Online Journal of Applied Knowledge Management
A Publication of the International Institute for Applied Knowledge Management

Volume 3, Issue 2, 2014

Risk assessment of knowledge management system

Ljiljana Ruzic-Dimitrijevic, *The Higher Education Technical School of Professional Studies, Novi Sad, Serbia, ljdimitrijevic@gmail.com*

Abstract

This paper considers the risk assessment in the field of knowledge management. Since knowledge management systems can be observed at the stage of implementation and use, the risks also differ. An overview of the factors critical to the success of a knowledge management system is presented, as well as one method of risk assessment including its possible application to a knowledge management system. It is pointed out that the identification of risk factors is highly significant, together with the evaluation of their impact on knowledge management system. The presented method provides for the quantifying of risk and allows corrections and comparison of the results.

Keywords: risk assessment, knowledge management system.

Introduction

This paper deals with the issues of risk management and knowledge management, as the integral elements of business management. There can be several relations between these two issues. One is how to improve the risk management process by applying the knowledge management system (KMS) to it. The other is how to identify risks in the knowledge management system and how to manage the risk in that system, in order to obtain the best results in terms of the risk reduction.

The aim of this paper is to consider the issue of the risk in the processes related to knowledge management system. We make the hypothesis that there is a need of risk managing in KMS, i.e. in applying and using KMS. We will use common risk managing methodology that could be applied to any field of work. Our focus will be on the defining of the risk factors and on the risk assessment.

What is KMS? According to one of the proposed definitions in techopedia dictionary: "A knowledge management system (KMS) is a system for applying and using knowledge management principles." (Janssen, 2015)

By Lehaney et al. (2004) the KMS is the collection of three subsystems:

- People interactions,
- Technology acting,
- Organizational structures.

This system consists of the processes of knowledge creation and its transmission, the knowledge transfer. Knowledge management systems belong to the class of information systems whose tasks are the following ones:

- to create new knowledge,
- to capture knowledge in an explicit form,
- to support and facilitate content management,
- to share knowledge, and
- to apply and re-use knowledge to generate value

Four processes that are important for knowledge management can be identified: creation, storage and retrieval, distribution, and application. (Alavi & Leidner, 2001)

The risks can be identified at two planes of the knowledge management system: in the process of implementing KM systems, and in the process of achieving the system objectives, which is the adopting and use. (Benoit et al., 2011)

The literature dealing with the issues of the implementation and the use of a KMS provides the factors that are recommended as being crucial for the successful implementation and use of KMS.

Noordin et al., (2013) singled out the following factors as the key factors for successful adopting and implementation of a KMS:

- efforts/strategy (infrastructure, training, resources for generating knowledge, motivation,…),
- the limitations to current KMS (insufficient functionality, lack of information and knowledge stored in repository, …), and
- inhibitors in terms of infrastructure and reluctance attitude.

Ishikawa and Naka (2003) point out the knowledge selection risk, which is associated with the fact that the value of knowledge is becoming more and more short-lived. Thus, employment policies and employees' strategies for gaining knowledge are becoming immensely important.

In the paper (Jafari et al., 2008), the authors present seven critical success factors that could be significant for the implementation of KM:

- Collaboration and knowledge workers,
- Technology Deployment,
- Learning Culture,
- Flat Structures,
- Supply Chain Integration,
- Comprehensive strategies, and
- Flexible Organizations

There are also papers dealing with the weaknesses and hazards that may occur in the KMS. For instance, the following list contains the risk factors recognized during the introduction of KMS into the organization (Stankosky, 2005):

- Organizational culture 80%
- Lack of ownership of the org. 64%
- Lack of IT technology 55%
- Nonstandard processes 54%
- Organizational structure 53%
- Top management support 46%
- Awards/ recognition 46%

Further, Riege (2005) recognizes three types of barriers in adopting and using KMS. These are individual, organizational, and technology barriers.

