9 July 2011

Defining Knowledge Management System Risk

Benoit A. Aubert
HEC Montreal, benoit.aubert@hec.ca

Jean-Gregoire Bernard
Victoria University of Wellington, jean-gregoire.bernard@vuw.ac.nz

Carlos Caro-Gonzalez
HEC Montreal, carlos.caro-gonzalez@hec.ca

ISBN: [978-1-86435-644-1]; Full paper

DEFINING KNOWLEDGE MANAGEMENT SYSTEM RISK

Aubert, Benoit A., HEC Montréal, Montréal, Canada, benoit.aubert@hec.ca

Bernard, Jean-Grégoire, Faculty of Commerce and Administration, Victoria University of Wellington, Wellington, New Zealand, jean-gregoire.bernard@vuw.ac.nz

Caro-Gonzales, Carlos, HEC Montréal (graduate student), Montréal, Canada, carlos.caro-gonzalez@hec.ca

Abstract

Knowledge Management Systems are becoming widely used in organizations. Early successes are encouraging but these systems entail their own set of challenges. This paper proposes a measure of risk exposure for knowledge management system use. Five undesirable outcomes and thirty two risk factors were identified. These elements were extracted from the literature and from cases, and validated using a Delphi exercise. This measure enables knowledge managers to assess the level of risk supported by their organization and to take the appropriate action to manage their risk exposure.

Keywords: Knowledge Management System, Risk, Risk factors

1 INTRODUCTION

Knowledge management systems (KMS) are becoming ubiquitous in organizations. Investments in KMS are growing (Logan, 2009) and a research firm has recently noted a resurgence of interest toward such systems (Mann, Rozwell, & Drakos, 2010). Many early success stories have contributed to legitimize and popularize the use of KMS in response to the organizational problems of codifying, storing, connecting, sharing, and re-using various forms of explicit knowledge. For instance, Xerox is said to have benefited from substantial savings in the 90s after it adopted a KMS to support the work of its technicians responsible for servicing the firm's customers (Brown & Duguid, 2000). Other early adopters include Kodak, Raytheon, and Royal Dutch/Shell, among others (Kontzer, 2002, 2003).

Yet, while the hype surrounding the expected outcomes of KMS has receded, the challenges tied to the adoption and use of KMS haven't disappeared. The scope of such projects has increased to encompass core knowledge-based processes in organizations and the diversity of the technologies available to design such systems has increased as well. Successfully reaping the benefits of KMS remains notoriously difficult and they often fail to deliver expected outcomes (Mann, 2010).

One of the key challenges associated with KMS lies in the difficulty in making such system relevant, useful and easy to use. It often requires that workers contribute content to the system although they may not be the ones who benefit from the outputs of the system. The short-term adoption of a KMS is often plagued by collective action dilemmas while their long-term usefulness is often dependent upon a critical mass of users adopting the system (Fulk, Heino, Flanagin, Monge, & Bar, 2004). Even if a KMS gets regular usage and contributions from its users, the quality of the content of a KMS might suffer depending on the social and task contexts in which it is embedded, such as pressures for accountability and the rate at which tasks change (Bernard, 2006), the existence of social capital (Wasko & Faraj, 2005), and the patterns of advice seeking behaviours within the adopting organization (Leonardi, 2007). Furthermore, post-adoption investments in resources to curate KMS content are often overlooked and dismissed despite the importance of such activity to keep the system current, fresh, and useful (Desouza & Awazu, 2005; Markus, 2001).

While many papers have looked at the risks associated with software implementation, KMS entail an additional set of risks. As already noted, the fact that a KM system is very dependent on continuous usage and enrichment of its content challenges its sustainability. Also, the pitfalls associated with the capture of knowledge in a system have to be considered. This paper contributes to the KMS literature by assessing the risk that is specific to these systems. The identification of such risk will facilitate its management. It will enable managers to foresee potential undesirable outcomes that may occur when using this type of system. A comprehensive list of risk factors will facilitate the identification and active management of potential threats to these systems. Finally, a risk measure will allow organizations to compare the risk they are taking with the expected returns of such initiatives.

The paper is organized as follows. First, the goals associated with the implementation of KMS are briefly reviewed. The following section presents the definition of the key risk concepts; undesirable outcomes, risk factors, and risk exposure. The third section outlines the methodology. It describes how the undesirable events, the risk factors, and the linkages between these elements were validated using cases and experts. Finally, a discussion highlights some interesting or unique aspects of the KMS risk measure.

2 KNOWLEDGE MANAGEMENT SYSTEMS

Knowledge management systems (KMS) are a class of information systems that aim (1) to promote the creation of new knowledge, (2) to capture knowledge in an explicit form, (3) to support and facilitate content management, (4) to share knowledge among occupational communities within and across organizations, and (5) to apply and re-use knowledge to generate value (Alavi & Leidner, 2001; Birkinshaw & Sheehan, 2002). KMS differ from in substantial ways from enterprise and business intelligence systems. They usually support unstructured and emergent work processes, for which unplanned and non-routinized interactions between workers are common, such as new product development, customer service, software programming, and artistic creation. They are also often used to collect and codify critical incidents and learning episodes in industries such as health care and aviation (Bernard, 2006).

Many technology features may be employed to design and assemble KMS (Gallupe, 2001). The following four types of features are commonly bundled together as packages sold by software vendors such as IBM Lotus, Microsoft, EMC, Atlassian and Open Text, among others.

- Unstructured databases and repositories, which provide document retrieval features, search engines, and intelligent agents to classify and categorize content (Kankanhalli, Tanudidjaja, Sutanto, & Tan, 2003; Markus, 2001; Tyrvainen, Paivarinta, Salminen, & Iivari, 2006);
- Expert profiling, social networking and directory features (Kankanhalli et al., 2003; Lindgren, Henfridsson, & Schultze, 2004; Markus, 2001; Skeels & Grudin, 2009);
- Real-time collaborative tools such as email, listserv, bulletin boards, instant messaging, and video conferencing (Kankanhalli et al., 2003);
- Web publishing, editing and filtering features, such as blogging, wikis, social tagging, podcasting, and micro-blogging features (Danis & Singer, 2008; Efimova & Grudin, 2007; Marlow, Naaman, boyd, & Davis, 2006; McAfee, 2006; Zhao & Rosson, 2009).

