

# Presenting a Model for Ranking Organizations Based on the Level of the Information Security Maturity

Abbas Toloie Eshlaghy

Department of Industrial Management, Faculty of Management & Economics, I.A.U.

Science & Research Branch, Tehran, Iran

Tel: 98-912-310-8756 E-mail: toloie@gmail.com

Alireza Pourebrahimi

Department of Industrial Management, I.A.U., E-campus, Tehran, Iran

E-mail: poorebrahimi@gmail.com

Babak Zendehdel Nobari (Corresponding author)

Department of Information Technology Management, Faculty of Management & Economics

I.A.U., Science & Research Branch, Tehran, Iran

Tel: 98 -912-247-5701 E-mail: zendehdel@ut.ac.ir

## Abstract

Undoubtedly, in today's new business information has donated the most competitive advantage for the organizations. Although just collecting, processing and retrieving of data were significant in the past, the subject of information security is turned into a serious challenge in micro and macro levels of organizational management. Indeed, observance of the information security principals is counted as a critical infrastructure in today's knowledge based organizations. In order to realize this purpose, we need to make a strategic plan for IT security. However, we cannot expect to design a comprehensive plan, if we don't have accurate statistics about the level of the information security maturity in current organizations.

The goal of this paper is ranking organizations about the level of the information security maturity by presenting a model based on the knowledge of multi criteria decision making. So, first of all, in the literature review, the models and different standards presented in the information security maturity were studied. After determining information security criteria in technical and managerial forms, considering the triple criteria of security, safety and stability, weight devoting was performed by using the expert's views in the IT departments of three chosen organizations A, B and C. Ultimately, ranking of these organizations based on the level of information security maturity was done by applying the algorithm of PROMETHEE II. In the final step there was a comparison between the result of this model and two other security maturity models. The same results show reliability and validity of proposed ranking model.

**Keywords:** Information Security Maturity, ISO Standard 27001, COBIT Security Maturity Model, MCDM, PROMETHEE II, Security, Safety and Stability

## 1. Introduction

The most valuable property of today's organizations is information. In order to move to the knowledge based society, accessing the accurate and on time information can help. The more valuable information has the organization, the more sensible will be the subject of the information security. In fact, the observance of the information security principles is counted as a critical infrastructure in today's knowledge based organizations.

To access the goals and the missions, an organization will be more successful if the level of the information security maturity increases. Because this level will be different for varied organizations, studying and evaluating of the level of this maturity in these institutes can help verify successful organizations in this field. The aim of this paper is presenting a model for ranking different organizations based on the level of the information security maturity.

First of all, it is essential to explain and review some of the key definitions used in this research.

*1.1 Information Security:* preservation of Confidentiality, Integrity, and Accessibility of information.

*1.2 Confidentiality:* Guarantees that the data only can be accessed by authorized personnel.

*1.3 Integrity:* Safeguarding of the accuracy and completeness of data and data processing methods.

*1.4 Accessibility:* Guarantees that data can be accessed through authorized personnel and used when needed. (Andrew Ren-Wei Funga, et al., 2003)

*1.5 Safety:* means resistance vs. rigid and semi rigid physical threats.

*1.6 Stability:* is the continuity of products and services presentation in different circumstances.

### *1.7 Security Maturity Model*

A maturity model is a structured collection of elements that describe certain aspects of maturity in an organization. This type of security model indicates the degree of development and the strength of the organization's security measures, and provides an organization with a distinct security framework. The development and application of Security Maturity Models enable organizations to (Lessing, 2008):

- Generate reproducible and valid measurements;
- Establish actual progress in the security milieu;
- Rank themselves against a range of organizations;
- Determine the order in which security controls should be applied; and
- Determine the resources needed to apply to the security program (Chapin & Akridge, 2005)

This research was performed in three main phases:

- 1) Verifying the criteria for evaluating of the level of the information security maturity
- 2) Criteria weighting
- 3) Ranking organizations based on the level of the information security maturity

These steps will be discussed later.