Individual barriers are mainly considered to be the lack of time or awareness of the importance of sharing knowledge, as well as communication skills (both verbal and written), difference in education, culture, and position.

Generally, it is difficult to say which organizational structure is the most suitable for knowledge management, but it is important to take into account particular and specific characteristics of a company since "Knowledge sharing practices often seem to fail because companies attempt to adjust their organizational culture to fit their KM, instead of implementing them so that they fit their culture." (Riege, 2005, p.28)

Technology is undoubtedly a very important factor that supports and facilitates knowledge sharing processes, but it can be regarded as a barrier if it is inadequate or insufficiently accepted by the participants in the KMS.

What stands out as the main factor of success is the overcoming of the above-mentioned barriers, which are:

- motivation, encouragement, and stimulation of individual employees,
- flat and open organizational structures and
- modern technology with a suitable sharing platform

There is also an opinion regarding a decline in KM popularity, although "it was once a very popular buzzword ". It is attributed to the failure of KM projects (Frost, 2014). Frost recognizes two categories of failure factors: causal and resultant. Causal factors are more common and related to organizational and managerial issues required for the implementation of KM. Resultant factors refer to specific problems such as lack of quality and usability, loss of knowledge, etc. (Frost 2014)

In fact, it is difficult to make a general matrix to select the best KM strategy, because it must be based on the specific characteristics of a company, its activities, organization, and available resources. In any case, in order to achieve success in the KM, we firstly must identify the barriers, i.e. the risk factors that may lead to the failure both in the implementation and in the application and use.

Risk and risk management

The risk or uncertainty should be considered and monitored in all areas of work and business. Risk management is a continuous process which consists of several steps and which is repeated periodically. It includes (Risk Management, 2006):

- the determining of the level of protection,
- the defining of the risk criteria, i.e. the risk evaluation,
- the risk identification, analyses and assessment,
- the risk treatment (recommendation of measures for the risk reduction, and the assessment of the residual risk),
- the accepting of the desired level of the risk, and
- the maintenance of the risk.

Risk assessment is a part of the risk management process which is performed for each level of protection. The ultimate aim of the risk assessment is the decision on the level of the acceptable risk and the measures that will ensure the maintenance of risk at the determined level. The risk assessment procedure is based on the identification of hazards and the assessment of risk arising from the identified hazards. The most important and the most demanding part of this process is the identification of hazards and possible harm.

The risk in the area of IS security is related to the possibility of damaging or losing of information, hardware, intellectual property, prestige or reputation and is usually expressed as the function of hazard, vulnerability, and effects, i.e. harm. (BSI Standard 100-1,2,3, 2008), (McCumber, 2005).

Safety is the process of maintaining an acceptable level of risk, but it is not the final state. It includes procedures, policies, training, raising of the awareness and constant monitoring of the situation.

Today, every business organization has more or less developed information systems. Therefore, risk management in any company should include the risk of information systems as well. (Ruzic-Dimitrijevic, 2013)

Since the KMS could be viewed as a class of information systems (Alavi & Leidner, 2001) where the use of information technology is of special importance, the risk of KMS can be observed in a similar way as in the Information Technology Systems, using some of the standards that deal with information security, such as the NIST Risk Management Guide for Information Technology Systems, as a starting point. (NIST, 2011, 2012), (Stoneburner, et all, 2002).

Dr. Blaize Horner Reich, of Simon Fraser University, and her colleagues recognized five principles for managing knowledge risks in IT projects (Reich, 2007).

- establishing a learning climate;
- mitigating knowledge loss;

- creating channels for knowledge flow;
- developing a shared team memory and
- using the risk register to monitor knowledge risks. Although these principles refer to IT projects , they can be considered common to every project.

Furthermore, there is a list of 10 risks that should be considered. They refer to the adoption and transfer of knowledge, improper use, and loss of knowledge or poor organizational relations within a team.

