Risk Assessment of Information Technology Systems

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

Risk assessment is a structured and systematic procedure, which is dependent upon the correct identification of hazards and an appropriate assessment of risks arising from them, with a view to making inter-risk comparisons for purposes of their control and avoidance. There are differences in the methodology used to conduct risk assessments.

This paper presents some methodologies of risk management in the IT (information technology) area. In addition, a method of risk assessment created and applied by our expert team in this area is described. As there is a similarity between these methodologies, the paper presents the use of methods from the occupational health area in the IT area. All items in the risk assessment methodology for working environment and workplace are modified to IT as working environment and to an application as a workplace.

In that way, the risk assessment process in the safety analysis of an IT system is carried out by an original method from the occupational health area.

Keywords: risk assessment, information technology, risk management.

Introduction

Information technology, as a technology with the fastest rate of development and application in all branches of business, requires adequate protection to provide high security. The aim of the safety analysis applied on an information system is to identify and evaluate threats, vulnerabilities and safety characteristics. IT assets are exposed to risk of damage or losses. IT security involves protecting information stored electronically. That protection implies data integrity, availability and confidentiality. Nowadays, there are many types of computer crimes: money theft 44%, damage of software 16%, theft of information 16%, alteration of data 12%, theft of services 10%, trespass 2% (Boran, 2003).

In order to minimize losses, it is necessary to involve risk management and risk assessment in the areas of information technology and operational risks. Risk management and risk assessment are the most important parts of Information Security Management (ISM). There are various definitions of Risk Management and Risk Assessment [ISO 13335-2], [NIST], [ENISA Regulation], but most experts accept that Risk Management involves analysis, planning, implementation, con-

trol and monitoring of implemented measurements, and Risk Assessment, as part of Risk Management. It consists of several processes:

- Risk identification,
- Relevant risk analysis,
- Risk evaluation

Risk Management recognizes risk, accesses risk, and takes measures to reduce risk, as well as measures for risk maintenance on an acceptable level. The main aim of Risk Assessment is to make a decision whether a system is acceptable, and which measures would provide its acceptability. For every organization using IT in its business process it is significant to conduct the risk assessment. Numerous threats and vulnerabilities are presented and their identification, analysis, and evaluation enable evaluation of risk impact, and proposing of suitable measures and controls for its mitigation on the acceptable level.

The security policy has changed in the last years. From checklists for identifying specific events, the information security has risen onto a higher level, i.e. the security policy and strategy consider threats and weaknesses of the business environment, and IT infrastructure (Dhillon, 2001).

Risk Management

In the process of risk identification, its sources are distinguished by a certain event or incident. In that process, the knowledge about the organization, both internal and external, has an important role. Besides, past experiences from this or a similar organization about risk issues, are very useful. We can use many techniques for identifying risk: checklists, experienced judgments, flow charts, brainstorming, Hazard and Operability studies, scenario analysis, etc.

In order to assess the level of risk, likelihood and the impact of incidental occurrences should be estimated. This estimation can be based on experience, standards, experiments, expert advice, etc. Since every event has various and probably multiple consequences, the level of risk is calculated as a combination of likelihood and impact. Risk analysis or assessment can be quantitative, semi-quantitative, and qualitative (Macdonald, 2004).

Quantitative approach to risk assessment assigns numerical values to both impact and likelihood. The quantitative measure of risk calculated by statistical model is used to judge whether or not it is acceptable. Figure 1 represents relations between consequences, likelihood and limits of acceptance.

Event A has both low values, and risk is acceptable as far as it is under the limits. Event C is above the limits with high frequency and huge consequence. It is unacceptable, and it needs some measurements to reduce consequence and/or probability. For event B, which is in grey zone between the limits, it is hard to make decision.

