RISKS IN THE INFORMATION SYSTEMS AND THEIR EVALUATION

Miroslava Dolejšová

1. Introduction

The present entrepreneurial environment forces the companies to pursue all sorts of analyses such as the market analyses, the resource analyses, the competitive analyses, the assortment analyses, the customer analyses and their requirements, the cost and benefit analyses, SWOT analyses for all time. These business analyses are often added with the financial situation analysis and the evaluation of the company in the product life cycle. The implementation of the business analyses is connected with a certain level of risk and uncertainty of the development of entrepreneurial environment and its changes in the future. That's why the risk analysis and its evaluation becomes one of the dominant factors that play a significant role in the judgement of contemporary and future performance of the company.

The information system consists of the different components. These components are the computer software, the computer hardware, the communication equipment, data and people. Each of these components may be the subject of potential threats. These threats represent a risk. That's why the information systems are very vulnerable.

2. Risks in the Information Systems

Risks in the information systems are possible to classify into two different groups. The first group is the characteristics of risks threatening the components of the information system. The second point of view is the division of risks in light of their exposure.

The risks that may threat the particular components of the information system can be the following:

Software: occurrence of mistakes and faults in the computer programs, insufficient online help, unsuitable procedure during the development of the information system, insufficient testing of the system and data, viral infection, software theft, undetected failure of the software

Hardware: unreliable data processing, undetected failure of hardware, hardware theft, failure of the security mechanisms

Data: unauthorized data access, data damage during the processing, insufficient data security, deficiently designed data base

Network: problems in the data transmission, system breakdowns, unsecured network

People: unauthorized access to the system, inexperienced users, staff training underestimation, evasion of the security procedures, installation of the improper programs, browsing of the dangerous web sites, hacking, unauthorized data copying, data thefts

Except these risks there are general risks in the information system that isn't possible to associate with the particular component of the system unambiguously. These general risks may be the insufficient physical security of the components of the information system, natural effects and the irrecoverable data loss during the power cut, the acquisition of hardware or software equipments that don't correspond with the user's requirement.

Risks in the information systems can be divided according to their exposures as follows:

1. Unconscious risks

These kinds of risks can be divided into three following groups:

- Natural effects (fire, floods, smoke, dust, too high temperature, insufficient system cooling)

These risks can interrupt the processing of computer operations. It will last relatively for long time before data restoring.

Tab. 1: Scale System for the Estimation of the Risk Probability of Occurrence and Impact

PROBABILITY OF OCCURENCE		
Category	**Description**	**Range of the values**
Very low	Occurrence of risk is scarcely possible	1
Low	Occurrence of risk is quite sporadic	2 - 3
Average	Risk occurs only sometimes within a given period of time, it is a random occurrence that can't be exclude	4 - 6
High	Risk occurs several times within a given period of time	7 - 8
Very high	Risk occurs very often	9 - 10
IMPACT		
Irrelevant	Unimportant failure, there is no threat	1
Low	Account small failure, risk can be remove	2 - 3
Average	Seldom threat, risk can occur or not, we have to count on it	4 - 6
Very grave	Considerable threat, it is suitable to take actions to mitigate risk	7 - 8
Catastrophic	Permanent threat, excessive occurrence of damage, it is necessary to take action to mitigate risks	9 - 10

Source: own proposal [1]

- Failure of information systems (poor quality of materials, software and hardware incompatibility)
- Failure of the human factor

The most frequent risks in the information systems are the unconscious mistakes or faults of people. These mistakes or faults can occur during any stage of the information system life cycle. They can arise during the programming and testing of the information system, system analysis and design, underestimation of the user's requirements, exclusion of users from the development of the information system, improper program instructions, insufficient data collection and analysis, incorrect data entries.

2. Intentional risks

Information systems can be threatened in consequence of the intentional activities. These activities can be for instance:

- Intentional encroachments into program instructions
- Violation of computer resources
- Intentional hacking into information system
- Thefts of computer hardware
- Thefts of computer software
- Viral infections
- Unsuitable data exploitation (input adjustments)
- Thefts of business data

The similar classification of risks is mentioned in [2].

3. Methods for Risk Evaluation

When we know that there are certain risks in information systems, this idea isn't sufficient for us. At the same time, we should be interested in the way how we can express these kinds of risks, how the incidence of the particular risk is and first of all - why these risks rise and how we can mitigate their impact to be as lowest as possible.

The methods for the risk evaluation can be separated into two groups: quantitative methods and qualitative ones. Example of the qualitative way of the risk expression is the verbal description. But how is its importance the „high risk" for us? What does it mean the „average risk"?

