Information System and Risk Reassessment

Božo Nikolić and Ljiljana Ružić-Dimitrijević
The Higher Education Technical School of Professional Studies, Novi Sad, Serbia

direktor@vtsns.edu.rs; ljaga@eunet.rs

Abstract

This paper belongs to a group of papers dealing with the problems of risk assessment, at first only in the field of occupational health and safety, from where the assessment method originates, but later its implementation is extended to the field of information technology. However, the paper is a step forward regarding what was said in our previous papers on risk management issues. In these discussions, the method of our School was created regarding risk assessment and a model for risk assessment was developed for application in other areas, including information technology. Furthermore, it stresses possible influences on the formation and definition of the system, both external and some internal concerning business planning. For these cases, a repeated risk assessment was carried out to perceive on a practical example the environmental impact on an information system. Risk reassessment is inevitable when an information system undergoes changes and this is insufficiently covered in the literature.

Keywords: risk assessment, risk management, information system

Introduction

In every working area, assets are exposed to risk of various harms. In the information technology area, there is risk of damaging or losing resources. Risk assessment is a process that determines what information resources require protection, and it documents potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability. The purpose of risk assessment is to help management create appropriate strategies and controls for the steering of information assets (BSI Standard 100-1,2,3), (ENISA Regulation).

IT resources are tangible assets (such as hardware, equipment, buildings), data, documents, software, users, and intangible resources (reputation, confidence, etc.)

Management of the information system (IS) is a component of the company management and makes its inherent part. The planning of the continuity of IS operation and development must be entirely coordinated with the same activities on the company level. Both short-term and long-term strategies must be harmonized within the framework of business, development, changes, and planning.

Risk management and its maintenance on an acceptable level is part of the work process and its development. Its basic characteristic must be continuity (Nikolic, 2007). The chosen acceptable risk level after the implementation of particular measures also means a decision on balance referring to costs concerning the achievement of the selected

Material published as part of this publication, either on-line or in print, is copyrighted by the Informing Science Institute. Permission to make digital or paper copy of part or all of these works for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage AND that copies 1) bear this notice in full and 2) give the full citation on the first page. It is permissible to abstract these works so long as credit is given. To copy in all other cases or to republish or to post on a server or to redistribute to lists requires specific permission and payment of a fee. Contact Publisher@InformingScience.org to request redistribution permission.

risk level and benefits, i.e., profit of the company.

Methodology

The methodology of risk assessment implies recognized procedure (Macdonald, 2004), detailed system description, identification of hazards, defining causes of emphasized hazards, risk assessment, measures for risk reduction and mitigation, risk reassessment according to remaining hazards, and conducting measures for maintaining risk at an accepted level.

Figure 1 displays the methodology of risk assessment with elements of the risk management system.

Risk assessment in the IT area can be conducted by way of various methods. We use the method established and developed by our expert team (Nikolic & Laban 2008). The method was created for the occupational health and safety area, and is successfully applied in the IT area as described in Nikolic and Ruzic-Dimitrijevic (2009). This method enables the achievement of one of the main goals of risk assessment: risk assessment for every employee, workplace, and work environment, i.e., the assessment of all risks.

The work environment can be a company, building, floor, or office. It can also be a plant, building site, park, field, or any system, as well as an information system and its components, such as hardware, communication equipment (network), and system software.

The workplace in an information system is application software with data as final products, and it can be considered in the same way as in the occupational health and safety area.

IT resources are buildings, hardware, communication equipment, software, data, and, of course, people who take part in IT processes. Risk assessment is carried out on more levels (items in the work environment). Software also has several levels – environmental software, operating system, program supported application, and finally a single application – as well as the data used and gained in application executing. Risk assessment of each level involves conducting appropriate protective measures in order to obtain the layered protection.

Therefore, the risk assessment of an information system (IS) is conducted through the risk assessment of every application and through the evaluation of the system's state.

Risk identification involves the knowledge about the organization (internal and external), as well as earlier experiences about risk issues. The evaluation of risk classifies risk in certain categories (quantitative and/or qualitative) according to which adequate measures are carried out. Depending on the risk category, the decision is made what risks require conducting measures in order to be reduced (Harms-Ringdahl, 2001).

