Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 7, Issue 1, 2019

A measurable approach for risk justification of explicit and tacit knowledge assessment

Boštjan Delak, Faculty of Information Studies, Slovenia, bostjan.delak@fis.unm.si

Christiaan Maasdorp, Department of Information Science, Stellenbosch University, South Africa, chm2@sun.ac.za

Abstract

Knowledge has become a central organizing principle in society to the extent that knowledge management has become a mainstream activity in organizations. Nevertheless, knowledge-related risks remain relatively neglected in the risk management domain. Whilst knowledge reduces uncertainty and the associated risks, the increased knowledge intensity in organizations also represents a risk factor that has to be assessed. The paper describes and validates an organizational risk assessment approach that considers knowledge-related and knowledge management risks in an integrated manner. The approach makes it possible to calculate risk ratings in terms of vulnerability and likelihood for 50 threats to all activities and phases of the knowledge life cycle. These risk ratings are plotted against 24 potential risks in the human, organizational, and technical domains. To impress on management the significance of these knowledge-related risks, the risk ratings are transformed to approximated financial figures. The approach is applied to 10 Slovenian organizations, two of which are discussed in detail in the paper, to demonstrate that it can be successfully used in a wide variety of organizations. It is concluded that the approach offers a way to assess both knowledge-related and knowledge-management-related risks, that the costs that individual risks potentially hold can be approximated, and that for a diversity of organizations mitigation strategies can be suggested for the identified risks.

Keywords: Knowledge management system, knowledge management system risks, knowledge risk assessment, knowledge risk classification.

Introduction

Drucker (1999) wrote that the most valuable asset of a 21st-century organization would be its knowledge, its knowledge workers, and their productivity. According to Nonaka and Takeuchi (1995), organizational knowledge is of different kinds specific to the context and can epistemologically be classified in two dimensions: tacit and explicit. As a result, from an organizational perspective, there are two distinct knowledge-related goals, namely to generate knowledge and apply knowledge (Chou, 2005). Knowledge is also one of the most important resources of an enterprise. It is the currency of the current economy, a vital organizational asset and a key to creating a sustainable competitive advantage (Ragab & Arisha, 2013, p. 873).

Risk is usually considered as something that might go wrong in a process. Seen differently, risk is the effect of uncertainty on objectives, and this uncertainty is often expressed in terms of a

combination of the consequences of an event and the likelihood of it happening (ISO, 2009). The risk exposure is the probability of an undesirable outcome seen in combination with the magnitude of potential loss due to that undesirable outcome (Aubert, Bernard, & Caro-Gonzalez, 2011). Risk management is a key activity in organizations that aims to minimize the probability and mitigate the impact of risks. Accordingly, Tiwana and Keil (2005) considered risk assessment the most crucial part of any risk management activity.

Controlling knowledge management risks is one of the enterprise management tasks where managers and researchers focus on how to effectively evaluate risks when doing risk assessment (Yang & Gao, 2016). Risk assessment is a type of knowledge evaluation and whilst multiple models of knowledge evaluation have been proposed, a general conceptual framework is still lacking (Babik, Qian, Singh, & Ford, 2014). Without such a general framework, presenting knowledge-associated risks in a way that risk managers can appreciate is a particular challenge. We propose an approach for measuring and assessing the risks related to tacit and explicit knowledge as well as knowledge management within organizations. The approach converts identified risks into financial values that are more concrete for management and proposes possible solutions to mitigate the identified risks.

This paper is organized as follows: first, we present the aim of our research along with the research questions. Then follows the literature review, the research design and the methodology. The proposed approach is described in detail and then case studies of selected organizations are described to illustrate the results that can be achieved using the approach. Finally, we discuss the results and make concluding remarks.

Aim of the Research

The knowledge society is based on knowledge and its availability (Aggestam, Söderström, & Persson, 2010). Knowledge management is the concomitant management paradigm used in organizations as a response to the rise of the knowledge economy. Knowledge management views knowledge as an asset that adds productive value to organizational processes, but increased knowledge intensity also means an increase in knowledge-related risks.

The aim of this paper is to propose and validate an organizational risk assessment approach from the perspective of the knowledge life cycle that presents knowledge-related risks in the form of financial values and thus provides for the possibility of mitigating the identified risks. The approach assesses risks related to explicit and tacit knowledge within the organization. To prove the viability of our proposed approach, we need to demonstrate, firstly, that it can be used for a wide variety of organizations (or ideally in principle any organization) to assess the organization's knowledge-related and knowledge-management-related risks, and secondly, that the risk ratings derived by this method can be convincingly transformed to financial values that will be sensible to managers. We evaluate the results obtained using the approach by asking whether it allows the assessment of knowledge-related risks, knowledge-management-related risks, and the costs that individual risks potentially hold.

Literature Review

A number of knowledge management thinkers believed that it is impossible to develop direct, meaningful measures of knowledge assets, but the new paradigm allows managers to view knowledge as an asset that can be observed, measured, and managed (Housel & Bell, 2001). They also stated that without knowledge metrics, knowledge will be hoarded by organizations as a scarce resource. Schiuma (2009) wrote that a key challenge for both researchers and practitioners is to understand how to measure and manage knowledge assets dynamics. He suggested three processes for knowledge assets: identification, knowledge assets mapping and knowledge assets flow. Liebowitz (2016) mentioned that a number of organizations have approached knowledge management metrics from Balanced Scorecard, Intellectual Capital, Activity-Based Costing, or other borrowed approaches from the accounting and human resources disciplines. Liebowitz (2016) analyzed over 80 publications on knowledge management metrics, whereby metrics can be divided into system measures, output measures and outcome measures.

