AENSI Journals

Advances in Environmental Biology

ISSN-1995-0756 EISSN-1998-1066

Journal home page: http://www.aensiweb.com/AEB/

Information Security Management System effectiveness Measurement Case: study: East Azarbaijan Telecom Company

Ali Fakoori-e-Moeen, Yaghoob Alavi-e-Matin, Jafar Beigzad

Department of Management, Bonab Branch, Islamic Azad University, Bonab, Iran

ARTICLE INFO

Article history:
Received 15 June 2014
Received in revised form
8 July 2014
Accepted 4 September 2014
Available online 20 September 2014

Keywords:
information security, COBIT,
ISO 27001

ABSTRACT

Background: The general object of this study is to see how effective the information security management system is. **Objective:** To do so throught its statistical society of East Azarbaijan Telecom company, one main hypothesis and eleven minor hypotheses based on ISO/IEC 27001 and COBIT format have been developed and ISO 27001 standard questionair including 133 item in 11 control zones has been used to test them.. **Results:** To analyze statistical data descriptive and deductive statistics methods were incorporated and after the verification of 11 minor hypotheses, the main hypothesis, **Conclusion:** that is the effectiveness of the information security management system, was verified, too.

To Cite This Article: Ali Fakoori-e-Moeen, Yaghoob Alavi-e-Matin, Jafar Beigzad., Information Security Management System effectiveness Measurement Case: study: East Azarbaijan Telecom Company. ***Adv. Environ. Biol., 8(12)****: 893-902, 2014*

INTRODUCTION

Producing, processing, transferring and managing information and communications to establish individual, public, organizational and national knowledge bases comprises the structural format of the present age. Therefore information technology which consists of the technologies used in the process is a vital and decisive element for human societies [1].

Today, the development of national management in execution and administration or comprehensive development programs is not possible but through establishing the electronic and information foundation which is measurable with the information storage and management patterns, and this measure should be taken simultaneous with an information security management system. The environment in which such activities are done Is known as the information exchange environment. Such as environment should always be secure and there should be no possibility of penetration or misuse and on the other hand it should be possible to daily add-up of experiences, thoughts, sciences and technology and also flexibility towards reforms with a view on more productivity in business should be possible [2].

Information security management is of the type which should practically be established in system, especially with the increasing rate of criminal activities of information business in some countries nowadays, moreover establishing and deploying this management will work as a source of organizational various information passage and will thereby result in uniformity and universality of information. The objective of information security management system is to protect assets (organizational sources and data) to ensure the endurance of the business, to minimize the vulnerability of the system and to maximize money return [3].

Today, information has turned into a key device in human interactions, a device which has affected all human activities from the most preliminary to the most complicated ones. New information technologies and fundamental changes in the traditional information cycle have created new areas to produce and used information.

Threats to information security are of two types: intentional and unintentional. Intentional threats are those which attack the information security of the system with a preplanned program and a special target, such as hackers. Unintentional threats are those which are imposed on the system through human error and this is what makes the most damage to the system. Threats resulting from natural disasters such as flood, earthquake, storm, etc. are considered unintentional ones, too [5].

Incorporating information technologies to increase the efficiency in most areas is booming rapidly. Computers have been used increasingly in governmental offices, industries, organizations, and also in domestic

Corresponding Author: Ali Fakoori-e Moeen, Department of Management, Bonab Branch, Islamic Azad University, Bonab, Iran.
E-mail: ali.fakoori2000@yahoo.com

usages. The increase of the number of uses and webusers and changes in information technology, have changed the nature of security issues through organizations. Although tremendous progresses have turned out in computer technology, security weakness in computer and information network, lack of proper training for all the users regardless of their job responsibilities regarding the position and importance of information security, lack of essential instructions to information security deficiencies and lack of distinct and compiled policies to address security problems duly and on time, will entail some problems [7].

It seems various organizations including Telecom company need a powerful management of security, regarding the importance of information security within their systems. Information security refers to the protection of information and to minimize the unauthorized access to it. The concept of information security management system: information security is a section of general and overall management system of an organization based on business threats approach and its objective is to establish, deploy, execute, perform, manitor, revise, protect and optimize information security and it presents standards to secure the information exchange environment in

The organization. These standards include a set of instructions to secure the information exchange environment in an organization through administering a special plan. Because of increasing need to use modern technologies in information and communications areas and the necessity of its security, in computer networks of Telecom Company, too, establishment of an information security managements system is necessary more than ever [13].