Thus, the authors Aljafari and Sarnikar (2010) used the methodology for the risk of information technology systems (ITS), and extended the risk assessment frameworks for IT to include knowledge assets and risks related to knowledge sharing. In this study, the authors perceive the risk that arises from the transfer of knowledge assets, apart from the benefits that collaboration brings into inter-organizational network structures. Therefore, the identification and risk assessment of knowledge sharing is recommended. The following risk factors are mentioned:

- Unauthorized learning
- Unauthorized sharing of sensitive knowledge
- Unauthorized use of knowledge asset
- Manipulation of knowledge asset
- Appropriation of knowledge asset

As in any other risk assessment procedure, the methodology is the same:

- Identify inter-organizational processes
- Value knowledge assets (people, documents, or technology artifacts)
- Identify collaboration technologies (create a Process-Technology-Asset matrix pointing out the knowledge asset vulnerabilities)
- Map risks to knowledge assets
- Provide evidence (evaluate the current measures and estimate the likelihood of the identified threats)
- Calculate risk (calculate the level of risk associated with sharing each knowledge asset via particular technology)
- Develop policy (in order to mitigate the calculated risks)

Risk assessment in KMS

Risk management includes the analysis whose purpose is to identify hazards, assess the risk and predict mitigation mechanisms. This is a multidisciplinary job, reserved for experts because one has to be knowledgeable about the field of work in which risk is managed, and to understand the risk itself.

The risk is represented by the function of the degree of harm (the range of undesirable outcomes) and likelihood of the threat event occurrence.

The introductory section provides, within the literature review, the elements which are considered essential for the successful implementation and use of KMS when assessing risks.

The thing that differs KMS from other projects is that it is not final, i.e. its completion cannot be assessed as being successful or not. An implemented KMS should achieve the objectives and that is the measure of the project success. Thus, its use, knowledge acquisition, sharing, transmitting, and above all, the obtaining of the valuable results, i.e. the products of that knowledge, are not limited by deadlines. For the KMS, the undesirable outcomes are failure to achieve one or more of the KMS objectives.

Benoit et al. (2011) proposed a method for estimating the risk of KMS, which is based on the identification and assessment of risk factors, i.e. the relevant variables underlying this risk. The concept of this method is very similar to the BN (Bozo Nikolic) method that the author used in the IS risk assessment (Nikolic & Ruzic-Dimitrijevic, 2013, 2009).

To determine the risk and harm factors, Benoit et al. (2011) used historical cases to establish the starting lists, which were validated by five experts working in the field of KM. Thus, they provided the list of 32 risk factors. The BN method formed the list of risk factors in a similar manner, following the recommendations provided in the international standards and expert opinions.

Benoit et al. (2011) consider the unfulfilled objectives of KMS as undesirable outcomes, and there are five of them. The table shows the correlation between each factor and its undesirable outcomes. The discussion states that it is difficult to determine the importance of each factor, but it could be considered that those who produce all five outcomes have a greater significance.

According to the BN method, the harm should be evaluated firstly, i.e. undesirable outcomes. The method uses the following scale for IS:

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

Table 1. Degree of harm – BN method

If we adopt the following list for KMS, we raise the question regarding how we are to evaluate each of these five items:

1. Difficulty/impossibility to create new knowledge
2. Difficulty/impossibility to capture employees' knowledge

3. Difficulty/impossibility to improve content
4. Difficulty/impossibility to share knowledge
5. Difficulty/impossibility to generate value

The best approach would be to carry out a survey in order to assess opinion. In the example that has been provided in the paper of Benoit et al (2011), all participants recognize 3 items as valid. These items should probably have the same, maximum value, although the sample was not large.