From these packages, organizations may adopt and configure selected features into specific KMS applications to support one or more objectives of a knowledge management initiative (Gallupe, 2001). For instance, specific KMS applications may be adopted to enable a project team to share content and knowledge internally, to accelerate the learning of novice workers, to provide ways for secondary knowledge miners to discover new applications to old knowledge (Markus, 2001), or to provide a window upon the current affairs of various organizational units to build cohesion and a sense of belonging among workers (Scheepers, 2003). While each of these KMS applications involve particular adoption and implementation challenges, they also share many common challenges (Markus, 2001). This is why this paper elaborates a measure of KMS risk which is generic enough to encompass all types of KMS applications.

3 A DEFINITION OF RISK EXPOSURE

For the purpose of this paper, we adopt a conceptualization of risk assessment that has been widely used in the IS literature. It has been empirically validated in contexts such as information systems development projects (Barki, Rivard, & Talbot, 1993), of information systems outsourcing contracts (Aubert, Patry, & Rivard, 2005), and enterprise systems projects (Bernard, Rivard, & Aubert, 2004), among others. KMS are risky endeavors which can be costly for organizations and their stakeholders. Risk management has been found useful to fulfill to the need to proactively discern and act upon project failure threats (Du, Keil, Mathiassen, Shen, & Tiwana, 2007). Research has also showed that the success of information systems development projects is significantly influenced by the fit between the types of management practices enacted and the level of risk the projects (Barki, Rivard, & Talbot, 2001). From a practical standpoint, research has developed contingency frameworks which help managers select the most appropriate risk management method for their IS projects (Iversen, Mathiassen, & Nielsen, 2004).

Managing the risk of an activity involves two essential components: the assessment of risk exposure and the enactment of mitigation mechanisms. Boehm (1989) put forward a method to measure risk which is consistent with a definition of risk from a behavioral perspective. The behavioral perspective on risk departs from a classical conception of risk as the variance of the probability distribution of possible outcomes, which argues that managers will evaluate a trade-off between variations in performance and expected return (March & Shapira, 1987). Research about the cognitive processes of managers has shown that they are much more attentive to threats than opportunities (Jackson & Dutton, 1988) and that the meaning of risk is tied to negative outcomes, which are considered as dangers or hazards to avoid (March & Shapira, 1987). Instead of considering risk as a range of outcomes, managers consider risk as a threat of a very poor outcome.

To elaborate a measure of the risk associated with a KMS adoption and implementation project, we thus adopt the notion of risk exposure, which is defined as a function of the probability of an undesirable outcome and the importance of the loss due to the occurrence of this outcome:

$$\mathbf{RE = \Sigma_i\, P(UO_i) * L(UO_i)}$$

where $P(UO_i)$ is the probability of an undesirable outcome *i*, and $L(UO_i)$ the loss due to the undesirable outcome *i* (Barki et al., 1993, Aubert et al., 2005).. Figure 1 shows how risk exposure may be visualized by mapping each undesirable outcome according to its likelihood and the magnitude of the associated loss:

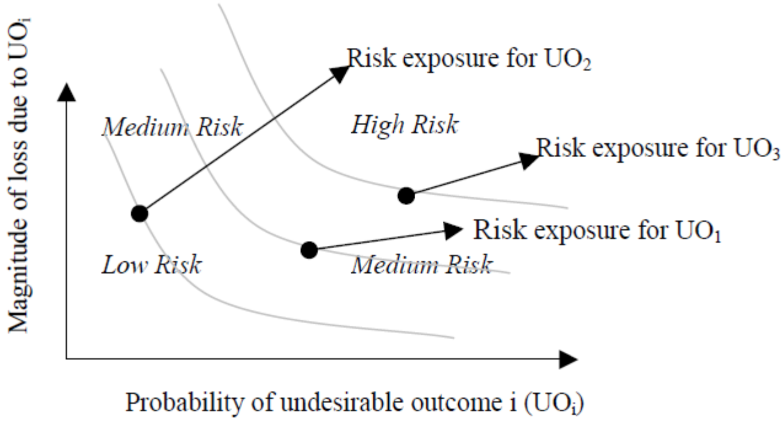

Figure 1. Risk Exposure Map (Adapted from Aubert et al. 2005)

To evaluate the risk exposure for a given KMS, it thus becomes crucial to identify and assess three components: (1) the range of undesirable outcomes that could occur; (2) the magnitude of the losses incurred should each of the undesirable outcomes materialize; and (3) the probability of the occurrence of such outcomes.

Undesirable outcomes consist of the failure to attain one or more of the KMS objectives and of threats to other aspects tied to the host organization's survival and health as well. The magnitude of loss due to a given undesirable outcome can be estimated either via quantitative analysis (e.g., by evaluating the sales lost due to disruption of service to customers) or via qualitative assessment of its organizational impact (e.g., by using Likert scales to assess its importance).

Our proposed method for assessing the probability of an undesirable outcome relies upon the identification and assessment of *risk factors*, which act as proxies for the probability of an undesirable outcome. Put simply, risk factors are objective attributes of a situation which have been empirically shown to be associated with the occurrence of an undesirable outcome within that given situation. This approach is similar to the one employed by physicians while assessing the risk of a disease for a patient. For instance, the probability of developing cardiovascular diseases is determined by the existence and level of specific risk factors which can be more or less amenable to control and mitigation: smoking habit, drinking habit, lack of physical exercise, poor dietary habits, genetic antecedents, etc. In an IS development context, Barki et al. (1993) identified five such factors to assess the probability of project failure: technological newness, application size, the IS development team's lack of expertise, application complexity, and organizational environment. Once identified and tied to undesirable outcomes, risk factors are usually qualitatively assessed by using Likert scales.