Is the establishment of information security management in Telecom Company of the state effective? And what is the hierarchy of the effective elements in establishing the information security management systems?

The importance and the necessity of study:

Information is one of the most valuable and sensitive assets of the organization and on time access and presentation of the needed information have a decisive and key role. Protection and maintenance of the information are essential for the continuity of economic corporations and businesses. Un authorized access and penetration into the information on disks and computers and illegal use of them has become a problem and this access maybe by the staff of an organization internet users or some other factors, therefore organizations and companies are going to establish security measures. To establish security it is not enough just to consider technical issues. To create and standardize monitoring policies and also to create accurate procedures will increase the level of information security and this has made it essential to incorporate information security management systems. At present, information security issues have got a new dimension and are under the focus of all organizations and businesses [9].

This study is aimed at measuring the effectiveness of establishing information security management in East Azarbaijan Telecom Company. To do so, the effectiveness of information security management system is evaluated based on COBIT model which includes plan and organize, access and establish, present and protect, monitor and evaluate criteria.

Theoretical format of the study:

In recent years, the need for a source format for development and management of internal control and suitable levels of information technology security has been apparent. Information technology has turned into the central core in commercial and strategic processes of most companies. Also, successful organizations need to have a fundamental understanding of threats and limitations of information technology in all levels to get to an accurate path and suitable controls. COBIT is trying to prepare such a control and security format for information technology [16].

The basic activities to guide information technology activities based on COBIT model are defined in 4 areas as follows:

- Programing and organizing
- Preparation and execution
- Delivery and support
- Monitoring and evaluating

Statistical society and sample:

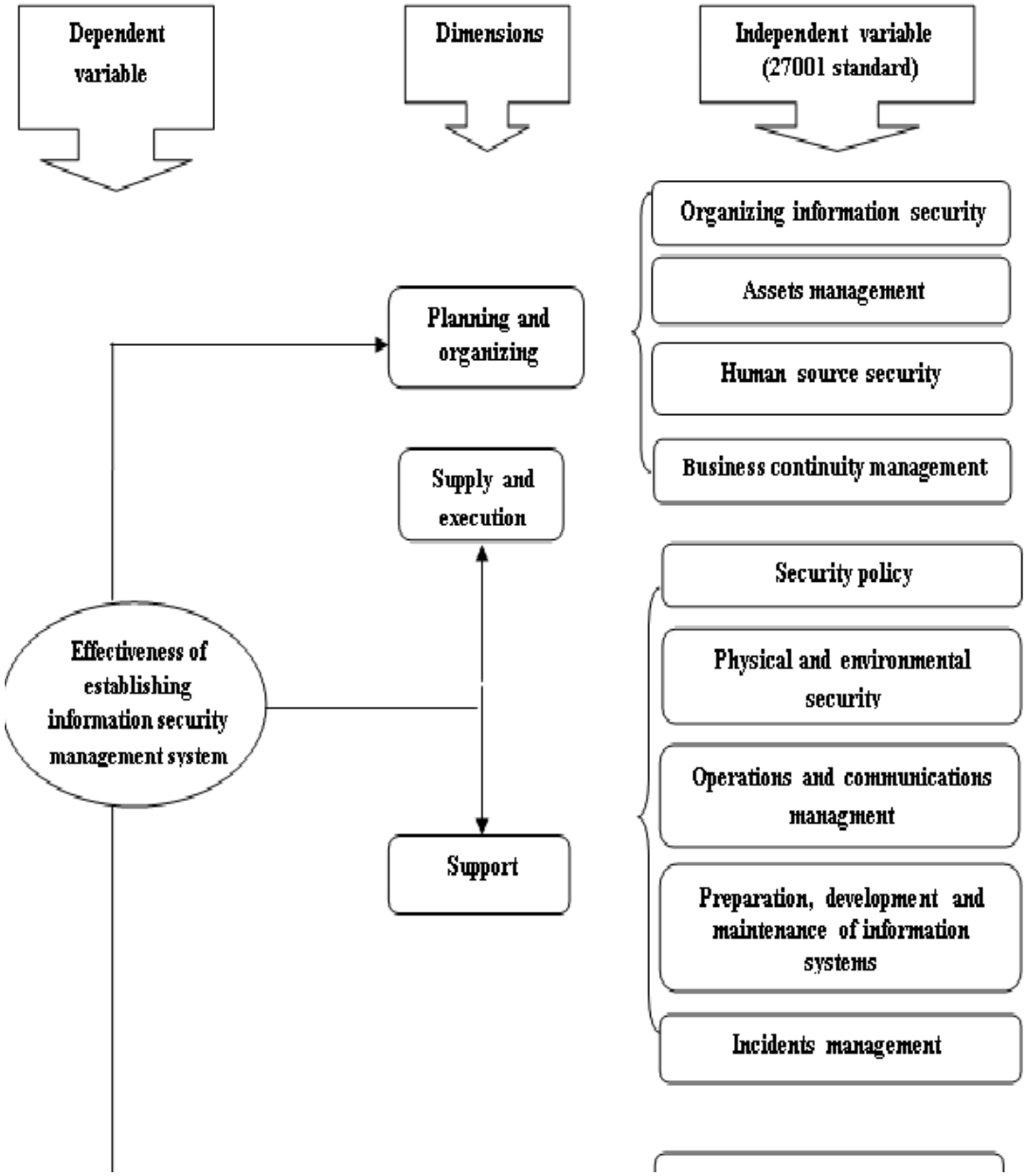
All exchanges in East Azarbaijan Telecom were chosen as the statistical society and because of the specialized nature of the subject, all members of the statistical sample including the director general, executives, bosses, and all officials accounting to 65 people who were all in direct relation to the subject of ISMS, were subjected to the study.