Measurements could be technical (hardware or software), organizational (procedures), or protective. After the consideration of all costs and benefits, an action plan can be developed, including proposed actions and responsibilities for conducting it.

The implementation of the action plan should modify the risk, in order to lower it, and the remaining risk has to be assessed. The management of the organization should accept this residual risk (Bozic, Kosic, & Nikolic, 2006). In addition, there is a need for recommended measures in order to maintain the residual risk on an acceptable level. This process of risk management is continuous, and assessments have to be updated, repeating the risk management cycle.

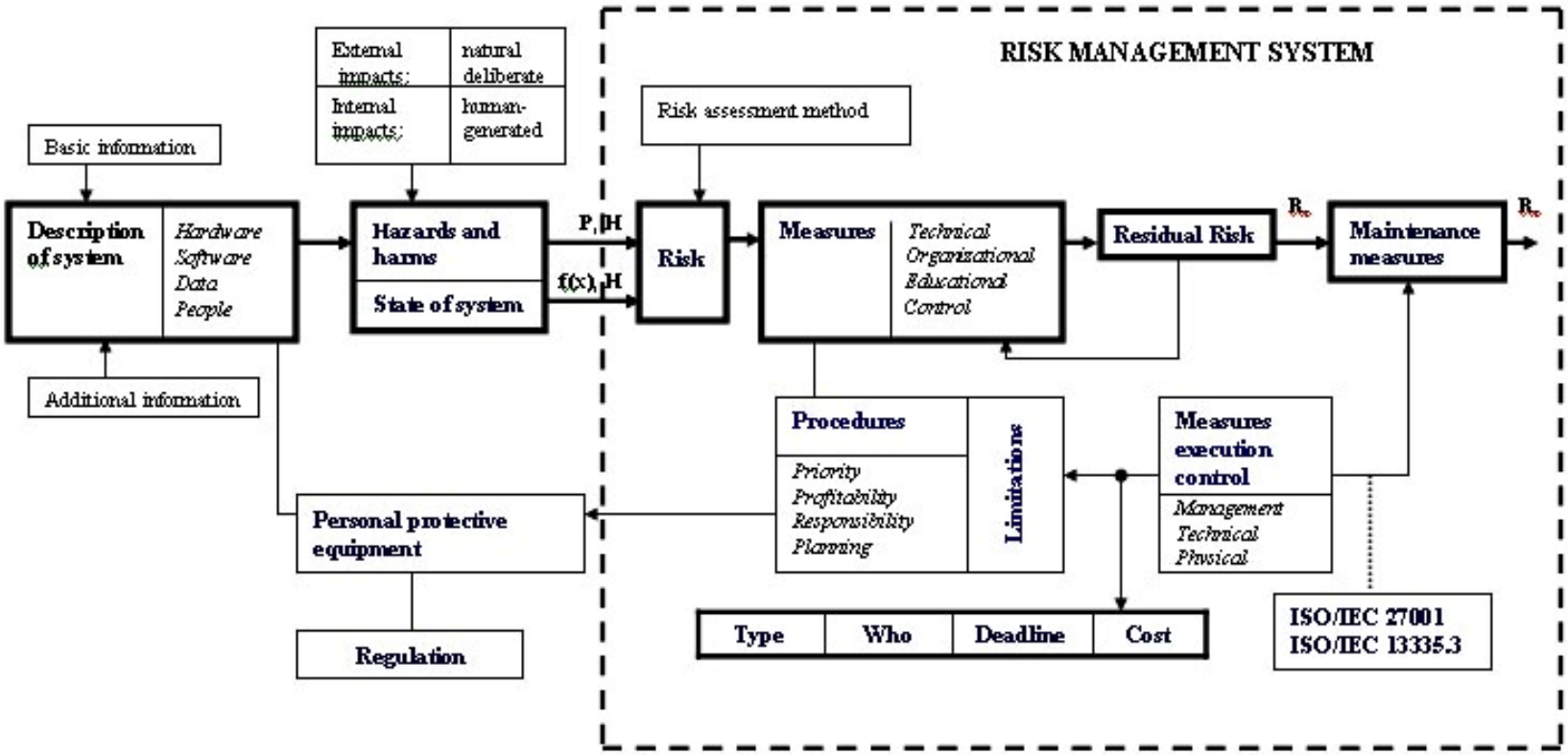

Figure 1 : Risk assessment methodology, risk management system, and information system

Risk Management

The greatest problem in risk assessment is the recognition of hazards and harms. This is actually the real and expert segment of the work, while risk assessment itself is just the implementation of tools and calculations. Besides the very hazards and harms, it is important to estimate well the degree of possibility of their occurrence. The hazards can be classified as natural (thunderbolt, fire, and alike that cannot be influenced), intentional human-generated (false information, hacking, viruses, etc.), and unintentional human-generated (based on ignorance and accident, from the management level to the lowest level).