This indirect approach to the assessment of probabilities of undesirable outcomes is functional for three reasons. First, this approach palliates to the usual scarcity, if not complete absence, of historical data about project management events and outcomes from which the probability estimates of undesirable outcomes may be inferred. The use of expert judgments as proxies to estimate probabilities is justified in such context (Paté-Cornell, 1996). Second, behavioral research has shown that managers are generally uncomfortable with probability estimates. They thus tend to focus their attention much more on the magnitude of an undesirable outcome rather than on the probability of the undesirable outcome (March & Shapira, 1987). Third, risk factors are not only useful in providing substitutes for unreliable and doubtful probability estimations, but also in providing "cognitive repairs" (Heath, Larrick, & Klayman, 1998) which help managers to discern threat cues before they become relatively serious and precipitate an undesirable outcome. Managers draw a sharp distinction between taking risks and gambling, as taking risk is amenable to control while gambling is not. The continuous monitoring of risk factors as projects and operations unfold allows managers to enact targeted mitigation mechanisms from which they can "try to change the odds" (March & Shapira, 1987, p. 1410). Mitigation mechanisms may help to reduce the probability of undesirable outcomes by preventing their occurrence or they may tamper the magnitude of loss tied with undesirable outcomes (e.g., insurance). Managers commonly evaluate the enactment of a specific mitigation mechanism as a trade-off between the marginal reduction in risk exposure and the cost of the mitigation mechanism.

It is important to note that this paper will focus on the risk associated specifically with knowledge management systems. Any project implementing a KMS would face two subsets of undesirable outcomes. The first subset includes the risk associated with the IT project and the implementation of the technology. There is no reason to presume that KMS would be different from other technologies in that respect. Therefore, project risk, as defined by Barki et al. (2001) would have to be considered by a project manager implementing a KMS. However, there is also a second subset of undesirable outcomes to consider. This second subset includes the undesirable outcomes that are unique to KMS. These outcomes are directly related to the goals of KMS as applications and to the management of the knowledge. Using the definition of Bernard et al. (2004) stating that an undesirable outcome is a deviation from a goal, we can focus our analysis of the risk specific to KMS adoption and use.

4 METHODOLOGY

The first step to assess the risk associated with KMS is to identify the relevant variables underlying this type of risk. This provides content and face validity of the tool. Further steps would be to determine the actual items of the measures and assess their psychometric properties (convergent and discriminant validity, reliability, etc.).

In order to measure the risks associated with knowledge management systems, we have to ensure that all the components of this type of risk are covered, providing content validity. Content validity is the extent to which a measure reflects the intended domain of content (Carmines and Zeller, 1979). This means, following the definition of risk provided earlier, that the undesirable outcomes have been identified, that the relevant risk factors are known, and that the relationships between risk factors and undesirable outcomes have been mapped. Bernard, Rivard, and Aubert (2004) argue that a way to ensure that the content of measure is valid is to create it using content generated from the literature. After this first step was done, and in order to continue improving the validity of the measure, a validation using case studies was done and a Delphi exercise was conducted.

4.1 Literature Review

An review of the literature was conducted to identify (1) the expected outcomes tied to KMS projects, (2) the risk factors which might prevent the realization of these outcomes, and (3) the hypothesized or empirically validated linkages between risk factors and specific expected outcomes. The scope of the review was initially focused on identifying influential studies from top journals of the IS field (i.e. AIS basket of eight journals) following keyword searches and was subsequently broadened by conducting both backward and forward citation searches for relevant studies using both ISI Web of Science and Google Scholar (Webster & Watson, 2002). No restrictions on research methodologies were put and studies originating from neighbouring disciplines (e.g., organization studies, library science) were included when their main focus was on the conduct of KM projects through technological means.

Five undesirable outcomes of KMS adoption were singled out following the literature review: (1) the failure to promote the creation of new knowledge, (2) the failure to capture knowledge in an explicit form, (3) the failure to support and facilitate content management, (4) the failure to share knowledge among occupational communities within and across organizations, and (5) the failure to apply and reuse knowledge to generate value. This emphasis on KMS-specific objectives is coherent with calls to broaden project success measures beyond the classic triangle of budget, schedule, and quality outcomes (Atkinson, 1999). It also distinguishes KMS risk from generic IS project risk. It further suggests that previous research considers that the challenges associated with KMS projects reside in “getting it right” rather than “doing it right”.

A large number of relevant risk factors were also identified. Due to space limitations, the relevance of each factor is not discussed in detail in this paper. Table 1 at the end of this paper shows the list of factors which were identified from this literature review. It also indicates which risk factors are expected to influence each of the undesirable outcomes.

4.2 Historical Cases

In order to validate the undesirable consequences and the risk factors identified in the literature review, historical cases were examined. Historical cases provide a wealth of information (Bernard, Rivard, and Aubert, 2004) and enable the researcher to increase content validity (Miles & Huberman, 1994). The cases were extracted mainly from academic sources like Harvard Business School and Richard Ivey School of Business. Cases had to detail the use (or lack of it) of knowledge management systems. They could not be focusing solely on the implementation of the technology. The cases selected are: Ernst & Young, Buckman Laboratories, Montgomery Watson Harza, Hill & Knowlton, Andersen Consulting, Siemens, Deutsche Bank, and Pharmacoepidemiology. These cases were deemed detailed enough to enable a first validation of the risk measure.

A known limit associated with the use of published cases is the lack of availability of cases describing failures. According to Chua and Lam (2005), failure is still very much a taboo subject in organizations. However, organizations should consider failure as an integral part of their development and learning process (Sitkin, 1992). Even if the cases do not represent pure failures, many challenges, problems, and issues related to KMS are described in the cases. This permits the identification of undesirable outcomes and their associated risk factors.

