Comparative Analysis of Two Risk Assessment Methods in Information 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 management is the process that has to be applied to all areas of business. The paper sets out to discuss risk management primarily in the field of information systems. Numerous national and international standards have dealt with this field of work. American National Institute of Standards and Technology (NIST) has developed standards, instructions and guidelines for particular issues relating to risk management in information systems, which can be compared to the international ISO standards. Special Publications 800-30, 39, 37...examine the risk assessment method in information system (IS) which is in this paper analyzed in comparison with the method created by B. Nikolic, who has developed it in the field of Occupational Safety and Health (OSH), and which has been applied in the field of information technology (IT).

Keywords: risk assessment, information system, methods.

Introduction

This paper is a continuation of several papers by the same authors on the topic of risk assessment of information systems (Nikolic & Ruzic-Dimitrijevic, 2009, 2010, Ruzic-Dimitrijevic & Nikolic, 2010, 2012). The authors have tried to apply the method of risk assessment originally developed in the field of occupational health and safety (OHS) in other areas, including also the field of information technology (IT) (Nikolic & Ruzic-Dimitrijevic, 2009), by correcting some of its elements.

The paper analyzes the risk assessment methodology regarding information systems and the manner of its performance, comparing the NIST method and the method created by prof. Bozo Nikolic (BN method). The analysis discusses the elements involved in the risk assessment of IS. The importance of recognizing different levels in the process of risk assessment is particularly emphasized. The identification of these levels and layering of IS according to the type of resources, infrastructure and value that they represent for the entire organization whose part they are, allow better risk management.

For some elements, such as hazards and vulnerability, the manner of their treating in the NIST and BN methods is described and analyzed. The method of determining the likelihood of hazardous events and their possible consequences, harms, and ways to present them in both methods are discussed in particular.

The aim of the paper is to test the settings of the BN method, and comparing it with the method recommended by NIST to indicate its advantages and disadvantages. The obtained results allow further work in this area with broadening of theoretical and practical knowledge, as well as the implementation in the curriculum of the appropriate course in specialist studies at our institution.

Risk Management

Risk management is a continuous process which includes risk framing, risk assessment, actions taken in response to the assessment results, and monitoring of the residual risk. Risk assessment is certainly the key component of the risk management whose aim is to:

- identify hazards of a particular system
- estimate the current conditions of a system, disclosing its vulnerabilities
- anticipate the likelihood of the threat event occurrence and
- assess the impact, i.e. harm that might arise as a consequence of the occurrence of the threat event

Since the risk is a measure of the entity's exposure to the threat event and circumstances, it means that it is represented by the function of the degree of harm and likelihood of the threat event occurrence.

The risks of information security arise due to loss of confidentiality, integrity, availability of information or information systems and might bring about possible negative impact on a variety of company activities (performance, function, reputation etc.), resources (assets), individuals, other organizations and a whole society.

Risk assessment is based on the assessment of several interconnected factors. The skill of risk assessment lies in identification of these elements and assessment of their values. This means that all hazards that might occur have to be recognized (empirically, according to the catalogue), the degree of system vulnerability has to be assessed, likelihood and frequency of the threat event occurrence have to be anticipated, harm that might arise has to be assessed, so that, finally, the risk assessment is conducted as a function of all the estimated values of the above-mentioned elements.

It is crucial not to omit a single risk when managing risk. This means that all the risks related to the observed system have to be assessed. Of course, information systems consist of technical parts: hardware, network, rooters etc, software parts: operating system, program environment, applications etc, people who make use of it, organization of system performance, and most importantly – information. However, the range of operations of IS is much wider. In view of the today's development of IT and its usage, the IS risk assessment has to include a variety of hazards together with consequences which might influence not only the owner of IS, but also the users, who might be external, in which case it is felt by an individual, other companies and, after all, a whole society.

Levels of Risk and System Assessment

In risk assessment, it is of vital importance to determine various levels of the system at which the assessment is carried out. According to NIST, for the purpose of information security these are: the level of organization, the level of business process and information systems level.

Based on our experience in the risk assessment in the field of OSH and Fire Protection, when conducting risk assessment the system levels have to be recognized, not only as parts of the structure, technological processes or organizational units, but these levels also have to reflect the need

for different ways of treating risks. The levels might be physically apart, which depends on the risk assessment framing. For instance, in risk assessment of information systems, it is necessary to conduct assessment of a whole facility where the equipment is situated, then of the floors, particular rooms, infrastructure, external and internal network and so forth. Such a division represents hierarchical levels, but division into levels could be also conducted according to specific characteristics of hazards that are encountered at them or there are vulnerabilities of entirely different type. For these levels, special protection measures have to be anticipated, and therefore it is reasonable that the conclusion on the assessment as well as the recommended procedures and measures have to differ.