Risk assessment is the process of establishing both the likelihood and potential impact of various risks (Noraini, Bokolo jnr, Rozi, & Masrah, 2015). Risk assessment processes enable organizations to manage their risks by identifying, categorizing, and prioritizing these risks. Whilst risk management usually concerns insurable physical assets, there are several papers describing the risk of knowledge loss in organizations, for instance Aggestam et al. (2010), Martins and Martins (2011), as well as Shumaker, Ward, Petter, and Riley (2017). More narrowly focused research includes Agudelo-Serna, Bosuea, Ahmed, and Maynard (2018), who considered ways to mitigate knowledge leakage by mobile devices. Aubert et al. (2011) presented measures of risk exposure for knowledge management systems use. Alhawari, Karadsheh, Nehari Talet, and Mansour (2012) explored a possible convergence between the field of risk management and that of knowledge management by proposing an integrated knowledge management process that includes risk management, and recommending a framework for knowledge and risk management in Information Technology (IT) projects. Mi (2014) argued for the importance of and called for more research on knowledge management risk identification and evaluation. He argued that the comprehensive risk evaluation of an organization's knowledge management helps organizations to understand their own knowledge management status quo and makes targeted measures to effectively reduce the possible risks. Yang and Gao (2016) suggested five risk domains of knowledge management: human factor risk, information risk, organization risk, technology risk, and market risk. Thalmann, Ilvonen, Manhart, and Sillaber (2016) emphasized knowledge protection and specifically how to protect explicit and tacit knowledge.

In contrast to these considerations of knowledge-related risks, there are several papers describing ways in which knowledge management can help manage risks in organizations. Alhawari et al. (2012) wrote that knowledge management can have a significant influence on organizational risk mitigation. Massingham (2010) demonstrated how knowledge management constructs could offer managers deeper insight into the real nature of organizational risks. Cheng and Kung (2017) presented issues related to knowledge management at patent infringement risks. Joubert and Van Belle (2017) outlined the requirements for an organizing framework to support innovation and reduce innovation-related risks.

Whilst there are several papers regarding knowledge-related risk assessment, as well as approaches for considering knowledge management system risk and proposals for using knowledge management to mitigate risk in general, an integrated way of dealing with these matters is still lacking.

We have already taken some steps toward a more comprehensive assessment with previous research. Delak, Majewski, and Damij (2014) researched the measurement of knowledge and knowledge management in organizations and described evaluation by way of the framework for information system due diligence informed by the Control Objectives for Information and Related Technology (COBIT) 5 methodology. Following on this paper, Delak and Damij (2015) continued to explore possible approaches for evaluating knowledge management with a detailed COBIT 5 questionnaire. However, it soon became clear that further development in this direction causes an overly complex and inefficient collection of data for knowledge risk assessment, and as a result we abandoned that approach. It became clear that we needed to consider options beyond the ordinary paradigms and develop another approach to measure knowledge-related and knowledge management risks.

In this paper, we want to address both knowledge-related risks and knowledge management risks in a single assessment that also communicates the risk magnitude in financial terms to make it easily appreciable by management. The basis for this is a small research project that we set up at the Faculty of Information Studies in Slovenia on the assessment of knowledge-related and knowledge management risks based on and aligned with the international standard organizational risk management assessment. The working title for this project is MARJETKA, which stands for Measurable Approach for Risk Justification of Explicit and Tacit Knowledge Assessment.

Research Design and Methodology

The MARJETKA approach comprises several phases: generating the knowledge and knowledge management risk ratings, analysing the risk ratings, evaluating the risks, converting the risks to financial values and selecting risk mitigation actions. In order to demonstrate that our proposed approach can successfully assess knowledge-related risks and knowledge-management-related risks and that these can be plausibly converted to financial cost representations, the approach is applied to a variety of organizations as case studies. Below, the proposed approach, the calculation procedure for the risk values, and the method for converting risk values to financial value are explained. Then, the results achieved by the MARJETKA approach are illustrated more concretely in two of the organizations where the approached were implemented. Specifically, two sufficiently different organizations were selected to demonstrate the wide applicability of the MARJETKA approach.

The Proposed Approach

A questionnaire was administered to organizational representatives from 10 widely different organizations and their responses were further analyzed by an analyst from the MARJETKA project team and captured in a spreadsheet. The questionnaire was designed to elicit information about various knowledge-related and knowledge management threats. The first part of the

questionnaire consists of 15 questions from the APQC KM basic questionnaire (www.apqc.org), four questions identifying the types of knowledge (strategic, organizational, professional, or personal), and three questions regarding risk assessments currently performed in the organization. For this part of the questionnaire, respondents could answer with yes, partially, somewhat, and no (yielding a four-point scale, where yes is 4 and no is 1). This part of the questionnaire aims to establish the knowledge management maturity of the organization and is not an essential part of the MARJETKA approach, which relies more on the data from the second part of the questionnaire.