Approach of the study:

Regarding its nature, this study is of the descriptive- analytic type (measurement type). In descriptive studies, the subject is described and commented on and present conditions or relationships, current processes,

apparent signs or developing procedures are all taken into account. And it is of measurement type because a questionnaire is used to collect data. It could also be called a practical study because findings could be tested objectively and the results could be used by telecom company itself [19].

The Analytic model of the study:



Validity and Reliability:

Concept of validity or credibility addresses the question how good the measuring device could measure the wanted property. Without a knowledge of the credibility of the measuring device, we cannot be sure about the resulting data.

There are different types of validity including: content validity, criterion validity and construct validity. Content validity is used to study the structural components of a measuring device.

Content validity of a measuring device depends on its composing components:

Content validity of both questionairs used in this study was verified by the honorable advisor professors and counselors and directors and officials of East Azarbaijan Telecom, and they enjoy the necessary validity. The questionnaires of the study also enjoy the facial validity.

Reliability or capability of confidence is one of the technical features of the measuring device. This concept refers to the question whether the device yields the same results under the similar conditions. The range of reliability quotient is from zero (irrelevance) to tl (toal relevance).

To determine the test reliability in this study Kronbach Alpha method has been used. This method is used to calculate the internal coordination of the measuring device which measures various properties [4].

Table 1: Reliability of study questionnaires.

Variable	Number of questions	Kronbach Alpha quotient	Statistical sample
ISMS measurement (prepolicy)	133	0.989	65
ISMS measurement (postpolicy)	133	0.980	65

At it is shown, because all the quotients are more than 0.7 so the reliability of the questionnaires used in the study is verified.

Device and data analysis method:

After the researcher decides on his approach and uses the suitable devices to collect the necessary data to test their hypotheses, now the collected data should be classified and analyzed using ghe suitable statistical techniques which are in harmony with the approach, type of variables, etc.

1. Reliability statistics
2. Deductive statistics through T-pair test
3. T-pair test

Test of hypotheses:

First, to study the normality of the data, kalmograph-Smirnov test is used and after the verification of the normality of the data to measure the meaningfulness of effectiveness of ISMS, hypotheses are tested using T-pair test.

Main hypothesis:

Establishing information security management system in East Azarbaijan Telecom Company is effective.

Table 2: T-pair test of information security management system variable.

T-pair statistics					
		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	preisms	2.7303	65	.59678	.07402
	postisms	3.7157	65	.49343	.06120

T-pair Correlation				
		N	Correlation	Sig.
Pair 1	preisms&postisms	65	.661	.000

T-pair test									
		Pair differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. error mean	Difference in reliab level 95%				
					Bottom limit	Top limit			
Pair 1	preisms - postisms	-.98537	.45864	.05689	-1.09902	-.87173	-17.321	64	.000

Table 3: T-pair test of information security policy variable.