The hazards can be external (out of the company) or internal (from the company). The harms due to various hazards, or even to the same ones, differ a lot; hence, the hazards are given special attention. They must be identified, from the source all the way to the goal, motive, frequency, and, of course, consequences. Only then, the measures can be effective, and the company management efficient in decision-making.

With regard to every hazard, risk is determined individually. It is the elementary rule. However, risk can be determined on the basis of a larger number of hazards all together, as the risk of a system, in order to enable the comparison of risks of different systems. There are other explanations for this in the literature ("Risk Management", 2006; Stoneburner, Gougen & Feringa, 2002), which depend on the method choice. This approach to risk assessment is characteristic for work environment risks, i.e., the system risk; the recognition of hazards and harms is performed through "the estimate of the condition" of that system.

The risk assessment is a permanent process that reiterates continually to obtain an acceptable risk level after one or more iterations. It is very important in conducting recommended protective measures and management in order to retain a desired acceptable level of risk.

The continuity of this process, changes, and new and old hazards require precise daily information on the system, both the basic ones already mentioned and the numerous additional ones.

The measures are carried out to prevent, diminish, or eliminate the risk. The other type of measures is the one serving to keep in the future the achieved risk level – the residual risk. Accepting of this risk level on behalf of the management means accepting of the establishment of all measures and represents the company policy, since the process of risk assessment and carrying out of the measures make the system of risk management. All limitations, organizational, financial, technical, and others are taken into account by all means. The measures refer to the entire system that is, to its managing, logical, and physical parts. There are numerous measures such as technical, organizational, educational, and control.

The measures provide the following:

- Implementation priority, which means that priority is given to the activities where risk level is the highest;
- Cost effectiveness analysis, which means the selection of measures with minimum expenses with justified decrease of risk level;
- Determination of responsibility of the persons in charge to realize specific measures; and
- Making of an action plan with deadlines (Nikolic & Gemovic, 2009).

The American National Standards Institute recommends (ASIS, 2009) the organization resilience management system that supposes understanding of an organization's risk, security, preparedness, response, continuity, and recovery requirements.

The organization resilience policy includes risk prevention, reduction, mitigation, and further resilience enhancement in order to attain continual improvement. In this document, it is emphasized that risk and impact should be re-evaluated within the context of any change: in the organization, procedures, functions, or in the organization's operating environment, services, and supply chains.

Any change of any system element requires reassessment, as well as every injury.

Forming and Defining of Our Information System

Description of Old System

The school's old information system was established as a network of computers in two school buildings. All computers were connected to the Internet either by wires or by a wireless system.

In the institution, there were three computer classrooms with 35 PCs in total and one classroom with 12 laptops. In the financial department, there were four networked PCs. In the student administration office there was a network of 5 PCs as workstations and one PC server. Also, there were one or two PCs in every staff office.

Two computer classrooms are in the same building with the financial and student administration offices, and there are two more in the other building with about 30 PCs in faculty offices.

There was an antenna for wireless Internet connection between the main server and the Internet provider. Internally, all PCs are connected to the main server by wires, switches, and routers. Additionally, two PC classrooms have the access to the main server by the internal wireless network.

Every computer has the Windows XP OS, MS Office, and additional software for specific purposes.

Change of Connection and Networking

We had some changes in our information system last summer. Above all, these changes were in networking. A new way of connection was initiated due to the increased number of computers placed in new computer classrooms, and computer equipment in faculty and administrative offices.

The wireless connection turned out to have a slow access, the provider could not offer faster data flow, and ADSL connection provides a better speed and costs less.

First of all, we changed wireless Internet connection with 2 ADSL connections. For each of the connections we linked a group of networked computers. The third group of computers remained on the wireless connection.