Knowledge-related and Knowledge Management Risk Ratings

The second part of the questionnaire concerns knowledge-related and knowledge-management-related threats in nine knowledge-related activities that cover all the phases of the knowledge life cycle. The nine activities are: knowledge creation, knowledge identification, knowledge capture, knowledge evaluation or validation, knowledge sharing, knowledge application or use, knowledge retention, knowledge obsolescence, and knowledge archiving. Each of these knowledge activities contains a battery of five to seven threats for a total of 50 potential threats (see Appendix A) to aspects of knowledge and knowledge management.

Respondents were first asked to rate each potential threat in terms of the seriousness of its consequences or vulnerability using a scale where 1 is low, 2 is medium, 3 is high, and 4 is very high; thereafter, respondents had to rate the frequency or likelihood of each threat occurring on a scale where 1 denotes less that once in three years, 2 once in three years, 3 yearly, 4 monthly, 5 weekly, and 6 denotes daily occurrences. This assessment method follows the risk assessment practices in the information security domain as per ISO (2012).

Analyzing the Ratings – Risk Evaluation

The level of knowledge-related risk is calculated in a risk matrix (see Table 1) as per the accepted best practice for risk assessment in information security management systems (ISO, 2012). In this matrix, the extent of a risk is expressed as a combination of vulnerability and its likelihood (ISO, 2012).

Table 1. The Risk Matrix

Likelihood / Vulnerability	Low	Medium	High	Very high
Less than once in three years	1	2	3	4
Once in three years	2	4	6	8
Once per year	3	6	9	12
Monthly	4	8	12	16
Weekly	5	10	15	20
Daily	6	12	18	24

Following the method used in the information security domain, we defined four risk levels with associated ratings: low (from 1 to 5), medium (from 6 to 11), high (from 12 to 17) and very high (from 18 to 24).

The MARJETKA project team followed Yang and Gao (2016), but reduced their five risk domains for knowledge management to focus on three risk areas: human-, organizational- or management-, and technical risk. This was achieved by conflating Yang and Gao's market- and organization risk as organization risk, and by combining technological- and information risk as technical risk. In total, the MARJETKA approach considers 24 potential risks (see Appendix B), of which nine are human risks, ten are organizational or management risks, and five are technical risks. These risk domains are similar to the domains of confidentiality, integrity and availability of information in the information security management system (ISO, 2013).

For each of the 24 risks, the MARJETKA project team defined up to 15 threats to a specific project from the knowledge life cycle threats list, allowing for the possibility that threats in one knowledge life cycle activity might also appear in other risk domains. In a pilot test of the MARJETKA approach, the analysis attempted to consider all 50 possible threats. There were however practical and analytical problems with this approach. Firstly, not all threats are equally important or present. Secondly, when considering all threats instead of the subset of the most important threats, it is more difficult to detect differences between companies. For this reason, the project team decided to consider the most important threats for up to two thirds of the total conceivable threats. Considering up to 15 threats for each of the 24 risks differentiates better between companies and still ensures that no important threats are neglected.

When implementing the MARJETKA approach, an analyst completes a scoreboard for assessing the threats collected from organizational representatives with the questionnaire. The analysis consists of relating the 50 threats in terms of their vulnerability and likelihood to the various risk groups. To do this, the scores of vulnerability and likelihood are multiplied to yield a risk rating (as per Table 1). Since the scale for vulnerability is from 1 to 4 and the scale for likelihood is from 1 to 6, on the risk matrix, low vulnerability and rare likelihood scores 1x1=1 and very high vulnerability and daily likelihood scores 4x6=24.

The analyst, who is a member of MARJETKA project team, then utilizes the data from the questionnaire to fill out a spreadsheet by inserting the risk rating values for the chosen threats from the knowledge life cycle threats list in the rows for each of the 24 risks. The sum of all threats for a particular risk is indicated by counting the instances for a risk value. This value is used to determine the threshold values for low, medium, high, and very high risk for the particular risk, which are then indicated in the same row as the risk on the spreadsheet. The threshold value for low risk is seen as the same as the sum of all threats and the threshold value for very high risk is treated as the sum of all threats multiplied by the number of risks considered (i.e. 24). The thresholds for medium and high risk are obtained by dividing the difference between the values for low and high into four equal portions. For example, if the sum of all threats for a risk is 3, then the threshold for low risk would be 3 and for very high risk it would be 72 (3 threats multiplied by 24 risks). Since the difference between 72 and 3 is 69, the intervals will be 17.25. This means that low risk is between 3 and 20.25; medium risk between 20.25 and 37.5; high risk between 37.5 and 54.75; and very high risk between 54.75 and 72.

The total risk value of a particular risk is calculated by adding up the risk ratings of the various threats in each row. This can then be compared to the threshold values to determine whether that particular score should be considered low, medium, high, or very high risk. Similarly, the total

risk exposure value for the organization across all 24 risks is the sum of the calculated totals in the total risk value column.

The analyst completes this scoring process for each of the 24 risks and marks low risk values in yellow, medium risk values in orange, high risk values in red, and very high risk values in dark red. This way of representing the data on the spreadsheet makes it possible to get an impression of the significance of the total risk scores at a glance. It is also possible to read the highest individual values off this column and so identify the particular high or very high risks and the risk group encompassing them.