T-pair statistics					
		Mean	N	Std. deviation	Std. error mean
Pair 1	Prepolicy	3.1308	65	.91548	.11355
	Postpolicy	3.9615	65	.67493	.08371

T-pair Correlation				
		N	Correlation	Sig.
Pair 1	prepolicy&postpolicy	65	.558	.000

T-pair test									
		Pair differences					T	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. error mean	Difference in reliab level 95%				
					Bottom limit	Top limit			
Pair 1	prepolicy - postpolicy	-.83077	.77700	.09637	-1.02330	-.63824	-8.620	64	.000

As the result show, according to the views of 65 experts, at reliability level of 95%, establishing ISMS in Telecom is effective for the meaningful level is zero and has increased ISMS mean from 2.73 to 3.72, therefore H0 is rejected and H1 is verified. Thus establishment of ISMS in East Azarbaijan Telecom company is effective.
Minor hypothesis 1: The existence of security policy in East Azarbaijan Telecom company is effective.

Minor hypothesis 2: The existence of information security organization in East Azarbaijan telecom company is effective.

Table 4: T-pair test of information security organization variable.

T-pair statistics					
		Mean	N	Std. deviation	Std. error mean
Pair 1	preorgnizing	2.8713	65	.65138	.08079
	postorgnizing	3.8238	65	.69530	.08624

T-pair correlation				
		N	Correlation	Sig.
Pair 1	preorgnizing&postorgnizing	65	.461	.000

T-pair test									
		Pair differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. error mean	Difference in reliab level 95%				
					Bottom limit	Top limit			
Pair 1	preorgnizing - postorgnizing	-.95245	.69997	.08682	-1.12589	-.77900	-10.970	64	.000

Minor hypothesis 3: Establishing the assets management in East Azarbaijan telecom company is effective.

Table 5: T-pair test of assets management variable.

T-pair statistics					
		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	preassets	3.0462	65	.69441	.08613
	postassets	3.8369	65	.55890	.06932

T-pair correlation				
		N	Correlation	Sig.
Pair 1	preassets&postassets	65	.640	.000

T-pair test									
		Pair differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. error mean	Difference in reliab level 95%				
					Bottom limit	Top limit			
Pair 1	preassets – postassets	-.79077	.54593	.06771	-.92604	-.65549	-11.678	64	.000

Minor hypothesis 4: Establishment of human source security in East Azarbaijan telecom company is effective

Table 6: T-pair test of human source security variable.

T-pair statistics					
		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	prehumansecurity	3.0000	65	.68606	.08510
	posthumansecurity	3.7077	65	.66160	.08206

T-pair Correlation				
		N	Correlation	Sig.
Pair 1	prehumansecurity&posthumansecurity	65	.658	.000

T-pair test									
		Pair differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. error mean	Difference in reliab level 95%				
					Bottom limit	Top limit			
Pair 1	prehumansecurity – posthumansecurity	-.70769	.55749	.06915	-.84583	-.56955	-10.235	64	.000

Minor hypothesis 5: Physical and environmental security in East Azarbaijan telecom company is effective.

Table 7: T-pair test of physical and environmental security variable.

T-pair statistics					
		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	prephysicalsecurity	2.8118	65	.73644	.09134
	postphysicalsecurity	3.6284	65	.67425	.08363

T-pair correlation				
		N	correlation	Sig.
Pair 1	prephysicalsecurity&postphysicalsecurity	65	.601	.000

T-pair test									
		Pair differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. error mean	Difference in reliab level 95%				
					Bottom limit	Top limit			
Pair 1	prephysicalsecurity - postphysicalsecurity	-.81657	.63224	.07842	-.97323	-.65991	-10.413	64	.000

Minor hypothesis 6: Operations and communications management in East Azarbaijan telecom company is effective.

Table 8: T-pair test of operations and communications management variable.