Similarly, the risk should be treated differently for the same hazards and vulnerabilities of the system if the likelihood of the occurrence is different or if there is significantly different frequency of the occurrence. For example, the same technical measures would not be recommended for the data access protection in the classrooms (closing USB ports) and for teachers' cabinets. Apart from that, there are some parts of information systems that have similar structure and which, at the occurrence of the threat event, would cause harm on a significantly different scale, because the resources of one part of the system are of greater importance for the company. Yet, if the harm occurs in the part of IS in the computer classrooms (educational contents), it is much easier to deal with it (cancellation of classes) than if the harm occurs in the part of IS which processes students' data (Nikolić, Ružić, 2010).

Should a company recognize hazards relating to levels that are not within its range of protection? How about an Internet provider? Higher Education Technical School has had a bad experience with the provider that made an error of erasing data during a standard procedure of making a copy. The clients suffered from the harm of losing reputation, while the provider suffered from the most severe harm – it did not survive, as all of the clients cancelled its services after not being able to retrieve their data.

With regard to layers, cloud computing is particularly interesting as the top leyer in IS. Cloud resources are external assets and they require risk assessment related to the entire Cloud computing domain. Risks of Cloud environments include service, data, and infrastructure layers (Fito & Guitrat, 2012).

This issue of levels is especially significant as it is important to recognize the units that share similar risk factors and to treat risks according to their nature. Therefore, it is vitally important to point up the necessity for forming an expert team to deal with risk assessment. Such a team should comply with the recommended standards and procedures, but as there are no universal marks, it is necessary to assess the current conditions of the system as accurately as possible including all the risks in all of its parts which might be a consequence of internal or external circumstances.

Hazards and Vulnerability

The foremost step in risk assessment is the identification of hazards, which has to include all possible sources of hazards. NIST recognizes hazard sources as:

- adversarial (internal and external), which usually result from the intention of an individual or an organization, and sometimes from a senior management due to the introduction of new requirements of running business which might pose hazards (e.g. e-trade and similar activities).
- Non-adversarial, resulting from a worker's unconscientious performance
- Structural, including

  - Equipment (hardware, communication lines)
  - Immediate environment, micro-climate (humidity, temperature, energy supply etc.)
  - Software (operating system, network software, applications etc.)
- Environment
  - Force de majeure (fire, earthquake, bombing etc.)
  - Infrastructure (telecommunications, electric power)

The BN method, which was originally used in the field of OSH, does not recognize adversarial hazard sources or adversarial risk, although these elements might be included for specific security related workplaces, and also for some other workplaces especially in view of the rise in terrorist attacks in the world. In the field of IT, this type of hazards is singled out for its distinctive features, since the virtual space opens up ample opportunities for adverse activities mistakenly giving an impression that it is not easy to determine the culprits of such attacks.

Hazards in the BN method are classified according to the levels and many of them are also the elements present in evaluation of the conditions of the observed part or level of the system. For the organization's information systems, the important data about hazard sources might be obtained from the provided catalogues of hazards, as well as from the statistics of the previous events, which is very important for determining the likelihood of the threat event occurrence.

NIST provides this invaluable catalogue, which could be a useful source for the hazard identification process. However, every system has its own specific environment – to begin with the building in which it is situated, infrastructure connecting it with the surroundings, and finally superior institutions that might bring about negative consequences by unexpected legislation (Nikolic & Ruzic-Dimitrijevic, 2010). The papers written by B. Nikolić also emphasize the methodological aspect, concerning the assessment of hazards and harms, as the most delicate one, and for this particular reason it has to be a privilege of the experts in the particular field for which the assessment is conducted.

Evaluation of Protection Conditions – System Vulnerabilities

NIST method discusses vulnerabilities and predisposing conditions. These two elements are closely related to each other and to the likelihood of the threat event occurrence.

The BN method (Nikolic, 2012) makes use of these elements at particular levels for determining likelihood as the function of protection conditions. Vulnerability of the system results from the current conditions of the protection, which are, actually, predisposing conditions.

The condition of a system is described by condition variables. These have to be known and always related to the essential issues, standards or legal regulations. In order to estimate system conditions, we have to know all the variables that characterize a particular system.

The more positively evaluated condition variables there are, the larger product of the total number of marks is obtained, which means better protection conditions and lower vulnerability. In fact, the method presents the protection condition by the function of protection which in combination with frequency or time frame of the system's exposure to attacks produces the likelihood of the threat event occurrence. The likelihood of such an event combined with particular consequences is the risk.