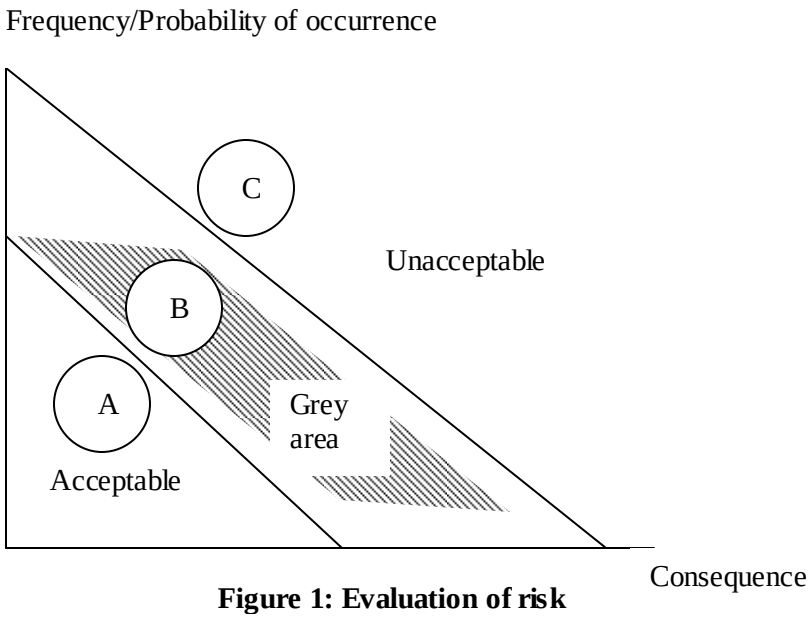

Figure 1: Evaluation of risk

Semi-quantitative assessment classifies threats according to the consequences and probabilities of occurrence. This approach is based on the opinion of the people making assessment. For example, probabilities can be divided into five classes: 0 – very unlikely (the probability 1 in 1000 years), 1 – unlikely (1 in 100 years), 2 – rather unlikely (1 in 10 years), 3 – rather likely (once a year), 4 – likely (once a month).

Qualitative approach describes likelihood of consequences in detail. This approach is used in events where it is difficult to express numerical measure of risk. It is, for example, the occurrence without adequate information and numerical data. Such analysis can be used as an initial assessment to recognize risk (Harms-Ringdhai, 2001).

Risk Treatment, Residual Risk, Risk Acceptance and Maintaining

Evaluation of risk involves making a decision which risks require conducting measures in order to be reduced. Measurements could be technical (hardware or software), organizational (procedures), operational, protective, and others. After consideration all costs and benefits of an action plan can be developed, including proposed actions and responsibilities of its conducting.

Implementation of the action plan should modify risk, and remaining risk has to be assessed. Management of the organization should accept this residual risk.

In addition, there is a need of recommended measures in order to maintain residual risk on the acceptable level. This process of Risk Management is continuous, and assessments have to be updated, repeating the risk management cycle.

Overview of Risk Management / Risk Assessment Methods

There are numerous methods applied in risk assessment. In different countries, there are different methods; even in the same area, there are various, and applying depends on a particular occasion. However, the methodology is the same: system characterization and description, threat and vulnerability identification, risk assessment, recommended measures, etc. The differences in methods are due to the level of development of methodology items. In ENISA (European Network

Information Security Agency) document about risk management, several of them, a total of 13, have been discussed ("Risk Management", 2006). Some of them are part of an ISO standard, i.e. Guidelines for the management of IT security; others are developed by governments or national offices for IT security.

All methods should present common descriptions of threats, vulnerabilities, assets groups, and, finally, a classification of risks. In that way they can be compared, and in order to achieve the best results, it is useful to apply the combination and optimization of methods.

ISO standards for IT security (13335, 17799, and 27001) are general guidelines for implementing the IT security management process, but there are no solutions for conducting it.

IT-Grundschutz (IT Baseline Protection Manuel)

This method is developed by the Federal Office for Information Security in Germany. IT-Grundschutz provides a configuration for IT security management. During the process of risk analysis threats are classified in 5 threat catalogues (BSI Standard 100-1, 2005; BSI Standard 100-2, 2005; BSI Standard 100-3, 2005). In addition, protection requirements categories are defined, possible damage scenario is assigned and, as a result, risk assessment is obtained.