In order to analyze the cases, a hierarchy of codes was built from the list of undesirable consequences and risk factors identified in the literature review. A code is assigned to a word, sentence, or paragraph making an explicit reference to an element of risk (outcome or factor).

The analysis of historical cases has three objectives. It seeks (1) to validate the undesirable outcomes and risk factors identified in the literature, (2) to discover new outcomes or factors that were not identified in the literature, and (3) to document the relationships between the risk factors and the undesirable consequences. Therefore, the coding process allows for the introduction of new codes. If an undesirable outcome or a risk factor is observed in the case, but was not previously identified in the literature review, a new code is generated.

Three tables were built for each case. First, a list of the undesirable consequences observed in the case was established. These undesirable consequences are deviations from the goals associated with the system use. In some cases, these consequences were severe while in others they were minor. Second, all the risk factors observed in the case were recorded, along with an evaluation of their value (high/low). For example, a risk factor like “Lack of collaborative culture in the organization” could be high; indicating that this variable increased the risk of an undesirable outcome, or low; suggesting that this factor was not menacing the objectives of the system. Finally, a third table listed all the links observed between the risk factors and the undesirable outcomes. The results show excerpts from these tables illustrating how the coding was done.

4.3 Delphi Method

After validating the list of undesirable consequences, risk factors, and their links using cases, an additional validation, using the Delphi method, was conducted with experts in the field of knowledge management. The goal of this additional step is to further validate the list of undesirable consequences, the risk factors, and the links between them.

The Delphi method is relevant for exploratory studies (Gordon and Gutierrez, 2006) and was widely used in the field of information technology (for example: Nambissan, and Tanniru Agarwal, 1999; Schmidt, Lyytinen, Keil & Cule, 2001; Gordon and Gutierrez, 2006). According to Linstone and Turoff (1975), the Delphi method provides a structure for a group communication process allowing it to deal with a complex problem. It facilitates the convergence of different views toward a consensus.

Two rounds were conducted in the Delphi exercise. They involved five experts. Three of them were involved in the implementation and the support of knowledge management systems and two were expert users of knowledge management systems. One participant came for the telecommunication sector, two participants came from the aerospace industry, and two from the retail industry. Having participants with different roles (support and user roles) and from different industries provided complementary perspectives on the risk measure.

In each round, the participants were provided with the list of undesirable outcomes, the list of risk factors, and a table showing the anticipated linkages between risk factors and undesirable consequences. The participants were asked to validate these elements. They could add any element or link that they felt was missing in the tables provided.

5 RESULTS

5.1 Results from the case analysis

Five objectives associated with KMS were identified in the literature review. According to the definition of risk, undesirable outcomes would be the deviations from these objectives. When analyzing the cases, all five objectives were found in the cases. No new objective was identified.

Table 1 shows how often each undesirable outcome was observed in the cases. Capture of employee’s knowledge, knowledge sharing, and value generation were the objectives challenged in all the cases. Six of the eight cases showed problems with the creation of new knowledge. In only two cases were threats to content improvement observed.

When looking at the risk factors, all the factors identified in the literature review were observed in the cases, with the exception of the learning ability. Seven new factors were identified in the cases: Trust, Information confidentiality, Cultural differences, Indicators to measure system value, Alerts for content, Organizational stability, and User support.

The cases enabled the identification of the linkages between specific risk factors and undesirable outcomes. Table 1 provides a summary. For each undesirable outcome, the number of cases in which this outcome was observed (at least partially) is mentioned. Then, the table indicates the number of cases in which the relationship between a given risk factor and the undesirable outcome could be observed (column “# of cases”).

5.2 Results from the Delphi Method

When conducting the first round of the Delphi exercise, all five participants validated the undesirable outcomes in the first round. They did not deem appropriate to add additional undesirable outcomes.

Respondents were also agreeing with most of the factors identified in the literature and in the cases. Twenty-five of them were confirmed by all the participants. Only four factors got partial support: content indicators and communication between communities of practice, business partners and clients were seen as risk factors by four of the five participants. Learning ability and content alerts were seen as relevant by three of the five participants.

Two participants suggested new risk factors: indicators measuring employee participation, time available to create and share knowledge, and the maturity level of the organization.

When assessing the relationship between risk factors and undesirable outcomes, the participants validated most of the links, except the ones associated with the risk factors they had discarded. Additional links were suggested for the new risk factors.

Objective of KMS	**Creation of new knowledge**		**Capture of employee's knowledge**		**Content improve-ment**		**Knowledge sharing**		**Value generation**	
Corresponding undesirable outcome (U.O.)	*Difficulty/ impossibility to create new knowledge*		*Diff./impos. 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	
Risk factors extracted from literature										
	# of Cases	% agree	# of Cases	% agree	# of Cases	% agree	# of Cases	% agree	# of Cases	% agree
Adequate strategy	6	100	8	100	1	100	8	100	8	100
Higher management involvement	6	100	8	100	1	100	8	100	7	100
Presence of incentives	3	100	4	100			3	100	2	100
Adequate roles and responsib.	5	100	5	100		100	5	100	*5	100
Quality of incentives	*2	100	*2	100		100	2	100	1	100
Learning abilities		60								60
Group work tools	5	100	7	100			7	100	5	100
Internal expertise							2	100	7	100
System ease of use	1	100	2	100		100	2	100	5	100
Adequate use of web tools	*2	100	3	100			4	100	6	100
Data integration		100		100	2	100	2	100	6	100
Content indicators						80			4	80
Adequate codification of knowledge					*1	100		100	3	100
Appropriate info. taxonomy					1	100		100	5	100
Adequate search tool								100	6	100
Content quality					1	100			6	100
Trust in the system									2	100
User participation in dev. project	3	100	4	100			4	100	4	100
User training	3	100	5	100		100	4	100	4	100
Communication between CoP, business partners and clients	1	80	*2	80		80	*2	80	*2	80
Collaborative culture	6	100	*7	100			7	100		
Adequate structure and processes	2	100	3	100	2	100	4	100	6	100
Risk factors added with the analysis of the historical cases										
Trust	2	100	2	100			2	100		
Information confidentiality	4	100	5	100			5	100		
Cultural differences	1	100	2	100			2	100	2	100
Indicators to measure sys. value	4	100	4	100	2	100	4	100	2	100
Alerts for content									1	60
Organizational stability			1	100			1	100		
User support	1	100	1	100			1	100	1	100
Risk factors added after the Delphi exercise										
Indicators measuring employee participation								100		100
Time available to create and share knowledge				100		100		100		
Maturity level of the organization				100		100		100		100

* Link that was observed in the cases but that had not been identified in the literature review.