## **2. Step 1: Verifying the criteria for evaluating of the level of the information security maturity**

After writing the review of literature, the evaluation criteria of the information security maturity were studied.

### *2.1 division of criteria based on being managerial or technical*

Via the first viewpoint, Information security discusses the technical parts (i.e. encryption algorithms, communication protocols, security hardware and software, etc) while it considers human and managerial subjects (i.e. organizing, organizational culture, organizational policies, hazards management, standards, legal rights, etc) by the second viewpoint.

### *2.2 division of criteria based on three general aspects of security, safety, stability*

For a comprehensive coverage of criteria from the information security maturity in an organization, first of all, the information security standards (such as ISO 17799 and ISO 27001) were studied and then the information security maturity models in organizations (i.e. COBIT model, Derek Schatz model) were studied carefully. Finally, twelve main criteria that covered the subject of the research comprehensively were chosen by using Delphi method and expert's views of information security. One sub criterion that related more to it was gained for each of these main criteria. Of course, it should be noted that although these two viewpoints study the information security maturity evaluation criteria from different aspects, aggregation criteria in each of these viewpoints lead to a unified collection. Table 1 shows the criteria gained from these two viewpoints by separated classifications. The criteria were derived from Derek Schatz Maturity Model (Schatz, 2008).

## **3. Step 2: criteria weighting**

In decision making sciences, there are different methods for criteria weighting that can be used in circumstances of decision problem. In this paper, according to the number of criteria and considering all of experts' votes, "Group Method" is used. The algorithm of this method is described here.

*3.1* After the criteria being verified and completed by "Delphi Method", the information security experts' ideas of every organization about the importance of each criterion by using Semi Metric Scale (between 0 to 100) in a format of a questionnaire were assessed. In fact, every expert expressed his or her idea about the significance of each criterion by a percent scale. Completing 6 to 7 questionnaire was needed in every studied organization. In this step, gained percents for each criterion are turned in to a constant percent for that criterion by using Geometric mean and the equation (1).

$$w_j = \left( \prod_{i=1}^n w_{ij} \right)^{\frac{1}{n}} = \sqrt[n]{\prod_{i=1}^n w_{ij}} \tag{1}$$

Indeed, by applying this method, not only the information security experts' different ideas are used in the percent of the importance of each criterion, but also this application can help gain a constant percent  $W_j$  for every criterion. Now, the weight of each criterion is obtained by using normalization with the equation (2).

$$w_j = \frac{a_{ij}}{\sum_{k=1}^n a_{kj}} \quad \forall i = 1, 2, \dots, n \tag{2}$$

Before ranking being started, a decision matrix should be formed. For the experts' ideas being considered, the best way is using "Group Method".

### 3.2 Formation of Decision Matrix by Group Method

Before ranking being started, first, a decision matrix should be formed. Because Group Method is applied for weighting in this study, this method should also be used for obtaining the values of decision table.

In fact, first of all, the decision table is formed according to the number of experts. Then, because the value of each criterion in every decision table is declared by percent, for the corresponding component of the decision table, a constant value (the result of Geometric Mean of the corresponding values in all previous decision tables filled by experts) is gained.

### 4. Step 3: Ranking of Organizations Based on the Maturity of Information Security

Basically, to rank options in multi criteria decision making, there are two general **compensatory** and **non compensatory** approaches. Compensatory models include methods in which exchange is allowed among criteria.

Non compensatory models include methods in which exchange is not allowed among criteria, therefore every criterion is not dependent on the others and comparisons are done based on the criteria one by one.

The PROMETHEE method (Preference Ranking Organization Method for Enrichment Evaluations) is one of the most recent MCDA methods that was developed by Brans (1982) and further extended by Vincke and Brans (1985). (Behzadian et al., 2009) PROMETHEE is an outranking method for a finite set of alternative actions to be ranked and selected among criteria, which are often conflicting. PROMETHEE is also a quite simple ranking method in conception and application compared with the other methods for multi-criteria analysis (Brans et al., 1986)

Regarding the circumstances of the problem, in this study, the algorithm of PROMETHEE II that is used, is counted as a compensatory model. Then, the stages of this method will be described briefly.

