Selection of Information Security Risk Management Method Using Analytic Hierarchy Process (AHP)

Slaven Smojver
Croatian National Bank
Trg hrvatskih velikana 3, 10002 Zagreb, Croatia
slaven.smojver@hnb.hr

Abstract. *Numerous existent information security risk management (ISRM) methods greatly differ in approach, complexity of usage, level of detail and applicability to organizations of different sizes and business models. Selection of a method that fits requirements of an organization can be complex and resource intensive process with significant possibility for suboptimal decision. This paper presents a model for selection of optimal ISRM method based on Analytic Hierarchy Process (AHP) and comparison of risk management methods performed by ENISA. The model is evaluated through selection of optimal ISRM method for a financial institution by a group of experts and results are presented.*

Keywords. Information security risk management method, Analytic Hierarchy Process, AHP, ENISA

1 Introduction

Note: The views expressed in this article are those of the author and do not necessarily reflect the views of the Croatian National Bank

Today, risk management is being perceived as a key component of information systems management and management of information security related risks is generally recognized as a cornerstone of safe and secure conduct of business processes in any organization [10]. That being said, there are numerous information security risk management (ISRM) methods in existence. For example, European Network and Information Security Agency (ENISA) refers to at least 13 widely used ISRM methods [4], and there are many other methods.

It is important to note that although majority of ISRM methods follow some basically comparable steps they also vary substantively according to:

- Scope of the method (e.g. whether the method includes steps for risk treatment or not),
- Method's level of detail (e.g. some methods give just broad overview of the tasks that have to be performed and other provide step-by-step guidance and utilize large databases of vulnerabilities and threats),
- Type of organizations at which a method is aimed (government vs. business; large vs. small organizations; industry specific methods, etc.),
- Availability of method in various languages, availability of tools that support risk assessment and/or treatment, availability of consultancy support, etc,
- Costs of implementation and execution,
- Various other factors.

Number of available ISRM methods and their differences illustrate problems that organizations face when trying to select the ISRM method that is optimal for their particular needs. One way for an organization to surmount those obstacles is to perform a detailed analysis of available methods and to choose one preferred method. It is immediately clear that such a process would put significant strain on the organizations' resources and probably would not be cost-effective.

Another option is to compare ISRM methods according to some meaningful, well-defined, objective and comparable criteria. This solution raises it own set of problems with defining the criteria on which the methods should be

compared and with finding relevant and independent source(s) of information on those methods.

This paper presents a model for evaluation of ISRM methods according to a set of significant and comparable criteria for selection of optimal ISRM method. The model is developed on the basis of Analytic Hierarchy Process (AHP). The functionality and applicability of the model is tested on a case study of selection of optimal ISRM method for a non-particular larger Croatian credit institution. Prioritization of criteria is performed by a group of experts with significant ISRM experience.

Finally, the goal of this article is to demonstrate possibility of comparing various widely used ISRM methods and selecting the optimal method (from a viewpoint of an organization) according to a set of criteria that are relevant and that can be directly and objectively compared across those methods.

2 Literature review

The number of research papers and other relevant literature that deals with selection of appropriate ISRM method is less than plentiful and overview of published research shows that there is no uniform approach towards this subject (a fact that ENISA also recognized [4, p.1]). Several authors noted this deficiency and proposed a few methods or frameworks for comparison of different ISRM and in some cases information security risk assessment (ISRA) methods. This chapter briefly notes some approaches to the subject.

Garrabrants et al. [7] in 1990 proposed the CERTS method that is composed of 7 criteria (each criterion has 2 to 4 attributes) according to which an ISRM method can be measured (defined criteria are displayed in Table 1). In 1996 Lichtenstein [12] compiled a list of 17 factors (criteria) that should be considered in selection of ISRA method. Further on, the list was distilled to 7 highly significant factors/criteria (list of all 17 factors is displayed in Table 1, and significant factors are in boldface). Of those 7 criteria, 5 correspond to criteria put down in the CERTS method.

Campbell and Stamp [2] came up with different approach and proposed a classification scheme for ISRA methods that enables comparison of various methods and facilitates selection of the optimal method. The scheme is based on 3x3 classification matrix that catalogs ISRA methods according to approach (temporal, functional or computative) and according to level (abstract, mid-level and concrete) of the method.

