability of key performance indicators, controlling viruses, etc. Furthermore, the confirmatory factor analysis revealed that there are four infrastructural groups, the most important of which is the group of financial factors. Finally, the correlation between these structures was examined. Confirmatory factor analysis was done by PLS (2β) software, and demographic and Friedman analyses were performed by SPSS (20) software.

Keywords: Information Security Systems, Key Success Factors, Private Banks

1. Introduction

Management Information Systems (MIS) plays a vital role in today's business market. Its results appear in the effects it has on human and material resources of business. The main function of MIS is to provide comprehensive and proper information for making best decisions (Hassan, Zhi, Wang, & Abdalla, 2014). Given such an important and effective functioning, maintaining such systems as MIS is a management task which should be considered seriously.

Information systems may be influenced by many factors but the effects do not necessarily provide positive results for the process of making decision in business. In other words, the system may be faced with threats. These threats encompass a wide range of factors that are providing negative results for the organization. These include the occurrence of natural and physical incidents, access to the system by competitors, inadequate control on the media and many other threats. Furthermore, threats are in a dynamic state and hence they change over time (Robert, 2009). Information security systems have evolved to act against these threats. Information security means to protect the confidentiality (ensuring that only authorized individuals have access to it), integration (protecting the authenticity and integrity of information and processing methods) and availability (ensuring that competent people are able to access the information when needed) (Mellado, Fernández-Medina, & Piattini, 2007). Therefore, the systems creating

these features for the information are called information security systems (Huang et al., 2004).

However, implementation of information security systems in business, regarding their nature, is a capital-intensive activity and hence widely influences the assets and business activities. As creating such systems can ensure the confidentiality, integrity and availability of information for businesses, failure to set up such systems leads to waste of resources for businesses and even a small defect in the installation process may lead to serious damage during the deployment stages. So far, not so many studies have examined the effective factors in successful implementation of information security systems. For example, Al-Awadi and Renaud (2007) cited variety of factors such as awareness and training, management support, funding, and implementation of strategies and organizational mission in successful implementation of information security systems (Al-Awadi & Renaud, 2007). The factors mentioned above are somehow general and are not so effective in the field of business policy. Thus, in the present study, the researchers took a field approach in order to identify success factors in the implementation of information security systems, and also relatively prioritize them. Finally, she took a statistics-based approach to group these factors.

2. Literature Review

Anders (2011) defines information security as: protecting information and information systems from unauthorized access, use, disclosure, disruption, destruction and unauthorized modification (Andress, 2011). Zidane et al (2011) cited information security as a scientific background addressing issues related to data protection and information against invaders or security threats (Zaidan, Zaidan, & Kiah, 2011). Broadly speaking, information security deals with the information assets and the organization's ability to maintain an appropriate level of confidentiality, integrity and availability. Accountability and stable accessibility are also among these features. Security information is a set of actions to minimize the risk of damage to the confidentiality, integrity, availability and accountability of information systems (Åhlfeldt, 2005). The review of research literature in this field suggests that not so many studies, so far, investigated a comprehensive and organized review of the factors that lead to successful implementation of information security systems. However, all the few studies that explicitly or implicitly have cited these factors are presented in the following.

Setiadi et al (2013) have classified success factors for implementing information security systems into four groups. According to the researchers, these factors include: (1). Factors related to leadership: the active support of senior management, information security policy, (2). Financial factors: funding, (3). factors of organizational culture: Awareness and training of staff, past negative experiences, job responsibilities, employee motivation (4). Technical factors: protection of information assets, maintaining the integrity of electronic records, compliance with standards, using the services of external consultants (Setiadi, Sucahyo, & Hasibuan, 2013). Furthermore, Waly et al proposed that factors influencing the success in the implementation of information security include: communications, risk management, reward and punishment, definition of roles and responsibilities, reporting events, motivation, recovery after the events, awareness, get feedback, sanctions, beliefs, attitudes, tendencies, behavior, continuous training, effective training, continuous assessment and stability of security in the organization (Waly, Tassabehji, & Kamala, 2012).

Al-Awadi (2009), as a measurement tool in his doctoral thesis, stated that the success factors in the implementation of information security include:

- clear organizational goals about information security
- information security practices with regard to corporate culture
- clear commitment to management
- a clear understanding of the information security risks
- a clear understanding of the requirements for information security
- regular and effective employee awareness about information security program
- practicalizing information security program
- providing appropriate training staff
- allocating adequate funding
- organization's IT infrastructure (Al-Awadi, 2009)

In his paper, presented in 2007, Al-Awadi had proposed these concepts in the form of: Awareness and training, management support, funding, and implementation of strategies and organizational mission in successful implementation of information security (Al-Awadi & Renaud, 2007).

