A Multiple Attribute Decision Making for Improving Information Security Control Assessment

Nadher Al-Safwani
InterNetWorks Research Laboratory
Universiti Utara Malaysia

Suhaidi Hassan
InterNetWorks Research Laboratory
Universiti Utara Malaysia

Norliza Katuk
InterNetWorks Research Laboratory
Universiti Utara Malaysia

ABSTRACT
Information security control assessment provides a comprehensive control analysis approach to assist an organization in measuring the effectiveness of its current and planned security controls. ISO/IEC 27005 is a risk management framework that can manage and treat risks in organizations. However, ISO/IEC 27005 does not define a clear guideline on how to select and prioritize information security control despite the need for an efficient security analysis method. The ISO 27005 framework mostly depends on subjective judgment and qualitative approaches for security control analysis. This paper aims to improve the ISC analysis method by proposing the concept of multiple attribute decision making to provide clear guidelines in solving these issues. Order performance by similarity to ideal solution (TOPSIS) method was utilized to determine the critical vulnerable controls on the basis of different evaluation criteria. We argue that evaluating ISC by using TOPSIS leads to a cost-effective analysis and an efficient assessment in terms of testing and selecting ISCs in organizations.

Keywords
Information security controls assessment, multiple attribute decision making, security controls analysis.

1. INTRODUCTION
Information security is becoming increasingly important as the basis and premise for information system security [4, 11]. The principle goal of all business decision makers is to protect the organization and the ability to protect their IT assets, as well as to ensure the confidentiality, integrity, availability, and accountability features of the resources of the organization [16].

According to Singh [15], a risk assessment exercise involves several steps: identification of controls to be tested, testing of controls for their efficacy, analysis of test results, and recommendations for security enhancements on the basis of the analysis. The implementation of control risk management over the past few years has been ambiguous [9]. Numerous risk analysis methods and models have been developed to solve the issues and the challenges of these methods. Most security researchers attempt to enhance the framework to improve security decisions by applying quantitative or qualitative modeling techniques [10]. Quantitative techniques and methods that consider decision-making criteria and cost effective analysis remain lacking. Good references from standards organizations, such as ISO/IEC 27005, are available on the process aspects of risk management [7]. However, this framework typically and extensively focuses on the issue of defining a process around risk management. The framework may be excellent from a process perspective but does not define a clear guideline on how to accomplish control security assessment and mostly depends on a qualitative analysis approach [15]. The remainder of the paper is organized as follows. Section 2 provides a summary of ISO/IEC 27005 related work on Information Security Control Assessment. Section 3 describes the multiple attribute decision making (MADM) concept and the TOPSIS method. Section 4 presents the experimental results of a case study. Section 5 discusses the results. Finally, Section 6 provides the summarized conclusions and the highlights of our future work.

2. RELATED WORK
This section reviews the details of the ISO/IEC 27005 risk management framework and identifies the gaps in risk assessment standards and methods.

2.1 ISO/IEC 27005
ISO 27005 [7] provides the guidelines for information security risk management in an organization and the requirements of an Information Security Management System (ISMS), as shown in Figure 1. The common concepts in ISO/IEC 27001 are supported by the international standard and are designed to assist in the satisfactory implementation of information security according to the risk management approach. The process establishes the background and assesses the risks, which are mitigated by using a risk treatment plan to implement the recommended control and decisions. The standards attempt to determine the actual causes of the risks before deciding on what should be done and when to reduce the risk to an acceptable level.

Before risk assessment is conducted in the ISO/IEC 27005 framework, the organization provides a general description of the entire goal of the risk assessment and its processes. In this assessment, the risk should be identified, quantified, qualitatively described, and prioritized against the risk evaluation criteria and objectives relevant to the organization. The input of this assessment becomes the basic criteria, the scope and boundaries, and the roles and responsibilities of the organization. The output of this assessment is a list of assessed risks prioritized based on the risk evaluation criteria. Figure 2 illustrates the steps for risk assessment in ISO/IEC 27005.

