IT Risk Assessment: Quantitative and Qualitative Approach

Artur Rot

Abstract— **IT risk management currently plays more and more important role in almost all aspects of contemporary organizations' functionality. It requires reliable and cyclical realization of its key task which is risk analysis. Literature of subject presents problems of risk analysis in different way, the most often skipped or selectively treated the problem of quantitative methods application for the purpose of risk analysis. The article presents the issue of one of the most significant stages of risk analysis which is IT risk assessment, especially focusing on chosen quantitative methods such as ALE (*Annual Loss Expected*) method, Courtney method, Fisher's method, using survey research ISRAM model (*Information Security Risk Analysis Method*) and other derived ratios. There were also shortly presented chosen qualitative methods – FMEA (*Failure Mode and Effects Analysis*) and FMECA (*Failure Mode and Effects Criticality Analysis*), NIST SP 800-30 method and CRAMM methodology.**

Index Terms— **IT risk, IT security risk analysis methods, qualitative risk assessment methods, quantitative risk assessment methods.**

I. Introduction

The risk connected with the wide application of information technologies in business grows together with the increase of organization's correlation from its customers, business partners and outsourced operations. Technological progress generates dependencies which evoke growth of diversities, complexity, non-descriptiveness and quantity of risk factors. In insufficient investments on information security the issue of IT risk assessment becomes more significant, concentrating on searching optimal proportion between threats and costs of IT systems protections. In such a dynamic development of Information Technologies the time needed for appropriate reaction on risk is decidedly shortened. The lack of appropriate preparation may lead the company to collapse, thus appropriate reaction on risk constitutes about possibilities of survival and development of enterprise. The problem of IT risk management is very complex issue. One of the most important stages of this process is risk analysis, used for optimization, and correctly for minimizations of losses connected with risk. One of its key elements is evaluation stage or risk assessment. The literature of subject very often skips the issue of quantitative methods of risk assessment, only concentrating on rare, chosen qualitative methods. Also in literature concerning security of IT systems this problem is totally skipped or has no great meaning. It is caused by huge difficulty in conduct of this process and selection of appropriate methods of measures. That is why in publications from this scope there most often are presented simple qualitative methods, where assessment of Information Technology risk value is connected only with qualitative description, and definition of quality scales for frequencies of threat occurrence or description of so called threats scenarios [12].

The aim of this article is to present chosen methods of Information Technology risk assessment. There will be discussed chosen quantitative and some qualitative methods of IT risk assessment.

II. Notion of Risk

Theoreticians and practitioners do not give one universal definition, thus there exist many of them in the literature. According to ISACA, the risk is a possibility of occurrence of event, which will have undesirable effect on a given organization and its Information Systems [6]. The science about the risk is developed in most of scientific disciplines and applied in all technologies. There should be remembered that in different scientific disciplines, the risk is perceived differently. Also in different forms of business activity we will have individual forms of risk. Other types of risk will occur in production enterprise and other ones for example in financial sector.

In the context of IT systems security the risk of IT systems is overall measure of probability and seriousness of situation, in which a given threat uses specific weakness, causing loss or damage of system assets, therefore indirect or direct loss for organization.

IT risk it is the threat that Information Technology applied in a given organization (independently from its type and scale of business activity) [5]:

- Does not fulfill business requirements,
- Does not ensure appropriate integrity, security and availability,
- Was not appropriately implemented and does not work according to assumptions.

III. IT Risk Analysis

Analysis of IT risk is undoubtedly key element of the process of Information Systems security management and therefore management of risk. Publications connected with these problems – both domestic and international – seem to treat it in arbitrary way. It manifests in multitude of

Manuscript received July 22, 2008.

Dr Artur Rot is with the Department of Management Information Systems Engineering, Business Informatics Institute, Wroclaw University of Economics, Wroclaw, Poland (e-mail: artur.rot@ue.wroc.pl).

definitions of risk analysis, and also in the fact that risk analysis is often identified with its management [12]. Risk analysis is main and the most important process of risk management, identifies and evaluates risk which has to be controlled, minimized or accepted.

Risk analysis is comprehensive identification of threats and susceptibility if IT system’s assets and determination of the need of its control or acceptance of determined measures at previously stated level. The aim of risk analysis is provision of information which is indispensable for decision on application of specified methods, security resources in the enterprise. In figure 1 there was presented general model of risk analysis.

