Security risk analysis and management

Nicolae Anton[1] and *Anișor* Nedelcu[2,*]

[1]Transilvania University of Brasov, Faculty of Technological Engineering and Industrial Management, B-dul Eroilor nr.29, Brasov, Romania
[2]Transilvania University of Brasov, Faculty of Technological Engineering and Industrial Management, B-dul Eroilor nr.29, Brasov, Romania

Abstract. The management system of informational security is a part of the management system of an organization, that approaches the management of risk from the point of view of the involved information, approach that is used in order to set, to implement, to function, to monitor, to revise, to maintain and to improve the informational security at the organizational level, referring to the progress of the processes required by the management of risk in order to guarantee the security of the information. The appreciation of the efficiency of the security system represents a difficult problem and it contains many elements of subjectiveness, because the analysis of the security risks of information implies using some interviewing techniques based on questionnaires provided by experts in security, that in most of the cases come from outside the organization. This study does not analyse the risk concept, it focuses more on the analysis and the risk management on the practical part using AHP method. Managing the risk and the security requirements are connected by a set of practices and management tools generally used in order to manage the security risk of information. It is essential that the tool and the model used should reflect the objective needs of the organization from the point of view of the management of risk.

1 Security risk analysis and management

Information is a powerful resource of an organization that, like any other resources, adds value to the organization and needs to be protected. An Information Security Management System (ISMS) is an approach at the system level to a way of managing sensitive information with the aim of protecting it. Creating an ISMS should be a priority of the management system of any organization.

What is information security? Information security can be characterized by considering its processing and storage characteristics, its type and source, the main purpose being to ensure the confidentiality, availability and integrity of information.

An ISMS developed in accordance with the requirements of ISO / IEC 27001: 2005 contains the "plan-do-check-act" model (Figure 1), namely planning, implementation, monitoring and ultimately maintaining and improving performance [1].

[*] Corresponding author: anton_nicolae_07@yahoo.com

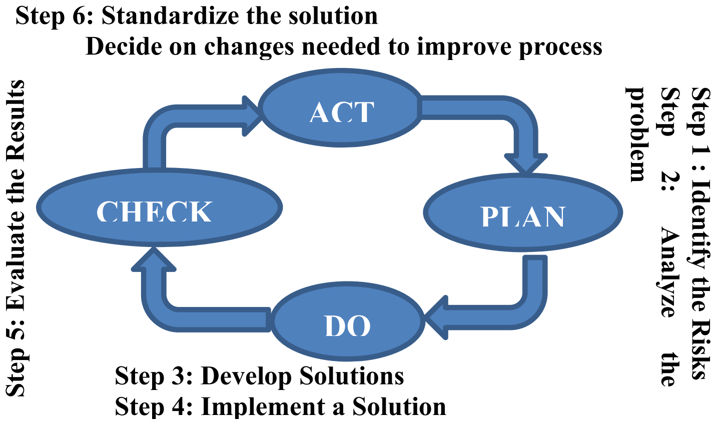

Step 6: Standardize the solution
Decide on changes needed to improve process
ACT
CHECK
PLAN
DO
Step 1 : Identify the Risks
Step 2: Analyze the problem
Step 3: Develop Solutions
Step 4: Implement a Solution
Step 5: Evaluate the Results

Fig. 1. ISMS developed in accordance with "plan-do-check-act".

ISO / IEC 27005: 2011 standard sets out the following risk treatment options [2, 3, 4]:
- Risk diminution - the level of risk is to be reduced by applying control means so that the residual risk is at an acceptable level.
- Acceptance of risk - conscious and objective acceptance of risk to open an opportunity provided that the risk is not in contradiction with the organization's policies and risk acceptance criteria.
- Avoiding risk - giving up activities or conditions that can generate a risk.
- Risk transmission - risk is passed on to a third party who has higher skills to control risk.

1.1 Risk evaluation

In any risk assessment or risk management methodology, the concept or risk occupies a central role. There may also be differences in the number, meaning and relationships of the risk factors, as well as how they can be operationalized, measured, and calculated to quantify the risks significantly. The risk analysis can be: **Qualitative**, when no allocation of financial resources is required and at the end the risk classification is made on a scale of appreciation, or **Quantitative**, when it is necessary to allocate financial resources, determining the cost associated with each risk

The qualitative analysis of risk is based on the subjective judgment of the security risk assessment members to determine the overall security risk to the information systems. Sometimes, qualitative security risk equation variables are expressed as numbers.

Many risk management methods promoted by management consultants and international standard organizations involve calculating a numerical value for risk based on simple point scales combined in some way. Such scales are subjective and are usually based on some kind of ordinal comparisons or classifications [5].

An approach that relies on specific formulas and calculations to determine the value of the security risk decision variables defines the Quantitative analysis. There exist several formulas more commonly associated with quantitative security risk analysis. They cover the expected loss for specific security risks and the value of safeguards to reduce the security risk.