Some studies have also suggested a different approach. For example, Hagan et al (2008) expressed that since success is measured by the effectiveness, four perspectives can be deduced in the field of information security: (1). risk management, (2). economic standpoint, (3). legal standpoint and (4). cultural perspective. According to these authors, indicators of effectiveness (success factors) in information security include:

- availability of information security guidelines for the staff
- policy
- non-disclosure agreement
- participation in information security groups
- user instructions
- internal assessment
- risk analysis
- guidelines for communication systems
- availability of action plans in the event of emergencies
- user training
- senior management involvement
- user participation
- awareness
- system for announcing events / conditions

- external evaluation (audit)
- classification of persons and property
- availability of the regular processes
- availability of key performance indicators (Hagen, Albrechtsen, & Hovden, 2008)

Fitzgerald (1995) proposed that the process of establishing an information security, considering 10 key subjects is important. These include:

- Information security policy document: a written document about information security should be available to all employees who are working in this area.
- Allocation of information security responsibilities: responsibilities related to the protection of individual assets and specific security processes should be clearly defined.
- Education and training: users should be given adequate security and technical training.
- Reporting security events: security events should be reported using appropriate channel and as soon as possible.
- Virus control: tools for detecting and preventing viruses, as well as the necessary knowledge, should be provided to people.
- Business continuity-planning process: there should be a managed process available for developing and maintaining business continuity plans.
- Control private copying: materials subject to copyright should not be copied without the permission of original owners.
- Protection of business records: important records should be protected from loss, destruction and falsification.
- Compliance with data protection regulations: all requests that are dealing with personal data must comply with the principles and rules of data protection.
- Compliance with security policy: systems should be reviewed regularly to ensure their compliance with security policies and standards (Kevin, 1995).

Kazemi et al (2012), while examining the factors influencing successful security management system, have concluded that these factors include:

- senior management support
- information security policy
- awareness and training programs
- job responsibilities
- compliance with international standards of information security
- motivating employees
- using the services of security advisers outside the organization (Kazemi, Khajouei, & Nasrabadi, 2012)

Table 1, briefly indicates the key success factors in the implementation of information security in terms of existing literature:

Table 1. *Summary of the Key Success Factors in Implementation of Information Security Systems Based on the Literature Review.*

No	Factors	Refrences
1	Active support of the senior management	Kazemi et al., 2012; Hagen et al., 2008; Setiadi et al., 2013; Al-Awadi, 2009; Al-Awadi & Renaud, 2007
2	Application of information security policy in the organization	Setiadi et al., 2013; Al-Awadi, 2009; Al-Awadi & Renaud, 2007; Hagen et al., 2008; Kevin, 1995; Kazemi et al., 2012
3	Allocation of financial resources	Al-Awadi & Renaud, 2007; Al-Awadi, 2009; Setiadi et al., 2013
4	Staff awareness of information security program	Setiadi et al., 2013; Waly et al., 2012; Al-Awadi & Renaud, 2007; Al-Awadi, 2009; Hagen et al., 2008; Kazemi et al., 2012
5	Learning from past experiences	Setiadi et al., 2013
6	Defining the roles and responsibilities	Kazemi et al., 2012; Kevin, 1995; Waly et al., 2012; Setiadi et al., 2013
7	Motivating employees	Setiadi et al., 2013; Waly et al., 2012; Kazemi et al., 2012
8	Protection of information assets	Setiadi et al., 2013; Kevin, 1995
9	Maintaining the integrity of electronic records	Hagen et al., 2008; Setiadi et al., 2013;
10	Compliance with approved and accepted standards of information security	Al-Awadi & Renaud, 2007; Setiadi et al., 2013; Kevin, 1995; Kazemi et al., 2012
11	Using the services of external consultants	Setiadi et al., 2013; Hagen et al., 2008; Kazemi et al., 2012
12	Defined and effective communication	Hagen et al., 2008; Waly et al., 2012
13	Risk management	Hagen et al., 2008; Waly et al., 2012; Al-Awadi, 2009
14	Reporting and documentation of events	Kevin, 1995; Hagen et al., 2008; Waly et al., 2012
15	The existence of recovery system after the events	Hagen et al., 2008; Waly et al., 2012
16	Receiving feedback	Waly et al., 2012
17	The existence of counter-sanctions system	Waly et al., 2012
18	Positive beliefs associated with information security	Waly et al., 2012
19	Positive attitude to information security	Waly et al., 2012
20	The propensity of individuals to information security	Waly et al., 2012
21	Proactive behavior of individuals in the implementation of information security systems	Waly et al., 2012
22	Availability of continuing professional education system	Kazemi et al., 2012; Kevin, 1995; Hagen et al., 2008; Al-Awadi & Renaud;,2007 Al-Awadi, 2009; Waly et al., 2012
23	The effectiveness of staff training system	Waly et al., 2012
24	Continuous measurement of performance	Hagen et al., 2008; Waly et al., 2012
25	Stability of security in the organization	Waly et al., 2012
26	Applying information security with regard to organizational culture	Al-Awadi, 2009
27	A clear understanding of the requirements for information security	Al-Awadi, 2009