Financial Knowledge Risk Evaluation

The MARJETKA approach does not only aim to represent risk values, but aims to express these risks in financial terms. Owners, shareholders, and top management seem to understand risk much better when it is expressed in financial figures, rather than as a numeric rating derived from the overall risk assessment. Such a transformation of risk ratings to financial figures is at best an approximation. The question is how to arrive at an approximation that will be sensible and plausible for management and practitioners whilst improving their ability to grasp the significance of knowledge-related and knowledge management risks. Whilst the risk ratings arrived at using the risk matrix can be considered valid and accurate in terms of that well-established method, the question as to what the raw risk rating number should mean to managers cannot have an absolute answer; to be useful in practice, what is needed is a financial approximation that is in principle defensible and meaningful to management.

In Slovenia and the European Union in general, organizations are categorized into four different sizes: micro enterprises, small enterprises, medium enterprises, and large enterprises. Table 2 presents the characteristics of organizational sizes.

Table 2. The Characteristics of Organizational Sizes

Size	Number of employees	The net sales revenues do not exceed EUR	The value of assets does not exceed EUR
Micro	Up to 10	700,000	350,000
Small	Up to 50	8,000,000	4,000,000
Medium	Up to 250	40,000,000	20,000,000
Large	More than 250	> 40,000,000	> 20,000,000

To achieve a plausible approximation of risk assessment in financial terms, one of the biggest Slovenian public companies was selected as a benchmark organization. In this company's annual report, their financial thresholds for low, medium, high, and very high risk were declared (as shown in Table 3). These values represent their self-assessment of risks and their chosen insured levels (which is a common approach to managing risks in organizations).

Table 3. The Financial Figures of the Risk Limits Characteristic of the Organization

Annual net income in EUR	Low risk level in EUR	Medium risk level in EUR	High risk level in EUR	Very high risk level in EUR
372,161,638.00	100,000.00	1,000,000.00	10,00,000.00	50,000,000.00

In particular, they reported that for insurance purposes, they considered risks of up to 100,000 Euro to be low risk, up to 1,000,000 Euro to be medium risk, up to 10,000,000 Euro to be high risk, and up to 50,000,000 Euro to be very high risk. In addition, this company posted an annual net income of 372,161,638 Euro.

Using these figures as a guideline, the analyst then calculates the financial value of each risk as assessed as well as the total financial exposure of the organization to knowledge-related and knowledge management risks. Equivalent financial values for each risk level can be calculated for each of the case organizations by comparing the net income (in the case of the eight private companies) or budget (in the case of the two public organizations) to the net income of the benchmark organization.

The resultant equivalent financial values were used in the transformation of the risk scores to a total risk exposure in financial terms. The total risk exposure is calculated by multiplying the number of risks per risk level with the equivalent financial values for each risk level. For instance, the number of medium risk assessments is multiplied with the equivalent medium risk financial value of the case organization in question, and this process is repeated for each risk level. Added together, the maximum total risk exposure of the organization can thus be expressed in financial terms. Similarly, the highest single risk can be expressed as a financial figure too.

Risk Mitigation

The final step in the MARJETKA approach is to identify measures to mitigate the identified risks. Our approach has a prepared list of risk mitigation activities. The analyst, alone or in consultation with the process or business owner, has to choose for every risk, or at the very least for the risks evaluated as high or very high, an appropriate risk mitigation activity from the list. In the end, the analyst prepares a written report for stakeholders and presents it to top management.

Case Studies

The proposed approach was used for knowledge-related risk assessment in 10 Slovenian organizations between July 2017 and August 2018. We can treat these organizations as case studies to help demonstrate the successful application of the MARJETKA approach in a wide variety of organizations as a key step toward its validation. The summarized results from all case studies can be seen below in Table 4. For all of these cases, the analyst followed the procedure described earlier to determine up to 15 threats related to the 24 risks in the three knowledge-related risk domains and used a scoreboard in a spreadsheet set up as described. The summarized results seen in Table 4 are the result of this process. However, to illustrate the process in more detail in the space available, we selected the first and the ninth cases to discuss how these results were obtained by applying the MARJETKA approach. These two cases were chosen because they present two very different contexts, the one being a micro organization in manufacturing and the other being a medium-sized municipality. Furthermore, showing that useful results can be derived in both organizations indicates the generic virtues of the approach.

Table 4. Summarized Results from the 10 Slovenian Case Studies

No.	Organization	Size	KM Risk Level	Highest Single Risk	KM Total Risk Financial Exposure	Highest Single Financial Knowledge Risk Exposure	No. of Risk Mitigation Recommendations
1	Car sales	Micro	Low	Medium	387,600 €	34,000 €	4
2	Retail	Small	Low	Low	510,782 €	17,373 €	5
3	Manufacturing	Large	Low	Medium	10,413,752 €	3,155,682 €	6
4	Locksmiths	Small	Medium	Medium	59,944 €	2,700 €	4
5	Transport	Small	Medium	Medium	99,753 €	4,889 €	4
6	Pharmaceutical	Large	Low	Low	7,573,638 €	315,568 €	3
7	Tourism	Large	Medium	Medium	1,595,744 €	78,222 €	4
8	Production	Large	Medium	Medium	1,694,804 €	412,316 €	5
9	Municipality	Medium	High	High	1,368,327 €	97,044 €	8
10	State administration	Medium	Medium	High	38,994 €	9,284 €	3

Case Study - A

We take as our first case study a car sales organization (also the first case in Table 4), with eight employees (in other words a micro organization in the private sector). The initial phase consisted of gathering the knowledge-related and knowledge management ratings. Here, the respondents to the questionnaire from the organization assessed all threats with an individual vulnerability or consequence assessment and an appearance or likelihood assessment. Table 5 presents the highest figures for this organization.