The first group consists of 3 PC classrooms and 1 laptop classroom (each of them has between 12 and 15 computers), the library with 4 computers, and several classrooms and labs (13) with one computer per room for lectures. There are about 60 computers in total, situated in two different school buildings.

The second network consists of the student administration office, financial department, and other administration computers.

The third group is made of computers in teachers' offices, and they are also distributed in two buildings.

Cables were used in networking, except in two classrooms, where wireless router networks computers.

There were problems during the new system installation including the following:

- Inappropriate computer distribution with complex allocation required 3 independent networks;
- Adjusting of routers;
- Network testing; and
- Network viruses blocked the network.

In the open system network, without a server-controlled access, the hazard from viruses exists on each networked computer. It was obvious that antivirus software had not been updated regularly, but this problem was not identified until the network was separated in 3 parts. (Figures 2.1, 2.2, and 2.3 given in the Appendix display the distribution and configuration of the information system hardware).

Change of Activities

At first, it was planned to keep the wireless connection for faculty offices and install 2 ADSL connections for other computers.

Besides the replacement of equipment, new activities can also cause unpredicted difficulties and hazards. We started the implementation of distance learning system (DLS) in our school programs. Consequently, the problem of data flow appeared due to uploading of a large amount of teaching material on the sub domain of the official website for DLS purposes.

Therefore, we had to include more observed items (elements) in order to assess the protection status of our IT system. New activities required an unexpected enhancement of equipment. The management had to anticipate the future development and provide advanced devices.

Software Modification due to External Factor

The application software used in the student administration office that processes student data was described in Ruzic-Dimitrijevic and Nikolic (2008). The data used and obtained in this process are very important for our School. This application contains procedures considering students enrolment and rules to determine student status: government-financed students or self-financed. In addition, there are rules about the calculation of tuition fees for self-financed students. The program code was created according to recent conditions and regulations of studies.

Herein, it is important to point out that 2/3 of our school's income is its own financial means raised from tuition fees and other services it offers.

Unfortunately, faced with students' pressure to relax study and enrolment requirements the Government changed its own rules at the beginning of the last school year. There was very little time for editing the program code in order to adjust it to the changes. Our institution was in danger of financial lost, as well as of losing its credibility because of errors and issuing invalid results and wrong data.

Therefore, we had to include one more threat, the jeopardy from short notice changes in the working process due to external requirements, which can cause serious consequences. Unfortunately, little can be done to reduce this risk. Hence, we cannot recommend any appropriate measure for that particular threat.

Example of Risk Reassessment

We had an example of the application with an organized IS that was well set from the risk aspect (Nikolic & Ruzic-Dimitrijevic, 2009). The forms below are from this example. Form 1 includes the application description. Form 2 is a descriptive analysis of identified hazards and estimated harms. Form 3a involves risk assessment with values from Table 1 for estimated level of damage, and Form 3b involves risk assessment after proposed measures for risk reduction. The final row is added in all forms referring to a new external hazard with a high risk level.

The hazards were assessed, as well as harms, measures were taken based on obtained values, and other phenomena were not expected. The decision of the Government made a lot of harm to the application with hardly any possibility to successfully apply any adequate measures, which led to the appearance of high risk.

The results in Forms 3a and 3b related to the appearance of high risk due to the Government decision confirmed our assumption about a possible scenario. The consequences are serious since there are no measures that can diminish them. They include financial loss, possible issue of incorrect data due to unexpected disturbance of IS, and loss of credibility in the eyes of the students concerning the institution and management.

Form 1: Application description

<table>
<tr><td>Company: Higher Education Technical School of Professional Studies</td><td>Department: Student administration</td><td>Application: Information system for student administration</td><td>Page Number:</td></tr>
<tr><td colspan="2">Equipment, installations: PC computers – clients and server, networking hardware, printers</td><td colspan="2">Software: OS Windows, student administration software</td></tr>
<tr><td colspan="4">General description of the program, process, types of information stored
There are three processes: application process of potential students, teaching process and payments. The application of potential new students is conducted once or twice per year and it can be divided in two processes: application and entrance examination and ranking and enrolment.
The payment process divides into the payment of: application and entrance examination and tuition fees.
The Board of Studies prepares inputs for these processes and the management receives reports about it.
The teaching process consists of several processes with possibilities of further division:
• students enrolment
o enrolment of academic/school year,
o registering of subjects,
o semester verification, which becomes student’s record for the completed semester and defines the study year on the basis of accumulated credits,
o enrolment of study year, which offers possibilities for registering corresponding subjects.
• tuition
o updating of curricula and syllabi,
o tuition delivery, which besides lectures involves student evidence and fulfilling conditions for taking a particular exam.
• examination
o applying for exams,
o assessment.
• issuing documentation
o issuing records,
o issuing certificates,
o issuing the final diploma.</td></tr>
<tr><td colspan="3"></td><td>Protective measures:
Using admission password
Antivirus software
Weekly data backup</td></tr>
</table>