No	Factors	Refrences
28	Practicalizing information security program	Kevin1995 ,; Al-Awadi, 2009
29	The Information Technology Infrastructure	Al-Awadi, 2009
30	Alignment with organizational mission	Al-Awadi & Renaud, 2007
31	Non-Disclosure Agreement	Hagen et al., 2008
32	Participation in the groups of information security	Hagen et al., 2008
33	Existence of user instructions and manuals	Hagen et al., 2008
34	User participation	Hagen et al., 2008
35	The existence of regular and appropriate processes	Hagen et al., 2008
36	The existence of key performance indicators	Hagen et al., 2008
37	Virus control	Kevin, 1995
38	Control personal copying	Kevin, 1995
39	Following the data protection regulations	Kevin, 1995

3. Research Methodology

The present study is an applied one in terms of the purpose, and according to the method of data collection, given that none of the variables can be controlled or modified, the study is a non-experimental (descriptive) research. The approach to data analysis of the study is the correlation with confirmatory factor analysis techniques. The population of the study includes IT managers of private bank branches in Tehran. Our investigation revealed that there are 2170 private bank branches in Tehran. Therefore, a limited sampling relationship was used in this study. In this relation, presented in the following, Z is the coefficient of normal distribution to a confidence interval of 95% (equal or 1.96); P is the probability of observing the trait of interest (from a total of 20 managers who answered a pilot questionnaire, 14 people expressed that they have been somehow involved in information security. This ratio is equal to 90%) (Sarmad, Bazargan and Hejazi, 2008); and D is the considered margin of error (5 percent).

$$n = \frac{NZ^2P(1-P)}{d^2(N-1)+Z^2P(1-P)} \quad (1)$$

(Daniel, 1999)

Hence, we will have:

$$n = \frac{2170*1.96^2*0.9(1-0.9)}{0.05^2(2170-1)+1.96^2*0.9(1-0.9)} = 131$$

Therefore, in this study, 131 people were chosen from a total of aforementioned managers. Sampling approach in this study is random sampling, which has been applied in table 2 respectively.

Table 2. *Number of Branches and Share in the Sample.*

No	Bank Name	Number of Branches in Tehran	Percentage of Total	Share in the Sample	Total
1	Eghtesad Novin	107	4.93%	6	2170
2	Parsian	35	1.61%	2	2170
3	Karafarin	20	0.92%	1	2170
4	Saman	81	3.73%	5	2170
5	Pasargad	196	9.03%	12	2170
6	Sarmaye	40	1.84%	2	2170
7	Sina	48	2.21%	3	2170
8	Shahr (City)	58	2.67%	4	2170
9	Day	55	2.53%	3	2170
10	Ansar	88	4.06%	5	2170
11	Tejarat	348	16.04%	21	2170
12	Refah Kargaran	131	6.04%	8	2170
13	Saderat	434	20.00%	26	2170
14	Mellat	287	13.23%	17	2170
15	Hekmat Iranian	8	0.37%	0	2170
16	Gardeshgari (Tourism)	23	1.06%	1	2170
17	Iran Zamin	25	1.15%	2	2170
18	Ghavamin	9	0.41%	1	2170
19	KhavarMianeh	8	0.37%	0	2170
20	Ayandeh	92	4.24%	6	2170
21	Mehr Eghtesad	77	3.55%	5	2170
Total		2170	100.00%	131	2170

Data collection for this study was conducted through the use of questionnaire. The questionnaire consisted of two parts: in the first part the demographic characteristics of the subjects was measured, and in the second part the key success factors in the implementation of information security based on a five-point Likert spectrum was given to the experts in order to determine the priority. Determining validity in terms of construct validity was conducted by convergent and divergent validity and due to the necessity of presenting it along with the model, it is presented in the

analysis section. Coefficient of Cronbach's alpha is presented as the reliability index in the same section as well. In general, the results support the desired validity and reliability of the data collection tool.

4. Data Analysis

Data analysis includes the following steps.

4.1. Demographic Characteristics of Subjects

Analysis of the data collected in this study first conducted by examining demographic characteristics of the subjects. Table 3 shows the demographic characteristics of the subjects.