IT security modules are grouped as generic aspects (organization, personnel, data backup policy, and computer virus protection concept), infrastructure (buildings, server room, and protective cabinet, home-based workstation modules), IT systems (servers, clients), networks, and applications (e-mail, web server, and databases for modeling modules).

Protection requirements categories:

1. Violation of laws, regulations or contracts
2. Impairment of the right to informational self-determination
3. Physical injury
4. Impaired performance of duties
5. Negative internal or external effects,
6. Financial consequences

Threats catalogues are:

T1: Force majeure

T2: Organizational shortcoming

T2: Human error

T3: Technical failure

T5: Deliberate acts

Safeguards measures include: infrastructure, organization, personnel, hardware and software, communication, and contingency planning.

This method, before starting the risk analysis, does a basic security check to verify implemented security measures. Risk assessment identifies threats, which are not avoided by the measures, such as residual threats. These threats can be eliminated by additional security measures. In this way, risk will be reduced to an acceptable level.

The quality of this method is in creating threat and safeguard catalogues, which can be used in all other methods.

Sp800-30 NIST (National Institute of Standards and Technology)

This is Risk Management Guide for Information Technology systems with recommendations of the National Institute of Standards and Technology in the United States. This guide gives check-lists in risk analysis, graphics in risk treatment and references based on US regulatory issues (Stoneburner, Gougen, & Feringa, 2002).

By this Institute risk assessment is the first process in the risk management, and methodology includes nine steps:

1. System characterization
2. Threat identification
3. Vulnerability identification
4. Control analysis
5. Likelihood determination
6. Impact analysis
7. Risk determination
8. Control recommendations
9. Results documentation

Steps 2, 3, 4 and 6 can be performed jointly after step 1 has been done.

Information relevant to the IT system must be collected. Specific hardware, software, system interfaces, performed processes, data and information, system and data criticality and sensitivity characterize an IT system. There are various techniques for gathering system-related information: questionnaires, interviews, document reviews, or use of automated scanning tools.

In step 2 threat actions and threat sources are identified. The threat sources can be classified as natural threats (floods, earthquakes…), human threats (unintentional or deliberate actions) and environmental threats (power failure, pollution...)

Information about system characteristics is a source for identifying IT system vulnerabilities of the assets (hardware, software, and information), procedures, processes and information transfer. Also NIST offers a vulnerability database (http://icat.nist.gov). Vulnerabilities can be identified by verifying whether security standards are fulfilled. In this step security requirements check list is used.

Step 4 provides the analyzing of the controls implemented in order to minimize likelihood of an event, which exercises system vulnerability. This likelihood is determined in step 5 and can be described as high, medium and low depending on the level exercising vulnerability by a given threat-source.

Step 6 – impact analysis requires information about performed processes, regarding the value of the system to the organization. The impact level can be determined on the basis of the IT system and data sensitivity, i.e. loss of their integrity, availability and confidentiality. Qualitative assessment can be done by terms: high, medium and low, and quantitative can include an estimation of the frequency occurrence, costs of repairing, and assumed damage factor.

During step 7 the level of risk is assessed. This assessment can be derived by multiplying values assigned to threat likelihood and threat impact. This is expressed in form of risk-level matrix 3*3, with the following assigned values for likelihood: 1.0 – high, 0.5 – medium, 0.1 – low, and for impact: 100 – high, 50 – medium, and 10 – low, as shown in Table 1.

Table 1: Risk-Level Matrix

Threat Likelihood	Impact		
	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

Risk scale is presented as: High (>50 to 100); Medium (>10 to 50); Low (1 to 10).

Derived risk values are expressed quantitatively and qualitatively. Values classified as high risk level require fast corrective measures. In the case of medium risk level corrective measures are required within a reasonable period of time, and low risk level can be accepted with or without any action.

Step 8 provides control recommendations in order to reduce the risk to an acceptable level, and all results from all performed steps are documented in an official risk report in the last step. This report describes the threats, vulnerabilities, measured risk level, and recommended controls.