Table 1. Summary of the Results

In the second round of the Delphi, all participants agreed with the inclusion of the new risk factors. They also agreed with the suggested linkages between these risk factors and the undesirable outcomes. However, none of the participant changed its opinion on the few risk factors on which there was no consensus in the first round. This suggested that the Delphi had come to an end. In Table 1, the level of agreement between the experts is indicated in the column “% agree”.

Table 1 shows that a total of 28 risk factors gained support from all respondents (on a total of 32 factors). Among the remaining four factors, two were supported by four out of five respondents, and two gained the support of three respondents. When assessing the links between risk factors and undesirable outcomes, 81 links were found in the literature, observed in the cases, and supported by the respondents. 9 additional links were observed in the cases and supported by the respondents, even if the literature review had not uncovered these links. Finally the respondents suggested 22 additional links, many of which were associated with the new risk factors suggested by these respondents. It is interesting to note that respondents were very much in agreement: 102 links received 100% support from them and only ten links received partial support. This suggests a highly coherent view of the risks associated with KMS among the experts participating in the study.

6 DISCUSSION & LIMITATIONS

Knowledge management software has become increasingly easy to implement from a technical perspective (Mann et al., 2010). However, such software is usually similar to an empty shell. It is through usage and user effort that the knowledge is added, constructed, and reused. This means that the initial costs associated with the first step of a knowledge management system implementation are not very costly for an organization. The risks associated with KMS reflect this low initial cost. The undesirable outcomes associated with KMS and detailed in Table 1 can be seen as opportunities lost. They are different from the undesirable outcomes measured for other types of risks. In outsourcing risk, undesirable outcomes are “increased cost of service”, “lock-in”, “service debasement”, etc. (Aubert et al., 2005). In ERP implementation risk, the undesirable outcomes are “cost overrun”, “undelivered functionalities”, “schedule overrun”, etc. (Bernard et al., 2004). The fact that the KMS undesirable outcomes are lost opportunities instead of “losses” may create a false sense of security for managers. The risks associated with KMS might not be managed as actively, or with the same level of attention than more traditional risks. However, for an organization, not reaping the benefits associated with an asset should be viewed as the same thing as a loss. Therefore, a better understanding of KMS risks may entice managers to devote more time to these initiatives.

One limitation of this measure of KMS risk is that it does not take into account security risks related to the leakage of intellectual property and trade secrets (Hannah, 2005). This scoping choice was driven by the results of the literature review, case analysis, and Delphi survey, as the undesirable outcomes that emerged were all related to the attainment or failure to reap the benefits of a KMS. Fortunately, research has already been conducted on this important aspect of KMS use in organizations (Majchrzak & Jarvenpaa, 2004). The risk measure proposed in this paper complements this work on the security risk of KMS. Furthermore, previous research has convincingly shown that such security risk should be managed as part of an integrated security risk management approach encompassing additional types of information systems resources, such as enterprise systems and IT infrastructure assets as many prevention and mitigation mechanisms can target more than one system at a time.

The other element that differentiates the KMS risks from other types of risk is the infinite horizon it requires. KMS are not simply implemented and then used. They are implemented and augmented continuously. Therefore, KMS risk cannot be measured like a project risk. It has not termination date like a project would (unless the system is decommissioned). It means that the risks associated with a KMS have to be measured continuously. They have to be managed on an ongoing basis. The owner of the KMS will have to develop a form of scorecard to track changes in the organization structure, incentives, distribution of expertise, etc. all these elements are risk factors and can modify the risk profile of a given KMS. The measure of KMS risk is a measure of risk associated with system usage, not with system implementation. It is different from other risk measures often developed in the information systems field.

Without a survey measuring these risks, it is difficult to assess the relative importance of each of the risk factors. It is likely that some of them will be more important than others. However, the structure of the linkages between risk factors and undesirable outcomes gives us interesting insights. There are a total of 32 risk factors. If we consider the unanimous evaluations of the experts, nine of these factors were deemed influencing the probability of occurrence of all five undesirable outcomes. Seven of the factors were viewed influencing the probability of occurrence of four of the five undesirable outcomes. This means that half of the risk factors influence at least four (out of five) outcomes. It suggests that the risks associated with KMS are highly correlated. The risk literature in information systems has not given detailed attention to the actual distribution of the events studied. While it was recognized that some factors might influence the probability of more than one event, other measures of risk mentioned earlier did not show so many commonalities. This means that KMS are probably more "at risk" of large problems than other systems. The large number of risk factors common to all undesirable outcomes suggests that several of these outcomes might occur simultaneously. This would entail severe consequences.

7 CONCLUSION

This paper proposes a measure of risk exposure for knowledge management system use. Five undesirable outcomes were identified, corresponding to threats to the goals associated with KMS. Thirty two risk factors were identified, enabling an estimation of the likelihood of occurrence of the undesirable outcomes. These elements were extracted from the literature and the examination of historical cases. They were validated using a Delphi exercise.