#### 4.1 Determining the threshold value for each criterion:

First, a threshold value is determined for every criterion in the decision matrix, by using equation (3).

$$\text{Threshold Value} \rightarrow TV_j = \frac{\max_i(r_{ij}) - \min_i(r_{ij})}{2} \tag{3}$$

#### 4.2 Calculation of the difference between the elements of the decision matrix to the threshold:

The difference between the values of both elements of the decision matrix to the related threshold is calculated in this step.

#### 4.3 Applying Preference Function with 0

In this stage, according to the status of criteria being positive or negative, one of Preference Functions 4 or 5 is used for all elements of the fourth step matrix:

$$\begin{cases} \text{if } \pi(i, j) < 0 \rightarrow 0 \\ \text{else} \rightarrow \pi(i, j) \end{cases} \quad \text{For Positive Criteria} \tag{4}$$

$$\begin{cases} \text{if } \pi(i, j) < 0 \rightarrow -\pi(i, j) \\ \text{else} \rightarrow 0 \end{cases} \quad \text{For Negative Criteria} \quad (5)$$

#### 4.4 Applying Preference Function With 1

In this step, Preference function with 1 (equation 6) is applied on the fifth step matrix:

$$\begin{cases} \text{if } \pi(i, j) > 1 \rightarrow 1 \\ \text{else} \rightarrow \pi(i, j) \end{cases} \quad (6)$$

#### 4.5 Creating Weighted Matrix

The sixth step matrix is weighted by the first step weighting vector in this stage. In fact, each column of the matrix is weighted by the weight of its related criterion.

#### 4.6 Formation of Collective Utility Function

In this step, the collective Utility function is calculated by the equation (7):

$$\varphi_1 = \sum_{j=1}^n \pi(i, j) - \sum_{j=1}^n \pi(i, j) \quad (7)$$

In fact, the collective **Utility** function will have members to the numbers of options.

#### 4.7 Ranking of alternatives

In this step, alternatives (the studied organizations) are ranked based on the seventh equation Utility function. Indeed, each option that has the highest Utility is ranked higher. In the other word, the studied organizations are ranked in the order of accessing to different levels of the information security maturity by using the algorithm of PROMETHEE II.

Table2 is declaring the result of performing this model in three studied organizations: A, B, and C. (It is shown by alias names because of security considerations.)

As it is observed in table 2, after ranking the organizations based on Utility, Organization A is the most secure alternative than the others. That shows that the level of the information security maturity is higher than the other organizations. Organization B has also better position in the security levels than Organization C. Additionally there is a comparison between our proposed model results and the other reliable and valid security maturity models. Simply, it is observed, there is a descending rank order in the three sample organizations. For example Organization B, has the second position in final results in all models. Same ranking orders can be considered as the best assessment tool, for validity and reliability of our proposed security maturity ranking model.

## 5. Conclusions and Suggestions

### 5.1 Results

The results of this research are expressed briefly here:

1-1-4: the first tangible result of this research is careful classification of criteria that is mentioned in the first step.(Table1) Because these criteria are obtained by the information security maturity standards (i.e. ISO 27001, ISO 17799, etc) based on the studies upon the available information security maturity models (i.e. COBIT Model , Derek Schatz) and are consolidated by using the expert's views of information security with the help of Delphi Technique and interviews, they can be used as references in practical researches.

2-1-4: Weighting Vector has not entered in none of information security maturity models yet. This research tries to join multi criteria decision making concepts to the information security maturity evaluation problems by a different approach and using mathematics. In fact the experts of information security can consider the criteria in the information security maturity evaluation according to their value and importance and by entering the weighting element.

3-1-4: By studying literature review section about the information security maturity, it was understood that any research has not performed yet about ranking organizations based on the level of the information security maturity. This ranking will help decision makers adopt strategic information technology security decisions and edit strategic plans of information systems.

