Provide a model for identifying and ranking the managerial factors affecting information security in organization by using vikor method; Case Study: Tehran University of Medical Sciences

Somayyeh shafeghati
Master of Information Technology
Management, Islamic Azad University,E-campus,
Tehran, Iran
s_shafaghati@yahoo.com

Nazanin pileveri
Department of industrial management, college
of management and accounting, Yadegare-e-
Imam Khomeini (RAH) branch, Islamic Azad
University, Tehran, Iran
Nazanin.pilevari@gmail.com

ABSTRACT

Nowadays, by the expansion of Information Technology in human life and dependence of business upon it, data protection, as one the most valuable and critical assets of the organization, has become the vital tool of modern industry and prerequisite for sustaining business process. In order to face the challenges and to take advantage of new opportunities brought forth by IT advances we suggest organizations shift the focus from a technology-based information security to a managerial-based approach. Also, as the organizations get familiar with the importance and priority of key managerial factors affecting information security, they will be able to increase the efficiency of organization considering limited resources and the importance of each criterion. In this study, it has been tried to identify managerial factors affecting information security in Tehran University of Medical Sciences. Also, it was intended to address more important factors in order to increase efficiency. For group decision-making, Delphi method, and for modeling linguistic valuables and uncertainty in the theories, fuzzy theory was used in order to extract major managerial indices affecting information security in the organization. Then, by using VIKOR technique as one of the multi-criterion decision-making methods, the indices obtained by Fuzzy Delphi method were prioritized.

Keywords

Fuzzy Delphi method, fuzzy logic, information security, VIKOR method

1. INTRODUCTION

Information has always been considered as one of the most valuable and critical assets of the organization and on-time access to and supply of necessary information are of great importance, and protecting information is the necessary condition for sustaining business process [4].

Despite increasing investment in information security and its strategic role in today's business success, effective implementation of information security strategy still remains one of the top challenges facing global organizations and lack of a proactive information security strategy to make information available, accessible, assured, and appropriately protected can disrupt operations and pose serious risks to the organization's performance and competitiveness as well as to those of customers [13]. Information security is an interdisciplinary field encompassing organizational, managerial, and technical aspects [36].For Implementation of security, attention to technical issues is not sufficient; rather, control policies and standardization of it, as well as creating proper procedures would enhance information security [4]. In fact, the security obtained by purely technical methods is often limited, and it is necessary to increase its range through appropriate management and predefined procedures [18]. Organizations are recommended to shift their focus from technology-based information security strategy to an attitude based on the management and organization which involves a set of organizational and managerial capabilities [6]. Besides, considering the limitation of organizational recourses, awareness of factors priority help organizations attend to more important factors for increasing their efficiency. The nature of issue requires cooperation of experts for solving it. Therefore, in this study, Fuzzy Delphi method was used for developing managerial factors affecting implementation of information security in the organization, and VIKOR technique was used for ranking the factors extracted.