T-pair statistics					
		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	precommunication	2.7082	65	.65691	.08148
	postcommunicatin	3.7779	65	.55157	.06841

T-pair correlation				
		N	correlation	Sig.
Pair 1	precommunication&postcommunicatin	65	.538	.000

T-pair test									
		Pair differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. error mean	Difference in reliab level 95%				
					Bottom limit	Top limit			
Pair 1	precommunication - postcommunicatin	-1.06971	.58814	.07295	-1.21545	-.92398	-14.664	64	.000

Minor hypothesis 7: Information access control in East Azarbaijan telecom company is effective.

Table 9: T-pair test of access control variable.

T-pair statistics					
		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	precontrol	2.6185	65	.75770	.09398
	postcontrol	3.7908	65	.56328	.06987

T-pair correlation				
		N	Correlation	Sig.
Pair 1	precontrol&postcontrol	65	.515	.000

T-pair test									
		Pair differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. error mean	Difference in reliab level 95%				
					Bottom limit	Top limit			
Pair 1	precontrol - postcontrol	-1.17231	.67234	.08339	-1.33891	-1.00571	-14.057	64	.000

Minor hypothesis 8: Maintenance, protection, utilization and development of systems in East Azarbaijan telecom company is effective.

Table 10: T-pair test of systems maintenance and development variable.

T-pair statistics					
		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	preutilization	2.4433	65	.76791	.09525
	postutilization	3.6298	65	.60498	.07504

T-pair correlation				
		N	Correlation	Sig.
Pair 1	preutilization&postutilization	65	.691	.000

T-pair test									
		Pair differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. error mean	Difference in reliab level 95%				
					Bottom limit	Top limit			
Pair 1	preutilization – postutilization	-1.18654	.56005	.06947	-1.32531	-1.04776	-17.081	64	.000

Minor hypothesis 9: Incidents management related to information security in East Azarbaijan telecom company is effective.

Table 11: T-pair test of event management variable.

T-pair statistics					
		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Prevent	2.3938	65	.82611	.10247
	Postevent	3.4092	65	.73095	.09066

T-pair correlation				
		N	Correlation	Sig.
Pair 1	preevent&postevent	65	.678	.000

T-pair test									
		Pair differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. error mean	Difference in reliab level 95%				
					Bottom limit	Top limit			
Pair 1	preevent - postevent	-1.01538	.63078	.07824	-1.17168	-.85908	-12.978	64	.000

Minor hypothesis 10: Business permanence management in East Azarbaijan telecom company is effective.

Table 12: T-pair test of business permanence management variable.

T-pair statistics					
		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	prepermanence	2.5662	65	.90662	.11245
	postpermanence	3.6092	65	.75202	.09328

T-pair correlation				
		N	correlation	Sig.
Pair 1	prepermanence&postpermanence	65	.689	.000

T-pair test									
		Pair differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. error mean	Difference in reliab level 95%				
					Bottom limit	Top limit			
Pair 1	prepermanence - postpermanence	-1.04308	.66941	.08303	-1.20895	-.87720	-12.563	64	.000

Minor hypothesis 11: Level of conformity with the regulations in East Azarbaijan telecom company is effective.

Table 13: T-pair test of conformity with the regulations variable.

T-pair statistics					
		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	preadaptation	2.4431	65	.85586	.10616
	postadaptation	3.6969	65	.61997	.07690

T-pair correlation				
		N	correlation	Sig.
Pair 1	preadaptation &postadaptation	65	.572	.000

T-pair test									
		Pair differences					T	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. error mean	Difference in reliab level 95%				
					Bottom limit	Top limit			
Pair 1	preadaptation - postadaptation	-1.25385	.71394	.08855	-1.43075	-1.07694	-14.159	64	.000

Regarding the final results since meaningfulness leve (sig=0.000) is less than 0.05, so H0 is rejected and H1 is verified, meaning all the hypotheses are verified which shows there is a meaningful relationship between ISMS and the effectiveness of the organization.

Recommendations based on the findings of the study:

Regarding the findings which show eleven minor hypotheses including security policy, information security organization assets management, human source security, physical and environmental security, operations and communications management, access control, utilization, systems maintenance and development, information security incidents management, Business permanence management and conformity with the regulations, are all effective on the efficient establishment of information security management system in East Azarbaijan Telecom Company, the following recommendations are presented to promote and deploy the system.