Table 5. The Highest Figures for Threat Assessment for Case Study A

Knowledge life cycle	Threat	Vulnerability /consequence	Appearance /likelihood
Create / Invent	Knowledge does not spread throughout the organization	3	5
Identify / Contribute or define	Tacit knowledge is not identified	4	4
Collect / Capture or Organize	Loss of already acquired knowledge	4	4
	A poor overview of company knowledge	4	4
Use / Transfer, Reuse, Adapt or Adopt	Old knowledge is used	3	5

The analyst inserted the assessed threat marks from the completed questionnaire in a spreadsheet so that the numeric risk rating is shown for each risk as well as for the total knowledge-related and knowledge management risk exposure. Table 6 presents the highest risks determined by this method.

Table 6. The Highest Figures for Risk Assessment for Case Study A

Risk domain	Risk	Numerical value
Human risks	1.2 inadequate transfer of knowledge at the time of departure or replacement of the post	74
	1.3 Inadequate knowledge management by the manager / owner of the process	86
	1.6 Quality of knowledge is not properly assessed	97
Organizational/ management risks	2.1 Inadequate acquisition / development strategy	108

The total risk exposure of case study A was 1,098, which means that the total risk exposure of knowledge-related and knowledge management matters for case study A was at a low level.

The next step was to convert the calculated numeric value of the risk into financial values. The financial risk values in Table 3 should be adjusted with the correction factor to the ratio between the net annual income of the company for which we published the financial risk values in Table 3 and the annual net income of the company that is case study A, as shown in Table 7.

Table 7. Calculate Financial Risk Values for Company A

Annual net income in EUR	Low risk level in EUR	Medium risk level in EUR	High risk level in EUR	Very high risk level in EUR
12,652,581.00	3,400.00	34,000.00	340,000.00	1,700,000.00

Given this re-calculation, the total risk exposure for knowledge-related and knowledge management risks for case study A was 387,600.00 EUR. This figure was arrived at as per the scoring method explained earlier: of the 24 risks, 14 fell in the low risk category and 10 in the medium risk category. Since for this organization, the low risk level is valued at 3,400.00 EUR and medium risk at 34,000.00 EUR, these amounts were multiplied by 14 and 10, respectively, before being added together for the total risk exposure value.

The last step in our approach is the selection of risk mitigation measures for the risks assessed as at a high and very high level of risk. From the list of risk mitigation measures, 11 were identified as appropriate, with the understanding that the specific implementation of each mitigation measure depends on the size and management of the particular organization. For the company in case study A, the following mitigation measures were deemed appropriate:

- M2 Establishing a knowledge base,
- M7 Changing the company's culture by rewarding knowledge sharing and encouraging mentoring,
- M10 System maintenance: backup and security,
- M11 Providing support in the company's management.

Case Study - B

As our second case study, we discuss the risk assessment at a state administration organization, specifically a Slovenian municipality (the ninth case in Table 4). The municipality has 55 employees (in other words, it is a medium-sized organization in the public sector). In the initial phase of gathering the knowledge-related and knowledge management risk ratings, respondents

to the questionnaire assessed all threats with individual vulnerability or consequence assessment and appearance or likelihood assessment. Table 8 presents the highest figures in case study B.

Table 8. The Highest Figures for Threat Assessment for Case Study B

Knowledge life cycle	Threat	Vulnerability /consequence	Appearance /likelihood
Create / Invent Collaborate or publish	Workers do not accept new knowledge	4	5
Identify / Contribute or define	Management does not recognize the knowledge that individuals have	4	4
Collect / Capture or Organize	A poor overview of company knowledge	3	6
Use / Transfer, Reuse, Adapt or Adopt	Old knowledge is used	3	6
Keep / Retention	Tacit knowledge is stored in the minds of coworkers	3	5
Obsolete	New knowledge is lost / forgotten	4	4

The analyst captured the assessed threat values from the completed questionnaire in a spreadsheet so that the numeric risk rating is shown for each risk as well as for total knowledge-related and knowledge management risk exposure. Table 9 presents the highest risks captured by this method.

Table 9. The Highest Figures for Risk Assessment for Case Study B

Risk domain	Risk	Numerical value
Human risks	1.5 There is no readiness to transfer knowledge	91
	1.7 Improper trust in the knowledge management system	49
	1.8 Inadequate education	190
	1.9 Inappropriate processes of cooperation in knowledge transfer	47
Organizational / management risks	2.1 Inadequate knowledge acquisition / development strategy	206
	2.2 Inadequately defined knowledge management processes	74
	2.3 Inappropriate competences	40
	2.8 Inadequately organized knowledge transfer	76
	2.9 Unsuitable taxonomies	78
	2.10 Unsuitable user support	105
Technical risks	3.1 The failure of an information system on documented knowledge	73
	3.5 Lack of tools for knowledge searching	75

The total risk exposure of case study B was 2,135, which means that the total risk exposure for knowledge-related and knowledge management risks for case study B was at a high level. Since municipalities do not have profits, annual net revenue cannot be used as an anchor from which to derive financial values. Therefore, instead of annual net revenues, the municipal budget for 2018 was taken as the anchor value for the correction factor on the financial risk values in Table 3.