Vorster and Labuschagne [19] defined a framework that compares ISRA methods according to 5 criteria that are scaled according to their importance. The criteria include approach to assets (risk analysis performed on single asset vs. group of assets), level of preparation that is needed before risk analysis can be performed, type of personnel involved (in-house vs. outside experts), the formulae for calculation of risk and relative vs. absolute results of the assessment. In a different approach Niekerk and Labuschagne [14] performed structured comparison of popular ISRM methods according to phases of a generic ISRM process.

Table 1. Method comparison criteria

Criteria for evaluating ISRM/ISRA methods	
Garrabrants et al. [7]	**Lichtenstein [12]**
Consistency	**Cost**
Usability	External influences
Adaptability	Agreement
Feasibility	Organizational structure
Completeness	**Adaptability**
Validity	**Complexity**
Credibility	**Completeness**
	Level of risk
	Organizational size
	Organizational security philosophy
	Consistency
	Usability
	Feasibility
	Validity
	Credibility
	Automation

As it is obvious from the mentioned research, approaches to comparison of ISRM/ISRA methods significantly differ, and the approach utilized in this paper relies considerably on the works of Garrabrants et al. [7] and Lichtenstein [12].

It is important to note that Sajko et al. [17] in 2010 demonstrated a model that utilizes AHP in evaluating ISRA methods. The model consists of a hierarchy of criteria that was *determined by analyzing the available literature, integral methods of security risk assessment and the preferences of IS leaders from business organizations which participated in the research* [17, p.1217]. The complete list of criteria for evaluation is not included in that article.

3 The selection model

From the onset of the problem (selection of optimal ISRM method) it is clear that this is a multi-criteria decision making (MCDM) problem, and Analytic Hierarchy Process (AHP) was chosen as preferred MCDM method for this problem based on AHP's applicability to choice decisions [6, p.474], AHP's known applications to similar problems [17] and its popularity in the MCDM field [20]. AHP was developed by T. L. Saaty [16] and it enables structuring of a MCDM problem into a hierarchy of criteria (a criterion can be decomposed to a set of sub-criteria) which are then prioritized through an array of pairwise judgments. For each possible solution (alternative) and for each leaf criterion a score is assigned. All judgments must be acceptably consistent for the model to give meaningful results.

In 2006 ENISA published a document [4] that contains an inventory of information on some existing ISRM/ISRA methods. One of the aims [13] of that document is to enable comparison of risk management structure among ISRM/ISRA methods. The inventory includes information on 13 ISRM/ISRA methods that were selected by an expert working group. Each of those methods is described though a set of 21 attributes categorized into 3 groups (product identity card, product scope and users viewpoint). Those attributes provide a kind of "data mart" for objective comparison across different methods. On the basis of information contained in that "data mart" and based on research done by Garrabrants et al. [7] and Lichtenstein [12] a model that supports selection of optimal method is presented in this article.

The development of the model and selection of the preferred method was done in several phases. In the first phase, a hierarchy of criteria was developed. In the second phase, alternatives were evaluated with respect to the leaf criteria and in the third phase the model was tested through assigning priorities to defined criteria by a group of experts. General elements of the process are displayed in the Figure 1. It is important to note that availability of data (from the ENISA's document [4]) on one hand influenced the design of criteria hierarchy, but on the other hand reflections on criteria for ISRM selection influenced the choice of data that was taken into account.

To facilitate better understanding of the decision making process, all calculations were performed in Microsoft Excel.

Criteria and alternatives were compared (judged) via Saaty's generic gradation scale [16, p.15] that measures intensity of importance from 1 (equal importance) to 9 (extreme importance).

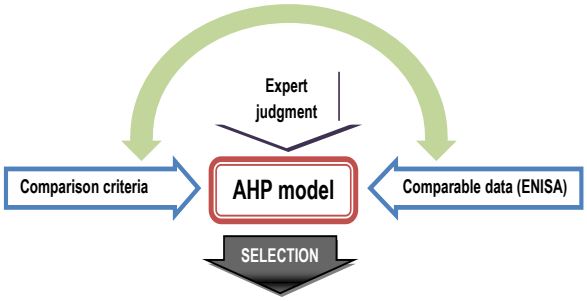

Figure 1. Selection process

3.1 Hierarchy of criteria

The developed hierarchy of selection criteria is shown in the Figure 2 and short description of each criteria and sub-criteria is displayed in the Table 2 (letters and numbers in curly brackets uniquely identify certain criteria or sub-criteria).