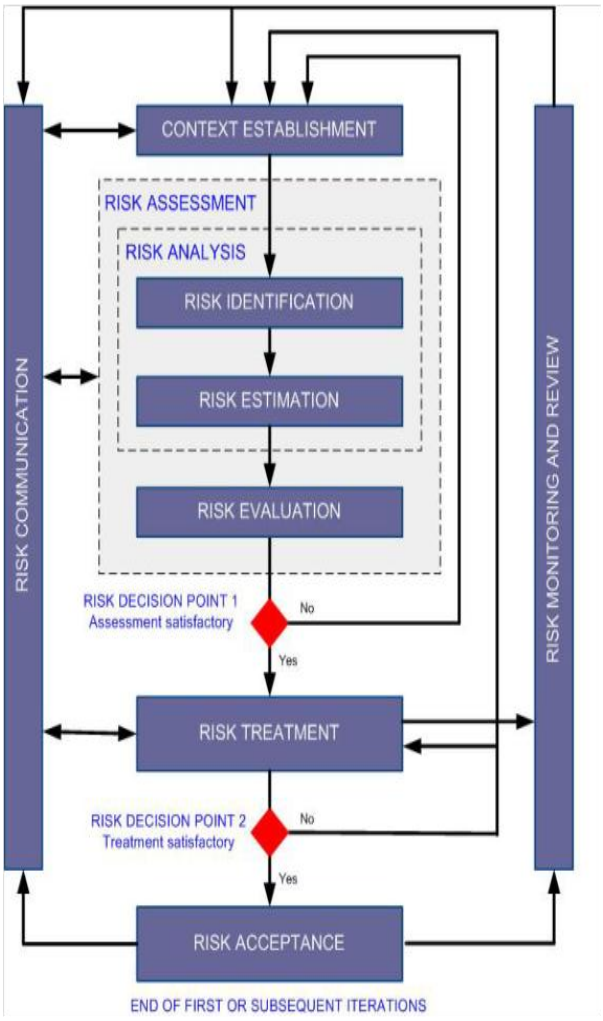

Fig 1. ISO 27005 Risk Management Framework [7].

Step 3 is the identification of the existing controls that should be made to avoid unnecessary work or cost. An existing or planned control might be identified as ineffective, insufficient, or unjustified. However, Singh [15], [9] showed that ISO 27005 does not clearly define a proper analysis for the current controls despite having a generic guideline that describes the managed approach to risk. ISO 27005 fails to provide granular guidance on the key steps of critical control identification and tends to focus on qualitative data, thus reducing the value of the approach for decision makers [5]. The process of selecting an ISC from common practices is difficult, and choosing the best controls is based on the organization [13].

The standard provides a process framework and leaves the act of defining the risk management process and approach to the process guidelines of the organization, such as Information Security Management System (ISMS) or the context of risk management. According to some researchers [3], [1], the ISO standards family does not describe the practical aspects and shortens certain parts when evaluating the sufficiency of security mechanisms in a formal approach. The situation of the knowledge base has recently improved, but the standardization of the entire risk assessment process remains necessary.

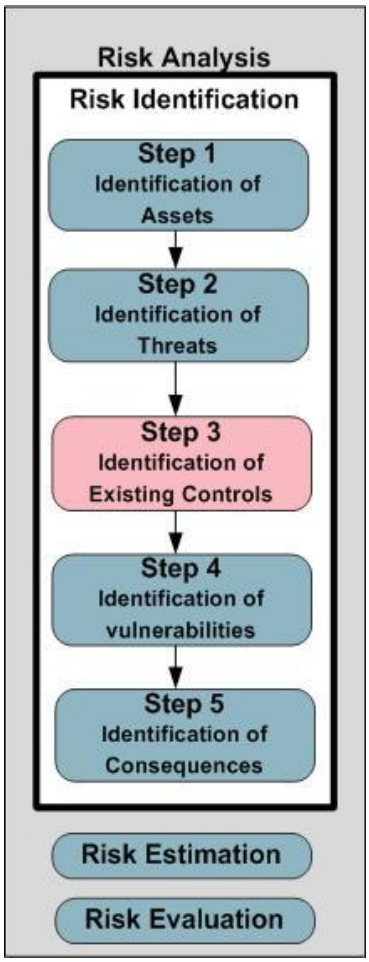

Fig 2. ISO/IEC 27005 Risk Analysis Steps [7].