Table 3. *Demographic Characteristics of Subjects.*

	Groups	Frequency	Percent	Valid percent	Cumulative percent
Sex	Female	28	21.4	21.4	-
	Male	103	78.6	78.6	100
Age	26 to 30	4	3.1	3.1	3.1
	31 to 35	1	0.8	0.8	3.8
	36 to 40	51	38.9	38.9	42.7
	Older than 40	75	57.3	57.3	100
Level of Education	Bachelor's Degree	104	79.4	79.4	79.4
	Master's Degree	26	19.8	19.8	99.2
	PhD	1	0.8	0.8	100
The Years of Service	5 to 10 years	6	4.6	4.6	4.6
	10 to 15 years	98	74.8	74.8	79.4
	More than 20 years	27	20.6	20.6	100
Total		131	100	100	

The study of demographic characteristics of the subjects showed that the subjects studied in this research were in good status in terms of education and service records; hence they were eligible to respond to the questionnaire.

4.2. Priority of the Key Success Factors

In the following, the relative priority of each of the key success factors in the implementation of information security has been provided. This prioritization is performed using Friedman's ANOVA analysis. The significance level for this test is equal to 0.000 and less than 0.05 indicating a lack of equality between the variables' points in terms of mean. This shows the feasibility of their prioritization.

Table 4. *The Relative Priority of Key Success Factors in the Implementation of Information Security Systems.*

Priority	Factor	Average Rank
1	The existence of regular and appropriate processes	29.29
2	The existence of key performance indicators	29.29
3	Virus control	28.74
4	Control personal copying	24.92
5	Positive beliefs associated with information security	24.53
6	Existence of user instructions and manuals	23.44
7	Protection of information assets	23.33
8	Positive attitude to information security	23.08
9	Motivating employees	23.03
10	Staff awareness of information security program	22.91
11	Following the data protection regulations	22.66
12	Reporting and documentation of events	21.82
13	The effectiveness of staff training system	21.59
14	Defined and effective communication	21.46
15	Maintaining the integrity of electronic records	21.44
16	Application of information security policy in the organization	21.24
17	Allocation of financial resources	19.94
18	User participation	19.94
19	Proactive behavior of individuals in the implementation of information security systems	19.93
20	The existence of recovery system after the events	19.85
21	Alignment with organizational mission	19.69
22	Practicalizing information security program	19.59
23	Defining the roles and responsibilities	18.21
24	The existence of counter-sanctions system	18.16
25	Using the services of external consultants	18.09
26	Non-Disclosure Agreement	17.98
27	Participation in the groups of information security	17.98
28	Risk management	17.85
29	Applying information security with regard to organizational culture	17.83
30	Compliance with approved and accepted standards of information security	17.52
31	Receiving feedback	17.21
32	A clear understanding of the requirements for information security	16.63
33	Stability of security in the organization	16.44
34	The Information Technology Infrastructure	15.74
35	Availability of continuing professional education system	15.63
36	The propensity of individuals to information security	15.51
37	Active support of the senior management	14.05
38	Continuous measurement of performance	12.37
39	Learning from past experiences	11.08

So, in general, it is clear that among the factors influencing successful implementation of information security systems, "existence of regular and appropriate processes" and "learning from past experiences" are given the highest and lowest priority respectively. The relative priority of other factors is presented in the table above.

4.3. Final Results of Confirmatory Factor Analysis

With regard to determining the relative priority of factors influencing the success in the implementation of information security, there is a need to determine the underlying factors

causing this phenomenon. Therefore, in accordance with the remarks of Karakaya and Canel (1998) and Karakaya and Stahl (1992), we make an effort to identify the factors described above through using factor analysis (Karakaya & Chanel, 1998; Karakaya & Stahl, 1992). On the other hand, given the specificity of preliminary groups (factors), confirmatory factor analysis conducted in four groups identified by Setadi and et al (2013) including: 1. Factors related to leadership (and management), 2. Financial factors, 3. Factors of organizational culture and 4. Technical factors. The final results of confirmatory factor analysis are presented in Table 5. It should be noted that the following table is the final version, so the factor loadings less than 0.4 (Chin, 1998) or factors which their existence on the research model caused drastic decrease of the validity (Abdi, 2003) were excluded from the model. These factors include:

- The structure of "leadership-managerial factors"
  - defining the roles and responsibilities
  - motivating employees
  - personal copy control
- no variable was removed from the structure of "financial factors"
- The structure of the factors for "organizational culture"
  - proactive behavior of the individuals in the implementation of information security systems
  - positive beliefs about the information security
  - learning from past experiences
- The structure of "technical factors"
  - maintaining the integrity of electronic records
  - compliance with approved and accepted standards of information security
  - comply with data protection regulations
  - existence of regular and appropriate processes
  - using the services of external consultants
  - receiving feedback
  - protection of information assets