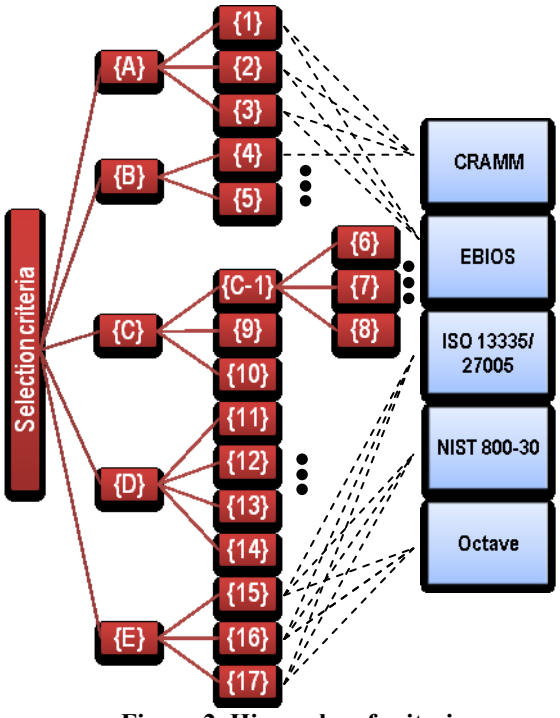

Figure 2. Hierarchy of criteria

The criteria have the following meaning:

Method Scope {A}. This criterion evaluates how important is scope of the method as a selection criterion. On sub-criteria level is evaluated how important is for the ISRM method

to include risk assessment process, risk treatment process and to provide maturity model (that enables assessment of maturity of information security and/or benchmarking to best practices).

Costs {B}. The costs criterion evaluates how important are ISRM related expenditures. On sub-criteria level importance of ISRM implementation and ISRM performance costs is analyzed.

Ease of use {C}. This criterion evaluates how important is ease of use (i.e. simplicity of use) of the method as a selection criterion. Under this criterion importance of level of skills that are needed for implementation, usage and maintenance of ISRM method, availability of support (e.g. availability of open market or licensed consultants) and adaptability of method (at which groups of organizations is the ISRM method aimed, whether the method is applicable for the organization in mind and whether the method can be custom-fitted for needs of a specific industry) are evaluated.

Table 2. Criteria and sub-criteria

Criteria (level 1)	Sub-criteria (level 2)	Sub-criteria (level 3)
{A} Method Scope	{1} Risk assessment	
	{2} Risk treatment	
	{3} Maturity model	
{B} Costs	{4} Implement. costs	
	{5} Performance costs	
{C} Ease of use	{C-1} Needed skills	{6} Implementat.
		{7} Usage
		{8} Maintenance
	{9} Support availability	
	{10} Method adaptab.	
{D} Method matureness	{11} Spread of use and renewability	
	{12} Availability of tools	
	{13} Compliance with standards	
	{14} Certification/ Accreditation	
{E} Target audience/ Information detail	{15} Management	
	{16} Operational	
	{17} Technical	

Method matureness {D}. This criterion evaluates importance of matureness of ISRM method as a selection criterion. Matureness of ISRM method encompasses spread of use of the method (e.g. how long the method exists, how often it is updated and its geographical spread of use), availability of tools that support implementation and performance of risk management process according to a specific ISRM method, alignment with information security related standards (e.g. ISO 27001, ISO 15408, ISO 17799 ISO 13335, ISO 21827, NIST SP 800-30) and possibility of certifying organizations and/or personnel.

Target audience/Information detail {E}. This criterion evaluates importance of target audience of the ISRM method or, in other words, level of detail that the ISRM method possesses as a selection of criterion. The concept of target audience/information detail refers to the fact that ISRM methods can contain high-level generic guidelines on risk management process (i.e. management level information), operational guidelines on how to implement and perform risk management process (i.e. operational level information) and/or very detailed technical step-by-step guidelines on how to establish and perform risk management process.

The defined hierarchy of criteria can now be compared with important ISRM/ISRA selection criteria defined by Garrabrants et al. [7] and Lichtenstein [12].

From the Table 1 it is visible that authors agree on 5 significant criteria: usability, adaptability, completeness, validity and credibility. Besides those criteria, Garrabrants et al. [7] define consistency and feasibility as important criteria (Lichtenstein [12] recognizes feasibility as a criteria, but not important one), and Lichtenstein [12] adds cost and complexity.