The second process of risk management is risk mitigation, which performs evaluation, and implementation recommended controls for risk elimination or reducing.

Risk assessment is an absolutely relative process. That could be confirmed by the example in Table 1, by changing values in the risk scale. For instance, with the next risk scale: High (50<= x <100); Medium (10<= x <50); Low (0< x < 10), we would obtain Table 1a with different risk values.

Table 1a: Risk-Level Matrix

Threat Likelihood	Impact		
	Low (10)	**Medium** (50)	**High** (100)
High (1.0)	**Medium** 10*1.0=10	**High** 50*1.0=50	**High** 100*1.0=100
Medium (0.5)	**Low** 10*0.5=5	**Medium** 50*0.5=25	**High** 100*0.5=50
Low (0.1)	**Low** 10*0.1=1	**Low** 50*0.1=5	**Medium** 100*0.1=10

Possibilities are various, since the same procedures are applied on impact or threat likelihood, assigning different values to each level. It means that the risk assessment is the only assessment, but in the same time it means that experts must be vary careful and with great experience.

The advancement of this method is in clear visualization given in the form of risk matrix as a combination of threat likelihood and impact. However, this matrix should be used for the development of one's own matrix depending on experience.

Occupational Health and Safety Risk Assessment Method

Risk assessment is the important component of safety analysis. Nowadays, accidents and risks are serious problems from the global point of view, and particularly in the occupational area.

Recognizing and identifying hazards and harmfulness in the workplace and in the work environment is one of the most important steps in the risk assessment. The accepted risk method has to be clearly presented in documentation. Different methods can be used and there is no bad method, but some of them are preferable. The expert team from our institution, developed the original method for occupational health and safety risk assessment, based on EU Directives, our laws and regulations, industrial standards and recommendations, and on 20 years of previous experience in this field. The method enables the quantification of qualitative values regarding workplace and working environment, and it has been successfully tested through carrying out many Risk Assessment Acts (Nikolic & Laban, 2008).

After the initial steps (getting to know the company, job processes, organization, technology, etc.) risk analysis is performed according to the regulations in the following order:

- Recognizing and identifying hazards and harmfulness in the workplace and in the work environment
- Risk assessment, considering hazards and harmfulness
- Establishment of ways and measures for removing, reducing or preventing risk
- Risk reassessment according to the remaining hazards and harmfulness, after implementing the above measures
- Conclusion
- Conducting the measures to maintain the achieved risk level

The first approach is the using of an existing method with tables and mostly quantitative values of all elements needed for the risk assessment: accident probability, harm consequences and frequency, as well as the risk.

This approach considers the individual workplace of any kind and begins by defining four levels of risk:

- negligible x <5
- low, but significant 5<= x < 50
- high 50<= x <500
- unacceptable >=500

Risk descriptors and their numerical values could be modified according to the user. Tables 2 through 5 display accident probability values, event frequencies, degrees of consequence and the number of endangered people.

Table 2: Likelihood of occurrence (P)

Almost impossible – possible only under extreme circumstances	0.033
Highly unlikely – though conceivable	1.0
Unlikely – but could occur	1.5
Possible – but unusual	2.0
50% possible	5.0
Probable – not surprising	8.0
Likely – only to be expected	10.0
Certain – no doubt	15.0

Table 3: Frequency of exposure to hazard (F)

Once in working life	0.1
Annually	0.5
Monthly	1.0
Weekly	1.5
Daily	2.5
Hourly	4.0
Constantly	5.0

Table 4: Degree of possible harm (H)

Scratch/bruise/motivation	0.1
Laceration/mild ill-effect/burn/management support	0.5
Communication/knowledge and skill	1.0
Break of minor bone or illness/all psychophysical abilities	2.0
Break of major bone or major illness (temporary)	4.0
Loss one limb, eye, hearing loss (permanent)	6.0
Loss two limbs, eyes (permanent)	10.0
Fatality	15.0

Table 5: Number of persons exposed to hazard (N)

1-2 persons	1
3-7 persons	2
8-15 persons	4
16-50 persons	8
50+ persons	12

Risk is calculated as:

$$R = P * F * H * N \quad (1)$$

Form 1 presents hazards and harmfulness based on the description of the work process. Forms 2.1 and 2.2 give risk elements from Tables 2-5 and the calculated risk, as well as measures for removing, decreasing and preventing risk, followed by risk reassessment, conclusion and recommended measures to maintain the achieved risk level.