There are three classic quantitative security risk analysis formulas: Annual Loss Expectancy (ALE) (= Single Loss Expectancy × Annual Rate of Occurrence), Single Loss Expectancy (= Asset Value × Exposure Factor) and Safeguard Value (= ALE Before × ALE After × Annual Safeguard Cost).

Attempts to assign real numbers to the costs of countermeasures and the amount of damage that can take place. Provides concrete probability percentages when determining the likelihood of threats and risks. Purely quantitative risk analysis is not possible because the method is attempting to quantify qualitative items [6].

2 Steps of risk management

Risk management is a continuous process that involves risk identification, analysis, use, monitoring, planning, and on-going documentation throughout the entire process. The main stages of the risk management process are: **Risk identification** (It is the process of examining critical areas for events that represent potential risks to ensure costs, programs, performance goals), **Risk analysis** (It is the process of assessing each risk that allows both its description of the likelihood of production, the severity of the consequences and the relationship with other risk areas or processes, as well as setting some priorities), **Risk management** (It is the process of identifying, evaluating, selecting and applying ways to reduce the risk, transferability, permissiveness or acceptance of options to ensure an acceptable level of risk, subject to constraints and limitations in the program) and **Risk evaluation** (It is the process of systematically tracking and evaluating the performance of risk handling actions compared to the limits set in the program)

3 Risk assessment based on AHP

The Analytic Hierarchy Process (AHP) was developed by Thomas L. Saaty in the 1970s and has been extensively studied and refined since then. The vast and diverse application of AHP evidence that AHP is a credible decision-making tool. The AHP can be implemented in several consecutive steps:
Step 1 - Computing the vector of criteria weights by defining the Structure and Hierarchy.
Step 2 - Computing the matrix of option scores by creating a pairwise comparison matrix.
Step 3 - Ranking the options by estimating the relative weights (as the final step, the option ranking is accomplished by sorting the global scores in decreasing order).

3.1 Computing the vector of criteria weights – Define the structure and hierarchy

At this stage, AHP decomposes a complex multi-criteria decision-making problem into a hierarchically interconnected decision criterion, taking into account decision alternatives.

Table 1. A hierarchically interconnected decision criteria in security management risk.

CRITERIA 1	CRITERIA 2
Confidentiality C1	Asset Management (C2a): Any means that enable the organization to achieve its business purposes such as the data, personnel, devices.
Integrity C2	Data Security and Access Control (C2b): Information and records (data) are managed consistent with the organization's risk strategy to ensure protection of the confidentiality, integrity and availability of information.
Availability C3	Security Continuous Monitoring (C2c): The information system and assets are monitored at discrete intervals to identify cyber security events and verify the effectiveness of protective measures.

3.2 Computing the matrix of option scores - creating a pairwise comparison matrix

In order to determine the relative importance of a criterion within each level (Table 2), a prioritization procedure starts. In order to compute the weights for the different criteria, the AHP starts creating a pairwise comparison matrix A. The matrix A is a m×m real matrix, where m is the number of evaluation criteria considered. Each entry C_{jk} of the matrix A represents the importance of the j^{th} criterion relative to the kth criterion. If $C_{jk} > 1$, then the j^{th} criterion is more important than the *k*th criterion, while if $C_{jk} < 1$, then the j^{th} criterion is less important than the *k*th criterion. If two criteria have the same importance, then the entry C_{jk} is 1.

Table 2. The relative importance of a criterion within each level.

Value of Cjk - Intensity of Importance	Interpretation
1	j and k are equally important
3	j is slightly more important than k
5	j is more important than k
7	j is strongly more important than k
9	j is absolutely more important than k
2, 4, 6, 8	Intermediate value between adjacent scales value.

Let C = {Cj| j = 1, 2, …, n} be the set of criteria. The result of the pair-wise comparison on n criteria can be summarized in an (n×n) evaluation matrix A in which every element aij (i, j = 1, 2, …, n) is the quotient of weights of the criteria, as shown in Eq. (1):

$$A = \begin{bmatrix} a11 & a12 & \cdots & a1n \\ a21 & a22 & \cdots & a2n \\ & & \ddots & \\ & & \cdots & \\ an1 & an2 & & ann \end{bmatrix}, \quad aii = 1, \quad aij = \frac{1}{aji} \tag{1}$$

Where $a11$ represents the comparison between element i and element j.