Table 5. *Summary of the Final Results of Confirmatory Factor Analysis.*

No	Factor	Factor Symbol	Structures			
			Managerial-leadership factors	Organizational culture factors	Financial factors	Technical factors
1	Applying information security with regard to organizational culture	F26	0.839			
2	Non-Disclosure Agreement	F31	0.783			
3	Application of information security policy in the organization	F2	0.706			
4	Practicalizing information security program	F28	0.685			
5	Alignment with organizational mission	F30	0.678			
6	The existence of counter-sanctions system	F17	0.645			
7	Active support of the senior management	F1	0.591			
8	Risk management	F13			0.777	
9	Allocation of financial resources	F3			0.741	
10	The existence of key performance indicators	F36			0.637	
11	Reporting and documentation of events	F14				0.810
12	Existence of user instructions and manuals	F33				0.794
13	Virus control	F37				0.717
14	The Information Technology Infrastructure	F29				0.703
15	Continuous measurement of performance	F24				0.699
16	The existence of recovery system after the events	F15				0.694
17	Proactive behavior of individuals in the implementation of information security systems	F22				0.688
18	The effectiveness of staff training system	F23				0.598
19	Positive attitude to information security	F19		0.689		
20	The propensity of individuals to information security	F20		0.622		
21	Stability of security in the organization	F25		0.878		
22	A clear understanding of the requirements for information security	F27		0.770		
23	Participation in the groups of information security	F32		0.761		
24	User participation	F34		0.670		
25	Staff awareness of information security program	F4		0.669		
Average Variance Extracted (AVE)			0.501	0.528	0.519	0.512
Composite Reliability (CR)			0.874	0.885	0.762	0.892
Cronbach's alpha			0.831	0.848	0.758	0.862

Finally, from among 39 variables that we had at the beginning of the analysis, 25 variables remained as the key success factors in the implementation of information security systems. Also, the final results of confirmatory factor analysis revealed that for all structures the average variance extracted (AVE) was above 0.5 and the composite reliability was higher than 0.707. Akin (2009) believes that these values are sufficient to confirm the validity and reliability of structures (Akin, Bloemhof, Wynstra, & van Raaij, 2009). The Cronbach's alpha value for all structures is above 0.6. Moss et al (1998) believe that this is another confirmation of the reliability of structures (Moss et al., 1998).

4.4. Correlation Between Research Structures

In the following, the relative priority of each of the identified structures will be examined according to their average rating and using Friedman ANOVA analysis. The significance level for Friedman test is equal to 0.00 and smaller than 0.05. Therefore, it is possible to prioritize the structures according to their average rating. The rating is presented in Figure 1.