Hence, it is suitable to use the quantitative methods. It means that we try to express the risk in the form of number or a certain value. If we have the basic knowledge of statistics we can determine the probability of the occurrence and the impact of the particular risk. If this area of knowledge is very far from us we have to help out the other way. The simplest way is the application of the scale system. Example of this scale system shows the table (Tab. 1):

4. Information System Audit

Risk is the basic concept for the information system audit. We usually associate the term audit with the verification of the financial statements. This kind of verification is well-known as a financial audit. Generally, audit is related not only to the financial statements. We can pursue it during the screening any business activity - accounting, production, communication between employees, human resources, quality, environment. Application of audit is available in the area of information systems likewise.

Audit is often included in the risk management as its final stage [4]. Likewise there are the stages of the life cycle in the information system there are the stages of the risk analysis and management.

The procedure for risk analysis and management follows in this way [1]:

1. Nomination of the project manager and his or her project team
   Risk analysis and management of the information system will not carried out by the only person but by a group of people, a team. This team will work on the common project. The project team defines the objectives and the area of analysis, division of tasks among the members of the project team, specifies the working time schedule.
2. Analysis of the present situation and the economic evaluation of the project
   If the project is economically acceptable, the project team will work on the project. Provided that the project is carried by the top management the project team revises the project characteristics. It appraises whether the project is consistent with the corporate strategy, meets financial criteria of the project selection (positive net present value, results of the financial analysis) and contains clear defined objectives, terms, resource and quality requirements and clear defined project outcomes.
3. Risk identification
   The main purpose of this stage is to identify utmost risks in the problem solving. The project team will investigate the risks within the particular stages of the information system life cycle. The source information for the risk identification will be the results of the analysis of the present situation. The output information forms the primary risk list that can be expressed in the form of table. This table will contain the unique description of the identified risk, associative number and the expected risk effect.
   Risk identification can be pursued with the help of different methods. We can utilize the Delphi method (method of expert examination), brainstorming (the discussions among the members of the project team, support of the unconventional ideas), structured questionnaires, exploitation of experience and intuition.
4. Risk separation
   The primary risk list may contain the risks that can but don't need to be important for the execution of the project. The main purpose of the risk separation is to verify every risk included in the primary risk list in term of significance. Some of these risks can be excluded from the list because we don't think them as important ones.
   The source information for the risk separation creates the primary risk list. The output information will form the risk separation list in the form of table. This table will not contain the risk effect but the appropriate stage of the life cycle.
5. Estimation of the risk probability of occurrence and its impact
   The estimation of the risk probability of occurrence and its impact forms the crucial part of the risk analysis. To do this, we can

use quantitative and qualitative methods. The probability of occurrence and the impact is better to express numerically. We can utilize the probability theory or the scale system. Indeed, we aren't able to express all risks in the numeric form. Consequently, we are obliged to express these risks in the qualitative form. We can use the classification rating with the appropriate adjectives such as „high", „average", „low". The word „average" may have the different meaning for various people. That's why it is suitable to add this classification range to the more detailed description. The same thing applies to the classification range in the quantitative methods. We can select another range of values for the estimation of these risk parameters. The choice is up to us.

The source information for the estimation of the risk probability and its impact is the risk separation list. The output information is the risk estimation table. Example of this table shows the table (Tab. 2).

Tab. 2: Risk Estimation Table

Risk number	Risk name	Probability of occurrence	Risk impact
82	Unprotected hardware	5	10
90	Unused antivirus programs	4	9
92	There are no procedures for the interim system breakdown	8	7

Source: own proposal [1]

6. Risk alignment according to its importance
Risks can be classified in the critical, important or irrelevant risks. One of the suitable methods for the risk alignment is the graphic presentation of the risk probability of occurrence and impact in the form of two-dimensional graph. The horizontal axis is the estimation of the probability of occurrence and the vertical axis is the estimation of the particular risk impact. Two-dimensional graph is better to generate for the particular stages of the life cycle separately for the better lucidity.
The source information for the risk alignment is the risk estimation table. The output information is the table of risks divided according to their relevancy and the two-dimensional graphs.

7. Proposal of actions for risk mitigation or removal
After pursuing the risk analysis the project team has a brighter idea of the risk significance. Now it can propose the actions for the risk mitigation or removal. The main purpose of the risk mitigation is to eliminate or mitigate either the risk probability of occurrence, or its impact or both of them. There are four strategies for the risk mitigation:

- Risk avoidance (the elimination of the source of the particular risk),
- Risk transfer on someone else (subcontractor, insurance companies, customers),
- Risk reduction (the proposal of actions for the further risk mitigation),
- Risk acceptance (to reconcile with the particular risk, risk will be only monitored).