There is a long tradition of risk assessment in the IS literature (Boehm, 1989; Barki et al., 1993, 2001; Aubert et al., 2005). This paper contributes to the IS risk literature by mapping the specific risk factors associated with knowledge management systems. These factors have to be considered in addition to the traditional ones associated with any software development. One interesting aspect of KMS risk is that the undesirable outcomes all pertain to knowledge itself, which is close to the core of IS objects. In project risk assessment, elements considered are budget, schedule, functionalities, user satisfaction (Barki et al., 1993). For KMS, the undesirable outcomes are related to the identification, capture, share, and usage of knowledge. Therefore, these risks challenge directly our ability to represent and capture information and knowledge.

The other interesting aspect form a theoretical perspective is the variety of risk factors. Some of the risk factors identified include elements that are often observed in other types of risk measures: managerial elements, organizational elements, structural features, individual and cultural characteristics. In addition, the risk factors include many elements linked to the content of the system (content quality, data integration, content indicators, adequate codification of knowledge, appropriate information taxonomy, information confidentiality). This raises the issue of comparability of different knowledge management systems. Different KMS instances, involving similar technology affordances implemented in similar organizational settings, might actually present very different levels of risk.

This also suggests contributions for practitioners. As mentioned earlier, knowledge is becoming a strategic asset of organizations. Leveraging this asset becomes critical for organizations. The identification of the risk factors will enable managers to assess adequately the potential threats to their KMS initiatives. Once identified, the risk factors steer managerial attention toward concrete aspects of organizations which are amenable to managerial control. The variety of risk factors associated with the content of the system will raise managerial awareness about the uniqueness of KMS implementation and usage. Tools or strategies that have worked in similar settings might still be inappropriate if the content of the system is different from past implementations.

The examination of the list of risk factors suggests that most of these factors are manageable. Risk factors include many technical elements (tools, indicators, alerts, etc.) and managerial elements (incentives, structure decisions, role distribution, etc.). In this sense, the KMS risk is an endogenous risk; it depends in large part on managerial decisions (unlike exogenous risks like earthquakes). This means that once managers are informed of the risk factors influencing KMS, they should be able to take the appropriate actions. Managers can put in place risk mitigation measures to lower the risk to an appropriate level. Such practice would ensure that all the potential benefits are extracted from knowledge management systems.

8 APPENDIX – CODING OF THE SIEMENS CASE

The Siemens case was written by Heier, H., Borgman, H.P., and Manuth, A. (2005). Siemens is a German multinational company operating in the electrical and electronics engineering industry. The case presents the story of a KMS in the Information and Communication Network. It provides a good description of the use of this system. Siemens had clear objectives associated with the introduction of the system. The company sought to create more value with knowledge. The case shows that user involvement was an important factor for the acceptance of the concept of knowledge management and the idea to share knowledge. Another key aspect was the creation of incentives for users to share and reuse knowledge. However, incentives have also caused problems associated with quality content. The case shows that economic incentives are not necessarily the only solution to encourage users to participate in knowledge sharing. Users attributed value to the recognition of work well done. Finally, other important aspects of knowledge management at Siemens were the training of users, the efforts to create a collaborative culture within the organization, the creation of a process to identify and obtain knowledge and the creation of roles and responsibilities for maintenance and system support. The case analysis identified several risk factors. Some of these factors were "positive" in the Siemens case, indicating that these elements were actively managed to ensure that the project did not encounter undesirable outcomes. Other risk factors were not as favorable. The following table lists all the factors observed in the case, and indicates if the level of these factors was favourable or negative in the case.

Four potential undesirable outcomes were observed in the Siemens case:

Objective	**Form taken by that objective in the case**	**Corresponding undesirable outcome**
Creation of new knowledge	"Siemens aimed to … strengthen its innovation power" (p. 94)	Difficulty/ impossibility to create new knowledge
Capture of employee's knowledge	"For "explicit knowledge," the aim was to provide structured knowledge objects … For "tackt knowledge," the system was intended to provide functionalities such as newsgroups, discussion forums, and chats. (p.94)	Difficulty/ impossibility to capture employees' knowledge
Knowledge sharing	"knowledge sharing between employees and partners in remote areas was seen as a key driver" (p.94)	Difficulty/ impossibility to share knowledge
Value generation using knowledge	"Siemens realized it had to be able to provide flexible bundles of services and products that could be easily adapted to individual customers. To this end, the company recognized that a major improvement in the fast and purposeful identification and exchange of relevant information and knowledge was needed" (p.94)	Difficulty/ impossibility to use knowledge to generate value

Table 2. Undesirable Outcomes (Siemens)

Risk factor	**Information from the case**	**Favourable or negative in the case**
Adequate strategy	"Four crucial elements were defined to guide the KMS' conceptual development, prototyping, and later implementation: Sales Value Creation Process, ShareNet Content, ShareNet Community, and ShareNet Systems." (Heier et al., p.95)	Favourable
Higher	"Siemens ICN's group president and high ranking sales managers formed	Favourable