Thus, the protection condition is described by variables of the protection condition whose number is "N", and these variables are defined by standards. If the number of negatively estimated variables is "n", then the function of the condition f(x) is

$$f(x)=n/N$$

and it represents system vulnerability. In the OSH method, this function is obtained from the likelihood table, using the method of engineering experiment. Its form is

$$f(x)=16{,}46\ (n/N)^{2,7}.$$

This function of the condition in combination with frequency or the time frame of exposure to a hazard provides the likelihood of the event occurrence (V)

$$V= f(x)\ F.$$

The combination of the likelihood of the event occurrence with the known impacts (H) represents the risk

$$R=V\ H = f(X)\ F\ H$$

Now, it is clear that the risk might be reduced through the function of condition, i.e. through the improvements to system conditions. These improvements are protection measures, but it should be also taken into account that the risk could be reduced through frequency or time frame of exposure, as well as by reducing harms, i.e. impacts.

It is assumed that every organization has prescribed certain protection measures and they have been applied. When conducting risk assessment, the current protection conditions have to be estimated. This step is crucial as it is a starting point of the risk assessment process. In order to estimate the protection conditions, it has to be checked how much the system is protected for each of the assumed hazards. There are rules and procedures which have to be passed and brought into force, but in view of the possible changes to processes, equipment and support, which is a common practice in the field of IT, the protection conditions have to be estimated periodically to have most system vulnerabilities eliminated.

There are approaches that adversarial or non-adversarial avoidance of applying the prescribed protection measures is the most common cause of the threat event occurrence. Adversarial or non-adversarial avoidance of applying the prescribed safety procedures should not be taken into consideration when assessing risks, however, what has to be included is the control of the application of the prescribed measures for maintaining the risk at the reasonable/desirable level, i.e. monitoring of the residual risk.

NIST refers to the vulnerability that can be identified even out of the information systems boundaries. If the information systems is seen in a wider context, the source of its vulnerability could be ineffective legislation, forced decisions made by higher instances which have to be implemented (Nikolić & Ružić, 2009), or services provided by external suppliers (e.g. energy or Internet provider).

The easiest way to estimate the system vulnerability at a certain level is through estimating protection conditions. In other words, it means to set the anticipated system hazards for every level and estimate the risk according to the method, taking the anticipated vulnerability for each of them, and a negative or positive value depending on the fact whether the protection measure has been introduced.

Likelihood of Threat Event Occurrence and Harm Size

Both methods are semi-quantitative. NIST provides a scale of values equal for all of the observed factors. This scale, apart from numerical values ranging from 0 to100 or from 0 to 10, provides a thorough description of each value in terms of the observed factor. This is of great significance since this description is essential for understanding and makes for obtaining quality results. It is also recommended to the users of the BN method (Nikolic, Laban, 2008) to have as detailed a description as possible.

Table 1: Assessment scale – likelihood of threat event occurrence (non-adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times a year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times a year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times a year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year**, but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

Table 2: Assessment scale – likelihood of threat event resulting in adverse impacts

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

NIST: Overall likelihood of the threat event occurrence resulting in adverse impacts is obtained on the basis of a matrix including the likelihood of occurrence and likelihood that the event results in adverse impacts. In risk assessment, the results obtained from overall likelihood and the values of impacts are included in the matrix. In this way, the harm size affects the risk assessment twice, but this dual influence is probably mitigated by the way in which the matrix is formed. However, a question should be raised concerning the reason why an event is deemed a threat if it does not result in adverse impacts.

Table 3: Assessment scale – overall likelihood

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Table 4: Assessment scale – level of risk (combination of likelihood and impact)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

The factors that are included in risk assessment are: characteristics of the threat event, system weak points – system vulnerabilities, likelihood of the threat event occurrence resulting in adverse impact, and impacts themselves. The method is semi-quantitative, but as the numerical values are the same for all of the factors and have descriptive equivalents (Very high, High, Moderate, Low, Very low), both likelihood and risk are obtained through the combination of these values in matrices, so that there are no calculations, and numerical values are not included in the assessment, as they only express the values such as Very high, High etc.

BN method deals with likelihood of the threat event occurrence separately, as well as the frequency or degree of exposure, and the harm that might be inflicted, assigning numerical values to each of these elements that then are included in producing the numerical value of the risk.