The usability criterion closely corresponds to the {C} criterion (ease of use) of the model, and adaptability directly matches sub-criterion {10} (method adaptability) of the model. The completeness criterion (defined as: *providing comprehensive coverage of all considerations of the risk management* [6, p.254]) is covered by criterion {A} (method scope), and somewhat less by criterion {E} (target audience/information detail) of the model. Other 2 criteria mentioned by both authors (validity and credibility) are not directly covered by the model, but there is a dependence between those criteria and sub-criteria {11} (Spread of use and renewability), {13} (Compliance with standards) and {14} (Certification/Accreditation) of the model. Consistency is not covered by the model and feasibility (feasibility is *concerned with the amount of data that must be collected, the economy of gathering that data, and whether the data is obtainable without extraordinary measures* [6, p.254]) is indirectly covered by several criteria and sub-criteria of the model: {A}, {C}, {12} and {E}. The costs criterion is

directly covered with the criterion {B} of the model and complexity is closely related to criteria {C} and sub-criteria {12} of the model.

As it is visible from this analysis, majority of the criteria for selection of the preferred ISRM/ISRA method that were defined by Garrabrants et al. [7] and Lichtenstein [12] are adequately covered by the model.

3.2 Choice of alternatives

From 13 ISRM methods that are included in ENISA's report [4], for the sake of simplicity, 5 were selected as possible alternatives, based on research done by Fenz and Ekelhart [5] in which they identified CRAMM, EBIOS, NIST SP 800-30, ISO 13335/27005 and Octave as a *mix of five commonly used international, US, and European methodologies*.

For each leaf criterion, pairwise comparisons were performed in which each alternative was compared with every other alternative with respect to a given criterion and the resulting priorities' vector was calculated. It is important to note that because of the structure of the hierarchy of criteria in the model and the fact that it is based on ENISA's inventory [4] of comparable and mostly measurable information; it was possible to make strictly objective judgments on preferability of alternatives. E.g. in evaluating alternatives according to the sub-criterion {2} (risk treatment) numbers proportional to detailedness of risk treatment, acceptance and communication steps of certain method were summed up and compared. Similarly, alternatives were evaluated according to the sub-criterion {10} (method adaptability) by adding up types of organizations in which a certain method can be used and comparing the resulting numbers.

4 Criteria priorities

The key step in wrapping up and testing the model is providing expert judgment that would define priorities of the criteria and test model's applicability.

10 experts with extensive knowledge and experience in ISRM were chosen to test functionality and applicability of the defined AHP model. To have an assurance on the relevance of the experts' judgments, only individuals who are or were engaged on information security risk assessment, treatment, control or audit tasks in credit institutions in Croatia and who have working experience in line with ISACA's requirements for CISM [9] or CISA [8] designations were selected. It is important to note that, according to Lichtenstein [12, p.25] 2 significant groups of stakeholders with different agendas are involved in the selection process: managers and security specialists. This research focuses only on security experts. A test case was developed and experts were asked to select an optimal ISRM method for an environment that was in line with their experience (a generic larger credit institution in Croatia). Structured interviews were conducted with each expert and their judgments were recorded (each expert was introduced in a standardized manner with observed institution's size, IT environment, business model, risk appetite, regulatory environment and detailed information on hierarchy of criteria for selection of optimal ISRM method).

Consistency ratios (CR) for every expert and for each comparison were calculated and were in the acceptable range (CR < 0.1). In line with Saaty's recommendation [16], individual judgments of experts were added up via calculation of geometric mean values and resulting local and global priorities were calculated accordingly (Table 3).