2. Literature Review

Professor Steven Furnell and Anish Rajendran (2012) argued that researchers have investigated inconsistencies in organizations' attitudes toward security for years. The success of security policies depend on the personnel's awareness of information security as well as its publicity and even the best information security systems in terms of design and implementation dependent on people supported by those systems.H.Hall et al. (2011) have noted that more and more businesses around the world now regard information as a vital business asset critical to the success of organizations in today's globally connected and complex business environment. An organization can benefit from its ability to protect information and the environment in which it exists. Among these benefits are, maintaining compliance with the law, preserving brand strength, and company reputation, increasing customer trust, sustaining business resiliency, and thereby achieving organizational objectives and improving business performance. Fratto (2009) has noted that despite increasing investment in information security and its strategic role in today's business success, effective implementation of information security strategy still remains one of the top challenges facing global organizations. Al-awadi and Renaud (2007) have noted that more employees are interacting with technology to undertake their daily tasks, and employees constitute a greater threat because they have direct access to an organization's assets. Organization's systems still remain vulnerable to attack after thirty years of accumulated work on security. Information security has been regularly considered to be a technological problem with a technological solution. That is simply untrue because information security is about managing risk. When organizations fail to manage their information security, the organization's integrity will be compromised and loss of money could occur. The inescapable conclusion is that *information security is people* and is actually more of a managerial problem than a technical problem. Brown and Duguid (2002) stated that since organization's security branches are steadily developing, and the more information is available the more at risk it is, the security issue must be seriously considered. Solmz (2000) argued that information security has several stages. Until early 80s, the first stage viewed security through technical perspective. Since mid-80s to mid-90s, information security was viewed as depending upon the policy of information security and organizational structures. However, since the mid-90s, a combination of two previous stages was proposed which is still continued and is being completed. Standard Association of Great Britain (2005) stated that today information, as a valuable asset, needs security and protection. Protecting information security, information and processing integrity and its availability seems necessary for business and society and is considered as major challenge for developing technology. Danesh kia (2004), points that information, systems, and decision-support systems are important assets of the organization. Information privacy, comprehensiveness, accuracy, and availability can have a great impact upon profitability, efficiency, competitiveness, legitimacy, and operational outlook of the organization. Motamedifar (2008) stated that IT, besides many advantages, poses threats to security of human life and it is necessary to protect information in an acceptable and appropriate manner. Information security is defined by considering privacy, integrity, and accessibility, and is obtained through the application of a set of control processes. The security obtained by technical methods is often limited, and it is necessary to increase its range through appropriate management. Table 1 introduces some cases used in the field of information security in the present paper briefly

Table 1: Selection of literature review

Authors	Description
Bohrani &Yazdi (2009)	Information has always been considered as one of the most valuable and critical assets of the organization and protecting information is the necessary condition for sustaining business process.
fratto, (2009)	Despite increasing investment in information security and its strategic role in today's business success, effective implementation of information security strategy still remains one of the top challenges facing global organizations
Motamedifar (2008)	The security obtained by technical methods is often limited, and it is necessary to increase its range through appropriate management and predefined procedures
Elahi et al. (2008)	Today, managerial issues have become prominent in information security and the role of higher management, user awareness, and security policy are mentioned as major principles
Jafari et al. (2008)	Three main features of information security are as following: 1- Information security is not a technical problem; rather it is a managerial and business issue. 2- Information security is a cyclical managerial process (Act, Plan, Check, Do) which is called information management system. 3- Information security is stated based on risks management because obtaining absolute security is impossible, and a degree of risk must be considered for information security.
Ruighaver et al. (2007)	Different organizations need different levels of security, but although security requirements of a given organization might not be as much as those required for other organizations, achieving optimal security is still important for all organizations.
Vima Salazar (2006)	To achieve proper information security, complete involvement of executive managers and business owners is necessary. All sectors should be involved in this process. It must be ensured that all individual roles, responsibilities, and authorities have been understood by all.
Mitchell et al. (1999)	Information security of the organization plays a great role in sustaining businesses. Many organizations take information security for granted which makes them vulnerable against risk.

3. Research Method

In this study, it was sought to achieve a framework of managerial factors affecting information security using international criteria and global standards, as well as experts' opinions and prioritizing the identified factors to achieve efficiency and competitive advantage. For group decision-making, Delphi method was used for developing managerial factors affecting information security implementation in the organization. Of course due to factors such as lack of access to accurate information and individual and subjective ideas, fuzzy theory had to be integrated in it. Hence, fuzzy Delphi method was employed for having a better communication with experts so that whereas creating interaction among them, achieve a consensus on the issue. Then, using ANP method, the weights of selected criteria were calculated and using VIKOR technique they were prioritized. Hereafter, the steps of the proposed methodology will be explained in detail.

