Practical Methods for Information Security Risk Management

Cristian AMANCEI
Academy of Economic Studies, Bucharest, Romania
cristian.amancei@ie.ase.ro

Abstract - The purpose of this paper is to present some directions to perform the risk management for information security. The article follows to practical methods through questionnaire that asses the internal control, and through evaluation based on existing controls as part of vulnerability assessment. The methods presented contains all the key elements that concurs in risk management, through the elements proposed for evaluation questionnaire, list of threats, resource classification and evaluation, correlation between risks and controls and residual risk computation.

Keywords: *Risk Management, Threats, Vulnerabilities, Information Security*

1 Introduction

Research on risk has evolved from an approach based on the negative dimension of the risk to a complex approach, where the risk is seen as a threat and as an opportunity.

Risk management for information security consists in risk assessment, risk control and documentation, and risk reporting [2].

Risk management for information security is an iterative process that passes through interconnected steps, from risk assessment, risk control and documentation, to risk reporting.

A risk management approach must address at least the following criteria: the criteria for risk assessment, the impact criteria, and the risk acceptance criteria [3].

Beside this, the organization assess whether it has the necessary resources to perform: risk assessment and the development of a risk treatment plan, definition and implementation of policies and procedures, including the implementation of selected controls for risk treatment, controls monitoring, risk management process monitoring.

Risk assessment criteria are developed to assess information security risks on the organization, taking into account the following [1]:

- strategic value of information processes within the organization;
- the importance of information assets involved;
- legal requirements and contractual obligations;
- organization and operational importance of the availability, confidentiality and integrity of information;
- expectations and perceptions of shareholders, customers and suppliers of the company and the negative consequences it can have on reputation.

Impact criteria are developed and specified as the level of damage caused or the cost for organization, produced by an event that affected the security of information, taking into account: the classification of information assets affected; the security gap produced (loss of confidentiality, integrity and availability); affected operations (internal or external); financial losses; delay in meeting deadlines; loss of reputation for the organization.

Risks treatments involve choosing an action or response strategy for each risk analyzed, and present it in the risk treatment plan. The treatment options, that are not necessarily mutually exclusive or appropriate in all cases, include the following:

- risk avoidance eliminates uncertainty by not undertaking the actions appreciated as very risky to the business. Usually for critical risks this method may be applied for avoidance.
- risk transfer by using risk ownership transfer, or by using insurance, guarantees or contractual clauses;
- reduce risk by changing the risk exposure (through impact and / or probability

mitigation). The measures listed in this category can be used both when identifying and assessing risk, and also at the time of their occurrence, and are aimed at either reducing the likelihood or impact or both components of risk. Methods to reduce risk:
  - implementation of security controls;
  - improving procedures;
  - changing the environment by reducing exposure to vulnerabilities;
  - implementation of early detection methods to catch the threat when it happens and to reduce potential damage that this may cause;
  - change continuity plan, to address how the business can continue if a specific threat appears;
  - security awareness training sessions where applicable.
- risk acceptance, relates to getting approval from top management to accept the current level of risk, without implementing security measures. This approach is preferable in the situations where the cost of implementing protective measures exceeds the benefits, or when the level of risk is necessary for business development.

Risk acceptance criteria depend on policies, objectives and interests of parties involved in the organization. Organizations define their own classification of risk acceptance levels, taking into account the following [4]:
- risk acceptance criteria include multiple thresholds, each associated with a risk level, present in the risk treatment plan;
- risk acceptance criteria must be expressed as a percentage of estimated profit (or other benefits of the organization) associated with the estimated risk;
- different risk acceptance criteria apply to different classes of risks, such as non-acceptance of non-compliance risks, while high risks can be accepted as a contractual requirement;
- risk acceptance criteria for high risks include additional treatments, such as commitments and approvals that will be taken to reduce risk to an acceptable level in a defined time period.

Risk acceptance criteria are different, corresponding to the period in which the risk exists (long or short term). The development of risk management process for information security, involves a careful identification of assets, threats to those assets, and vulnerabilities to which they are exposed. The results of these activities are used to assess risk and to identify risks that need treatment [6].

To assess the likelihood of a threat, we have to assess how long the asset will have value or for how long it has to be protected. The likelihood of a threat is affected by the following [5]:
- attractiveness of the asset or the possible impact that occurs when a deliberate action is taken into account;
- how easy it is to convert vulnerability exploitation into earnings, when deliberate action is taken into account;
- technical capabilities of the agent who carries the threat, applicable for deliberate actions;
- susceptibility of vulnerability exploitation, which applies to technical and non-technical vulnerabilities.

2 Methods for information security risk management

The following approaches are proposed for risk management: questionnaire method for assessing internal control, and evaluation based on existing controls as part of vulnerability assessment.