Table 3. Local and global priorities

LOCAL PRIORITIES			GLOBAL PRIORITIES
Criteria (L-1)	Sub-criteria (L-2)	Sub-criteria (L-3)	
{A} 0.206	{1} 0.684		{1} 0.141
	{2} 0.221		{2} 0.046
	{3} 0.095		{3} 0.020
{B} 0.268	{4} 0.249		{4} 0.067
	{5} 0.751		{5} 0.201
{C} 0.204	{C-1} 0.209	{6} 0.209	{6} 0.009
		{7} 0.592	{7} 0.025
		{8} 0.199	{8} 0.008
	{9} 0.592		{9} 0.121
	{10} 0.199		{10} 0.041
{D} 0.127	{11} 0.202		{11} 0.026
	{12} 0.356		{12} 0.045
	{13} 0.304		{13} 0.039
	{14} 0.137		{14} 0.017
{E} 0.195	{15} 0.307		{15} 0.060
	{16} 0.534		{16} 0.104
	{17} 0.159		{17} 0.031

Based on calculated global priorities of selection sub-criteria and previously calculated priorities of alternatives for each leaf sub-criterion, scores for all alternatives were calculated (Table 4 - in

the last row of the table is the sum of scores for each sub-criterion for a given alternative). From the end results it is visible that the EBIOS method has significantly better score than other analyzed ISRM methods and should be selected as preferred ISRM method for given criteria priorities.

Table 4. Alternatives' scores

Crit.	CRAMM	EBIOS	ISO 27005	NIST 800-30	Octave
{1}	0.044	0.050	0.016	0.016	0.016
{2}	0.001	0.016	0.016	0.006	0.006
{3}	0.002	0.012	0.002	0.002	0.002
{4}	0.002	0.019	0.008	0.019	0.019
{5}	0.012	0.047	0.047	0.047	0.047
{6}	0.001	0.002	0.002	0.002	0.002
{7}	0.002	0.006	0.006	0.006	0.006
{8}	0.001	0.002	0.002	0.002	0.002
{9}	0.013	0.034	0.006	0.034	0.034
{10}	0.002	0.020	0.007	0.010	0.002
{11}	0.008	0.005	0.006	0.002	0.005
{12}	0.019	0.012	0.006	0.003	0.005
{13}	0.004	0.019	0.011	0.003	0.002
{14}	0.002	0.009	0.002	0.002	0.002
{15}	0.015	0.015	0.015	0.002	0.015
{16}	0.021	0.021	0.021	0.021	0.021
{17}	0.013	0.001	0.001	0.013	0.001
Σ	**0.161**	**0.289**	**0.174**	**0.189**	**0.186**

5 Conclusion

Selection of appropriate ISRM method is an important task in the ISRM process since choice of an inadequate method can hamper all subsequent steps and prevent ISRM process in achieving desired results. This article presented an approach to selection of optimal ISRM method that is based on objective and comprehensive (although not panoptic) comparison of various widely used ISRM methods. The comparison and selection was performed via an AHP model that was constructed based on previous research and on inventory of information on ISRM/ISRA methods.

To summarize, the defined model is characterized by the following:

- The model is comprised of a hierarchy of criteria that enables transparent and objective comparison of different ISRM methods.
- ISRM method comparison does not require in-depth analysis of different ISRM methods.
- The model enables selection of the optimal ISRM method (a method that most closely fits the needs of a particular organization).

The developed model might be of assistance to professionals tasked with selecting an ISRM method since it provides sound framework and a selection tool that should enhance decision making process. It is important to note that the model can easily accommodate additional ISRM methods and include them in the selection process which can greatly enhance model's usefulness.

5.1 Shortcomings

The defined selection model has several shortcomings and more important ones are discussed here. Firstly, the model is based on ENISA's inventory [4] that was compiled in 2006 and there might have been significant developments in ISRM methods since then. One example is ISO 27005 method that had been considerably upgraded since 2006, but given scores for that method are based on data that was current in 2006. However, although additional information on ISRM methods might change final results of the selection process it does not influence the soundness of the model.

Apart from that, additional concern might be completeness and quality of data in ENISA's inventory since the sources of data, their objectivity and integrity are not properly addressed in the document [4]. However, ENISA's inventory should be judged as more objective and unbiased than other comparable sources because of ENISA's non-stakeholder role in the ISRM methods field.

Further on, it is important to note that there is a certain loss of cardinal information since some of the available information on costs had absolute (monetary) values and the model works with ordinal scales. This loss of information is a classic pitfall of AHP [15, p.1044]. It is, however, important to note that this loss of information was inevitable since the monetary amounts were available only for some components of total costs and only for some methods and hence weren't directly comparable among various alternatives.

5.2 Further research

There are several lines along which the research described in this article might be expanded and upgraded. Additional resources with up-to-date, comparable, objective and trustworthy information on ISRM methods would neatly fit into the model and improve its validity and

usefulness. Additional information might also enable further development of the model and allow direct and more extensive analysis of criteria like validity, credibility, consistency and feasibility. Taking into account great significance that the expert group that worked on the model gave to costs criteria, it might be gainful to try to quantify costs related with implementation and performance of various ISRM methods as to give better foundation for decision making.