Objective of KMS	**Creation of new knowledge**	**Capture of employee's knowledge**	**Content improvement**	**Knowledge sharing**	**Value generation**
Corresponding undesirable outcome (U.O.)	Difficulty/ impossibility to create new knowledge	Difficulty/ impossibility to capture employees' knowledge	Difficulty/ impossibility to improve content	Difficulty/ impossibility to share knowledge	Difficulty/ impossibility to generate value
Number of cases in which U.O. was observed to some extent	6	8	2	8	8

Table 2. Summary of the Results
Source: A. Benoit, J.G. Bernard, C.G. Carlos, Defining Knowledge Management System Risk

Regarding the size of the harm in the KMS system, the values from the table which could be relevantly used, according to the description, should range from 1 to 6. For example, we could assign the value 6 to the second, fourth and fifth items on the list of harm, value 4 is assigned to the first item, and 2 to the third one. The values are selected in this way in order to make the results comparable with the risk assessment conducted by means of this method in other fields of work, particularly in the field of IS.

In any case, the BN method provides the risk assessment using the equation

$$R=V^* H = f(X)^* F^* H$$

Where H is the degree of harm, F frequency of the occurrence of undesirable events, and f(x) function of the protection status which is obtained by using the risk factors marked with + or -, as is defined in the work of Benoit et al (2011) as "favourable" or "negative".

The function of the condition f(x) is $f(x)=14{,}78*(n/N)^{2{,}434}$

N is the total number of the observed risk factors, and n is a number of negatively rated factors.

This function is obtained from the likelihood table, using the method of engineering experiment. (Nikolic, 2012, 2014). The risk is considered acceptable if it is lower than 5.

It is obvious that some elements from the list of outcomes are important but they do not have the same importance for every company or business. It is true that those companies have recognized the importance of such harm, but its degree varies depending on a case. Thus, it might range from 0.1 to 15, and its value will depend on the level of risk.

The frequency, which is the time of company exposure to a particular hazard can be also different for each of the hazards. The BN method provides the following table for the frequency.

Frequency of exposure to hazard (F)						
Once in working life	Annually	Monthly	Weekly	Daily	Hourly	Constantly
0.1	0.5	1	1.5	2.5	4	5

Table 3. Frequency of occurrence of undesirable events – the BN method

It is very unlikely that the KMS system is exposed to constant or daily hazards that lead to undesirable outcomes. The values from the table which could be relevantly used for the frequency range from 0.5 to 1.5, given the nature of hazard and the selection of risk factors.

Research

On the basis of the above-presented facts, we can conclude that in the formula for the probability of events, which changes depending on the number of negative marks, the outcomes and the frequency may be different. When conducting risk assessment, the experts and people directly involved in the particular KMS should work together to determine the appropriate value.

Using the example presented in the paper Benoit et al (2011) for Siemens (Table 5), the risk assessment can be conducted according to the BN method. In this example, only four undesirable outcomes were taken into account, whereas the item *Difficulty/impossibility to improve content* was omitted. We will carry out separate risk assessment for every harm, whereas N will represent only the number of observed risk factors for that particular harm. Thus, for the last harm we have observed 14 risk factors, and 5 out of these 14 are rated negatively.

The following table shows the value of risk that is obtained for various values of harm and frequency. These values indicate that the selection of frequency ranging from 0.5 to 1.5 is the most acceptable, because this method was used in various fields of work and the risk commonly entered the red zone in the cases when about one-third of the factors were negatively rated (here we have 5 out of 14).

$$R = 14.78*(5/14)^{2.434}*F*H$$

	F=5	**F=4**	**F=2.5**	**F=1.5**	**F=1**	**F=0.5**	**F=0.1**
H=6	36.2	28.9	18.1	10.9	7.2	3.6	0.7
H=4	24.1	19.3	12.1	7.2	4.8	2.4	0.5
H=2	12.1	9.6	6	3.6	2.4	1.2	0.2
H=1	6	4.8	3	1.8	1.2	0.6	0.1

Table 4. Risk for various harm and frequencies

In the case when the risk value is greater than 5, which is unacceptable according to the BN method, the risk can be reduced if the negative marks are corrected to become positive. In order to facilitate this process, we created an Excel table (Tables 6, 7) that provides the insight into the number of factors which should be corrected so that the acceptable risk level could be obtained.