Security policy:

Regarding the findings of the first hypothesis and the effectiveness of security policy on the creation of ISMS, it is recommended that: The document of policy, and general strategies of ISMS which includes roles and responsibilities of the management, the objectives of management in establishing the system, measurement criteria, legal obligations and organizational regulations and risk-taking range, may be complied and supported by high rank managers.

Organization of information security:

Regarding the findings of the hypotheses and verification of the efficiency of information security organization within ISMS it is recommended that:

1. A Specific managerial format should be defined and developed to create, maintain and control the information security within the range of organization's activities. Also special managerial circles should be defined to compose and verify security policy-making and to assign security roles and encourage cross-sectional cooperation in security issues, and these circles should be guided by the highest rank of the management.
2. Organizing methods should be planned in a multi-lateral manner and should be programed based on the cooperation of all involving groups including managers, users, software writers, auditors, and direct security managers of the system [20].

Assets managements:

Regarding the finding of the third hypothesis and the verification of the efficiency of the assets management in ISMS it is recommended that:

Assets should be identified carefully and their ownership and security classification should be determind and documented and their location should be identified clearly.

Humansource Security:

Regarding the findings of the fourth hypothesis and the clarity of the efficiency of human source security in ISMS it is recommended that:

To realize security policy-making objectives of the organization all users should get the necessary training both in specialized areas and in social and psychological engineering through security instructions and should learn how to use the information assets of the organization in a way to minimize the security risks.

Physical and environmental security:

Regarding the finding of the fifth hypothesis and verification of the efficiency of physical and environmental security in ISMS it is recommended that:

The document on physical security measures according to ratified technical standards should be prepared.

Operations and communications Management:

Regarding the findings of the hypothesis 6 and confirmation of the efficiency of operations and communications management in ISMS it is recommended that:

1. The maintenance condition of the media should regularly be checked and the equipment should physically be protected.
2. Proper procedures should be taken to protect paper documents, computer media and the equipment and the capabilities of the communication network infrastructure should be ensured through accurate controlling procedures.
3. Information exchange among different organizations should be under close control and done under legal obligations.
4. Probable future necessary capacity should be estimated to avoid the system inability to respond at the time of the increase of the demands.

Access control:

Regarding the findings of the hypothesis 1 and confirmation of the efficiency of access control in ISMS it is recommended that:

1. Access to organizational information and processings should be controlled based on security and organizational needs and this procedure should be observed in authorization and information circulation methods policy-making.
2. To establish a link between internal network, public networks or any other network, the accurate interface should be incorporated.
3. All software devices and operating systems which are capable of access to raw information or could pass through control procedures should be protected against unauthorized access.

Utilization, development and maintenance of systems:

Regarding the finding of the 8th hypothesis and confirmation of the efficiency of development and maintenance of systems in ISMS it is recommended that:
1. Setting security obligations, incorporating controlling mechanisms and controlling pursuits, preserving security of applicational programs and information.
2. All security needs should be identified and defined carefully and agreed upon and documented as part of the information development activities.

Incidents management of information security:

According to the findings of the 9th hypothesis and confirmation of the efficiency of incidents management of information security in ISMS it is recommended that:

Regular and complete report-making of the circulating information security incidents and identification of the weak and strong points to remedy the weak points and strengthen the strong points along with recording the experiences on the system as a precaution to confront the future events related to security [21].

Business permanence management:

Regarding the findings of the 10th hypothesis and confirmation of the efficiency of business permanence management in ISMS it is recommended that:
1. Controlling mechanisms in emergency plans managements should be programmed in a way to be able to identify the present risks and limit the results of destructive events and restart the main activities of the organization based on a timetable model.
2. It is needed to plan the cohesion of the organizational operations through a combination f preventive and renewal mechanisms of a management process to minimize the loss resulting from natural disasters or security errors.

Conformity with the regulations:

According to the findings of the 11th hypothesis and efficiency of conformity with the law in ISMS it is recommended that:
1. The security of information systems should regularly be monitored. Such inspections should be based on complied security policies and it is essential that technical infrastructure and information systems be investigated from viewpoint of their adaptation to the approved security standards.
2. The information body within ISMS should conform with the laws and regulations permanently and input, present, and output knowledge should adapt to the national information circulation and business management.