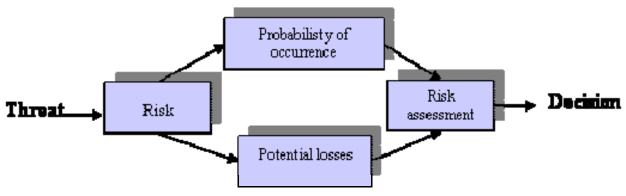

Fig. 1 Risk analysis model
Source: [11, p. 232]

Risk analysis inclines to carry out works in areas [4, p. 283-284]:

– Resource evaluation (information, software, hardware and physical resources) – value of resource it is not only value of its purchase but also short term effects and long term consequences from its destruction,
– Assessment of consequences – definition of the degree of destruction or losses, which can supposedly occur,
– Identification of threats – analysis of threats should determine probability of its occurrence and possibility of resource destruction,
– Analysis of protections in the aspect of effectiveness of existing means of protections,
– Analysis of susceptibility of particular IS resources,
– Assessment of probability, it is frequency of threat occurrence – this mark should embrace presence, duration time and strength of threat, and protections effectiveness as well.

Information of such type will always have approximate character, however accurate, based on i.e. experiences of another enterprises, execution of risk analysis may be very helpful in realization of next processes of security management in organization. However, very important problem of estimation and evaluation of Information Technology risk is left.

IV. IT Risk Assessment as an Element of Risk Analysis

Quantitative and qualitative methods are two fundamental groups of methods are applied for analysis of risk on which assets are exposed in organizations. The most important advantages and disadvantages of IT risk assessment methods have been presented in table I. Groups of IT risk analysis methods [10]:

– Quantitative, where estimation of risk value is connected with application of numerical measures – value of resources is defined in amounts, the frequency of threat occurrence in the number of cases, and susceptibility by the value of probability of its loss, those methods present results in the shape of indicators. The examples of quantitative methods: Annual Loss Expected, Courtney’s and Fisher’s methods, ISRAM model, etc.
– Qualitative, which do not operate on numerical data, presenting results in the form of descriptions, recommendations, where risk assessment risk is connected with:
  – Qualitative description of assets’ value, determination of qualitative scales for the frequency of threat occurrence and susceptibility for a given threat or:
  – Description of so called threat scenarios by prediction of the main risk factors.

The examples of quantitative methods: FMEA/FMECA, The Microsoft Corporate Security Group Risk Management Framework, NIST SP 800-30, CRAMM.

Depending on the seriousness of a given threat there can be applied different risk measures from very simple assessments, determining the risk as high, medium and low,

Table I.
The most important advantages and disadvantages of quantitative and qualitative methods of IT risk analysis

Risk Analysis	Quantitative methods	Qualitative methods
Chosen advantages	– They allow for definition of consequences of incidents occurrence in quantitative way, what facilitates realization of costs and benefits analysis during selection of protections. – They give more accurate image of risk.	– It allows for putting in order risks according to priority. – It allows for determination of areas of greater risk in a short time and without bigger expenditures. – Analysis is relatively easy and cheap.
Chosen disadvantages	– Quantitative measures depend on the scope and accuracy of defines measurement scale. – Results of analysis may be not precise and even confusing. – Normal methods must be enriched in qualitative description (in the form of comment, interpretation). – Analysis conducted with application of those methods is generally more expensive, demanding greater experience and advanced tools.	– It does not allow for determination of probabilities and results using numerical measures. – Costs-benefits analysis is more difficult during selection of protections. – Achieved results have general character, approximate etc.

Source: [1, p. 107]

to very precise indicators presented as probability of a given event occurrence [11, p. 230]. In the case of evaluation of information security risk in Information System there is normally conducted qualitative analysis of risk. This method is most often based on information security criteria such as: confidentiality, integrity and accessibility. Full analysis of risk may be carried out separately for each of mentioned criterion. For the purpose of analysis there is being fixed value scale of information (low, medium, high). Finally the value of risk may be defined as e.g. very low, low, medium, high and very high.

Correct assessment of risk and evaluation of its occurrence probability gives clear image of its impact on functionality of the whole Information System.

V. Quantitative Methods of IT Risk Analysis

Using quantitative methods analyst stands before the problem of appropriate assessment of values indispensable for calculation. The value of risk can be presented with the use of any type of scales or directly in the financial scope as predicted amount of losses connected with a given type of risk, in assumed period [10].