## 5.2 Suggestions

Here are some suggestions for practical usages of the result of this research and also some approaches for the future researchers.

1-2-4: Ranking organizations based on the information security criteria and finding threshold values for the classification of the organizations in this part (excellent, average, poor organizations in the information security criteria)

2-2-4: Classifying of organizations based on the type of business and the purposes and obtaining related weights to each category of these organizations based on the expert's views of that category

3-2-4: studying the relationship between the result of this model and other reference models such as COBIT for organizations at the country level

## References

Andrew Ren-Wei, F., Kwo-Jean, F., & Abe, C. L.. (2003). A study on the Certification of the Information Security Management Systems. *Computer Standards & Interfaces*, 25, 447-461.

Behzadian, M, Kazemzadeh. R. B., Albadvi, A., & Aghdasi. M. (2009). PROMETHEE: A Comprehensive Literature Review on Methodologies and Applications. *The European Journal of Operational Research*. Paper in Press.

Brans, J. P., & Vincke, P. (1985). A Preference Ranking Organization Method: The PROMETHEE Method for MCDM. *Management Science*, 31, 647-656.

Brans, J. .P., Mareschal, B., & Vincke, P. H. (1986). How to Select and How to Rank Projects: The PROMETHEE Method. *European Journal of Operational Research*, 24, 228-238.

Brans, J. P., B. Mareschal., & Vincke, P. (1984). 'PROMETHEE: A New Family of Outranking Methods in MCDM. Paper presented in IFORS'84, North Holland.

Chapin, D. A., & Akridge, S. (2005). How Can Security Be Measured? *Information Systems Control Journal*. Vol. 2. Retrieved July 4, 2011, [Online] available:

<http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=24174&TEMPLATE=>

Lessing, M. M. (2008). Best Practices Show the Way to Information Security Maturity. Retrieved August 2, 2011, [Online] available: [http://researchspace.csir.co.za/dspace/bitstream/10204/3156/1/Lessing6\\_2008.pdf](http://researchspace.csir.co.za/dspace/bitstream/10204/3156/1/Lessing6_2008.pdf)

Schatz, D. (2008). *Setting Priorities According to the Maturity Level of Your Information Security Program: A Step-by-Step guide*. Orlando: InfoSec World.

Table 1. The main criteria for security maturity assessment in two different viewpoints

Main sub criterion	Main criterion	Security / Safety / Stability	Technical / Managerial	
Percentage of security policy creation and distribution, standards and laws	Security policies	Security	M	1
Percentage of budget appropriation to the information security plans to all organization budget	Management support	Security	M	2
Percentage of products being under security tests before use	Security integration into the SDLC (Note 1)	Security	T	3
Percentage of devoting enough funding references for updating security skills of IT departments	Security personnel	Security	M	4
Percentage of sensitivity of the organization to update of Anti Virus, Firewall, etc	Security infrastructure and tools	Security	T	5
Percentage of being a comprehensive viewpoint to the vulnerabilities of the organization	Threat and vulnerability management	Security	M	6
Proportion of allowed people to use changes to all staff	Configuration management	Security	M	7
Percentage of access limitation observance to systems and network based on the demands of business	Access control	Security	T	8
Percentage of close working relationship between the internal audit and the information security departments	Audits and assessments	Safety	M	9
Percentage of annually(Note 2) DRP for training and test purposes in the organization	Business Continuity	Stability	M	10
Percentage of IR(Note 3) Process Documentation in organization	Incident Handling	Stability	M	11
Percentage of employee security awareness program in organization	Training and awareness	Safety	M	12

Description for the above table.

Note 1. System development life cycle

Note 2. Disaster Recovery Plan

Note 3. Incident Response

Table 2. The last result of ranking the studied organizations based on the level of the information security maturity

Organization	The level of Information Security Maturity by Derek Schatz Model	The level of Information Security Maturity by COBIT Model	<b>Utility</b> with the main criteria
Organization A	4	5	1.15
Organization B	2	3	-0.07897
Organization C	1	1	-1.06842