Of course, one has to estimate the value of harm and exposure, i.e. the frequency, and then has to find the intersection of the number of observed and negatively rated risk factors in the table. Thus, for example, in the Table 6 (with the selection H = 6, F = 1) we obtained the risk R = 7.2 and it can be seen that it is enough to "fix" one factor only, whose positive mark will enable entering into the green zone.

In case when F = 1.5, two factors need to be to "fixed" (Table 7).

Risk Factors	Creation o new	Capture of employee knowledg	Knowledg sharing	Value generation using
Adequate strategy	●	●	●	●
Higher management involvement	●	●	●	●
Presence of incentives	●	●	●	●
Adequate roles and responsibilities	●	●	●	●
Quality of incentives	●	●	●	●
Learning abilities	Not observed in the case			
Group work tools	●	●	●	●
Internal expertise				●
System ease of use	Not observed in the case			
Adequate use of web tools				●
Data integration				●
Content indicators	Not observed in the case			
Adequate codification of knowledge	Not observed in the case			
Appropriate information taxonomy	Not observed in the case			
Adequate search tool	Not observed in the case			
Content quality				●
Trust in the system	Not observed in the case			
User participation in the development project	●	●	●	●
User training	●	●	●	●
Communication between community of practice, business partners and clients	Not observed in the case			
Collaborative culture	●	●	●	
Adequate structure and processes				●
Trust	Not observed in the case			
Information confidentiality	●		●	
Cultural differences	Not observed in the case			
Indicators to measure system value	●	●	●	●
Alerts for content	Not observed in the case			
Organizational stability	Not observed in the case			
User support	Not observed in the case			

Table 5. The correlation between undesirable outcomes and risk factors
Source: A. Benoit, J.G. Bernard, C.G. Carlos, Defining Knowledge Management System Risk.

The total number of observed factors	The number of negatively evaluated factors															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	88.7															
2	16.4	88.7														
3	6.1	33.1	88.7													
4	3.0	16.4	44.0	88.7												
5	1.8	9.5	25.6	51.5	88.7											
6	1.1	6.1	16.4	33.1	56.9	88.7										
7	0.8	4.2	11.3	22.7	39.1	60.9	88.7									
8	0.6	3.0	8.1	16.4	28.2	44.0	64.1	88.7								
9	0.4	2.3	6.1	12.3	21.2	33.1	48.1	66.6	88.7							
10	0.3	1.8	4.7	9.5	16.4	25.6	37.2	51.5	68.6	88.7						
11	0.3	1.4	3.8	7.6	13.0	20.3	29.5	40.9	54.4	70.3	88.7					
12	0.2	1.1	3.0	6.1	10.5	16.4	23.9	33.1	44.0	56.9	71.8	88.7				
13	0.2	0.9	2.5	5.0	8.7	13.5	19.7	27.2	36.2	46.8	59.1	73.0	88.7			
14	0.1	0.8	2.1	4.2	7.2	11.3	16.4	22.7	30.3	39.1	49.3	60.9	74.0	88.7		
15	0.1	0.7	1.8	3.6	6.1	9.5	13.9	19.2	25.6	33.1	41.7	51.5	62.6	75.0	88.7	
16	0.1	0.6	1.5	3.0	5.2	8.1	11.9	16.4	21.9	28.2	35.6	44.0	53.5	64.1	75.8	88.7