3. MULTI-ATTRIBUTE DECISION MAKING

MADM problems are encountered under various situations when the decision maker has several alternatives and actions or when the candidates must be chosen on the basis of a set of attributes [18]. MADM methods are classified into three according to the type of information that the decision maker provides: no information, information on attribute, and information on alternative [6], [17], [8]. Hence, the focus of the research will pay the attention to the type where the decision maker provides information on the attribute. Therefore, we need to select information on attribute methods. The optimal MADM methods, i.e., Simple Adaptive Weighting (SAW), Hierarchical Adaptive Weighting (HAW), or TOPSIS, must be selected and applied in each study case. Several studies compared between these techniques and others to find the optimal technique. TOPSIS is considered theoretically more robust than SAW because TOPSIS considers the alternative on the basis of the most desirable result by considering the distance of each result from the most and least desirable method. TOPSIS further increases the accuracy of the final result. Therefore, TOPSIS can be considered a stronger weighing model than MEW and SAW [14]. TOPSIS is also considered one of the major decision-making techniques. Opricovic and Tzeng [12] stated that the highest ranked alternative by TOPSIS is the best in terms of the ranking index, which does not mean that the alternative is always the closest to the ideal solution. However, they did not

consider the trade-offs involved by normalization when obtaining the aggregating function. Nevertheless, TOPSIS is considered one of the major multi-attribute decision making (MDAM) techniques with an advantage over other MDAM techniques and group decision-making methods [2].

In any MDAM ranking, fundamental terms must be defined such as the decision matrix (DM), the evaluation matrix (EM), the alternatives, and the criteria.

The EM has m alternatives and must create n criteria. The intersection of each alternative and criteria is given as x_{ij}. Therefore, we have a matrix $(x_{ij})_{m*n}$

$$D = \begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \dots & C_n \end{array} \\ \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{bmatrix} \end{array},$$

where $A_1, A_2, \dots, A_m$ are the possible alternatives among which the decision makers have to choose (i.e., technical security controls), $C_1, C_2, \dots, C_n$ are criteria with which the alternative performances are measured (i.e., vulnerabilities, threats, valid vulnerabilities, severity, and cost remediation effort), x_{ij} is the rating of the alternative A_i with respect to criterionC_j, and W_j is the weight of criterion C_j (i.e., threats weight, severity weight, and cost remediation weight). Certain processes must be performed to rank the alternatives, such as normalization, maximization indicator, adding the weights, and other processes depending on the method.

3.1 Technique for Order Performance by Similarity to Ideal Solution Method

3.1.1 Construct the normalized decision matrix

This process attempts to transform the various attribute dimensions into non-dimensional attributes, which allows a comparison across the attributes. The matrix $(x_{ij})_{m*n}$ is then normalized from $(x_{ij})_{m*n}$ to the matrix $R = (r_{ij})_{m*n}$ by using the normalization method:

$$r_{ij} = x_{ij} \Big/ \sqrt{\sum_{i=1}^{m} x_{ij}^2} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (1)$$

This process results in a new Matrix R, where R is as follows:

$$R = \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ r_{21} & r_{22} & \dots & r_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ r_{m1} & r_{m2} & \dots & r_{mn} \end{bmatrix}.$$

3.1.2 Construct the weighted normalized decision matrix

In this process, a set of weights $w = w_1, w_2, w_3, \cdots, w_j, \cdots, w_n$ from the decision maker is accommodated to the normalized DM. The resulting matrix can be calculated by multiplying each column from the normalized decision matrix (R) with its associated weight w_j. The set of the weights is equal to 1:

$$\sum_{j=1}^{m} w_j = 1 \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (2)$$

This process results in a new Matrix V, where V is as follows:

$$V = \begin{bmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ v_{21} & v_{22} & \dots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{m1} & v_{m2} & \dots & v_{mn} \end{bmatrix} = \begin{bmatrix} w_1 r_{11} & w_2 r_{12} & \dots & w_n r_{1n} \\ w_1 r_{21} & w_2 r_{22} & \dots & w_n r_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ w_1 r_{m1} & w_2 r_{m2} & \dots & w_n r_{mn} \end{bmatrix}.$$