Form 1: Hazard and harmfulness identification

COMPANY:		PLANT:		WORK PLACE:			
N°	Hazard code	Hazards and harmfulness	Auxiliary means for determining hazard exposure	DESCRIPTIVE ANALYSIS			
				Occurrence probability	Consequences	Exposure frequency	Risk

Form 2.1: Risk assessment, valuation and reduction

Responsible Person:	Person in charge of safety :	ANALYST :

Risk ASSESSMENT, valuation and reduction

QUANTITATIVE RISK ANALYSIS						RISK REDUCTION MEASURES			
Event Probability	Level of Damage	Frequency of Exposure	Number of Workers	RISK	RISK LEVEL	Protection Aims	Constructional	Protective	Organizational

Form 2.2: Risk reassessment and risk management

DATE :						ID OF THE WORKPLACE :			Links with other documents	
RISK ASSESSMENT, VALUATION AND REDUCTION						RISK MANAGEMENT				
REMAINING RISK ASSESSMENT						MEASURE ENFORCEMENT			CONCLUSION	
Event Probability	Level of Damage	Frequency of Exposure	Number of Workers	RISK	RISK LEVEL	WHO	DEADLINE	PROCEDURE		RECOMMENDED MEASURES FOR MAINTAINING AN ACCEPTABLE RISK LEVEL

The second approach is to create a matrix of risk as a combination or multiplication of probability and consequence. Probability is created as a matrix of safety assessment and frequency. Safety

assessment is defined by analyzing common and particular measures of safety in the workplace and in the work environment.

This method can be used for non-production workplaces, group workplaces, work environment, collective offices, etc. The following assessment levels can be performed by this method:

- level of company location
- level of object or object's part (floor, work office, plant, administrative and non-productive workplaces …)
- level of a particular workplace and work activity

In the second approach, the probability is not defined in Table 1, but on the basis of safety assessment in the next step-by-step procedure:

Step 1**:** safety assessment is defined as the ratio of negative marks *n* and the total number of observed risk dimensions *N*

Step 2: probability values from tables are dependent by function:

$$y = 0.06\ (x)^{2.7} \tag{2}$$

where y = P, event probability, x periods for different probabilities.

In this case, safety status assessment variable x is equal to $8^{*}\frac{n}{N}$

Step 3**:** probability equation finally becomes $P = 16.462 * \left(\frac{n}{N}\right)^{2.7}$ (3)

Step 4**:** the above value and values for frequency (Table 2) and consequence (Table 3) are used for calculating the risk.

At all levels, risk assessment is conducted by finding out probability of accident (P), its frequency (F), and harm degree as

$$R = P * F * H * N \tag{4}$$

For each level is created a form with various elements observed in risk assessment. To each element's column is assigned the mark +, or – depending on the fulfilled safety status.

Form 3: Analysis of general and specific protection measures on every floor

Company :	Building : MAIN BUILDING	Building part/floor : GROUND FLOOR	Unit: ALL MAIN AND AUXILIARY PREMISES	Page Number

GENERAL DATA				ELEMENTS OBSERVED FOR RISK ASSESSMENT								
No.	FLOOR NAME	NUMBER OF WORKERS	JOB/WORK POSITIONS (NUMBER OF PERSONS EXPOSED TO RISK)	Fire risk	Evacuation possibilities	Evacuation Routes the shortest routes are well-marked, well-lit and with fresh air supply.	Doors to staircases open towards the exit of the building	Doors with glass areas (staircases, passages, hallways) are marked, protected from breakage	Automatic doors can be opened manually	Large moving doors (garages, warehouses), have a separate door at least 70 cm wide	There is a safe approach to the roof and onto the roof and for moving on the roof	Corridors and internal staircases satisfy the current regulations
				+	+	–	+	–	/	/	+	+