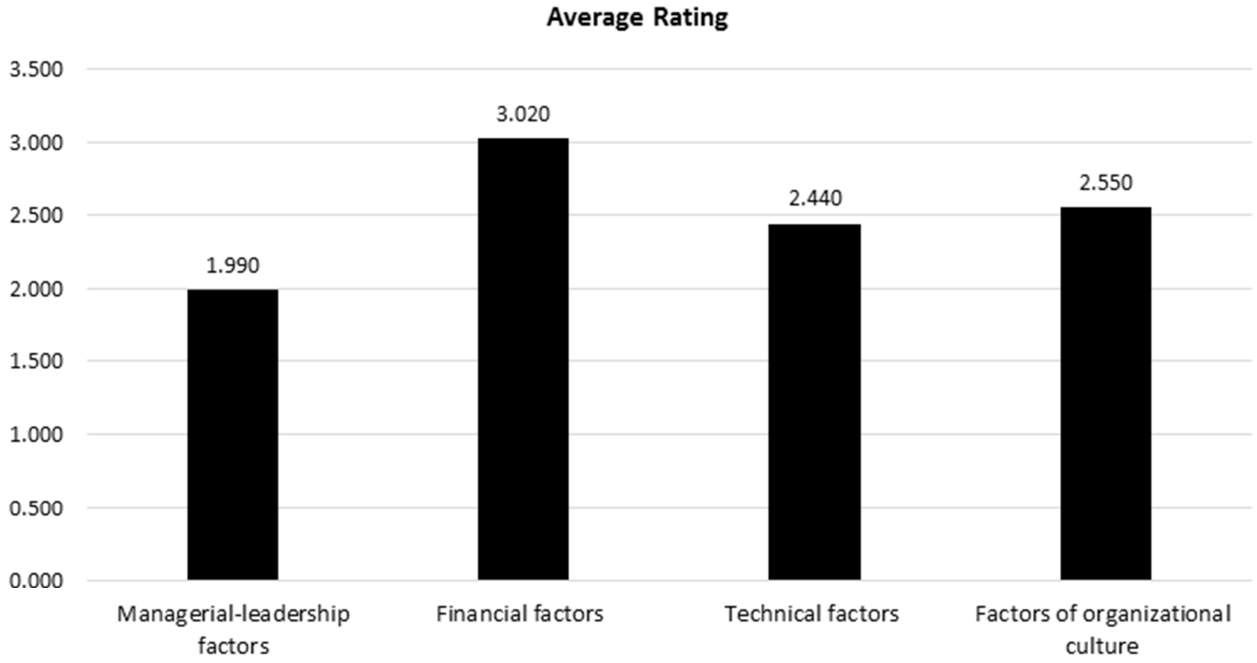

Figure 1. *Prioritizing the Main Structures of Key Factors Influencing the Successful Implementation of Information Security Systems.*

Finally, Pearson's correlation test was performed to examine the relationship between the final research structures. The results of this test are presented in the table below.

Table 6. *The Correlation between Research Structures.*

		Leadership-managerial factors	Financial factors	Technical factors
Financial factors	Correlation coefficient	0.624**		
	Significance level of the two sequences	0.00		
	Number of subjects	131		
Technical factors	Correlation coefficient	.821**	.617**	
	Significance level of the two sequences	0.00	0.00	
	Number of subjects	131	131	
Factors of organizational culture	Correlation coefficient	.834**	.564**	.718**
	Significance level of the two sequences	0.00	0.00	0.00
	Number of subjects	131	131	131

The results of Pearson correlation test show that:

- There is a positive correlation between the leadership-managerial and financial factors (R=0.624)
- There is a positive correlation between the leadership-managerial and technical factors (R=0.821)
- There is a positive correlation between the leadership-managerial and the factors of organizational culture (R=0.834)
- There is a positive correlation between financial factors and technical factors (0.617)
- There is a positive correlation between financial factors and factors of organizational culture (0.564)
- There is a positive correlation between technical and factors of organizational culture (0.718)

5. Discussion and Conclusion

As it was stated, the main function of MIS is to provide comprehensive and proper information for making best decisions (Hassan et al., 2014). Hence, the protection of such systems is a managerial task and should be considered seriously. These systems are influenced by many factors that may be considered as threats for organizations. These threats include the occurrence of natural and physical events, access to the systems by competitors, inadequate controls on the media and many other threats. Furthermore, threats are in a dynamic state and hence change over time (Robert, 2009). Hence there is a need for information security systems. Along

with such necessity, implementation of information security systems in business, regarding their nature, is a capital-intensive activity which widely influences the assets and business activities. Failure to set up such systems leads to waste of resources for businesses and even a small defect in the installation process may lead to serious damage during the deployment stages. Our preliminary studies showed that, so far, not so many studies have examined the effective factors in successful implementation of information security systems. Furthermore, the few studies conducted on this subject lacked a coherent framework of effective factors in successful implementation of information security systems. Meanwhile, they did not examine the priority of these factors and they did not review the specific relationship between these factors. Thus, in the present study, the researchers adopted a quantitative approach in addition to identifying success factors in the implementation of information security systems and identify the relative priority of the factors. Finally, with a statistics-based approach, she grouped the factors and identified the relationship between them.

The study of demographic characteristics of the subjects showed that the subjects studied in this research were in good position in terms of education and service records. So, they were eligible to respond to the questionnaire.

Prioritization of identified variables from research literature showed that among the factors influencing successful implementation of information security systems in the services sector, "existence of regular and appropriate processes" has the highest priority. In other words, specific, coherent and orderly processes should be defined and implemented for such activities. The significance of this variable is specifically emphasized in the research literature (Hagen et al., 2008). Also, according to the indicators with less priority, "key performance indicators" should also be identified and kept up to date in the process of implementing information security systems. This finding is in line with Hagen's findings (Hagen et al., 2008). Accordingly, the roles and responsibilities of each sector and consequently the entire system are specified and the time and source of response are available to decision makers. In this process, according to the preliminary nature of this stage and depending of system's next performance on the quality of implementation, virus control is the next priority. Kevin (1995) had pointed to this factor in his study, too. At all stages of system implementation, personal copy should be placed under control and if possible, unnecessary duplication should be prohibited. This conclusion has also been supported by Kevin (1995). In this way, confidentiality features are well placed under the control of information security project management. Also, "positive beliefs associated with information security" is the next priority in this field. These findings have also been supported by Waly et al (2012). This finding reflects the idea that, creating and strengthening the belief in the positive effects that the security of information systems have in business, can help this process be more successful. The "existence of user instructions and manuals" was also given a relative priority during the implementation process (as Hagen et al., 2008 had also expressed) and "protection of information assets" was the next important priority which is well supported by the research literature (Setiadi et al., 2013; Kevin, 1995). In implementing information security, positive attitude towards information security is identified as an important variable which was also discussed in the research literature (Waly et al., 2012).