3.1.3 Determining the ideal and negative ideal solutions

In this process, two artificial alternatives, A^* (the ideal alternative) and A^- (the negative ideal alternative), are defined as

$$A^* = \left\{ \left(\left(\max_i v_{ij} \,\middle|\, j \in J \right), \left(\min_i v_{ij} \,\middle|\, j \in J^- \right) \middle| i = 1,2,\dots,m \right) \right\}$$

$$= \{ v_1^*, v_2^*, \dots, v_j^*, \cdots v_n^* \} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (3).$$

$$A^- = \left\{ \left(\left(\min_i v_{ij} \,\middle|\, j \in J \right), \left(\max_i v_{ij} \,\middle|\, j \in J^- \right) \middle| i = 1,2,\dots,m \right) \right\}$$

$$= \{ v_1^-, v_2^-, \dots, v_j^-, \cdots v_n^- \} \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (4).$$

J is a subset of $\{i = 1,2,\dots,m\}$, which presents the benefit attribute (e.g., size, robustness, and complexity). By contrast, J^- is the complement set of J, which can be noted as J^c or the set of cost attributes.

3.1.4 Separation measurement calculation on the basis of the Euclidean distance

Separation measurement is conducted by calculating the distance between each alternative in V and the ideal vector A^* by using the Euclidean distance, which is given by

$$S_{i^*} = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^* \right)^2}, \qquad i = (1,2,\cdots m) \quad \dots\dots (5)$$

The separation measurement for each alternative in V from the negative ideal A^- is similarly given by

$$S_{i^-} = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^- \right)^2}, \quad i = (1,2,\cdots m) \quad \cdots\cdots \quad (6)$$

At the end of step 4, two values, namely, S_{i^*} and S_{i^-}, for each alternative are counted. These two values represent the distance between each and both alternatives (the ideal and the negative ideal).

3.1.5 Closeness to the ideal solution calculation.

The closeness of A_i to the ideal solution A^* is defined as

$$C_{i^*} = S_{i^-} / (S_{i^-} + S_{i^*}), \quad 0 < C_{i^*} < 1, \quad i = (1,2,\cdots m) \dots (7)$$

$C_{i^*} = 1$ if and only if ($A_i = A^*$). Similarly, $C_{i^*} = 0$ if and only if ($A_i = A^-$).

3.1.6 Step 6: Ranking the alternative according to the closeness to the ideal solution.

The set of the alternative A_i can now be ranked according to the descending order of C_{i^*}. The highest value has the best performance.

3.2 Experimental Study

This section describes the experiments setup and the implementation of TOPSIS steps within ISO 27005 standard. The experiments were conducted in a small- and medium-size enterprise (SME) based in Kuala Lumpur, Malaysia that specializes cyber security consulting. The scope of study is to examine the information security controls of IT department. The organization assigned four people for the implementation who are expert in vulnerability assessment and penetration test.

3.3 Procedure and Materials

The study has determined the scope and infrastructure boundaries of security controls. Security controls are classified into two types: technical and nontechnical. In this paper, we evaluated the technical ISC. Technical controls are defined as the safeguards built into the hardware and the computer software, such as firewalls, routers, databases, and servers.

All tests were conducted in a real time network. First, we identified a total of 18 technical security controls (see Table 4). We conducted more than 50 experiments to identify the vulnerabilities among these controls by using different vulnerabilities assessment tools, such as Nessus, Nmap, Dumpsec, Kismet, and Acunetix Web Vulnerability Scanner. We then ran over 100 experiments by using different penetration testing tools, such as Metasploit, AirSnort, Nstealth, Paros Proxy, ISS Database Scanner, and Spike. The aim of this step is to validate the analyzed data obtained from the vulnerability assessment.

Finally, the severity of the attack classes and the cost remediation effort level were evaluated based on the severity and cost remediation level scores as described in Table 4, respectively. We had to validate the data and obtain an accurate result estimation prior to data analysis. Therefore, we conducted a group analysis panel with different experts to estimate the severity and cost of the remediation effort. Finally, we analyzed the obtained results by using the TOPSIS method to prioritize the feedback and data of the expert. The results of TOPSIS experiment illustrated in detail in Section 4.