Form 4.1: Analysis of general and specific protection measures on every floor and risk calculation

Responsible Person:	Person in charge of safety :	Analyst :	Expert :	Consulted workers: all

							RISK ASSESSMENT				
No	Passages are clear, well lit and maintained in properly conditions	Internal transport routes satisfy the regulations	There are protection guards on crossways, passageways and work	There is at least one sanitary room on every floor	Number of sanitary points on each floor, with respect to number of workers	PROBABILITY $16{,}46\left(\frac{n}{N}\right)^{2{,}7}$	FREQUENCY	DAMAGE	RISK	QUALITATIVE RISK ASSESSMENT
	+	+	+	+	+					

Form 4.2: Risk management and remaining risk

Links with other documents	Date :	Document Number	Page Number

RISK MANAGEMENT	REMAINING RISK						
RECOMMENDED RISK REDUCTION MEASURES	PROBABILITY $16{,}46\left(\frac{n}{N}\right)^{2{,}7}$	FREQUENCY	DAMAGE	RISK	CONCLUSION	RECOMMENDED MEASURES FOR MAINTAINING AN ACCEPTABLE RISK LEVEL

Occupational Health and Safety Risk Assessment Method Applied in the Risk Assessment of an IS

All principles of risk assessment are the same in occupational health and safety area, as well as in IT systems. Our idea is to apply the above mentioned method for risk assessment considering a general IS as work environment such as a building, floor, and plant, while its applications are workplaces.

In order to assess the protection status of an IT system we created similar 3-page forms (like Forms 3, 4.1 and 4.2). The first page presents characteristics of the system: location, distribution, and equipment (hardware and software). The next two pages are two parts of the table with columns grouping the general data of the IS, monitored elements for protection status assessment, risk assessment, treatment of risk, and remaining risk with measures for maintaining the risk on acceptable level.

The plus sign or the minus sign is assigned to every observed element in order to assess the state of the current level of the IS safety.

Observed elements can be selected among many elements significant for the protection status. We have chosen the following:

- Compliance with fire regulations
- Compliance with environmental regulations
- Seismic characteristics of the location
- Admissible temperature and humidity
- Up-to-date certificate for electric installations and lightning strike installations
- Uninterruptible power supply
- Intensive magnetic fields causing loss of data (Electromotor, Transformer, Magnetic ID-card reading units)
- Adequate light – Loss of data can be due to strong light (sunlight - especially on cloudless summer days or at altitude, halogen lamps, special neon tubes)
- Dust and dirt
- Training of personnel
- Authorized admission to components of hardware -
- Authorized admission to components of software
- Authorized admission to data
- Hardware maintenance
- Software maintenance
- Voltage variations
- Adequate and updated antivirus software
- Backup and recovery procedures
- Adequate storage of media in case of emergency
- Systems placed behind firewalls and other network security devices that restrict access and filter unnecessary protocols
- Encryption used for wireless network traffic and, if necessary, for other traffic
- Restrictions regarding users and their connecting to wired and wireless LANs
- Segmented internal networks with internal firewalls and other protection in depth techniques
- Remote administration or access should be restricted; if used, connections should be encrypted.

There is an example of such forms. Values n (number of minus signs), and N (number of observed elements) are used for calculating of probability, frequency is estimated while corresponding values are from Table 2. For damage are used values from Table 3, but with modified descriptors as presented in Table 3a.

Table 3a: 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 the existence of the company	6.0
Financial loss, though significant, could be survived	10.0
Financial loss could not be survived	15.0

System characteristics

Company: Higher Educational Technical School of Professional Studies	**Building/part: floor** Ground floor	**Unit:** All main and auxiliary premises	**Page Number:**
Equipment, installations: PC computers, wireless internet hardware, networking hardware, printers, scanners,		**Software:** OS Windows, MS Office, educational software, financial software, student administration software	

System characteristics

The electrical mains supply is from two distribution power transformers with two separate supply cables into two school buildings. All computers are connected to the Internet either by wires or by a wireless system.