As the findings of the presents study show, "motivating the employees" is the next important priority and research literature supports this finding (Setiadi et al., 2013; Waly et al., 2012; Kazemi et al., 2012). Finally, the "staff awareness of information security program" is the tenth priority among the factors of success in implementation of information security systems. This factor has also been widely highlighted in the research literature (Setiadi et al., 2013; Waly et al., 2012; Al-Awadi & Renaud, 2007; Al-Awadi, 2009; Hagen et al., 2008; Kazemi et al., 2012).

After prioritization of these factors, confirmatory factor analysis conducted in 4 groups: Leadership-managerial factors, Financial factors, Technical factors and factors of organizational culture. The final results of this analysis showed that leadership-managerial factors ultimately include: information security practices with regard to organizational culture, non-disclosure agreements, information security policy, implementing information security program, alignment with organizational mission, counter effects of sanctions and active support of senior management. Again, all these are widely emphasized by the research literature (Setiadi et al., 2013; Al-Awadi, 2009; Renaud, 2007 & Al-Awadi; Hagen et al., 2008; Kevin, 1995; Kazemi et al., 2012; Waly et al., 2012;). In the second group or technical factors, indicators of success included: risk management, allocation of financial resource, and key performance indicators. Repeatedly, the indicators of this group had already been emphasized by the research literature (Al-Awadi, 2009; Hagen et al., 2008; Waly et al., 2012; Renaud, 2007 & Al-Awadi; Setiadi et al., 2013). In the third group or technical factors, indicators included: report and documentation of events, user instructions, virus control, IT infrastructure of organization, continuous evaluation of performance, system recovery after the events, the proactive behavior of individuals in the implementation of information security systems, and the effectiveness of staff training system. All of these factors were mentioned in the research literature as well (Setiadi et al, 2013. Al-Awadi, 2009; Renaud, 2007 & Al-Awadi, Hagen et al., 2008; Kevin, 1995. Kazemi et al, 2012; Waly et al, 2012;.). Lastly, the fourth group or organizational culture factors included: the effectiveness of staff training system, positive attitude to information security, individuals' propensity to information security, stability of security in the organization, a clear understanding of the requirements for information security, participation in information security groups, user participation and the employees' awareness of information security program. Research literature has well supported these variables (Waly et al., 2012; Al-Awadi, 2009; Hagen et al., 2008; Renaud, 2007 & Al-Awadi; Kazemi et al.,

2012). Prioritization of these four influential factors showed that "financial factors" have the highest priority, "organizational culture" and "technical factors" are in second and third priorities respectively, and "leadership-managerial factors" have the lowest priority. The relationship between these structures also revealed that there is a positive correlation between the leadership-managerial factors and financial factors. The correlation between leadership-managerial factors and technical factors were also supported. The results also showed that the relationship between leadership-managerial factors and factors of organizational culture is also positive. There is a positive correlation between financial factors and technical factors, and between financial factors and factors of organizational culture. Finally, it was realized that there is a positive correlation between technical factors and organizational culture.

Recommendations

The findings of the present study indicate that among the factors influencing successful implementation of information security, "existence of regular and appropriate processes" has the highest priority. Hence, it is recommended that for establishing information security systems in the branches of private banks in Tehran, a comprehensive process and pre-planned program be considered, through which these systems can be implemented with higher effectiveness. It is also recommended that the key indicators for performance be created and documented regularly in the branches of private banks in Tehran, so that each system operator's specific responsibility and accountability can be identified. Meanwhile, there will be the possibility of monitoring the performance regularly. Businesses dealing with implementation of information security systems should take adequate and efficient measurements to prevent any virus infiltrations to the information systems. Also, it is recommended that the managers of private banks in Tehran limit personal copying as much as possible, and some clearly articulated guidelines be provided for dealing with unauthorized copying. Since information security activities are quite costly and capital-intensive, it is recommended that the country's high ranking decision-makers lay down more facilitating custom and trade rules for importing the hardware needed for providing information security in businesses. Finally, it's recommended that in the future studies, the possibility of using research findings in the branches of state banks as well as similar businesses including insurance be evaluated. Future studies can also evaluate the impact of each of the variables identified in this study on the performance indicators of the success of information security project (such as decreasing the damages with causal approach).