4. RESULTS

This section depicts the results obtained from the prior experiments conducted in a small-medium enterprise, wherein different technical security controls are implemented. We run the TOPSIS methods using java programming language. The developed program convert all mathematics equations into a programming code. The data of the five evaluation criteria such as know vulnerabilities, valid vulnerabilities, attack classes, severity of attacks, and remediation effort level were prioritized using TOPSIS methods. There are 18 security controls for evaluation and ranked based on the evaluation criteria. The weights of the evaluation criteria are defined by external cybersecurity team. The weight sum for each evaluation criteria must be equal to 1. The first step and second step of TOPSIS have been conducted to extract the normalized data based on weight rating as depicted in Table 1. In addition, ideal and negative ideals solution were identified to calculate the separation and closeness as described in Table 1. Table 2 describes the separations, closeness, and the ranking of the security controls. The separation measures of these criteria conducted through all mathematic equations. These results are discussed in detail in Section 5.

Table 1. Weight of Normalized Decision Matrix

Controls	C1	C2	C3	C4	C5
A1	0.013	0.009	0.009	0.009	0.013
A2	0.074	0.07	0.07	0.078	0.026
A3	0.004	0.004	0.004	0.004	0.004
A4	0.009	0.013	0.017	0.017	0.009
A5	0.039	0.048	0.026	0.061	0.044
A6	0.048	0.039	0.03	0.057	0.039
A7	0.03	0.026	0.022	0.039	0.03
A8	0.061	0.052	0.052	0.048	0.048
A9	0.044	0.035	0.061	0.052	0.061
A10	0.017	0.03	0.044	0.044	0.035
A11	0.035	0.044	0.048	0.022	0.07
A12	0.065	0.065	0.057	0.074	0.074
A13	0.022	0.022	0.039	0.013	0.017
A14	0.026	0.017	0.013	0.035	0.022
A15	0.07	0.074	0.074	0.026	0.065
A16	0.078	0.078	0.078	0.03	0.078
A17	0.052	0.057	0.035	0.065	0.052
A18	0.057	0.061	0.065	0.07	0.057
A^*	0.078	0.078	0.078	0.078	0.078
A^-	0.004	0.004	0.004	0.004	0.004

5. DISCUSSION

Inaccurate ISC selection and evaluation can create an unclear view of the risk of an organization during risk assessment exercise. The ISC prioritization method allows decision makers to create accurate decisions on the critical and important controls and threats to consider. We used the TOPSIS method to improve the ISO/IEC 27005 control assessment and the security decision-making of the organization by providing a clear prioritization steps to select the most vulnerable and critical controls. Security controls were rated on a scale of 1 (critical risk) to 18 (low risk). We selected the top eight critical risks of the ISC to the organization. The list of critical security controls in Table 4 shows that web application is the most important critical control to address, followed by the router, web server, Passive Mail server, VMware ESX server, CCTV server, database, and Active Directory. These controls are evaluated based on not only the number of known vulnerabilities but also the different evaluation criteria, such as severity and cost remediation effort level.

The controls for each criterion were ranked by using the TOPSIS method on the basis of the high risk of the control (1 as most critical and 18 as least critical). The ranks for each criterion were then ranked by using the TOPSIS method to determine an overall rank. Table 1 also shows that the most significant controls of an organization are the Windows update server and the development server.

Table 2. Summary Results of the TOPSIS Ranking

Technical Security Controls	S_{i^*}	S_{i^-}	C_{i^*}	Rank
Router	0.152	0.0144	0.0865	0.0
Firewall	0.0539	0.139	0.7206	0.0865
Web Application	0.1655	0.0	0.0	0.1265
Web server	0.1464	0.0212	0.1265	0.2596
DHCP Server	0.082	0.0912	0.5266	0.2646
Active Directory	0.0823	0.0879	0.5165	0.3453
CCTV Server	0.1098	0.0579	0.3453	0.4063
File server	0.0594	0.1076	0.6443	0.5165
Antivirus Server	0.0663	0.1057	0.6145	0.5244
Database	0.1017	0.0696	0.4063	0.5266
Active Mail Server	0.0856	0.0944	0.5244	0.6145
Windows Update Server	0.0293	0.1408	0.8277	0.6362
VMware ESX Server	0.1262	0.0454	0.2646	0.6443
Passive Mail Server	0.1258	0.0441	0.2596	0.7101
Wireless AP	0.055	0.1347	0.7101	0.7206
Email Gateway	0.0479	0.1503	0.7583	0.7583
DNS	0.0625	0.1093	0.6362	0.7691
Development Server	0.0387	0.1289	0.7691	0.8277