Form 2: Hazard and harm identification

COMPANY:		SECTION:	APPLICATION:			
N°	Hazard code	Threats and vulnerabilities	DESCRIPTIVE ANALYSIS			
			Occurrence probability	Exposure frequency	Consequences	Risk
1		Electrical supply interruption	Possible but unusual	Constant exposure	Loss of the last input data or data inconsis-tency	exists
2		Switch or router, card malfunction	Possible but unusual	Constant exposure	Work delay	exists
3		Deleting network installation	Possible but unusual	Constant exposure	Internal network interruption – delay	exists
4		Workstation failure	Possible but unusual	Hourly exposure	Loss of the last input data or data inconsis-tency	exists
5		Server disk failure	Possible but unusual	Constant exposure	Loss of data before last backup	exists
6		Unauthorized admission and data changing	Unlikely but could occur	Monthly exposure	Incorrect data, loss of confi-dence	exists
7		Virus in network	50% possible	Constant exposure	Loss of data, data inconsis-tency, loss of confidence	exists
8		Bugs (program flaws)	50% possible		Data inconsis-tency	exists
9		**External impact – regulations changing**	**50%, yearly exposure**		**Data inconsis-tency, loss of confidence, financial loss**	**exists**

Form 3a: Risk assessment and risk management

Responsible person:					Analyst :	
Risk assessment, valuation and reduction						
QUANTITATIVE RISK ANALYSIS					RISK REDUCTION MEASURES	
Event Probability	Level of Damage	Frequency of Exposure	RISK	RISK LEVEL	Protection Aims	Technical, Operational, Organizational
2	0.5	5	5	Low but significant	Data safety, process safety	Install UPS equipment
2	0.1	5	1			/
2	0.1	5	1	Negligible		/
2	0.5	4	4			/
2	2	5	20	Low but significant		Weekly backup, as well as after every larger data processing
1.5	4	1	6	Low but significant		Physical protection of workstation, protecting and frequent changing of passwords
5	4	4	80	High		Frequent updating of antivirus software, avoiding use of unverified external data media
5	0.5	4	10	Low but significant		Comprehensive testing and fixing of program flaws
5	**10**	**1.5**	**75**	**High**		-

Table 1: Degree of possible harm (H)

Violation of regulations and laws	0.1
Impairment of an individual's right to informational self-determination	0.5
Communication/knowledge and skill	1.0
Possible (serious) injury of an individual (danger to life and limb)	2.0
Impairment/loss of reputation, confidence	4.0
Endangering of the company's existence	6.0
Financial loss though significant, could be absorbed	**10.0**
Financial loss could not be survived	15.0

Form 3b: Risk assessment and risk management

DATE :									Links with other documents
RISK ASSESSMENT, VALUATION AND REDUCTION					RISK MANAGEMENT				
REMAINING RISK ASSESSMENT					MEASURE ENFORCEMENT			CONCLUSION	RECOMMENDED MEASURES FOR MAINTAINING AN ACCEPTABLE RISK LEVEL
Event Probability	Level of Damage	Frequency of Exposure	RISK	RISK LEVEL	WHO	DEADLINE	PROCEDURE		
2	0.1	5	1	Negligible	Technician	One week	Keeping the high quality level in accordance to the Quality System	Risk is acceptable	Maintaining of the UPS system
2	0.1	5	1		/	/			/
2	0.1	5	1	Negligible	/	/			/
2	0.5	4	4		/	/			/
2	0.5	5	5	Low but significant	System administrator	Continuous			Apply backup procedures regularly
1	1	4	4	Negligible	Security and staff	Continuous			Obey rules about access to workstation and regular changing of passwords
2	4	2.5	20	Low but significant	System administrator	Continuous			Obey rules about using external data media and regular update of antivirus software
2	0.5	4	4	Negligible	Programmer	Periodical			Comprehensive testing after every change in the application
5	**10**	**1.5**	**75**	**High**	-	-			-

Analysis and Discussion

A system can suffer different influences, but herein we are going to point out the uniqueness of the phenomenon indicating that IS and company policy must be harmonized so that risk management would not be disturbed.