Only occasionally happens that the team conducting the process of IT risk assessment had reliable data, allowing for realization of such task accurately and without any mistakes or problems. Moreover for some resources of assets in organization, losses presented in amounts are difficult to precise. It concerns e.g. loss of confidential information. In order to set value there should be defined meaning of information for proper realization of different business processes and theirs importance for functioning of organizational unit and as a consequence the whole enterprise [10], [2]. Basic correlation applied for IT risk assessment is presented as follows [10]:

$$R = P \times W \text{ and } P = F \times V \qquad (1)$$

where:
R – Risk value,
P – Probability or predicted number of incident occurrence causing loss of assets value in defined period ,
W – Value of loss – predicted medium loss of assets value, as a result of single incident occurrence,
F – Frequency of threat occurrence,
V – Susceptibility of Information system on (or its element) a threat; it is the measure of probability of usage of specified susceptibility by a given threat.

It results from the fact that assessment of IT risk is most often represented as the value of expected losses, which is based on definition of three basic volumes [10]:

- Resource value (e.g.. information) for correct functioning of enterprise, defined in amounts,
- Frequency of threat for resource occurrence (e.g. processed information), defined as the number of occurrences – in practice for definition of frequency of threats there is set a period in which will considered its occurrence (most often period of one year).
- Susceptibility of IT system on (or its element) threat, defined as probability measurement of loss occurrence as a result of event occurrence.

The most common and most frequently used quantitative method of risk assessment is ALE model (*Annual Loss Expected*), based on the idea of expected loss, which is the product of probability of occurrence of events which have negative impact on IT and values of caused by them losses. It is presented in the form of the following models [12]:

$$ALE = (Probability\ of\ event)\ x\ (value\ of\ loss) \qquad (2)$$

$$ALE = \sum_{i=1}^{n} I(O_i)F_i \qquad (3)$$

where:
$\{O_1, O_2, \ldots, O_n\}$ – set of negative effects of event;
$I(O_i)$ – value expressed loss resulting from event,
F_i – frequency of i event.

Annual predicted loss for organizations will be determined by the sum of all predicted annual losses. There exist many other models of IT risk evaluation and assessment, based on above method. They are adapted to concrete needs and situations existing in a given organization. Among such methods it worth taking consideration on Courtney's method elaborated by Robert Courtney, based similarly to ALE method on assessment of potential loss as the product of losses value connected with occurrence of threat and indicator determining probability of its occurrence. The concept of risk assessment according to Courtney is based on the following formula [5]:

$$R = P \times C \qquad (4)$$

where:
P – probability of occurrence of a given number of times in a year, of event causing loss for organization
C – loss for a given organization which is the result of single occurrence of event causing loss.

$$ALE = \frac{10^{f+i-3}}{3} \qquad (5)$$

where:
f – Index defining assessed frequency of event causing loss.
i – Index defining assessed level of loss caused by occurrence of event causing this loss.

Presented Courtney's method distinguishes six general groups of threats like: accidental data reveal accidental modification of data, accidental removal of data, deliberate reveal of data, deliberate modification of data, deliberate data removal. This method was accepted by national institutions in United States of America as official method of risk analysis [5].

In the elaboration of [7] there was presented a few derivative factors concerning risk assessment, based on presented expected loss (*ALE*) method. The ways of its value determination are presented in table II.

Among them there is indicator determining profit from applied protections (S) presented extensively in the work of [8]. Development of Courtney method into complete methodology of designing of Information Systems security solutions is Fisher's method elaborated in 1984. In order to apply it correctly there exist a necessity for organization to posses information security policy. This methodology distinguishes the following phases of the process of Information Systems risk management [5]:

- Phase 1 – collection of information, (identification and classification of Information Systems resources, collecting information concerning Information Systems resources which undergo further analysis);
- Phase 2 – identification of threats (process of threats mapping (previously mentioned 6 groups of threats from Courtney's method) into 11 Fisher control points such as.: acquirement, transmission, change of form, transport, reception, processing, migration, removal, data usage etc.);
- Phase 3 – risk evaluation (determination of the level of risk with the use of Courtney's method: R = P × C, where: P – probability of occurrence defined number of times in a year, of event causing loss for organization; C – loss for a given organization which is the result of single occurrence of event causing loss);
- Phase 4 – design of control mechanisms (in its result for every identified risk there should be selected appropriate mechanism of control: *preventive*, *detective* or *corrective*;
- Phase 5 – evaluation of economical profitability of mechanisms (business evaluation of identified mechanisms with the use of previously mentioned ROI indicator – *Return on Investment*), expressed with following formula:

$$ROI = \frac{Operationa\ l\ \ profit\ \ in\ a\ given\ \ period}{Value\ \text{of invested capital}} \qquad (6)$$

Determined in this method size of risk for particular control mechanisms is interpreted as operational profit, and assessed cost of control mechanism is treated as the value of invested capital [5].