In the institution there are three computer classrooms with 35 PCs in total and one classroom with 12 laptops. In the financial department there are four networked PCs. In the student administration office there is a network of 5 PCs as workstations and one PC server. Also, there is 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 is 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 OS Windows XP, MS Office, and additional software for specific purposes.

Form 3a: Analysis of general and specific protection measures

Company :	**Building** : Main building	**Building part/floor**: Ground floor	**Unit:** All main and auxiliary premises	**Page number:**

GENERAL DATA			ELEMENTS OBSERVED FOR RISK ASSESSMENT																	
No.	FLOOR NAME	NUMBER OF computers	NUMBER OF PERSONS EXPOSED TO RISK	Compliance with fire regulations	Compliance with environmental regulations	Seismic characteristics of the location	Admissible temperature and humidity	There is an up-to-date certificate for electric installations and lightning strike installations	Uninterruptible power supply	Intensive magnetic fields – loss of data	Adequate light - Loss of data due to strong light	Dust and dirt	Training of personnel	Authorized admission to components of hardware	Authorized admission to components of software	Authorized admission to data	Hardware maintenance	Software maintenance
				– +	+	+	+	+	– +	+	+	–	–	– +	+	+	+	+

Form 4.1a: Analysis of general and specific protection measures on every floor and risk calculation

Responsible Person:	Safety Person :	Analyst :	Expert :	Consulted workers: all

										RISK ASSESSMENT				
Voltage variations	Adequate updated antivirus software	Backup and recovery procedures	Adequate storage of media in the event of emergency	Systems placed behind firewalls and other network security devices that restrict access and filter unnecessary protocols.	Encryption used tor wireless network traffic and as appropriate for other traffic	Restrictions regarding users and their connecting to wired and wireless LANs	Segmented internal networks with internal firewalls and other protection in depth techniques	Remote administration or access should be restricted	PROBABILITY $16,46\left(\frac{n}{N}\right)^{2,7}$	FREQUENCY	DAMAGE	RISK	QUALITATIVE RISK ASSESSMENT
–	+	+	– +	/	/	–	/	/	1.39	5	4	27.73	**Low, but significant**

Form 4.2a: Risk management and remaining risk

Links with other documents Date :	Document Number	Page Number				
RISK MANAGEMENT	REMAINING RISK					
RECOMMENDED RISK REDUCTION MEASURES	PROBABILITY $16{,}46\left(\frac{n}{N}\right)^{2{,}7}$	FREQUENCY	DAMAGE	RISK	CONCLUSION	RECOMMENDED MEASURES FOR MAINTAINING AN ACCEPTABLE RISK LEVEL
Designing of stable automated fire protection system Purchasing of UPS equipment Improvement of physical protection Providing of security rooms for media storage	0.21	1	5	1.05	**Risk is acceptable**	Obey the rules on the access to data, software and hardware. Train staff periodically. Test the equipment periodically.

In the first risk assessment (Form 4.1a) the probability (1.39) is calculated using the ratio of the number of minus signs (8) and the total number of observed items (20). The values for frequency (5) and damage (4) are estimated from Tables 2 and 3a, and the calculated risk is 27.73.

Risk reducing measures are recommended in Form 4.2a and their application should eliminate four minus signs. The probability is now equal to 0.21, and the frequency is reduced to 1, with the same damage. Finally, the risk is assessed as 1.05, which is an acceptable level. In order to maintain the risk at that level the appropriate measures are recommended.

After a common IT system safety assessment, we conducted the risk assessment of an application. The first page includes the application description. Form 1a, Form 2.1a and Form 2.2a are similar to Form 1, Form 2.1, and Form 2.2 respectively, the workplace in the occupational health area.