In risk assessment in the field of occupational health and safety on several levels, such as company, building, floor, workplace, etc., we actually follow the traffic flow of employees during working time in order to detect all hazards and harms and accordingly make risk assessment for the observed workplace or employee. If we physically divided the company in two parts and the employees moved in only one of them, then we would have two risk assessments – a separate one for each entity as if they were two companies. In both parts, there are the same levels for assessment as before. In the IS area, regardless of the fact that the company is physically parted there is one network and we have one risk assessment (Nikolic & Ruzic-Dimitrijevic, 2009). Due to the described changes (increased number of computers in the network and bandwidth), we have three systems (three independent networks); therefore, there are three risk assessment, one for each network. Each of them is a system for which a separate risk assessment is to be done, including risk assessments for implemented applications.

Accordingly, it is quite possible and expected that their risks differ, since in these systems different values of condition assessment, event occurrence and size of damage are possible even for the same elements. For instance, the occurrence and level of damage from viruses in the first and second case can differ, and risks will definitely also be different. It does not mean that in the smaller system the risk will be smaller for it depends on the occurrence and size of damage.

The second influence is made of changes in activities that should be coordinated with the changes in the company and its development. It would be logical to plan these changes no matter how important they are, so that risk assessment can anticipate corresponding measures. We had such an example in case when a decision was made to introduce distance learning, which consequently had an abrupt increase of data upload to the official website.

The third influence, the exterior effect mentioned earlier, is far more dangerous from the aspect of interruption of the risk management system. The Government decision and disturbance of the legal regulation of the student status caused on the other side, new, big and unexpected hazards that were related to the system, in our case.

The Same Dangers – Different Consequences

The new organization in distribution and networking of IS resources requires the definition of all levels. The first level is each of the 3 independent networks connected to the Internet with 3 ADSL devices. The computers in one network make the second level. They are also grouped by applications that function as one (grouped) workplace.

Considering that similar applications (teaching software) are installed in the classrooms, each classroom can be treated as one grouped workplace.

The situation is the same with computers in the offices. Six computers in the student administration office have the same application and can be observed as one workplace, the financial department office with 3 computers as the second, whereas other computers with service applications in the administrative offices make the third workplace.

All computers in the faculty offices are provided with similar software applications and can be seen as one workplace with the same hazards and harms.

These 3 groups are exposed to diverse hazards, but with different degrees of participation in damage. The hazard from virus is a good example.

The most frequent probability regards the occurrence of computer viruses in classroom computers. Users are students and often breakdowns are expected, but there are not reliable data for the whole School. The minor damage (consequences) are computer failures in classrooms. The most complex harm is when some teaching software must be reinstalled.

There is a recommendation of avoiding the use of unverified external data media in teachers' computers, and it is supposed that the users are educated in maintaining their computers (updating antivirus programs, backup of valuable data, etc.) There is a possibility of connection break in with difficult consequences this sensitive area. The communication via these computers is important because they are used in our distance learning system to connect remote students and teachers.

The most complicated form of damage would be destroying of data in the student administration office and the financial department office. At the moment, there is no available external access there, which makes the risk smaller, but protecting data in that part of IS is very important.

Yet, there was a new hazard for the software application in the student administration office (Nikolic & Ruzic-Dimitrijevic, 2009) in the form of an external unpredictable fact, mentioned in the previous section.

Now it is possible to better understand the basic requirement in risk assessment regarding every employee (computer), every workplace (application), and every work environment (part of system or entire system).

Besides, the importance of any change in the system and its impact on the system of risk and company policy is quite clear.

Conclusion

Every working system is dynamic, and it is necessary to follow its modification. The organizational resilience management system proposes high quality foundations for successful fulfilling of all requirements that arise due to new circumstances.