Using this approach, the calculated values of financial risk for the observed company in case study B are shown in Table 10.

Table 10. Calculate Financial Risk Values for Company B

Annual net income in EUR / Municipality budget	Low risk level in EUR	Medium risk level in EUR	High risk level in EUR	Very high risk level in EUR
3,611,624.00	970.00	9,704.00	97,044.00	485,222.00

The total risk exposure for knowledge-related and knowledge management risks for Company B was 1,368,327.00 EUR. This is because of the 24 risks, 11 were medium risks and 13 were high risks, and for this organization, the medium risk level is valued at 9,704.00 EUR and the high risk level at 97,044.00 EUR. These amounts were multiplied by 11 and 13, respectively, before being added together.

The last step in our approach is the selection of risk mitigation measures for all the risks assessed to be at a high or very high level of risk. For case study B, the following mitigation measures were deemed appropriate:

- M1 Time to relax within working hours,
- M2 Establishing a knowledge base,
- M4 Team building, establishing a social environment outside the scope of the service;
- M6 Transfer of knowledge at departure from the company: delivering at departure;
- M7 Changing the company's culture by rewarding knowledge sharing and encouraging mentoring,
- M9 Introducing a coworker into work in case of departure to another post in the company;
- M10 System maintenance: backup and security,
- M11 Providing support in the company's management.

Results

The case studies have shown that the MARJETKA approach can be used in diverse organizations to yield risk assessments of knowledge-related and knowledge management aspects of the organization. Furthermore, the organizational risk exposure can be presented in financial figures by a re-calculation of the insured risk values of a large organization for various risk levels in a way that adjusts these for smaller organizations (that typically do not undertake such detailed risk insurance steps). Although the case study organizations were relatively small in size, they are representative of the majority of Slovenian organizations, and the 10 case studies cover various sizes and different types of organizations. As for the entire research project, of all 10 case studies, it was found that the most regulated and controlled company—a pharmaceutics organization—had low risk exposure, also for knowledge-related and knowledge management risks that fell outside of its compliance duty. Another result was that small- and medium-sized companies are subject to bigger issues regarding knowledge-related and knowledge management risks. Our findings from the 10 case studies confirm Mi (2016)'s argument that accurate risk evaluation improves organizations' understanding of their own knowledge management status. We could add that the MARJETKA approach can diagnose deficient knowledge management

practices by uncovering the extent of knowledge-related and knowledge management risk exposure. Effective risk management makes it easier to cope with problems and ensures that these do not lead to disaster through identifying, controlling, and minimizing the impact of threats (Noriani, 2015). The MARJETKA approach tries to assess and address knowledge-related risks and knowledge management risks in a way analogous to current good practice regarding information technology risks.

Conclusion

The aim of our research was to set up and validate a risk assessment approach for organizations from the perspective of the knowledge life cycle and the knowledge management system. The MARJETKA approach assesses risks related to explicit and tacit knowledge within the organization. Some limitations of the present research should also be noted. First, the case studies were limited to only 10 cases. Second, the selected case studies were concentrated in one country (Slovenia). Third, the initial risk rating is based on the subjective identification of knowledge threats and risks. Whilst these ratings are subjective, they probably represent the boundaries of this type or research. Although the MARJETKA approach was thus far only tried in 10 case studies, we demonstrated with a detailed discussion of two of those cases that it can be applied to, and is useful for, organizations of different sizes and types, whether commercial or in the public sector and therefor not-for-profit.

With the results of the case studies, we can confirm that the MARJETKA approach allows the assessment of knowledge-related and knowledge-management-related risks in an integrated and simple instrument. The case studies also confirm that risk can be re-calculated and presented as financial values, which are likely to be well understood and accepted by management and shareholders. The financial values, specifically for the total knowledge management risk financial exposure, raised awareness among management and shareholders. Due to the described limitations, we are not confident in generalizing our evaluation of MARJETKA approach, but we indicate a way for any organization to assess its knowledge-related and knowledge-management-related risks and present the results in financial terms.

Our findings can be the basis for further research on how to best represent risk values to management and practitioners and for further refinement of the MARJETKA approach. A limitation of the approach is that, whilst various mitigation strategies are suggested, the costs associated with mitigation are not factored into the calculation. Further development and improvement will integrate the cost of mitigation into this approach. In particular, further research is needed to validate the approach by applying it in a wider range of organizations internationally and by asking managers whether the financial representations of risk value resonate with them. Later, we plan to prepare this novel version of risk assessment for international validation by including cases from other countries and cultural contexts.

Calder (2005) wrote that information security is a journey, not a destination, and we can paraphrase him by saying that the activities aimed at knowledge-related and knowledge management risk assessment are ongoing undertakings and not a once-off project. The MARJETKA approach provides one avenue for furthering this journey.