The next presented in the article method is ISRAM model (*Information Security Risk Analysis Method*), based on presented ALE (*Annual Loss Expected*) method, however using survey researches as the main tool. Assessment of information technology risk is done by application of the following formula [3], [12]:

$$Risk = \left(\frac{\sum_m T_1 \left(\sum_i w_i p_i \right)}{m} \right) \left(\frac{\sum_m T_2 \left(\sum_j w_j p_j \right)}{n} \right) \qquad (7)$$

where:
i – the number of survey questions concerning assessment of probability of occurrence of incidents;
j – number of questions in survey concerning assessment of consequences;
m, n – number of survey's respondents;
w_i, w_j – weighs of questions „*i*" „*j*";
p_i, p_j – value corresponding to selected answers „*i*" „*j*";
T_1 – table of probabilities of events occurrence;
T_2 – table of negative results of events occurrence.

The example of qualitative method enriched in quality elements is Parker method, created for the needs of Computer Security Institute in 1981, embracing five different fundamental stages:

- identification and evaluation of resources,
- identification of threats,
- risk assessment,
- identification, selection and implementation of protections
- implementation of protections system.

TABLE II.
EXPECTED LOSS AND CHOSEN DERIVATIVE INDICATORS

No.	Factor	Symbol	Way of value determination
1	Annual Loss Expected	ALE	$ALE = \sum_{i=1}^{n} I(O_i)F_i$
2	Savings – reduction in ALE	S	S = ALE(baseline) – ALE(with new protections)
3	Benefits	B	B = S + Profit from new ventures
4	Return on Investment	ROI	$ROI = \frac{B}{C}$ C – costs of protections
5	Return on Security Investment	ROSI	$ROSI = \frac{(RiskExpos\ ure \times \%RiskMitig\ ated) - SolutionCo\ sts}{SolutionCo\ sts}$
6	Internal Rate of Return	IRR	$C_0 = \sum_{t=1}^{n} \frac{VA_t - C_t}{(1+IRR)^t}$ C_0 – initial cost of investment, Ct – cost of investment in t year.

Source: own elaboration on the basis of [7], [12] In risk assessment the Courtney's method is used, rebuilt with Exposure Analysis Matrix. Basis of this method is assumption that significance of threats is the function of number of people who may cause a loss, what leads to risk analysis with division into particular vocational groups in the enterprise. Thus Parker in his method uses Courtney's method, extending it on qualitative analysis of risk, also formalizes impact of human factor on risk, what distinguishes this method from the rest [6, s. 40].

VI. Qualitative Methods of IT Risk Analysis

There exist many qualitative methods of risk analysis. There will be discussed the following ones: FMEA/FMECA methods and NIST 800-30 and CRAMM methodologies.

FMEA (*Failure Mode and Effects Analysis*) and FMECA (*Failure Mode and Effects Criticality Analysis*) methods have theirs beginning in 50s years of the last century, when they were elaborated for the purpose of reliability analysis of weaponry and are used till now in e.g. aircraft industry, space and electronic industry. The essence of FMEA/FMECA is analysis of impact of every potential defect on functionality of the whole system and order of potential defects according to the level of its severity. FMECA method additionally introduces analysis of the degree of defect severity and examines whether it has critical character for functionality of the whole evaluated system. Those methods are quite laborious, require knowledge and experience of persons who apply them, they are supported with specialist tools, using elements of knowledge engineering and fuzzy logic [1, p. 83].

The process of IT risk assessment according to NIST SP 800-30 methodology is divided into 9 basis phases [6, p. 41-42]:

– Selection of systems which are subject to evaluation,
– Definition of the scope of evaluation, collection of needed information;
– Identification of threats of evaluated systems;
– Identification of susceptibility of evaluated systems;
– Analysis of applied and planned mechanisms of control and protections;
– Specification of probabilities of susceptibility usage by identification of the source of threats (probability is defined as: low, medium, high);
– Analysis and determination of incidents impact on system, data and organization (impact defined in three degree scale: high, medium, low)
– Determination of risk level with the help of matrix - *Risk Level Matrix* – for the whole risk for identified threats. This matrix is created by as a result of multiplication of probabilities of incidents occurrence (high probability receives 1,0 weigh, medium – 0,5, and low – 0,1) and strength if incident impact (high impact receives 100 weigh, medium – 50, and low – 10). On the basis of matrix there is defined level of whole risk for every identified threat, determined as high for product from range (50,100], medium for range (10,50] and low for product from range [1,10]. (The example of matrix according to NIST methodology was presented in table III).