6. CONCLUSION

Control assessment is a critical step in information security risk management. Control assessment and analysis methods have become increasingly more important to organizations that consider a continued defense technique against threats. The current ISO/IEC 27005 framework does not provide enough practical details on ISC selection and evaluation. The assessment process is niche and requires the use of more resources when conducted in organizations, particularly if the organization has a constant budget and limited resources to provide an entire risk picture. Few studies focus on improving the issues and challenges of information security systems. This paper proposes TOPSIS, to enhance ISC selection and prioritization. Our solution improves the risk assessment process by providing dynamic analysis methods to assist organizations in accurately evaluating the ISC by considering the weight of each attribute or evaluation criteria. This solution assists the organization in determining and selecting the effectiveness performance of security controls.

Table 3: Ranking Summary of the Results

Number	Technical Security Controls	Known Vulnerabilities	Valid Vulnerabilities	Attack Class	Severity	Remediation Effort level	Ranking
1	Router	3	2	2	2	3	2
2	Firewall	17	16	16	18	6	15
3	Web Application	1	1	1	1	1	1
4	Web server	2	3	4	4	2	3
5	DHCP Server	9	11	6	14	10	10
6	Active Directory	11	9	7	13	9	8
7	CCTV Server	7	6	5	9	7	6
8	File server	14	12	12	11	11	13
9	Antivirus Server	10	8	14	12	14	11
10	Database	4	7	10	10	8	7
11	Active Mail Server	8	10	11	5	16	9
12	Windows Update Server	15	15	13	17	17	18
13	VMware ESX Server	5	5	9	3	4	5
14	Passive Mail Server	6	4	3	8	5	4
15	Wireless AP	16	17	17	6	15	14
16	Email Gateway	18	18	18	7	18	16
17	DNS	12	13	8	15	12	12
18	Development Server	13	14	15	16	13	17

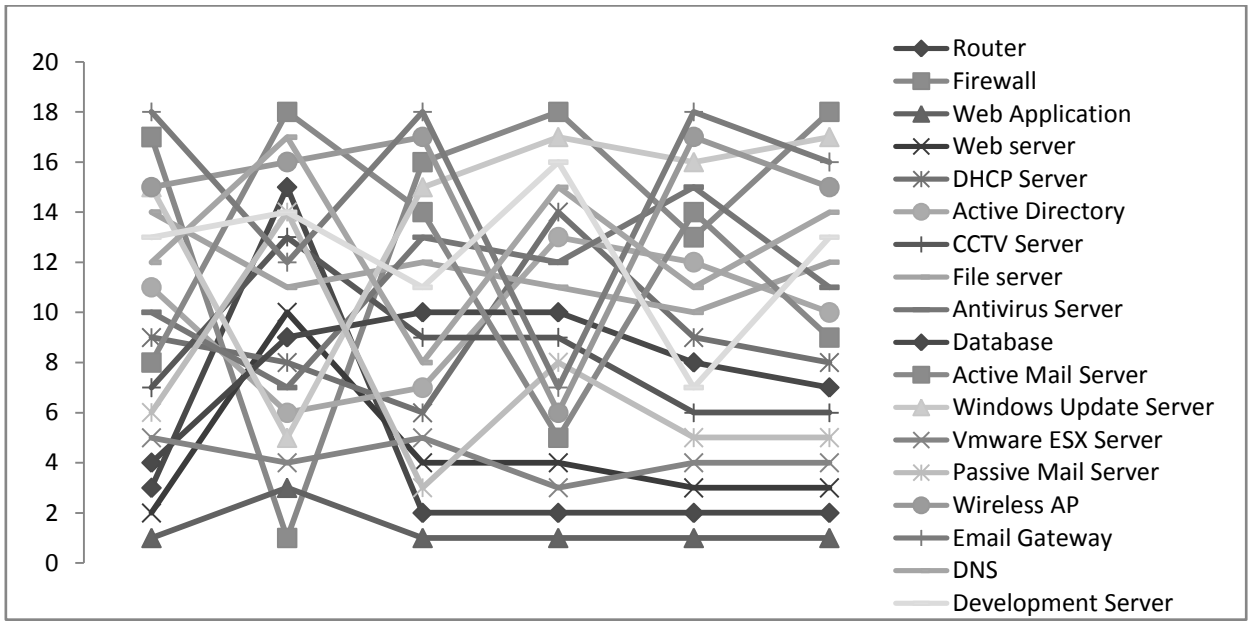

Figure 3. Technical Security Controls Ranking Using TOPSIS

In the future, these data may be used for different MADM methods. The results from this study can be examined to determine the most effective MADM method. Future research can also concentrate in evaluating this study by interviewing experts from organizations within similar industries.