Method based on the use of questionnaires to assess the internal control starts from the inherent risk assessment, depending on the probability of occurrence of a risk scenario (threat exploiting a vulnerability) and the impact on the organization's resources, as the following questionnaire to assess the internal control and calculate the residual risk remaining after implementation of controls. The method uses a list of threats that underlie the definition of risk scenarios and resources affected by the risk scenarios are evaluated in terms of loss of confidentiality, integrity, availability and reliability of the resource

class level. The method first calculates the risk inherent risk that obtained by assessing the likelihood and impact for each risk scenario that is applied to resources within the organization. Existing controls within the organization, which are assessed by questionnaire, are correlated with risk defined through a correlation matrix, and thus obtain the value defined for each risk controls, with which we calculate the residual risk remaining after application of the controls. Residual risk is classified according to Table 1, medium and critical risks will be included in the risk treatment plan reduce risk to an acceptable level for the organization.

Risk treatment plan based on the medium and critical risks, includes the proposed measures for implementation, with deadlines, responsible and risk residual value expected to be achieved after the implementation of the plan to verify that sufficient measures are proposed and approved, but also to have a basis for measuring the results.

Inherent risk (IR) is calculated using the following formula:

$$IR = P \times I$$

where:

P - probability that the risk scenario will occur;

I - the impact on the organization.

Probability will be evaluated using the levels defined in Table 1.

Table 1. Probability levels description

Level	Frequency of occurrence	Description	Probability interval
1	Very rarely	May occur in exceptional circumstances	0 – 0.1
2	Rarely	It can sometimes occur	0.1 – 0.3
3	Medium	Almost equal chance of occurrence	0.3 - 0.6
4	Probably	Appears frequent	0.6 - 0.9
5	Almost certain	Appears often	0.9 - 1

The possible levels of impact are: 1 – insignificant; 2 – minor; 3 – moderate; 4 – major; 5 - catastrophic. Inherent risk values are presented in the following table:

Table 2. Inherent risk values

Probability	IR = P x I				
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	Impact				
	Minimum risk (acceptable)		Medium risk		Critical risk

The following steps are applied in developing the method:

a) For each control that is evaluated to develop a set of questions; they may be single or multiple answer questions, but with the maximum response value of 10; the answers are aggregated at the control level, as shown in Table 3.

Table 3. Questionnaire

No.	Control / question / answer	Response selected	Possible answers value	Question value	Control value (average value of questions)
C1	Responsibilities assigned for information security				9
Q1	Is there a clear definition of roles and responsibilities for the management of various information security issues?	One response		10	
	No		0		
	Yes, but not formally		5		
	Yes, formally	x	10		
Q2	Which of the following responsibilities are formally assigned?	Multiple response		8	
	Information Security Officer	x	2		
	Application administrator/OS/DB	x	2		
	Application developer / design		2		
	Application testing	x	2		
	Users	x	2		

b) The list of threats to information security is developed. Based on experience, the following list of threats has been developed:

Table 4. List of threats

No.	Threat	Definition
1	Fire	An outbreak of fire which destroyed part of the organization's headquarters.
2	Earthquake	Earthquake with a magnitude severe enough to affect the organization's operations.
3	Flooding	Water infiltration or flooding as a result of cracks in walls, ceilings, broken windows, damaged water pipes.
4	Unauthorized network access	Penetration activity in a computer system, computer network with the intent to steal, corrupt data, information, or to impede the functioning of the organization's operations. Unauthorized access can be external / internal, intentional / unintentional, such as virus attacks, hacker attempts, denial of service attacks.
5	Theft and sabotage	Unauthorized removal, theft, modification, destruction of the organization's resources: hardware, software, paper documents, electronic documents. Any unauthorized use of intellectual property or organization outside the organization processes applications.
6	Inadequate use of applications	Use of unauthorized and/or unlicensed applications on the organization's systems, misuse of business applications by employees.
7	Equipment damage	Failure of IT equipment (servers, network equipment), or those non-IT (ventilation, air conditioning, fire protection equipment)

8	Utilities failure	Feathers in the provision of utilities are incidents that can cause an interruption of the operations organization and processes for a time: power failure, communication line failure.
9	Human error	Human errors can be caused by negligence or lack of information, knowledge of the organization's staff, leading to disruption of normal activities.
10	Insufficient staff	Mass of staff absence, which may lead to disruption of normal activities of the organization. Lack of staff may be voluntary and/or planned the strike, or spontaneous and unplanned, vacation due to bad weather, pandemic.
11	Extreme temperature and humidity	High heat can cause damage to magnetic media and equipment. The high humidity can cause corrosion of equipment.
12	Terrorism	The terrorist attack on or near a permanent, could affect the organization's IT operations.
13	Legislative changes	Legislative changes that may affect the organization's operations.
14	Social engineering	The staff of the organization may be confused and / or misdirected to obtain sensitive information.