We had several modifications of our information system, which caused new risks. It required repeated risk assessments with corrections and updating of data and measures.

The reasons for the modification are various: internal because of increased amount of work, company progress that requires updated equipment; external like impact of environmental requirements, or regulation changes.

The slightest change, even seemingly unimportant, requires risk reassessment. The maintenance measures include various controls to check the implementation of selected measures. Quite frequently, measures exist, but their application is wrong or inadequate. Sometimes they are not even carried out. The experience tells us that in risk assessment persons in charge of the assessment often count up measures that formally exist but are not applied. Even worse, it is done deliberately, and it is well known. Therefore, it is necessary to incorporate measures execution control and give them special importance. Moreover, it is necessary to talk about correct implementation of control.

The management control means the making of various regulations and their implementation, technical control refers to software and hardware components, whereas physical control is in the function of assets protection, monitoring, etc. The avoidance of measures and lack of control in

IT are particularly interesting, for in comparison to occupational health and safety, they are less visible and, therefore, can have greater consequences.

Successful business planning by way of anticipating such sources of hazards is difficult and can be compared to some events on which the employer cannot influence – like the natural disaster magnitude in occupational health and safety. Although in both cases the employer is not responsible, the question is whether this can be a sufficient comfort for lost lives in occupational health and safety or the crash of IS and huge financial loss.

References

ASIS SPC.1- 2009. (2009). *Organizational resilience Standard*. Approved March 12, 2009 American National Standards Institute, Inc.

BSI Standard 100-1: Information Security Management Systems (ISMS) (2005). Retrieved May 2008, from www.bsi.bund.de.

BSI Standard 100-2: IT-Grundszchutz methodology, (2005). Retrieved May 2008, from www.bsi.bund.de.

BSI Standard 100-3: Risk analysis based on IT-Grundszchutz, (2005). Retrieved May 2008, from www.bsi.bund.de.

Bozic, V., Kosic, S., & Nikolic, B. (2006). *Pravilnik o postupku procene rizika na radnom mestu i u radnoj okolini – komentari* [Regulation for risk assessment procedure in the work place and in the workspace – comments]. Novi Sad, Serbia: VTS Novi Sad

Harms-Ringdahl, L. (2001). *Safety analysis: Principles and practice in occupational safety*. CRC Press

Macdonald, D. (2004). *Practical machinery safety*. Pondicherry, India: Integra Software Services.

Nikolic, B. (2007). Enactment about risk assessment. *Symposium about occupational safety and health,* Novi Sad, pp. 32-43.

Nikolic, B., & Gemovic, B. (2009). Application of risk assessment method in workplace and working environment. *Scientific-Professional Conference" Safety and health in work and environmental protection," Banja Luka.*

Nikolic, B., & Laban, M. (2008). Occupational health and safety risk assessment method. *17th International Symposium ECOLOGY 2008*, Sunny Beach Resort, Bulgaria

Nikolic, B., & Ruzic-Dimitrijevic, L. (2009). Risk assessment of information technology Systems. *Issues in Informing Science and Information Technology, 6,* 595-615. Available at http://iisit.org/Vol6/IISITv6p595-615Nikolic673.pdf

Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools. (2006). Conducted by the Technical Department of ENISA Section Risk Management, June 2006

Ruzic-Dimitrijevic, L., & Nikolic, B. (2008). Designing and building an information system for a higher education institution. *Proceedings of the Informing Science and IT Education conference: InSITE 2008*, Bulgaria. Available at http://proceedings.informingscience.org/InSITE2008/InSITE08p283-300Ruzic521.pdf

Stoneburner, G., Gougen, A., & Feringa, A. (2002). *Risk management guide for information technology systems*. Recommendations of the NATIONALE Institute of Standards and Technology (NIST) USA.