Risk Calculation by BN Method

Risk is calculated as:

$$R = P * F * H * B,$$

where P is likelihood of occurrence, F is frequency of exposure to hazard, H is degree of possible harm, and B is number of participants in the event.

$$P = f(x) = 16.46\ (n/N)^{2,7}$$

Table 5: Likelihood of occurrence (P)

Almost impossible – possible only under extreme circumstances	0.06
Highly unlikely – though conceivable	0.39
Unlikely – but could occur	1.16
Possible – but unusual	2.53
50% possible	4.63
Probable – not surprising	7.57
Likely – only to be expected	11.48
Certain – no doubt	16.46

Table 6: 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 7: 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

Numerical and descriptive values in the tables have not been obtained statistically, but in an empirical way (Nikolic, 2012). The starting values from the tables and the values currently used differ numerically and descriptevily both in OSH and IT areas. Firstly, the data has been analyzed, then certain corrections and recommendations proposed by the standards have been applied and thus the final values have been adopted.

The numerical values in all the tables are such that their impact and share in the risk assessment process render a realistic picture. The investigation into each of the factors of risk can illuminate clearer elements, issues, concerns and gaps that may go otherwise unrealized. The advantage of using numerical values lies in the fact that when measures for reducing risk are applied, the lower values are obtained in one of the tables, because the application of a measure leads to the reduction of likelihood of the threat event occurrence or its frequency or the harm it inflicts, so that the re-assessed risk is going to be lower owing to a smaller value (or values) of variables in the calculation of its total value.

Conclusion

The authors have taken great pleasure in studying NIST. The starting point in the risk assessment of a system has to be standards that provide instructions and guidelines, as well as exceptionally useful empirical data. The aim of this paper has been to compare the method provided by the standards to the BN method. The authors hold the opinion that the former method is in

compliance with NIST and that the developed base of anticipated hazards and impacts can be used in their further work.

On the other hand, the authors would point up the advantages of the BN method due to the numerical values and opportunity for more operative usage of the estimated variabales and obtained results.

This method has been successfully used in hundreds of documents in the practice of risk assessment in the field of OSH and has produced realistic and acceptable results. Using it in the field of IT, we have percieved that it is highly applicable, on condition it is regularly checked and updated. Currently, the subject Risk management and risk assessment methods is included in the curriculum of the specialist studies of all the study groups. Upon completing the part on risk management that is mutual for all the study groups, the students focus on the risk assessment relating to the their specific fields of studies. The students of IT have been assigned a task to divide the chosen IS into the levels for risk assessment and to conduct risk assessment at a particular level using the BN method. We will make use of these invaluable results in further research, while the obtained results will help students grasp the importance of the risk assessment of IS and the impact of each of the factors on the risk, so that they will eventually become capable of successful management of IS security.

References

BSI Standard 100-1: Information Security Management Systems (ISMS) (2008). Retrieved December 2012, from www.bsi.bund.de

BSI Standard 100-2: IT-Grundszchutz methodology, (2008). Retrieved December 2012, from www.bsi.bund.de

BSI Standard 100-3: Risk analysis based on IT-Grundszchutz, (2008). Retrieved December 2012, from www.bsi.bund.de

Fitó, J. O., & Guitart, J. (2012). *Introducing risk management into cloud computing*. Barcelona Supercomputing Center and Technical University of Catalonia, Barcelona, Spain. Retrieved November 2012, from http://upcommons.upc.edu/e-prints/bitstream/2117/15944/1/Fito.pdf

GAIT for Business and IT Risk (GAIT-R) (2008). The Institute of Internal Auditors, 2.

GAIT Methodology: A risk-based approach to assessing the scope of IT general controls, The Institute of Internal Auditors, 3.

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

International Standard ISO 31000 First edition 2009-11-15.

McCumber, J. (2005). *Assessing and managing security risk in IT systems: A structured methodology*. Auerbach publication CRC Press LLC.

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

Nikolic, B. (2012). A new risk assessment method. *Monitoring and Expertise in Safety Engineering, 2*(1), 5-23.

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 system. *Issues in Informing Science and Information Technology, 5*, 595-615.

Nikolic, B., & Ruzic-Dimitrijevic, L. (2010). Information system and risk reassessment. *Issues in Informing Science and Information Technology, 7,* 191-207.

NIST Special Publication 800-39: Managing Information Security Risk. (2011).

NIST Special Publication 800-37: Managing Information Security Risk. (2011).

NIST Special Publication 800-30: Guide for Conducting Risk Assessments. (2012).

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. (2010). *Risk of losing data confidentiality in information system*. International Conference on Safety engineering, Kopaonik 2010, Serbia

Ruzic-Dimitrijevic, L., & Nikolic, B. (2012). *The importance of risk assessment of information systems.* Science and Higher Education in Function of Sustainable Development – SED 2012, Uzice, Serbia

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.