Stage 1: Implementation of fuzzy Delphi method for Constructing Conceptual Model

The model is developed based on books, articles, and recent research. This paper used experts' views to refine and finalize managerial factors affecting information technology. The process of access to a conceptual model by fuzzy Delphi method is presented in figure 1. The group of decision makers (DMs) should not be too large. Typically the modified fuzzy Delphi method summarizes the experts' opinions between 10 and 30 [7, 8]. Thus, in this study the number of anonymous experts participated is limited to 16. And after conducting three stages of Fuzzy Delphi method, the final model is obtained.

Table 2 shows attributes of the conceptual model and references.

Figure 2 shows completed concepual model of managerial factors affecting information security.

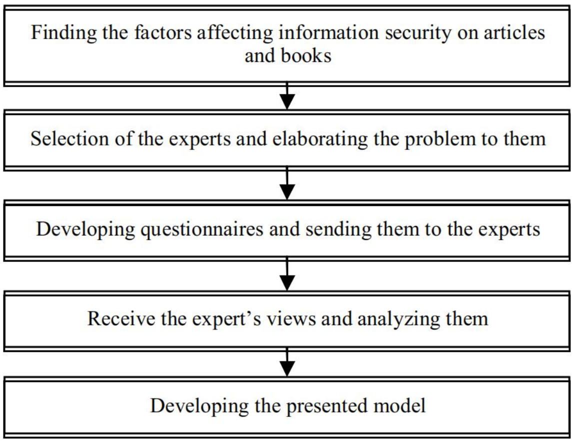
Finding the factors affecting information security on articles and books
Selection of the experts and elaborating the problem to them
Developing questionnaires and sending them to the experts
Receive the expert's views and analyzing them
Developing the presented model

Figure 1: stages of producing a conceptual model

Table 2: Attributes of the conceptual model

Attribute	Reference List
Management support and commitment	Solms 1998, elahi et al. 2008, maryam al-awadi et al. 2007, Bjork 2001, Vermeulen et al. 2002, kakanhalli 2003, solms et al. 2004
Adoption, implementation, and development of comprehensible and organization-specific security policies	maryam al-awadi et al. 2007, Herold et al. 2009, ISO/IEC 17799:2005
Risk Management	Solms 1998, ISO/IEC 17799:2005, Solms 1998, solms et al. 2002,Devinder et al. 2005
Finance and Asset Management	Bjork 2001, smith 2004, ISO/IEC 17799:2005, Devinder et al. 2005
Human Resource Management	smith 2004,solms 2006,Devinder et al. 2005, ISO/IEC 17799:2005
Management of information security incidents	Devinder et al. 2005, ISO/IEC 17799:2005
Developing levels of access to information resources	ISO/IEC 17799:2005, Solms 1998, Jafari et al. 2008

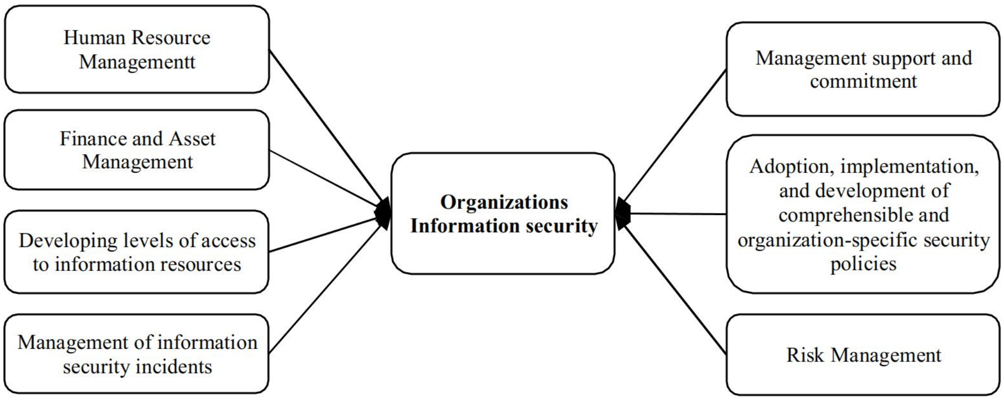
Human Resource Managementt
Finance and Asset Management
Developing levels of access to information resources
Management of information security incidents
Organizations Information security
Management support and commitment
Adoption, implementation, and development of comprehensible and organization-specific security policies
Risk Management

Figure 2: conceptual model

Stage 2: Implementation of ANP method for calculating weights of criteria

One important characteristic of any decision problem is the relative importance of each criterion. To resolve this issue, the well-known ANP method is used to calculate weights of criteria. Robbins organizational aspects indices [24] were used for decision-making criteria through experts' opinions. Table 3 indicates the weights calculated for the criteria based on experts' opinions and by using ANP method.