Acknowledgement

We would like to thank the Faculty of Information Studies, Novo mesto, Slovenia, for supporting us with this study. We would also like to thank the OJAKM reviewers who gave us comments and suggestions for improving this paper.

References

Aggestam, L., Söderström, E., & Persson, A. (2010). Seven types of knowledge loss in the knowledge capture process. *ECIS 2010 Proceedings*, Paper 13.

Agudelo-Serna, C. A., Bosuea, R., Ahmed, A., & Maynard, S. B. (2018). Towards a knowledge leakage mitigation framework for mobile devices in knowledge-intensive organization. *Proceedings of the 26th European Conference on Information Systems*, Portsmouth, UK, pp. 1-21. *Retreived from: http://ecis2018.eu/wp-content/uploads/2018/09/1426-doc.pdf*

Alhawari, S., Karadsheh, L., Nehari Talet, A., & Mansour, E. (2012). Knowledge-based risk management framework for information technology project. *International Journal of Information Management, 32*(1), 50-65.

APQC. *Knowledge Management Self Assessment Survey*. American Productivity & Quality Center. Retrieved from: https://surveys2.apqc.org/ViewsFlash/servlet/viewsflash?cmd=page&pollid=Advisory%21KM_Mini_Assess

Aubert, B., Bernard, J.-G., & Caro-Gonzalez, C. – G. (2011). Defining knowledge management system risk. *Proceedings of the* 15th *Pacific Asia Conference on Information Systems*. Paper 21.

Babik, D., Qian, R., Singh, R., & Ford, E. W. (2014). Examining Intersubjectivity in social knowledge artifacts. *Proceedings of the 20thAmericas Conference on Information Systems, Savannah, USA*, pp. 1-9.

Calder, A. (2005). *A business guide to information security – how to protect your company's assets, reduce risks and understand the law*. London, UK: Kogan Page Limited

Cheng, C-Y., & Kung, L-C. (2017). Quantifying the risk of innovation: A patent knowledge management approach. *Proceedings of the* 21st *Pacific Asia Conference on Information Systems.* Paper 91.

Chou, S. (2005) Knowledge creation: absorptive capacity, organizational mechanisms, and knowledge storage/retrieval capabilities. *Journal of Information Science, 31*(6), 453-465.

Delak, B., Majewski, G. M., & Damij, N. (2014). How to identify knowledge and evaluate knowledge management in organization – case studies report. *Online Journal of Applied Knowledge Management, 2*(2), 162-171.

Delak, B., & Damij, N. (2015). Knowledge risk assessment. *Proceedings of the 16th European Conference on Knowledge Management, Udine, Italy*, pp. 998-1004.

Drucker, P. F. (1999) Knowledge-worker productivity: The biggest challenge. *California Management Review, 41*(2), 79-94.

Housel, T. J., & Bell, A. H. (2001). *Measuring and managing knowledge*. New York, NY: McGraw-Hill Higher Education.

ISO. (2009). Guide 73 – *risk management – vocabulary*. International Standard Organization, Geneve, Switzerland.

ISO. (2012). *ISO/IEC 27000 – information technology – security techniques – information security management systems – overview and vocabulary*. International Standard Organization, Geneve, Switzerland.

ISO. (2013). *ISO/IEC 27001 – information technology – security techniques – information security management systems – requirements*. International Standard Organization, Geneve, Switzerland.

Joubert, J., & Van Belle, J-P. (2017). An integrated innovation and risk management framework for the ICT industry. *Proceedings of the 23rd Americas Conference on Information Systems, Paper 3.*

Liebowitz, J. (2016). *Successes and failures of knowledge management: An investigation into knowledge management metrics*. *Proceedings of the 3rd International Conference on Nuclear Knowledge Management – Challenges and Approaches*, Vienna, Austria, Paper 241.

Martins, E. C., & Martins, N. (2011). The role of organizational factors in combating tacit knowledge loss in organizations. *Southern African Business Review, 15*(1), 49-69.

Massingham, P. (2010). Knowledge risk management: A Framework. *Journal of Knowledge Management, 14*(3), 464-485.

Mi, J. (2014). The evaluation of comprehensive risks for enterprise knowledge management by theory of matter-element model and extension set. *Journal of Chemical and Pharmaceutical Research, 6*(4), 202-209.

Nonaka, I., & Takeuchi, H. (1995) *The knowledge-creating company*. New York, NY: Oxford University Press.

Noraini, C. P., Bokolo jnr, A., Rozi, N. H., & Masrah, A. A. M. (2015). Risk assessment of IT governance: A systematic literature review. *Journal of Theoretical & Applied Information Technology*, *71*(2), 184-193.

Ragab, M. A. F., & Arisha, A. (2013). Knowledge management and measurement: A critical review. *Journal of Knowledge Management*, *17*(6), 873-901.

Schiuma, G. (2009). The managerial foundations of knowledge assets dynamics. *Knowledge Management Research & Practice*, *7*(4), 290-299.

Shumaker, J., Ward, K., Petter, S., & Riley, J. (2017). Mitigating the threat of lost knowledge within information technology departments. *Proceedings of the 50th Hawaii International Conference on system Sciences, Big Island, Hawaii*, pp. 5440-5449.

Thalmann, S., Ilvonen, I., Manhart, M., & Sillaber, C. (2016). Knowledge protection for digital innovations: integrating six perspectives. *Proceedings of the 7th Workshop on Information Security and Privacy, Dublin,* Ireland, Paper 15.