management involvement	the steering committee responsible for project supervision and top management support." (Heier et al., p.95)	
Presence of incentives	"The ShareNet Systems included … managerial systems to encourage the capturing, sharing, reuse, and global leverage of knowledge and best practices. These comprised--among others--incitatifs and rewards..." (Heier et al., p.96)	Favourable
Adequate roles and responsibilities	"The ShareNet managers received in-depth formal training enabling them to take over the responsibility for the introduction and utilization of ShareNet in local companies." (Heier et al., p.100)	Negative
Quality of incentives	"The new team decided to focus incentives and rewards more on the users themselves to get a critical mass of content into the system, to make users active contributors, and to create awareness ... but the success in quantity imposed drawbacks on quality. Lots of users--especially ones that joined ShareNet in earlier stages--lamented the decrease of content quality. " (Heier et al., p.102)	Negative
Group work tools	"Designated functional modules (M), that is, knowledge libraries, discussion forums, chat, and news, could be flexibly adapted to each CoP's businesses processes to win over users." (Heier et al., p.103)	Favourable
Internal expertise	"The option of adding a corporate directory for the mapping of internal expertise (yellow pages functionality)--often found in KMS--was seen as less promising due to a perceived lack of data quality." (Heier et al., p.96)	Negative
Adequate use of web tools	"The technical systems employed three-tier client/server architecture. The first tier was the user inter-face/personal workspace accessible via regular Web browsers. The second tier did most of the processing: a SUN SparcServer served as the designated application and Web server for all local companies and business units. It ran a software toolkit based on open Internet standards: open source Web server (AOLServer) and open source community system (ACS--ArsDigita Community System). ShareNet's dynamic Web implementation was based on AOLServer Dynamic Pages (ADP), an HTML derivate." (Heier et al., p.97)	Favourable
Data integration	"Web pages were generated by scripts loading meta-data (e.g., object structure and graphical layout) and actual data (e.g., customer description) from the relational database management system (Oracle 8i). It was housed on the same server and comprised the third tier." (p.97)	Favourable
Content quality	Lots of users--especially ones that joined ShareNet in earlier stages--lamented the decrease of content quality. " (Heier et al., p.102)	Negative
User participation in the development project	"The ShareNet project team and four consultants from The Boston Consulting Group (BCG) realized early that the KMS' development should be no isolated effort, and later parachuted into the local companies. Consequently, the team was augmented by 40 sales representatives from headquarters and 15 local companies. Their involvement served three distinct change management goals: they specified KMS solutions, supported a network of people experiencing similar difficulties, and set examples for the combined KM and change initiative's progress. " (Heier et al., p.95)	Favourable
User training	"Technical systems accounted for only 25% of total project costs; the majority was spent on the selection and training of prospective ShareNet managers, communication campaigns, and training material. The ShareNet project team and the external consultancy Change Factory jointly developed a range of user trainings/workshops and tools for the global rollout, for example training videos, illustrated pocket references, and giveaways. ". (Heier et al., p.98)	Favourable
Collaborative culture	"Responsibilities included the mapping of business processes to establish supportive KM platforms, the creation of a common knowledge infrastructure and culture, and fostering the awareness that knowledge sharing generates value." (Heier et al., p.93)	Favourable
Adequate structure and processes	"ShareNet's central part--the Sales Value Creation Process--was a sequence of important sales activities and decisions where knowledge ought to be reused. It served as an abstract global sales process definition, where each individual local sales process could be mapped." (Heier et al.,	Negative

	p.95) “Strong hierarchies counteracted an atmosphere of openness, mutual respect, and ambiguity tolerance since they placed value on individual achievements at the expense of teamwork.” (Heier et al., p.102)	
Information confidentiality	“Designated functional modules (M), that is, knowledge libraries, discussion forums, chat, and news, could be flexibly adapted to each CoP's businesses processes to win over users. This design also reflected the security requirements of sub-communities dealing with sensitive topics.” (p.103)	Favourable
Indicators to measure system value	“Siemens ICN reported additional revenue of EUR130.9 million from international knowledge exchange, some 50% obtained through ShareNet.” (Heier et al., p.100)	Favourable

Table 3. Coding of the Risk Factors (Siemens)

Linkages between the risk factors and the objectives				
Risk Factors	Creation of new	Capture of employee’s knowledge	Knowledge 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 4. Linkages between Undesirable Outcomes and Risk Factors

References

Alavi, M., & Leidner, D. E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. MIS Quarterly, 25(1), 107-136.

Atkinson, R. (1999). Project management: Cost, time and quality, two best guesses and a phenomenon, its time to accept other success criteria. International Journal of Project Management, 17(6), 337-342.

Aubert, B. A., Patry, M., & Rivard, S. (2005). A framework for information technology outsourcing risk management. Data Base for Advances in Information Systems, 36(4), 9-28.

Barki, H., Rivard, S., & Talbot, J. (1993). Toward an assessment of software development risk. Journal of Management Information Systems, 10(2), 203.

Barki, H., Rivard, S., & Talbot, J. (2001). An integrative contingency model of software project risk management. Journal of Management Information Systems, 17(4), 37-69.

Bernard, J.-G. (2006). A typology of knowledge management system use by teams. Paper presented at the 39th Annual Hawaii International Conference on System Sciences (HICSS), Hawaii, USA.

Bernard, J.-G., Rivard, S., & Aubert, B. A. (2004). L'exposition au risque d'implantation d'erp: Éléments de mesure et d'atténuation. Systèmes d'Information et Management, 9(2), 25-50.

Birkinshaw, J., & Sheehan, T. (2002). Managing the knowledge life cycle. Mit Sloan Management Review, 44(1), 75-83.

Boehm, B. (1989). Software risk management. Los Alamitos, CA: IEEE Computer Society Press.

Brown, J. S., & Duguid, P. (2000). Balancing act: How to capture knowledge without killing it. Harvard Business Review, 78(3), 73-+.

Carmines, E.G., & Zeller, R.A. (1979). Reliability and validity. Sage University Paper Series on Quantitative Applications in the Social Sciences. Thousand Oaks, CA: Sage Publications.

Chua, A., & Lam, W. (2005). Why KM projects fail: a multi-case analysis, Journal of Knowledge Management, 9(3), 6-17.

Danis, C., & Singer, D. (2008). A wiki instance in the enterprise: Opportunities, concerns and reality. Paper presented at the ACM Conference on Computer Supported Collaborative Work.

Desouza, K. C., & Awazu, Y. (2005). Maintaining knowledge management systems: A strategic imperative. Journal of the American Society for Information Science and Technology, 56(7), 765-768.

Du, S., Keil, M., Mathiassen, L., Shen, Y., & Tiwana, A. (2007). Attention-shaping tools, expertise, and perceived control in it project risk assessment. Decision Support Systems, 43(1), 269-283.

Efimova, L., & Grudin, J. (2007). Crossing boundaries: A case study of employee blogging. Paper presented at the 40th Annual Hawaii International Conference on System Sciences (HICSS), Hawaii, USA.

Fulk, J., Heino, R., Flanagin, A. J., Monge, P. R., & Bar, F. (2004). A test of the individual action model for organizational information commons. Organization Science, 15(5), 569-585.