Based on the findings of the study which confirms the efficiency of ISMS in East Azarbaijan telecom company it is recommended that:
1. In the direction of establishing ISMS the instructions of the strategic documents of the security of national environment of information articulation and exchange should be observed.
2. The findings should be observed in determining strategies, organizational mission and prospect.

Recommendation for future studies:

1. As this study has been conducted within East Azarbaijan telecom, it is recommended the other researchers conduct their studies in other telecom companies of the country so that comparison could be made among different results to ultimately ensure the best utilization of them.
2. As ISO 27001 standard and COBIT model have been used in the present study, it is recommended that future researchers use other standards such as ISO 17799 as the basis of their study.
3. Another recommendation would be a contrastive analysis within the organizations which have started ISMS system and comparing pre- and post-establishment of the system and presenting suggestions to promote the performance.
4. ISMS could be experimented and tested in military or security and intelligence applications.

REFERENCES

[1] Arabi Seyed Mohammad, Dehghan, Nabiollah, 2011. Methodology in Strategic Management; Tactics Quarterly of Strategic Studiec Center; 20th year; No. Go; fall.
[2] Amjadipour, Masood, 2008. Security in network and internet; Tehran; publisher: Elm-o-Danesh; lst ed.
[3] American national Institute of Information Technology, 2011. translator: Moghaddasi, Koorosh; Iazaieri, Ali:; Tehran; Naghoos Publications; 1st ed.
[4] Bazargan, Abbas, Sarmad, Zohreh, Hejazi, Elaheh, 2009. Methodology of Research in Behavioural seciences; Tehran; Agah Publications.
[5] Barari, Masood, Asdaghi, Faezeh, 2011. Primary Principles for Information Security of small firms and Organizations: Tehran; Andik publications; 1st ed.
[6] Khaki, Gholamreza, 2000. Research Methodology with an approach of Thesis-writing: Tehran; National scientific Research Center Pub.
[7] Rashti, Mohammad Reza, Nikdel, Zahra, 2010. Collection of Articles Reports on the environment of Information Articulation and Exchange; Tehran; Nehzat-e-Pouya Pub.; 1st ed.
[8] Adb-al-Majid, Riazi, 2009. Executive Instruction on Information Security Management; Tehran; Nas pub., 1st ed.
[9] Sarlak, Mohammad Ali, Farati, Hasan, 2011. Advanced Information Management Systems; Tehran; payam-e-Noor Pub., 3rd ed.
[10] Son, James, C. Lovden, Kent, 2003. Information Systems in Management of Internet & e.Commece applications; trans. Rad, Mohammadi, Negah-e-Danesh Pub., 1st ed.
[11] Anderson, J., H. Segars, (2-3) "The Impact of Information Technology on Desislon Structure and firm performance Evidencoe from Tho Textile and Apparel Industrg". Information and Management, 39: 5-1.
[12] AWad, E.M., 1988. "MIS: Concept, stracture and Application" California: the Benjamin Cummings.
[13] Bovee, Courrtlandl, Thill, V. John, Wood, Marian Burk and Dovel, P. George, 1993. Management, International Ed., MeGrow Hill Book Ce.
[14] Davis, G.B and M.H. Olson, 1985. Management Information system: conceptual, foundation, structure, and development, 2nded, NewYork: Mc Graw-Hill.
[15] Gordon R. Steven, Cordon R Judith, 200A. "Information systems, A management Appreach" John wiley and sons, INC.
[16] Kline, R.B., 2010. Principlesand practice of structural equation modeling (Brded). NewYork: GuiLford press.
[17] Pintelon, L., N. Preez, F. Puyvelde, 1999. "IT opportunities for maintenance Management" Journal of Qualty in Maintenance Enginee ring, SNO, 1: 9-24.
[18] Schermerhorn, John R., 2005. "Management", JOHN wiley and sonsl INC.
[19] Senn, Jaems, 2004. "information Technology, principles, Practices, Opprotunities", Pearson Educathan, INC.
[20] Spiratava, Cheten, 2001. "Fundamentals of information technology". K. ALVANI PUBLISHRS.
[21] Stoner, James A.F. and Freeman, R. Edward and Gilbert R. Daniel Jr., 1995. Management, 6th. Ed., prentice Hall Inc.
[22] Turbon, Efraim, Mclean Ephraim, Wetherbe Jamos, 2005. Information Technology for managmenet JOHN wiley and sons/ INC.