Table 3: weights of criteria

criteria	Weight
organization size	0.063
internal and external environment of the organization	0.098
goals and strategies	0.207
organization structure	0.261
organization culture	0.372

Stage 3: Implementation of VIKOR method for ranking alternatives

To rank the alternatives, one of the most efficient methods (i.e., VIKOR method) that received enormous attention since its first introduction in 1998, is used [20, 21]. The VIKOR determines the compromise ranking-list, the compromise solution and the weight stability intervals. This ranking index is based on the closeness to the ideal solution [20]. The compromise ranking of alternatives is developed from the Lp-metric used in the compromise programming that was first introduced by Zeleny [37]. Assuming alternatives are denoted by a1, a2,…, an, and the rating of alternative, say j, with respect to criteria i is denoted by f_j , the VIKOR form of Lp-metric is as follows:

$$L_{p,j} = \left\{\sum_{i=1}^{n} \left[w_i\left(f_i^* - f_{ij}\right)/\left(f_i^* - f_i^-\right)\right]^p\right\}^{1/p}, \qquad (1)$$
$$1 \le p \le \infty; \quad j = 1,2,\dots,J$$

In the VIKOR method, Lj,i and ,$L_{\infty,j}$are utilized to formulate ranking measures. In this method, as will be discussed in more detail later in this paper, Lj,i is called Sj and , $L_{\infty,j}$is known as Rj. The compromise solution F^c is a feasible solution that is the closest to the ideal solution F*. The compromise in this method means an agreement established by mutual concessions, represented by $\Delta f = f^* - f^c$. This point or solution belongs to the set of non-inferior solutions as illustrated in Figure 3.

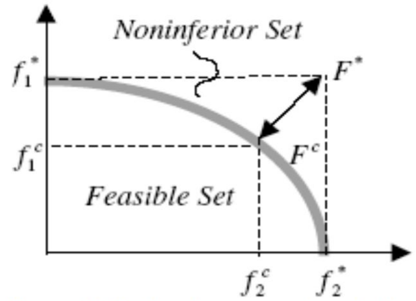

Figure 3. Ideal and compromise solutions

The VIKOR method is a helpful MCDM method, especially in those cases where the DM is not able to express his/her preference at the initial stage of the process [22]. The obtained compromise solution can be accepted because it provides the maximum group utility of the majority and the minimum of the individual regret of the opponent.

In this paper, we apply the VIKOR method for ranking managerial factors affecting information security because of the following reasons and advantages [23]:

1) Compromising is acceptable for conflict resolution.
2) There exists a linear relationship between each criterion function and a DM's utility.
3) The criteria are conflicting and noncommensurable (different units).
4) The alternatives are evaluated according to all established criteria (performance matrix).
5) A stability analysis determines the weight stability intervals.

The steps of the VIKOR Method are explained in detail below [23]:

Step1: Considering experts' opinions, the score matrix of each of the managerial factors affecting information security is formed based on the criteria. Table 4 shows the resulting decision matrix.