Finally, it might be valuable to additionally study and test soundness and completeness of the criteria that were described by Garrabrants et al. [7] and Lichtenstein [12] and which were referenced and used in the work described in this article. Such research would further enhance or alternatively disprove validity and hence applicability of the model defined in this paper.

6 References

[1] Bhushan N, Rai K: **Strategic Decision Making Applying the Analytic Hierarchy Process**, Springer-Verlag London Limited, USA, 2004.

[2] Campbell P L, Stamp J E: **A Classification Scheme for Risk Assessment Methods**, Sandia National Laboratories Albuquerque, New Mexico, USA, 2004.

[3] Bornman W G, Labuschagne L: **A comparative framework for evaluating information security risk management methods**, ISSA 2004 Proceedings, 30th June-2nd July, Gauteng, Republic of South Africa, 2004.

[4] ENISA: Risk Management: **Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools**, European Network and Information Security Agency (ENISA), Crete, Greece, 2006.

[5] Fenz S, Ekelhart A: **Verification, Validation, And Evaluation In Information Security Risk Management**, IEEE Security and Privacy, 2011, Vol. 9, No. 2, pp. 58-65.

[6] Forman E H, Gass S I: **The Analytic Hierarchy Process - An Exposition**, Operations Research, 2001, Vol. 49, Iss. 4, pp. 469-486.

[7] Garrabrants W M, Ellis A W III, Hoffman L J, Kamel M: **CERTS: a comparative evaluation method for risk management methodologies and tools**, Computer Security Applications Conference Proceedings 3rd-7th December, Tucson, AZ, USA, 1990, pp. 251-257.

[8] ISACA: **How to Become CISA Certified**, available at `http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/How-to-Become-Certified/Pages/default.aspx`, Accessed: 11th of March 2011.

[9] ISACA: **How to Become CISM Certified**, available at `http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/How-to-Become-Certified/Pages/default.aspx#cismreq4`, Accessed: 11th of March 2011.

[10] ISACA: **The Business Model for Information Security**, ISACA, Rolling Meadows, IL, USA, 2010.

[11] IT Governance Institute: **CobiT 3rd Edition**, The CobiT Steering Committee and the IT Governance Institute, 2000.

[12] Lichtenstein S: **Factors in the selection of a risk assessment method**, Information Management & Computer Security, 1996, Vol. 4 Iss: 4, pp. 20-25.

[13] Marions L: **Risk Management and Risk Assessment at ENISA: Issues and Challenges**, ARES 2006 Proceedings, 20th-22nd April, Vienna, Austria, 2006.

[14] Niekerk L v, Labuschagne L: **The Peculium Model: Information Security Risk Management for the South African SMME**, ISSA 2006 Proceedings, 5th-7th July, Gauteng, Republic of South Africa, 2006.

[15] Peters M, Zelewski S: **Pitfalls in the application of analytic hierarchy process to performance measurement**, Management Decision, 2008, Vol. 46 Iss: 7, pp. 1039-1051.

[16] Saaty T L: **How to Make a Decision: The Analytic Hierarchy Process**, European Journal of Operational Research, 1990, Vol. 48, Iss. 1, pp. 9-26.

[17] Sajko M, Hadjina N, Pesut D: **Multi-criteria model for evaluation of information security risk assessment methods and tools**, MIPRO 2010 Proceedings of the 33rd International Convention, 24th-28th May, Opatija, Croatia, 2010.

[18] Vaidya O S, Kumar S: **Analytic hierarchy process: An overview of applications**, European

Journal of Operational Research, 2006, Vol. 169, Iss. 1, pp. 1-29.

[19] Vorster A, Labuschagne L: **A Framework for Comparing Different Information Security Risk Analysis Methodologies**, SAICSIT '05 Proceedings, 20th-22nd September, Mpumalanga, Republic of South Africa, 2005, pp. 95-103.

[20] Wallenius J, Dyer J S, Fishburn P C, Steuer R E, Zionts S, Deb K: **Multiple criteria decision making, multiattribute utility theory: Recent accomplishments and what lies ahead**, Management Science, 2008, Vol. 54, pp. 1336-1349.