References

[1] Abdi, Hervé. (2003). Partial least squares regression (PLS-regression) (pp. 792-795): Thousand Oaks, CA: Sage.

[2] Åhlfeldt, Rose-Mharie. (2005). *Information Security in a Heterogeneous Healthcare Domain*. Paper presented at the 4th Security Conference. Las Vegas, USA.

[3] Akin, Melek, Bloemhof, Jacqueline M, Wynstra, Finn, & van Raaij, Erik M. (2009). *The Impact of Supply Chain-Related Factors on Environmental Performance of Manufacturing Firms in Turkey.* Paper presented at the 18 th IPSERA Conference Supply Management–Towards an Academic.

[4] Al-Awadi, Maryam. (2009). *A study of employees' attitudes towards organisational information security policies in the UK and Oman.* University of Glasgow.

[5] Al-Awadi, Maryam, & Renaud, Karen. (2007). *Success factors in information security implementation in organizations.* Paper presented at the IADIS International Conference e-Society 2007, Lisbon, Portugal.

[6] Andress, Jason. (2011). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*: Elsevier.

[7] Chin, Wynne W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research, 295* (2), 295-336.

[8] Daniel, WW. (1999). Biostatistics: a foundation for analysis in the health sciences. Wiley series in probability and mathematical statistics. Applied probability and statistics: Wiley New York.

[9] Hagen, Janne Merete, Albrechtsen, Eirik, & Hovden, Jan. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16* (4), 377-397.

[10] Hassan, Mohamed Eslam, Zhi, Fengwen, Wang, Ping, & Abdalla, Elhadi Osman. (2014). The Impact of the Sector Type on the Role of Management Information Systems for the Decision-Making Process: RNS-Sudan as Case Study.

[11] Huang, Yao-Wen, Yu, Fang, Hang, Christian, Tsai, Chung-Hung, Lee, Der-Tsai, & Kuo, Sy-Yen. (2004). *Securing web application code by static analysis and runtime protection.* Paper presented at the Proceedings of the 13th international conference on World Wide Web.

[12] Karakaya, Fahri, & Canel, Cem. (1998). Underlying dimensions of business location decisions. *Industrial management & data systems, 98* (7), 321-329.

[13] Karakaya, Fahri, & Stahl, Michael J. (1992). Underlying dimensions of barriers to market entry in consumer goods markets. *Journal of the Academy of Marketing Science, 20* (3), 275-278.

[14] Kazemi, Mehdi, Khajouei, Hamid, & Nasrabadi, Hashem. (2012). Evaluation of information security management system success factors: Case study of Municipal organization. *African Journal of Business Management, 6*(14), 4982-4989.

[15] Kevin, J. Fitzgerald. (1995). Information security baselines. *Information Management & Computer Security, 3*(2), 8-12. doi: 10.1108/09685229510088575.

[16] Mellado, Daniel, Fernández-Medina ,Eduardo, & Piattini, Mario. (2007). A common criteria based security requirements engineering process for the development of secure information systems. *Computer standards & interfaces, 29* (2), 244-253.

[17] Moss, Steve, Prosser, H, Costello, H, Simpson, N ,Patel, P, Rowe, S, … Hatton, C. (1998). Reliability and validity of the PAS-ADD Checklist for detecting psychiatric disorders in adults with intellectual disability. *Journal of Intellectual Disability Research, 42* (2), 173-183.

[18] Robert, B. (2009). *GENERAL DETERRENCE THEORY: ASSESSING INFORMATION SYSTEMS SECURITY EFFECTIVENESS IN LARGE VERSUS SMALL BUSINESSES Joseph H. Schuessler, BBAMBAMS.* UNIVERSITY OF NORTH TEXAS.

[19] Sarmad, Z., Bazarganm A., Hejazi, E. (2008). *Research methods in the behavioral sciences.* Tehran, Agah Publications.

[20] Setiadi, Farisya, Sucahyo, Yudho Giri, & Hasibuan, Zainal A. (2013). *Balanced E-Government security framework: An integrated approach to protect information and application.* Paper presented at the Technology, Informatics, Management, Engineering, and Environment (TIME-E), 2013 International Conference on.

[21] Waly, Nesren, Tassabehji, Rana & ,Kamala, Mumtaz. (2012). *Improving organisational information security management: The impact of training and awareness.* Paper presented at the High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on.

[22] Zaidan, BB, Zaidan, AA, & Kiah, ML Mat. (2011). Impact of data privacy and confidentiality on developing telemedicine applications: A review participates opinion and expert concerns. *Int .J. Pharmacol, 7* (3), 382-387.