<table>
<tr><td>Company: Higher Educational 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,
• ranking and enrolment.
The payment process divides into the payment of:
• application and entrance examination,
• 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 students’ 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="2"></td><td colspan="2">Protective measures:
Using admission password
Antivirus software
Weekly data backup</td></tr>
</table>

Form 1a: Hazard and harmfulness identification

COMPANY:		PLANT:	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 inconsistency	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 – delaying	exists
4		Workstation failure	Possible but unusual	Hourly exposure	Loss of the last input data or data inconsistency	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 confidence	exists
7		Virus in network	50% possible	Constant exposure	Loss of data, data inconsistency, loss of confidence	exists
8		Bugs (program flaws)	50% possible		Data inconsistency	exists

Form 2.1a: Risk assessment, valuation and reduction

Responsible Person:	Safety 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, processes 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, saving 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

Form 2.2a: Risk assessment, and risk management

DATE : Links with other documents

RISK ASSESSMENT, VALUATION AND REDUCTION					RISK MANAGEMENT				
REMAINING RISK ASSESSMENT					MEASURE ENFORCEMENT				
Event Probability	Level of Damage	Frequency of Exposure	RISK	RISK LEVEL	WHO	DEADLINE	PROCEDURE	CONCLUSION	RECOMMENDED MEASURES FOR MAINTAINING AN ACCEPTABLE RISK LEVEL
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

Analysis of the Method

During the process of risk assessment of the application, we had several dilemmas. The number of workstations, the computer rooms with networked computers, or the number of clients (students in this case) who are indirectly exposed to the risk are not included in the risk assessment. Our recommendation is to multiply the risk by 2 in the cases with larger number of computers, or clients, since that allows the access through the larger number of workstations, which causes the higher risk. This formula could be more complex, but we leave that for our future work.

This method has been developed and applied successfully (by users' validation) in the occupational health and safety area for a longer period. Its benefits are the implementation of all risk assessment methodology items, uniqueness, and possibilities of wide application in many areas. The attempt to apply the method in the IT area is based on analogy. It is possible because of the manner of application on several levels. As IT security is a very sensitive area considering risk, only that layering could bring a quality risk assessment, in order to recognize all risks to which a system or its part is exposed.

Conclusion

Advantages of our risk assessment method are:

- The method is original with the official name VTS method
- The application of method is complete because it has been approved in many enterprises from the health and safety area
- The possibility of method application is obvious in all areas, especially in the IT area.
- All methodology requirements are fulfilled completely
- The applied method based on event probability determination by status value allows correction of particular status values in order to remove, reduce or prevent risk
- The method gives quantitative risk values and provides results suitable for comparison
- The method processes the impact of all types of threats and vulnerabilities

All conclusions given for methodology of risk assessment in the occupational health area could be used in the risk assessment in the IT system area.

With corresponding modifications, this method offers good quality results in the risk assessment of an IT system as well as of any of its applications. Generally, our method is based on assessing risk level-wise from the most general to the most specific level. We applied this method to the risk assessment of our IS in 2 levels. One includes the whole IT system, while the second includes particular applications. This could be done in more levels, such as assessing the risk of IT systems in each building, the labs and offices. In addition, application software could be considered as a specific level. Depending on the applied software, you can come across different threats, risks and recommended measures. We are planning to deal with these problems in our future investigation.

References

Boran, S., (2003). *IT security cookbook*. Boran Consulting.

Bozic, V., Kosic, S., & Nikolic, B. (2006). *Regulation for risk assessment procedure in the work place and in the workspace – comments*. VTS, Novi Sad.

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

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

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

Dhillon, G. (2001). *Information security management: Global challenges in the new millennium*. Idea Group Publishing.

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

Laban, M., Krnjetin, S., & Nikolic, B. (2007). Risk management and risk assessment in the enterprise. *Symposium about Occupational Safety and Health*, Novi Sad, pp. 44-57.

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

Risk Management. (2006). *Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*. 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 2008 Informing Science and IT Education Conference - InSITE 2008*, Bulgaria. Retrieved from 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.

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 labour 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.