Table 4: decision matrix

Decision matrix	organization culture	organization structure	goals and strategies	internal and external environment of the organization	organization size
Management support and commitment	0.108	0.346	0.341	0.317	0.310
Adoption, implementation, and development of comprehensible and organization-specific security policies	0.261	0.201	0.198	0.189	0.157
Risk Management	0.213	0.085	0.121	0.111	0.122
Finance and Asset Management	0.182	0.069	0.073	0.105	0.107
Human Resource Management	0.054	0.139	0.062	0.154	0.192
Developing levels of access to information resources	0.118	0.110	0.153	0.068	0.059
Management of information security incidents	0.063	0.050	0.052	0.056	0.053

Table 5: values of $\square^*$ and $\square^\square$

	organization culture	organization structure	goals and strategies	internal and external environment of the organization	organization size
$\square^*$	0.624	0.769	0.759	0.732	0.719
$\square^\square$	0.129	0.111	0.116	0.129	0.123

Step2: Normalization of the final scores matrix using the following formula.

$$f_{ij} = x_{ij} \Big/ \sqrt{\sum_{j=1}^{n} x_{ij}^2}\ , i = 1,2,\ldots,m; \quad j = 1,2,\ldots,n \quad . \tag{2}$$

Step 3: Determining the best $\square_\square^*$ and the worst $\square_\square^\square$ values of all criterion functions, i=1, 2,…, n.
If the ith function represents a benefit then

$\square_\square^* = \max \square_{\square\square}$ $\quad \square_\square^\square = \min \square_{\square\square}$ if the i-th function represents a benefit;
$\square_\square^* = \min \square_{\square\square}$ $\quad \square_\square^\square = \max \square_{\square\square}$ if the i-th function represents a cost;

Step 4: Computing the values $\square_\square$ and $\square_\square$, j=1,2,…,J

$$\square_\square = \sum_{\square\square\square}^{\square} \square_\square \square\square_\square^* - \square_{\square\square}\ \square/(\square_\square^* - \square_\square^\square\ ), \tag{3}$$

$$\square_\square = \max[\square_\square \square\square_\square^* - \square_{\square\square}\ \square/(\square_\square^* - \square_\square^\square\ )],$$

Here $\square_\square$ are the weights of criteria, expressing their relative importance.

Step 5: Computing the values $\square_\square$, j=1, 2… J

$\square_\square = (\square)\square\square_\square - \square^*\ \square/(\square^\square - \square^*\ ) + (1 - \square_\square)\square\square^* - \square^\square\square/(\square - \square^*)$. *Where*:

$$\square^* = \min \square_\square \qquad \square^\square = \max_\square \square \tag{4}$$

$$\square^* = \min \square_\square \qquad \square^\square = \max \square_\square$$

v is introduced as weight of the strategy of “the majority of criteria” (or “the maximum group utility”), here *v* = 0.5 .

Step 6: Ranking the alternatives, sorting by the values S, R and Q, The results are three ranking lists.

Step 7: Proposing as a compromise solution the alternative (*a*′) which is ranked the best by the measure Q (minimum) if the following two conditions are satisfied:
C1: “Acceptable advantage”:
Q (a'') −Q (a') ≥ DQ Where a'' is the alternative DQ = 1/(J −1) ; J is the number of alternatives.
C2. “Acceptable Stability in decision making”: The alternative *a*′ must also be the best ranked by *S* or/and *R*. This compromise solution is stable within a decision making process, which could be the strategy of maximum group utility (when *v* > 0.5 is needed), or “by consensus” *v* ≈ 0.5, or “with veto” (*v* < 0.5). Here, *v* is the weight of decision making strategy of maximum group utility.

Step 8: Select the best alternative. Choose *Q (a')* as the best solution with the minimum of $\square_\square$.
Table 6 gives the scores of the managerial factors and their corresponding rankings.

Table 6: S, R and Q scores and ranks of the managerial factors

Managerial factors	S	Rank	R	Rank	Q	Rank
Management support and commitment	0.274	1	0.274	5	0.3	2
Adoption, implementation, and development of comprehensible and organization-specific security policies	0.314	2	0.127	1	0.028	1
Risk Management	0.594	3	0.229	2	0.433	3
Finance and Asset Management	0.704	4	0.244	3	0.541	4
Human Resource Management	0.842	6	0.372	7	0.9	6
Developing levels of access to information resources	0.752	5	0.256	4	0.599	5
Management of information security incidents	0.984	7	0.355	6	0.965	7

The best alternative, ranked by Q, is the one with the minimum value of Q. It can be seen that alternative "Adoption, implementation, and development of comprehensible and organization-specific security policies "is the best alternative.