The source information for this stage is the table of divided risks. The output information is the proposed actions for the risk mitigation.

8. Risk monitoring
Finally, the project team will monitor the particular risks after implementing actions. We should estimate the probability of occurrence and the impact of the particular risk at the same time. The final results are suitable to illustrate in the form of two-dimensional graphs. We can learn if the critical and important risks are down or whether some of the still small risks come the critical or important ones. Provided that the designed action was ineffective it is necessary to propose new action and to repeat the whole procedure again.
Risk audit makes possible to compare risk before and after implementation of appropriate actions and to evaluate them statistically.
Other phases of the risk management are shown in [3] [5].

5. Conclusion

Knowledge of the risks in the information systems is very important for each of us. Provided that we are able to identify these risks we are able to classify them into groups, estimate the impact and the probability of occurrence of these risks, estimate their significance, propose the suitable actions to mitigate risks and control them subsequently.

Audit of information systems is often regarded as the last stage of the risk management. From this point of view, the audit of information systems would be identical to the risk management. Of course, audit is more likely perceived as certain verification or a control of a certain matter of facts. To be able to learn these facts, we have to identify and measure them. In the larger sense the risk management is similar to the audit of information systems. That's why they are interconnected one another.

This paper provides only the fundamental overview of the risk audit issues. Its purpose is to make the readers pay attention relating to the work with the information systems and be aware of inherence of these risks. The further important purpose is to acquaint the readers with the application of different methods in the analysis and the evaluation of these risks.

The readers can familiarize with the audit and the security of information systems more closely in the references at the end of this paper. It is expected the enhanced request for the profession of internal auditors and the application of the internal audit in different areas of business activities. The academic area and research field will be no exception. It is assumed that the application of statistical methods in the audit of information systems will be utilized in the future.

References:

[1] DOLEJŠOVÁ, M. Analýza a řízení rizik podnikatelského projektu. *Disertační práce*. Ostrava: VŠB-Technická univerzita Ostrava, 2002.

[2] DOUCEK, P. Řízení bezpečnosti informačních systémů. *E+M Ekonomie a Management*, 2006, roč. 9, č. 2, s. 123-141. ISSN 1212-3609.

[3] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. vyd. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[4] DVOŘÁČEK, J., KAFKA, T. *Interní audit v praxi*. 1. vyd. Brno: Computer Press, 2005. ISBN 80-251-0836-8.

[5] JAŠEK, R. Bezpečnost (podnikových) informačních systémů v komplexním pohledu. *E+M Ekonomie a Management*, 2005, roč. 8, č. 3, s. 136-143. ISSN 1212-3609.

Ing. Miroslava Dolejšová, Ph.D.
Tomas Bata University in Zlín
Faculty of Economics and Management
Department of Informatics and Statistics
Mostní 5139
760 01 Zlín
Czech Republic
dolejsova@fame.utb.cz

Doručeno redakci: 24. 8. 2006
Recenzováno: 15. 12. 2006
Schváleno k publikování: 12. 9. 2007

ABSTRACT

RISKS IN THE INFORMATION SYSTEMS AND THEIR EVALUATION

Miroslava Dolejšová

The paper is dedicated to the risks of the information systems. The simplified classification of risks with the specific examples is described in the first part of the paper. We can divide the risks relating to the information systems into two different groups accordingly. The first group is concerned with the components of the information systems. The second group of risks is connected with their exposures. There are both the unconscious and intentional risks from this point of view.

The second part of this paper is engaged in the characteristics of the selected methods that are possible to employ in the risk evaluation of the information system. Because of the fact that the users of the information systems are not acquainted with the statistical methods the simplest demonstration of the formulation of the probability of occurrence and the impact of the risk event in the form of the scale system is offered for them. However, this scale system mentioned in this paper is not the only way to measure the risks.

The third part of the paper features the procedure of the audit of the information system. This procedure can help anyone who is interested in measuring and verification the risks of the information systems.

In addition to the scale system mentioned in this paper we can apply the additional methods of risk analysis and evaluation such as check lists, the Failure Mode and Effect Analysis, decision trees, the sensitivity analysis or Monte Carlo simulations. However, the application of the sensitivity analysis or Monte Carlo simulations requires the high level of the computer literacy.

Key Words: *risk, information system audit, risk management, information system audit, methods for risk evaluation, risk analysis*

JEL Classification: *D80, M15, M42*