3.3 Ranking the options - Estimate the relative weights (as the final step, the option ranking is accomplished by ordering the global scores in decreasing order)

In this final step, the mathematical process starts to normalize and identify the relative weights for each matrix. The relative weights are given by the eigenvector (**W**) corresponding to the largest eigenvalue ($\boldsymbol{\lambda}_{max}$), as $AxB = \boldsymbol{\lambda}_{max} W$, where $\boldsymbol{\lambda}_{max}$ – the maximum eigenvalue and **W** – eigenvector corresponding to $\boldsymbol{\lambda}_{max}$. If the pair-wise comparisons are consistent, then the matrix A has the rank n and $\boldsymbol{\lambda}_{max} = n$. In this case, weights can be obtained by normalizing any of the rows or columns of A. An important advantage that AHP has over other some other algorithmic methods is that it takes into account inconsistencies in the preferences. The quality of the output of the AHP is strictly related to this consistency of the pair-wise comparison judgments. The consistency is defined by the relationship between the entries of A: $a_{ij} \cdot a_{jk} = a_{ik}$. The consistency index (CI) [7] is

$$CI = \frac{\lambda\, max - n}{n - 1} \tag{2}$$

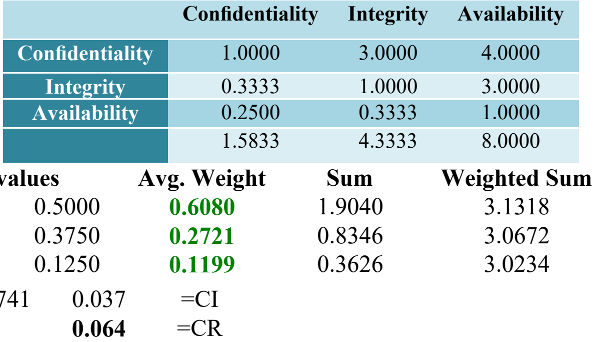
Where **λ** $_{max}$ is the largest eigenvalue of the judgment matrix A and n is the rank.

The final consistency ratio (CR), which permits someone to conclude whether the evaluations are sufficiently consistent, is calculated as the ratio of the CI and random index (RI), as indicated in the equation CR = CI / RI, where the random index (RI). The RI reference matrix (Table 3), is:

Table 3. The RI reference matrix.

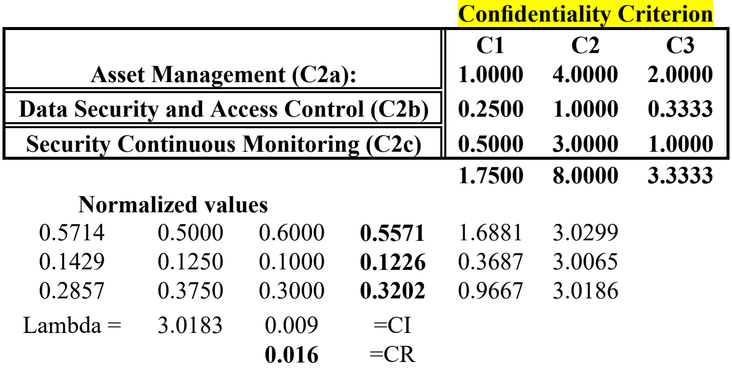
n	1	2	3	4	5	6	7	8	9	10	11
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49	1.51

The consistency ratio (CR) provides a measure of the probability that matrix ratings were randomly generated. The value of 0.1 is the accepted upper limit for CR. In the case studied here:



	Confidentiality	Integrity	Availability
Confidentiality	1.0000	3.0000	4.0000
Integrity	0.3333	1.0000	3.0000
Availability	0.2500	0.3333	1.0000
	1.5833	4.3333	8.0000

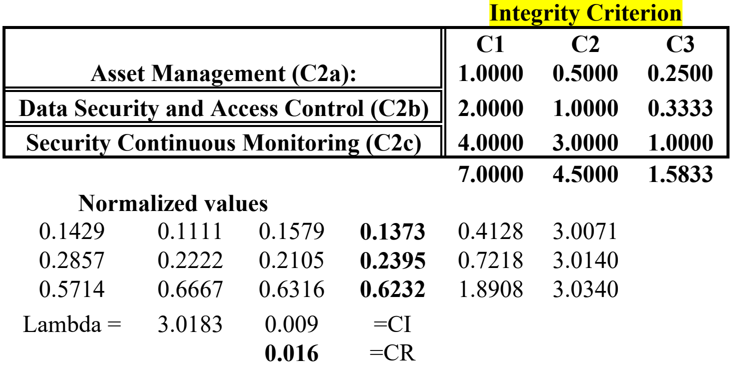
Normalized values			**Avg. Weight**	**Sum**	**Weighted Sum**
0.6316	0.6923	0.5000	**0.6080**	1.9040	3.1318
0.2105	0.2308	0.3750	**0.2721**	0.8346	3.0672
0.1579	0.0769	0.1250	**0.1199**	0.3626	3.0234
Lambda =	3.0741	0.037	=CI		
		0.064	=CR		