Table 6. The risk with the frequency F = 1 and the harm H = 6

The total number of observed factors	The number of negatively evaluated factors															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	133.0															
2	24.6	133.0														
3	9.2	49.6	133.0													
4	4.6	24.6	66.0	133.0												
5	2.6	14.3	38.4	77.3	133.0											
6	1.7	9.2	24.6	49.6	85.3	133.0										
7	1.2	6.3	16.9	34.1	58.6	91.4	133.0									
8	0.8	4.6	12.2	24.6	42.4	66.0	96.1	133.0								
9	0.6	3.4	9.2	18.5	31.8	49.6	72.2	99.9	133.0							
10	0.5	2.6	7.1	14.3	24.6	38.4	55.8	77.3	102.9	133.0						
11	0.4	2.1	5.6	11.3	19.5	30.4	44.3	61.3	81.6	105.5	133.0					
12	0.3	1.7	4.6	9.2	15.8	24.6	35.8	49.6	66.0	85.3	107.6	133.0				
13	0.3	1.4	3.7	7.6	13.0	20.3	29.5	40.8	54.4	70.2	88.6	109.5	133.0			
14	0.2	1.2	3.1	6.3	10.9	16.9	24.6	34.1	45.4	58.6	74.0	91.4	111.1	133.0		
15	0.2	1.0	2.6	5.3	9.2	14.3	20.8	28.8	38.4	49.6	62.5	77.3	93.9	112.5	133.0	
16	0.2	0.8	2.3	4.6	7.8	12.2	17.8	24.6	32.8	42.4	53.4	66.0	80.2	96.1	113.7	133.0

Table 7. The risk with the frequency F = 1.5 and the harm H = 6

Discussion and restrictions

The risk assessment of KMS is an important part of risk management for any company. Since there are various processes, it is necessary to recognize the specific characteristics for each of them and apply appropriate risk assessment. However, if you adopt one method with the same fundamental principles and the possibility of quantifying the size of the risk, then we will obtain the results that can be comparable. This means that the management structure will have a better insight into the overall system of risk management and will be able to predict shortcomings and manage risk in a more quality manner in all areas.

So far, the BN method has been used in the areas of occupational health and safety, environmental protection, information technology systems (Nikolic, 2014), (Nikolic et all, 2012), (Nikolic & Ruzic-Dimitrijevic, 2009), together with descriptions of hazards and harm that are specific for each of these areas. It is the identification of harm and hazard that is of immense importance and which might be a limiting factor. A team of experts from various fields of work should be engaged to analyze all elements and agree on their findings. For this reason we used the example provided by Benoit (Benoit et al., 2011) because the list of dangers and undesirable outcomes was formed in such a way.

Selecting the size of the damage ranging from 1 to 6, as well as the frequency ranging from 0.5 to 1.5 is recommended on the basis of the description provided in the tables 1 and 3, and also on the basis of the previous experience in the application of the method. The monitoring of the changes in the risk value in the Table 4 also confirms this choice. Here we should underline the importance of being able to compare the obtained risk values. Thus, the obtained risk values for various cases and the experience gained during this process will significantly help to assess the meaning and significance of the assumed value of the harm ranging from 1 to 6 and the frequency ranging from 0.5 to 1.5.

In addition, the BN method offers relatively simple mechanism for reducing the risk to the desired level by monitoring its size in the Excel table (Tables 6, 7).

Conclusion

KMS is, like any other system, exposed to hazards and risks that can threaten not only its implementation, but also its use and maintenance. Companies that recognize the importance of KMS for their successful performance and competitiveness must also have the risk of KMS included in their risk management system. Risk factors may differ depending on many external and internal circumstances and specific characteristics. The selection of these factors should be made by monitoring the process and drawing on other experiences. The assessment of their importance for achieving the objectives of KMS is crucial for making a good choice, because the failure to fulfill these objectives actually represents harm, i.e. undesirable outcomes.

The identified factors should be observed, and on the basis of their condition, the vulnerability of the system should be assessed. The method used by Beniot (Benoit et all, 2011) provided for the mapping of the specific risk factors associated with knowledge management systems. In this way, it presents a measure of risk exposure for knowledge management system use.

So far, the BN method has been used for the evaluation of IT systems and it enables quantitative evaluation of risk. The use of this method requires experience because the assessment of the value of harm and frequency should be conducted. A thorough analysis and active involvement of experts make it possible to obtain valid results. Of course, corrections are often necessary, because the risk is still only assessed, and that process cannot be made final, since it must be managed in accordance with the changes that are dependent on numerous circumstances.