7. REFERENCES

[1] A. Asosheh, B. Dehmoubed, and A. Khani. A new quantitative approach for information security risk assessment. In Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on, pages 222–227, 2009.

[2] Shuo-Yan Chou, Yao-Hui Chang, and Chun-Ying Shen. A fuzzy simple additive weighting system under group decision-making for facility location selection with objective/subjective attributes. European Journal of Operational Research, 189(1):132 – 145, 2008.

[3] A. Ekelhart, S. Fenz, and T. Neubauer. Aurum: A framework for information security risk management. In System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on, pages 1 –10, jan. 2009.

[4] Nan Feng and Minqiang Li. An information systems security risk assessment model under uncertain environment. Applied Soft Computing, 11(7):4332 – 4340, 2011.

[5] Douglas W. Hubbard. The Failure of Risk Management : Why It is Broken and How to Fix It. Willy, New Jeresy,USA, 2009.

[6] C.L. Hwang and K.P. Yoon. Multiple Attribute Decision Making Methods and Applications: A State-of-the Art Survey. Lecture Notes in Economics and Mathematical Systems Series. Springer London, Limited, 1981.

[7] ISO/IEC. Iso 27005 information technology security techniques information security risk management, 2008.

[8] Cengiz Kahraman and Selçuk Çeb. A new multi-attribute decision making method: Hierarchical fuzzy axiomatic design. Expert Syst Appl., 36(3):4848–4861, 2009.

[9] E. Kiesling, C. Strausss, and C. Stummer. A multi-objective decision support framework for simulation-based security control selection. In a, editor, Availability, Reliability and Security (ARES), 2012 Seventh International Conference on, pages 454–462, 2012.

[10] S. Lauesen and H. Younessi. Six styles for usability requirements. In Proceedings of the Fourth International Workshop on Requirements Engineering: Foundation for Software Quality: REFSQ'98, pages 155–166, Pisa, Italy, 1998. Presses Universitaires de Namur.

[11] Jun-Jie Lv, Yong-Sheng Zhou, and Yuan-Zhuo Wang. A multi-criteria evaluation method of information security controls. In Computational Sciences and Optimization (CSO), 2011 Fourth International Joint Conference on, pages 190–194, 2011.

[12] Serafim Opricovic and Gwo-Hshiung Tzeng. Compromise solution by mcdm methods: A comparative analysis of vikor and topsis. European Journal of Operational Research, 156(2):445 – 455, 2004.

[13] Angel R. Otero, Carlos E. Otero, and Abrar Qureshi. A multi criteria evaluation of information security controls using boolean features. Network Security and Its Applications (IJNSA), 2(4):1–11, October 2010.

[14] Hsu-Shih Shih, Huan-Jyh Shyur, and E. Stanley Lee. An extension of topsis for group decision making. Mathematical and Computer Modelling, 45:801 – 813, 2007.

[15] Anand Singh and David Lilja. Improving risk assessment methodology: a statistical design of experiments approach. In 4th International Conference Security of Information and Networks (SIN 2011), pages 21–29, Sydney, Australia, October 2009. ACM.

[16] Evan Wheeler. Building an Information Security Risk Management Program from the Ground Up. Waltham, 2011.

[17] K . Paul Yoon and Ching-Lai Hwang. Multiple Attribute Decision Making: An Introduction (Quantitative Applications in the Social Sciences, volume 104:83. USA, SAGE Publications, Inc., 1995.

[18] Edmundas Kazimieras Zavadskas, Arturas Kaklauskas, Zenonas Turskis, and Jolanta Tamošaitien˙e. Multi-attribute decision-making model by applying grey numbers. Informatica, 20(2):305–320, April 2009.