c) Classification and evaluation of resources by confidentiality, integrity, availability and authenticity;

Table 5. Resources classification and evaluation

No.	Resource category	Resource type	C	I	A	Au	Resource value
1	Information	Application	5	5	5	5	g(C,I,D,Au)
2		Documents on paper	4	5	5	4	g(C,I,D,Au)
3	Infrastructure	Software	5	5	5	5	g(C,I,D,Au)
4		Hardware	5	5	5	4	g(C,I,D,Au)
5		Buildings and utilities	3	3	4	2	g(C,I,D,Au)
6	Personnel	Operational and management personnel	4	3	4	3	g(C,I,D,Au)
7		Nonoperational personnel	5	5	5	5	g(C,I,D,Au)
8	Communication	Communication equipment	5	5	5	5	g(C,I,D,Au)
9		E-mail	5	5	4	5	g(C,I,D,Au)

The description of the quality characteristics resources. levels are defined based on the impact on the

Table 6. Quality characteristics (C, I, A, Au) levels description

Level	Description
1	Cases in which there is no impact on resources, if the quality characteristic is compromised.
2	Cases in which the impact on resources is reduced, if the quality characteristic is compromised.
3	Cases in which the impact on resources is medium, if the quality characteristic is compromised.
4	Cases in which the impact on resources is high, if the quality characteristic is compromised.

5	Cases in which the impact on resources is very high, if the quality characteristic is compromised.

d) Risk scenarios are defined, that may affect the organization's resources, based on the above threats, each scenario involving a probability level;
The impact is calculated using the following formula:

$$I = \sum_{i=1}^{j} RV_i \Big/ j$$

where:
j - the resource types affected by a risk scenario;
RV - resource value.

Table 7. Risk scenarios

	Risk scenario			**Affected resource types**				**Inherent risk**
No.	**Threat**	**Vulnerability**	**P**	**R1**	**…**	**R9**	**I**	**IR (P x I)**
1	Flooding	Lack of technical verification of pipelines	3	x		x	3,8	11,4
2	Unauthorized network access	Unclear or incorrect allocation of information security responsibilities	5	x	x	x	4,2	21
3	Unauthorized network access	Poor management of incidents	5	x	x	x	4,2	21
4	Human error	Reporting scheme misunderstanding	4		x	x	4	16
5	Insufficient staff	Absenteeism due to pandemic	4		x		4	16

e) Development of correlation matrix between scenarios and controls and evaluation of controls for each risk scenario

Table 8. Scenarios – controls correlation

	Applied controls value	**21,25**	**18,33**	**16,25**	**17,5**	**21,25**
No.	**Scenario / Control**	**1**	**2**	**3**	**4**	**5**
C1	Responsibilities assigned for information security	9	9		9	9
C2	Compliance with safety requirements in relation to third parties		5	5	5	
C3	Protection of physical storage media in transit	8	8	8		8

Applied controls value is calculated using the following formula:

$$CV = (\sum_{i=1}^{k} C_i \Big/ k) * 2{,}5$$

where:
k - controls applied to the selected scenario;
C - control value.

f) Computation of residual risk after controls implementation, for the selected scenario:

Table 9. Residual risk computation

	Risk scenario		Inherent risk	Applied controls value	Residual risk
No.	**Threat**	**Threat**	**IR**	**CV**	**IR-CV**
1	Flooding	Lack of technical verification of pipelines	11,4	21,25	-9,85
2	Unauthorized network access	Unclear or incorrect allocation of information security responsibilities	21	18,33	2,66
3	Unauthorized network access	Poor management of incidents	21	16,25	4,75
4	Human error	Reporting scheme misunderstanding	16	17,5	-1,5
5	Insufficient staff	Absenteeism due to pandemic	16	21,25	-5,25

Residual risk is classified according to table 2, medium and critical risks will be included in the risk treatment plan.

Method based on an assessment of existing controls as part of vulnerability assessment seeks risk evaluation as the current level of risk in the organization, taking into account existing controls. In this method affects the vulnerability of controls taken into account when calculating risk. The level of threat and value of the resource risk assessment is set at the beginning and remain unchanged during the annual or biannual process of risk management, pending changes in the computer systems of the organization. For risks that do not fall within the acceptable risk, the treatment plan to establish new controls will be implemented to reduce risk and assess the vulnerabilities that will be achieved after implementation.

Risk (RI) is given by the following formula:

$$RI = TL \times VL \times RV$$

where:

TL - threat level defined in table 10;

VL - vulnerability level defined in table 10;

RV - resource value.