Tiwana, A., & Keil, M. (2005). The one-minute risk assessment tool. *Communications of the ACM, 47*(11), 73-77.

Yang, G., & Gao, H. (2016). Uncertain risk assessment of knowledge management: based on set pair analysis. *Scientific Programming, 2016*, *1-9*. https://doi.org/10.1155/2016/2025892.

Authors Biographies

Boštjan Delak, Ph.D. CISA, CIS, is auditor at the Republic Slovenia Court of Audit, Ljubljana, Slovenia. He is a certified information system auditor and certified information security manager, he is also assistant professor at the Faculty of Information Studies – Novo mesto, Slovenia. He is lecturing: IS auditing and Fundamentals of Information Security. His research interests are: IS due diligence, IS analysis and Knowledge management.

Christiaan Maasdorp, Ph.D. is a lecturer in the Department of Information Science at Stellenbosch University and directs two postgraduate study programs that draws students from across Southern Africa, namely the Postgraduate Diploma in Knowledge and Information Systems Management and the Masters in Information and Knowledge Management. He lectures knowledge management and organization theory in these programs.

Appendix A – List of All Threats

Knowledge activities	Threats
Knowledge creation (Create / Invent)	Knowledge does not spread throughout the organization
	Knowledge is not used in new processes (technologies) and products
	Creating Knowledge with Incorrect / Unintentional Content
	Management does not have the necessary experience to create knowledge
	Employees do not accept new knowledge
Knowledge identification (Identify / Contribute or Define)	Management does not recognize the knowledge that individuals have
	An individual is unaware of the usefulness of his or her knowledge
	An individual does not recognize the usefulness of others' knowledge
	Management does not know where all the knowledge is
	Tacit knowledge is not identified as a company's knowledge
	Management does not recognize the knowledge necessary for the implementation of a particular process (competence)
Knowledge capture (Collect / Captture or Organize	Loss of already acquired knowledge
	Keep old unusable knowledge
	Incorrect accumulation of knowledge from external sources
	The presence of tacit knowledge
	A poor overview of company knowledge
Knowledge evaluation or validation (Evaluate, Validate or Analyze)	A poor overview of company knowledge
	Management does not have the knowledge to carry out the necessary activities for assessing knowledge
	Wrong classification of knowledge
	Wrong analysis and assessment of knowledge
	Management does not recognize the knowledge that individuals have
	Management does not know where all the knowledge is
	There is no awareness of the classification of knowledge by superiors and management
Knowledge sharing (Collaborate or publish)	The presence of tacit knowledge
	Individuals do not want to share knowledge
	Disabling direct contact with experts
	Knowledge does not spread throughout the organization
	Employees do not accept new knowledge
Knowledge application or use (Use / Transfer, Reuse, or Adapt or Adopt)	Old knowledge is used

	Employees do not have access to the knowledge they need and when they need it
	Management does not understand the concept of "re-use of knowledge"
	New knowledge is lost / forgotten
	Tacit knowledge is stored in the minds of minority of employees
Knowledge retention (Keep / Retention)	Inadequate storage of already acquired knowledge
	Poor protection of stored knowledge
	Inadequate structure of stored knowledge
	Undefined properties of individual types of knowledge (importance, usability, speed of content changes...)
	Tacit knowledge is stored in the minds of minority of employees
	The recorded knowledge is not protected properly (backup and archiving of knowledge)
Knowledge obsolescence (Obsolete)	Management does not recognize obsolete knowledge
	Current knowledge due to non-use become out of date
	Knowledge is not renewed
	Management does not understand the concept of "re-use of knowledge"
	New knowledge is lost / forgotten
	Obsolete knowledge is not archived properly
Knowledge archiving (Discard / Archive)	The knowledge base is still full of obsolete information and best practices that have worked in the past
	Old knowledge is discarded, it turns out that the new knowledge of the organization is not appropriate
	Undefined properties of individual types of knowledge (importance, usability, speed of content changes...)
	Management does not understand the concept of "re-use of knowledge"
	Management does not have the knowledge to carry out the necessary activities for assessing knowledge

Appendix B – List of All Risks

Risk domains	Risks
Human factor risks	Unauthorized access and modification
	Inadequate transfer of knowledge when leaving or replacing a post
	Inadequate knowledge management by the manager / owner of the process
	Leakage of information on project work and cooperation with suppliers
	There is no willingness to transfer knowledge
	Quality of knowledge is not properly evaluated
	Inadequate trust in the knowledge management system
	Inadequate education
	Inadequate process of cooperation in the transfer of knowledge
Organization/management risks	Inadequate acquisition / development strategy
	Inadequately defined knowledge management processes
	Inadequately defined competencies
	Inadequate assignment of authorizations
	Inadequate knowledge management by an authorized organizational unit
	Inadequate classification of knowledge / methods of measurement
	Inadequate protection of information on knowledge
	Inadequately organized knowledge transfer
	Untrusted taxonomy
	Unsuitable / inefficient user support
Technical risks	Failure of the information system of documented knowledge
	Lack of knowledge / knowledge for the continuity of information security protection
	Lack of appropriate knowledge management tools
	Lack of integration of information on knowledge
	Lack of tools for finding knowledge