Confidentiality Criterion

	C1	C2	C3
Asset Management (C2a):	**1.0000**	**4.0000**	**2.0000**
Data Security and Access Control (C2b)	**0.2500**	**1.0000**	**0.3333**
Security Continuous Monitoring (C2c)	**0.5000**	**3.0000**	**1.0000**
	1.7500	**8.0000**	**3.3333**

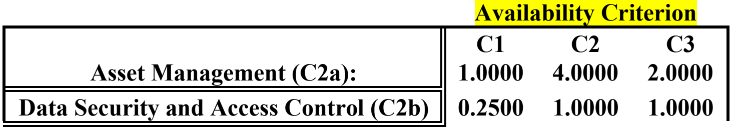
Normalized values					
0.5714	0.5000	0.6000	**0.5571**	1.6881	3.0299
0.1429	0.1250	0.1000	**0.1226**	0.3687	3.0065
0.2857	0.3750	0.3000	**0.3202**	0.9667	3.0186
Lambda =	3.0183	0.009	=CI		
		0.016	=CR		



Integrity Criterion

	C1	C2	C3
Asset Management (C2a):	**1.0000**	**0.5000**	**0.2500**
Data Security and Access Control (C2b)	**2.0000**	**1.0000**	**0.3333**
Security Continuous Monitoring (C2c)	**4.0000**	**3.0000**	**1.0000**
	7.0000	**4.5000**	**1.5833**

Normalized values					
0.1429	0.1111	0.1579	**0.1373**	0.4128	3.0071
0.2857	0.2222	0.2105	**0.2395**	0.7218	3.0140
0.5714	0.6667	0.6316	**0.6232**	1.8908	3.0340
Lambda =	3.0183	0.009	=CI		
		0.016	=CR		



Availability Criterion

	C1	C2	C3
Asset Management (C2a):	**1.0000**	**4.0000**	**2.0000**
Data Security and Access Control (C2b)	**0.2500**	**1.0000**	**1.0000**

Security Continuous Monitoring (C2c)	**0.5000**	**1.0000**	**1.0000**
	1.7500	**6.0000**	**4.0000**

Normalized values

0.5714	0.6667	0.5000	**0.5794**	1.7937	3.0959
0.1429	0.1667	0.2500	**0.1865**	0.5655	3.0319
0.2857	0.1667	0.2500	**0.2341**	0.7103	3.0339

Lambda = 3.0539 0.027 =CI
0.046 =CR

	Confidentiality C1	Integrity C2	Availability C3			
Asset Management (C2a)	**0.5571**	**0.1373**	**0.5794**	**0.6080**	**0.4456**	1st choice
Data Security and Access Control (C2b)	**0.1226**	**0.2395**	**0.1865**	**0.2721**	**0.1621**	3rd choice
Security Continuous Monitoring (C2c)	**0.3202**	**0.6232**	**0.2341**	**0.1199**	**0.3924**	2nd choice

4 Conclusion

In the life cycle of any information system, information security risk assessment is an important assessment method and mechanism. By using Analytic Hierarchy Process (AHP), ordinal scale to ratio scale can be converted and even its consistency can be checked. The AHP is a very flexible and powerful tool due to the fact that the scores, and thus the final ranking, are obtained on the basis of the pairwise relative evaluations of both the criteria and the options provided by the user. Having this in consideration, it can be used as a decision-making tool in security risk management. The AHP method is operable and efficient because it prioritizes and orders risk incidents, which can also satisfy the goal of risk management.

References

1. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements
2. ISO/IEC 27005:2011. Information technology. Security techniques. Information security risk management
3. I. Cojocaru, M. Guzun, R. Ionescu, *Information Security Management System of ISO / IEC 27001: 2013. Implementation Algorithm* (in Romanian), The 8-th International Conference and Computer Science & The 5-th Conference of Physicists of Moldova, Chisinău, Republic of Moldova, 362, (2014)
4. M. Guzun, I. Cojocaru, *Identifying, Assessing and Treating Risks of Information Security* (in Romanian), Institute for Information Society Development (IDSI, www.idsi.md), R. Moldova (https://idsi.md/files/Colocviu_Evrika_M_Guzun-Ig_Cojocaru-riscuri-securit-inform_2016.pdf), 117, (2016)
5. D. Hubbard, D. Evans, *Problems with scoring methods and ordinal scales in risk assessment* (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.163.4544&rep=rep1&type=pdf)
6. V. Dan, *InfoSec Adventures & More - CISSP CBK 3 – Security Management Practices* (https://www.pentest.ro/cissp-cbk-3-security-management-practices/)
7. K. Bunruamkaew, *How to do AHP analysis in Excel* (http://giswin.geo.tsukuba.ac.jp/sis/gis_seminar/How%20to%20do%20AHP%20analysis%20in%20Excel.pdf)