Table 10. Threat and vulnerability levels

Threat evaluation	
Level	**Description**
1	Unlikely or without known precedent.
2	Occurrence probability is once every two years.
3	Occurrence probability is once every quarter.
Vulnerability evaluation	
Level	**Description**
1	Controls operate effectively guaranteed at every occurrence of the threat.
2	The controls are partially effective and will work in most cases of the threat occurrence.
3	Controls, most likely, will fail at the emergence of the threat, or there is no control to mitigate the threat.

Risk values thus obtained are classified according to table 11. In this approach the organization may intervene in the modification of the vulnerability level through controls implemented.

Table 11. Risk values

	Threat level	**1**			**2**			**3**		
Resource value	**Vulnerability level**	**1**	**2**	**3**	**1**	**2**	**3**	**1**	**2**	**3**
	1	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27
	4	4	8	12	8	16	24	12	24	36
	5	5	10	15	10	20	30	15	30	45

The following steps are applied in developing this approach:

a) assessment of organizational resources in terms of confidentiality, integrity, availability and authenticity;
b) threats evaluated based on the level described in table 10;
c) vulnerability assessment for each threat, taking into account existing controls within the organization, as listed in the table below:

Table 12. Vulnerability assessment

Risk	**Threat**	**Vulnerability**	**Affected resources**	**Existing controls**	**VL**
1	Fire	Presence of flammable materials	Information, infrastructure, personnel, communication	The presence of flammable materials is not permitted on the premises of the organization	1
2		Failure to detect a fire startup	Information, infrastructure, personnel, communication	The organization's headquarters has installed smoke detectors	1
3		Failure responding to a fire startup	Information, infrastructure, personnel, communication	The organization is provided with fire extinguishing, which are checked regularly	2
4	Floods	Lack of a technical verification of pipelines	Information, infrastructure, communication	The organization has defined maintenance programs for facilities	1
5	Unauthorized network access	Unclear or incorrect allocation of information security responsibilities	Information, infrastructure, personnel, communication	The organization has defined staff responsibilities for information security	2

d) Risk assessment taking into account existing controls is performed, and residual risk is obtained:

Table 13. Residual risk value

No.	**Risk**	**TL**	**VL**	**RV**	**RI**
1	R1	3	1	5	15
2	R2	3	1	5	15
3	R3	3	2	5	30
4	R4	3	1	5	15
5	R5	3	2	4	24

Regardless of the approach for risk analysis, because this is done annually, it is recommended to develop a system of indicators to alert the responsible persons in respect of changes to the results obtained in previous analysis, which require a reassessment before the deadline established. This system of indicators should address most of the risks identified within the organization.

The risk analysis performed can also be used in business discontinuity, by providing the key risks that can interrupt the business processes. These risks are used for compiling a list of likely disaster scenarios and analyze their effects on processes, development of business continuity management strategies, define business continuity plan and procedures for continuity related.

3 Conclusions

Risk analysis on information security is important in any organization, in terms of ensuring the maintenance of controls implemented and for management risks evolutions. The monitoring of the risk indicators has to be defined and carefully performed in order to capture the modification of risk exposures for the organization.

Acknowledgement

This work was supported by CNCSIS-UEFISCSU, project number PNII – IDEI 1838/2008.

References

[1] I. Ivan, G. Noşca, S. Capisizu, *Auditul sistemelor informatice*, Editura ASE, Bucureşti, 2005, ISBN: 978-973-594-638-6

[2] ISO/IEC 27002:2005 *Information technology -- Security techniques -- Code of practice for information security management*

[3] J. Pathak, *Information Technology Auditing An Evolving Agenda*, Editura Springer, Berlin, 2005

[4] J. Schalken, H. Vliet, "Measuring where it matters: Determining starting points for metrics collection", *Journal of Systems and Software*, Elsevier, Vol. 81, Issue 5, 2007, pp. 603-615

[5] S. Vacca, "Risk Based Compliance Programs: Models of Success", *Governance, Risk and Compliance Conference*, The Institute of Internal Auditors, Florida, 2008

[6] M. Eppler, M. Aeschimann, "A Systematic Framework for Risk Visualization in Risk Management and Communication", *Risk Management*, Vol. 11, Issue 2, 2009, pg. 67-89.

Cristian AMANCEI is University Assistant at Academy of Economics Studies Bucharest, Faculty of Economic Cybernetics, Statistics and Informatics. He is a PhD candidate from October 2007 at Economic Informatics Department from Academy of Economic Studies. He holds a Master in Science – Computerized Project Management from Academy of Economic Studies, Bucharest. He is Certified Information Systems Auditor (CISA). He graduated in Economic Informatics at Faculty of Economic Cybernetics, Statistics and Informatics in 2006. His main research areas are: information system audit, data structures, metrics in information systems, IT controls and IT risks.