Appendix

Figure 2.1: Main building IS

Figure 2.2: Auxiliary building 1

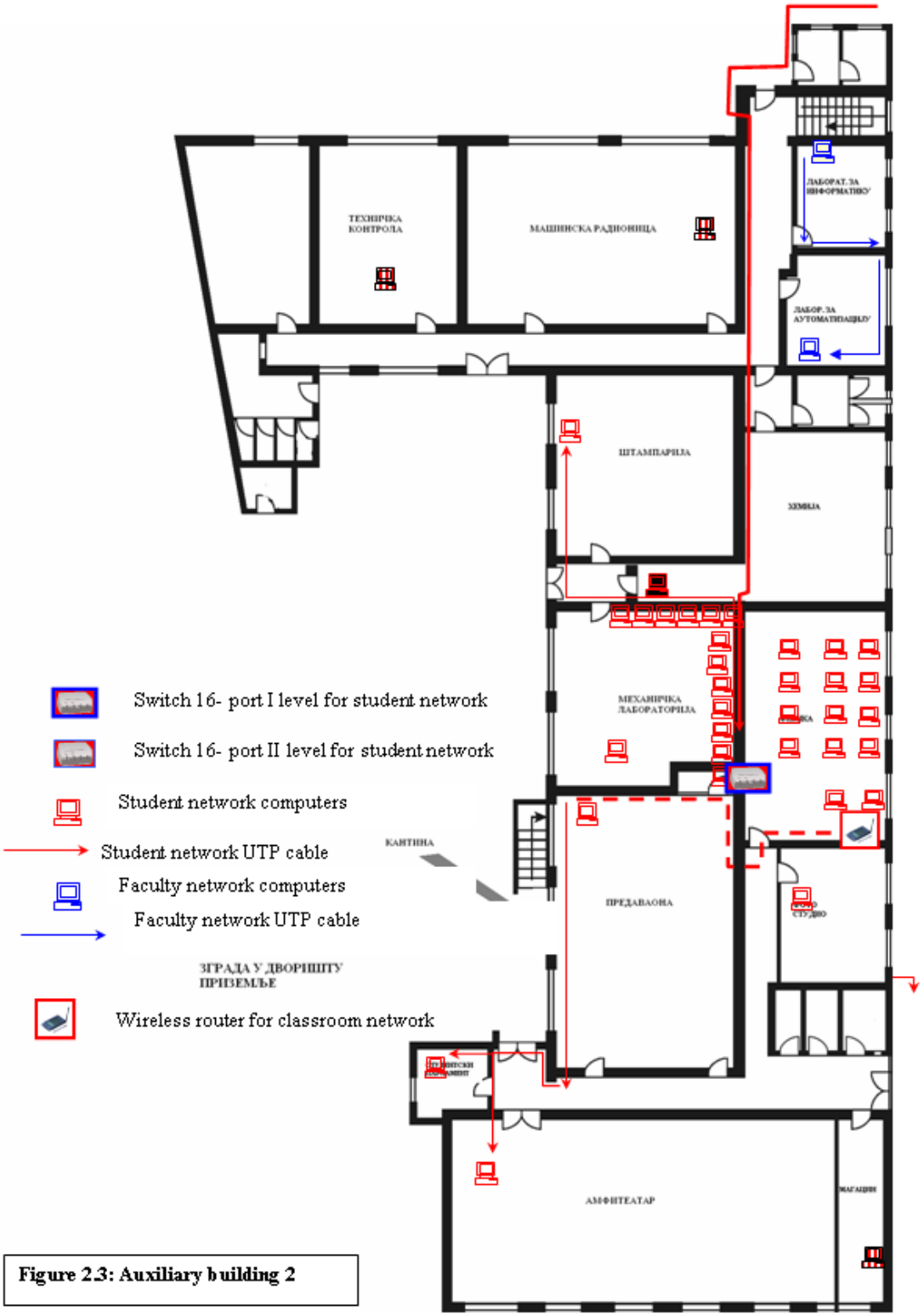

Figure 2.3: Auxiliary building 2

Biographies

Bozo Nikolić is a professor at the Higher Education Technical School of Professional Studies, Novi Sad, Serbia. He teaches courses in the fields of mechanical engineering and labor safety. He got his PhD degree in mechanical engineering at the Belgrade University in 1998. His areas of expertise are tools, accessories, and risk assessment regarding workplace and workspace. He is director of the Higher Education Technical School of Professional Studies.

Ljiljana Ružić-Dimitrijević is a professor at the Higher Education Technical School of Professional Studies, Novi Sad, Serbia. She teaches courses in Computers, Introduction to web design, and Development of the Internet. She got her MSc degree in mathematics at the Centre of Multidisciplinary Studies, Belgrade in 1991. Her field of expertise is computer graphics and web design. She is pro-dean in charge of tuition.