Further research could be aimed at analyzing various types of KMS, in different fields of work, in order to check and correct the validation of the achieved results.

References

Alavi, M., Leidner, D. (2001). Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues. *MIS Quarterly* Vol. 25, No. 1, pp. 107-136.

Aljafari, R., Sarnikar, S. (2010). A Risk assessment framework for inter-organizational knowledge sharing. Sprouts: Working Papers on Information Systems, 10(29). http://sprouts.aisnet.org/10-29

Benoit, A., Bernard, J.G., Carlos, C.G., (2011). Defining Knowledge Management System Risk. *Proceedings Pacific Asia Conference on Information Systems (PACIS).* Paper 21. http://aisel.aisnet.org/pacis2011/21

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.

Frost, A., (2014). A synthesis of knowledge management failure factors. Retrieved January 05, 2015 from www.knowledge-management-tools.net

Ishikawa, A., Naka, I., (2003). *Knowledge management and risk strategies.*World Scientific Publishing Co. Pte. Ltd.

Jafari, M., Fathian, M., Jahani, A., and Akhavan, P., (2008). Exploring the contextual dimensions of organization from knowledge management perspective. *The journal of information and knowledge management systems*, Vol. 38, No. 1, pp. 53 – 71.

Janssen, C., (2015). Knowledge Management System (KMS). Retrieved January 05, 2015 from http://www.techopedia.com/definition/7962/knowledge-management-system-kms

Lehaney, B., Clarke, S., Coakes, E. and Jack, G. (2004). *Beyond Knowledge Management*. Idea Group Publishing, Hershey, PA.

McCumber, J., (2005). *Assessing and Managing Security Risk in IT Systems: A Structured Methodology.* Auerbach publication CRC Press LLC.

Nikolic, B., Ruzic-Dimitrijevic, Lj., (2009). Risk assessment of information technology system, *Issues in Informing Science and Information Technology* pp595-615 Vol 6, Informing Science Institute

Nikolic, B., (2012). A new risk assessment method. *Monitoring and expertise in safety engineering* Vol. *2* No1, pp. 5-23

Nikolic, B., Sotic, A., Sotic, I., (2012). Risk assessment and risk criteria for temporary and mobile building sites. *Proceedings Risk assessment Conference* Kopaonik, pp.279-284.

Nikolic, B., Ruzic-Dimitrijevic, Lj., (2013). Comparative Analysis of Two Risk Assessment Methods in Information Systems. *Proceedings of Informing Science & IT Education Conference (InSITE)*, pp.173-182

Nikolić, B., (2014). A new risk assessment method with the corrected function of the state of protection. *Proceedings Regional international conference on Applied protection and its trends*, pp. 43-52.

Nikolić, B., (2014). Risk management and knowledge management as a function of technology management. *Online Journal of Applied Knowledge Management*, Vol. 1, Issue 2, pp.68-81

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).

Noordin, M.F., Othman, R., and Zakaria, N.A., (2013). Investigating Key Success Factors in Adopting Knowledge Management System, *World Applied Sciences Journal* Vol. 21 (2) pp.221-229.

Reich, B.H., (2007). Managing knowledge and learning in IT projects - A conceptual framework and guidelines for practice. *Project Management Journal*, vol. 38, No 2, pp. 5-17.

Riege, A., (2005). Three-dozen knowledge-sharing barriers managers must consider. *Journal of knowledge management.* Vol. 9 No. 3, pp. 19-35.

Risk Management: 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, Lj., (2013). Impact of information system safety on the business risk, *Proceedings of VIII International Conference Safety Engineering, Kopaonik, pp. 219-224.*

Stankosky M., (2005). *Creating the Discipline of Knowledge Management - The Latest in University Research*. Elsevier Inc.

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.