Alternative "Adoption, implementation, and development of comprehensible and organization-specific security policies "satisfies condition C1 and C2. Because Q (a″)-Q (a′) $= 0.3 - 0.028 = 0.272 \geq D_{?} = \frac{1?}{j - 1}$=1.666 and this alternative is also the best ranked by R.

4. CONCLUSION

In this study, it has been tried to identify and introduce managerial factors affecting information security of the organization as well as their importance in information security of the organization. First, fuzzy Delphi technique was utilized for identifying managerial factors affecting successful implementation of information security in TUMS. The results of this analysis are presented in table 2. Then, VIkOR multi-criteria decision-making method was used for ranking the factors obtained. Using the results of this study, organizations can employ the identified managerial factors, in addition to technical factors, to expand and develop their information security for protecting information capital of the organization. Also, considering the importance of each factor obtained based on experts' opinion, the organization is recommended to use the limited resources to attain better security properly.

After the evaluation, alternative "Adoption, implementation, and development of comprehensible and organization-specific security policies" has the highest rate among other alternatives and the main list of managerial factors can be seen in table 6 especially with respect to Q.

The VIKOR method is sensitive to criteria's weights (wi). So the researches using VIKOR may test the result with alternative weights. Also the weight v has an important role in identifying the ranking. Further researches may compare results with setting this value between 0 and 1. The VIKOR method can also be used another sectors as a ranking methods and VIKOR method may compare with other MCDM Methods.

REFERENCES

1. Al-Awadi, M., Renaud, K. (2007). Success factors in information security implementation inorganizations, IADIS International Conference e-Society. Lisbon, Portugal. 3-6 July 2007, pp.169-176
2. Ruighaver, A.B., Maynard, S.B., Chang, S.(2007). Organizational security culture: Extending the end-user perspective, Computers & Security, 26, pp. 56-62.
3. Bjorck, F. (2001). Security Scandinavian Style, Licentiate thesis, Stockholm University & Royallnstitue of Technology, pp.20-42.
4. Bohrani, P., Yazdi, M.(2009). The importance and necessity of information security management system in e-government. Second International Conference on Electronic Administrative System, available at: http://www.civilica.com/Paper-IRTAPCO02-IRTAPCO02_035.html
5. Brown, J. S., Duguid, P. (2002). The Social Life of Information. Boston, Harvard Business School Press, vol.3, pp.45-53.
6. Caralli, R.A. (2004). Managing for Enterprise Security", Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, available at: www.sei.cmu.edu/reports/04tn046.pdf (accessed 11 February 2010).
7. Chang, C. W., Wu, C. R., Chen, H. C. (2008). "Using expert technology to select unstable slicing machine to control wafer slicing quality via fuzzy AHP", *Expert Systems with Applications*, Vol. 34, No. 3, 2210–2220.
8. Chen, S. J., Hwang, C. L.(1992). Fuzzy multiple attribute decision making: Methods and applications, Springer, Berlin,vol. 375, pp. 289-486.
9. Danesh kia, M. (2004). Expansion of Internet and computer crimes", *Seday-e Edalat Journal, 2, pp.12-19*
10. Elahi shaban taheri, M., Hassan zadeh, A. (2008). Provide a framework for human factors affecting security of information systems", Human Sciences MODARES,vol 2, pp.1-8
11. Furnell, S., Rajendran, A. (2012), "Understanding the influences on information security behavior", computer Fraud & security, vol. 3,pp.12-15.
12. Fratto, M. (2009). 2009 strategic security survey, available at: http://i.cmpnet.com/cus tom/strategicsecurity/assets/ InformationWeek_Analytics_2009_Strategic_Security_Survey.pdf (accessed 28 October 2010).
13. Hall, H., Jacqueline Sarkani, S., Mazzuchi, T.(2011), "Impacts of organizational capabilities in information security",information management &computer security, vol9, no.3, pp. 155-176.
14. Herold, R., Beaver, K. (2009). The practical guide to HIPAA privacy and security compliance", 1nd edition.
15. International Standards Organization.(2005). Information Technology- code of Practice for Information Security Management, ISO/IEC17799, 2005, available at: http://www.ndu.edu/library/d ocs/iso17799.pdf
16. Jafari, A., Rahmani, M., Mehr azmay, H. (2008), "Identifying and ranking key factors affecting challenges of management of physical and environmental information security". The 5th International Conference on ICT Management, available at: http://www.civilica.com/Paper-ICTM05-ICTM05_055.html
17. Kankanhalli A., Hockhai T., Bernard C.Y., kwokkee, W.(2003). An integrative study of information systems security effectiveness, *international Journal of information management*,vol. 23, pp. 139-154.
18. Motamedifar, M.(2008). Standard implementation of information security (ISO 27001) in offices and organizations, 1nd edition, Iranian Industrial Research and Education Center.
19. Mitchell Ruth C., Marcella, R., Baxter, C. (1999). Corporate Information Security Management, New Library World, pp. 213-227
20. Opricovic, S. (1998). Multi-criteria optimization of civil engineering systems, Faculty of Civil Engineering, Belgrade.vol. 10.pp.23-31.
21. Opricovic, S., Tzeng, G. H.(2002). Multi-criteria planning of post-earthquake sustainable reconstruction,