Table III.
The example of matrix according to NIST methodology

Probability of threat appearance	Results		
	Low (10)	Medium (50)	High (100)
High (1,0)	Low 10*1,0=10	Medium 50*1,0=50	High 100*1,0=100
Medium (0,5)	Low 10*0,5=5	Medium 50*0,5=25	Medium 100*0,5=50
Low (0,1)	Low 10*0,1=1	Low 50*0,1=5	Low 100*0,1=10

Source: [1, p. 115]

– Elaboration of recommendation for control and protection mechanisms and other solutions having as its aim minimization of risk to acceptable level,
– Preparation of documentation of results of carried out evaluation of IT risk in the form of report for managerial staff.

CRAMM methodology (*CCTA's Risk Analysis and Management Methodology*), accepted by CCTA (*U.K. Government Central Computer and Telecommunications Agency*), as governmental standard of analysis and risk management. The process of risk management according to this methodology consists of three subsequent stages [6, s. 44]:

– identification and evaluation of resources,
– evaluation of threats and susceptibility,
– selection and recommendation of control and protection mechanisms.

IT risk analysis of which the main aim is determination of probability of occurrence of incidents interfering correct functionality of resources, where identified resources are allotted to asset groups, for which there are generated lists of main threats that could concern a given asset group, and there is determined level of risk for each group (in five degree scale).

This methodology uses dedicated software, which is its integral element supporting listed particular stages.

VII. Conclusion

Although some presented in the article methods of evaluation and assessment of IT risk require some refines, its advantage is that they show direction of deliberations and activities in discussed area. There exist many other methods of risk assessment and part of them is more advanced methods, which are derivatives from methods of risk assessment in finances. Benefits resulting from assessment of risk are multidimensional, because they can help in keeping balance between losses and costs of implemented protections, they help in planning expenditures, indicate legitimacy or lack of fundamentals to additional investment in Information Systems security, indicate new trends in the area of security. Practitioners claim that success in assessment of losses is achieved by systematic and solid approach to the issue e.g. by carrying out external audit. However, nowadays in practice potential losses are assessed rarely, on which have probably influence such factors as lack of knowledge, lack of willingness and lack of requirements from the side of managers of enterprises.

REFERENCES

[1] A. Bialas *Security of information and services in modern institution and company* (In Polish), WNT, Warsaw 2006

[2] A. Galach *Instruction of IT system security management* (In Polish), "Osrodek Doradztwa i Doskonalenia Kadr" Publishing House, Gdansk 2004

[3] B. Karabacak, I. Sogukpinar *Information Security Risk Analysis Method*, "Computers&Security Magazine" no 24 March 2005

[4] M. Pankowska *Multivariate of risk analysis for protection of management IT systems* (In Polish), [in:] *Application of informatics in accountability and finances*, ed.: Kubiak B., Korowicki A., PTE, Gdansk 2002

[5] M. Ryba *Analysis and management of Information Systems risk* (In Polish), Ernst & Young 2005 http://www.mimuw.edu.pl/~sroka/archiwalne/2005ey/materialy/

[6] M. Ryba *Multidimensional methodology of analysis and management of IT systems risk – MIR-2M* (In Polish), Doctoral thesis AGH, Cracow, 2006

[7] E. Schechter *Computer Security Strength & Risk: A Quantitative Approach*. Harvard University, Cambridge, Massachusetts, USA 2004

[8] K.J. Soo Hoo *How Much Is Enough? A Risk-Management Approach to Computer Security*. Doctoral thesis, Stanford University, 2000.

[9] G. Stoneburner, A. Goguen, A. Feringa *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology 2002

[10] E.I. Szczepankiewicz, P. Szczepankiewicz *Risk analysis in the IT environment for the purpose of operational risk management. Part 2 – Risk assessment stage* (In Polish), „Monitor Rachunkowosci i Finansow" Magazine no 7/2006

[11] Z. Szyjewski *Methodologies of IT projects management* (In Polish), Placet, Warsaw 2004

[12] D. Wawrzyniak *Models of IT risk assessment – classical approach and possibilities of its development* (In Polish), [in:] „Selected problems of electronic economics" ed. M. Niedzwiedzinski, Marian Niedzwiedzinski CONSULTING Publishing House, Lodz 2007