Computer-Aided Civil and Infrastructure Engineering, Vol. 17, 211–220.

22. Opricovic, S., Tzeng, G. H. (2004). Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS, *European Journal of Operational Research*, Vol. 156, 445–455.
23. Opricovic, S., Tzeng, G. H. (2007). Extended VIKOR method in comparison with outranking methods", *European Journal of Operational Research*, Vol. 178, 514–529.
24. Robbins, S. (1987). Organization Theory: Structures, Designs, and Applications,3rd Edition.
25. Smith, A.D.(2004).E-security issues and policy development in an information-sharing and networked environment, Aslib A"oceedings: New Information Perspectives, 56, 5, pp. 272-285.
26. Standard Association of Great Britain. (2005). Principles of information security management systems based on BS7799. Noora, A. Tr. 1st ed. Tehran: Iranian Industrial Research and Education Center.
27. Von Solms, B. (2000). Information security –the third wave?" *Journal of Computers & Security*, Vol.19, pp. 615-620.
28. Von Solms, R.(1998). Information Security management(3),the code of practice for Information Security Management (BS 7799), *information management & computer security*, vol. 6, pp. 224-225.
29. Von Solms, R. (1998).Information Security Management (1): Why information security is so important, information management & computer security,vol. 6, pp. 174-177.
30. Von Solms, R.(1998). Information security management (2): guide lines to the management of information tedmology security (G\IIITS), information management & computer security, vol. 6, pp. 221-223
31. Vermeulen, C., Von Solms, R. (2002).The information security management toolbox-taking the pain out of security management, information management & computer security, 10, pp. 119-125
32. Von Solms, B., Von Solms, R .(2004). The 10 deadly sins of information security management", computer & security, 23, pp. 371-376.
33. Vinh Thai, V., Devinder, G .(2005). Critical success factors of effective security management", available at: http://www.solom onchen.name/ download/7ms/1-013-s2-vinh.pdf
34. Von Solms, B. (2006). Information security-the fourth wave",Computers & Security, Vol.25, No.3, pp. 165-168.
35. Vima, S.(2006).Management of Information Security", CGIAR Internal Auditing unit, 18,pp. 1-18
36. Werlinger, R., Hawkey, K., Beznosov, K., (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.
37. Zeleny, M. (1982).Multiple Criteria Decision Making" McGraw-Hill, New York, pp. 1-95.