Gallupe, R. B. (2001). Knowledge management systems: Surveying the landscape. International Journal of Management Reviews, 3(1), 61-77.

Gordon X., & Gutierrez J. (2006). An Exploratory Study of Killer Applications and Critical Success Factors in M-Commerce. Journal of Electronic Commerce in Organizations, 4(3), 63-80.

Hannah, D. R. (2005). Should I keep a secret? The effects of trade secret protection procedures on employees' obligations to protect trade secrets. Organization Science, 16(1), 71-84.

Heath, C., Larrick, R. P., & Klayman, J. (1998). Cognitive repairs: How organizational practices can compensate for individual shortcomings. Research in Organizational Behavior, 20, 1-37.

Iversen, J. H., Mathiassen, L., & Nielsen, P. A. (2004). Managing risk in software process improvement: An action research approach. MIS Quarterly, 28(3), 395-433.

Jackson, S. E., & Dutton, J. E. (1988). Discerning threats and opportunities. Administrative Science Quarterly, 33(3), 370-387.

Kankanhalli, A., Tanudidjaja, F., Sutanto, J., & Tan, B. C. Y. (2003). The role of it in successful knowledge management initiatives. Communications of the ACM, 46(9), 69-73.

Kontzer, T. (2002). Tentative first step into knowledge management for kodak. Information Week.

Kontzer, T. (2003, August 18). The need to know. Information Week.

Leonardi, P. M. (2007). Activating the informational capabilities of information technology for organizational change. Organization Science, 18(5), 813-831.

Lindgren, R., Henfridsson, O., & Schultze, U. (2004). Design principles for competence management systems: A synthesis of an action research study. MIS Quarterly, 28(3), 435-472.

Linstone, H., & Turoff, M. (1975). The Delphi method: techniques and applications. Reading, MA: Addison-Wesley.

Majchrzak, A., & Jarvenpaa, S. L. (2004). Information security in cross-enterprise collaborative knowledge work. Emergence: Complexity & Organization, 6(4), 40-50.

Mann, J. (2010). What to do when knowledge management goes wrong (Vol. G00207068): Gartner.

Mann, J., Rozwell, C., & Drakos, N. (2010). Gartner's view on knowledge management, 2010 (Vol. G00175604): Gartner.

March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk-taking. Management Science, 33(11), 1404-1418.

Markus, M. L. (2001). Toward a theory of knowledge reuse: Types of knowledge reuse situations and factors in reuse success. Journal of Management Information Systems, 18(1), 57-93.

Marlow, C., Naaman, M., boyd, D., & Davis, M. (2006). Ht06, tagging paper, taxonomy, flickr, academic article, to read. Paper presented at the 17th SIGWEB ACM Conference on Hypertext and Hypermedia. Odense, Denmark.

McAfee, A. P. (2006). Enterprise 2.0: The dawn of emergent collaboration. MIT Sloan Management Review, 47(3), 21-28.

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook. Thousand Oaks, CA: Sage Publications, Inc.

Nambisan S., Agarwal, R. & Tanninu, M. (1999). Organizational mechanisms for enhancing user innovation in information technology. MIS Quarterly, 23(3), 365-395.

Paté-Cornell, M. E. (1996). Uncertainties in risk analysis: Six levels of treatment. Reliability Engineering & System Safety, 54(2-3), 95-111.

Scheepers, R. (2003). Key roles in intranet implementation: The conquest and the aftermath. Journal of Information Technology, 18(2), 103-119.

Schmidt, R., Lyytinen, K., Keil, M., Cule, P. (2001). Identifying Software Project Risks: An International Delphi Study. Journal of Management Information Systems, 17(4), 5-36.

Sitkin, S. B. (1992). Learning through failure - the strategy of small losses. Research in Organizational Behavior, 14, 231-266.

Skeels, M. M., & Grudin, J. (2009). When social networks cross boundaries: A case study of workplace use of facebook and linkedin. Paper presented at the ACM 2009 International Conference on Supporting Group Work (CSCW 2009).

Tyrvainen, P., Paivarinta, T., Salminen, A., & Iivari, J. (2006). Characterizing the evolving research on enterprise content management. European Journal of Information Systems, 15(6), 627-634.

Wasko, M. M., & Faraj, S. (2005). Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. MIS Quarterly, 29(1), 35-57.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS Quarterly, 26(2), XIII-XXIII.

Zhao, D., & Rosson, M. B. (2009). How and why people twitter: The role that micro-blogging plays in informal communication at work. Paper presented at the ACM 2009 International Conference on Supporting Group Work (CSCW 2009).

References – Cases collected for the historical case analysis

Davenport, T. & Hansen, M. (1998). Knowledge Management at Andersen Consulting. HBS No. 499032-PDF-ENG. Cambridge, MA: Harvard Business School Publishing.

Fulmer W. (1999). Buckman Laboratories (A) & (B). HBS No. 800160-PDF-ENG, 800033-PDF-ENG. Cambridge, MA: Harvard Business School Publishing.

Heier, H. & Borgman, H.P. (2004). Deutsche Bank: Leveraging Human Capital with the Knowledge Management System HRBase. Annals of Cases on Information Technology, 6, 114-127.

Heier, H., Borgman, H.P., & Manuth, A. (2005). Siemens: Expanding the Knowledge Management System ShareNet to Research & Development. Journal of Cases on Information Technology, 7(1), 92-110.

Manning, A. & Sarker, S. (2002). Enterprise information portal implementation: Knowledge sharing efforts of a pharmaceutical company. Annals of Cases on Information Technology, 4, 410-426.

Meister, D., & Mark, K. (2004). Hill & Knowlton: Knowledge Management. Ivey Case No. 9B04E003. London, ON: Richard Ivey School of Business, University of Western Ontario.

Parise, S., Rollag, K. & Gulas, V. (2004). Montgomery Watson Harza and Knowledge Management. Babson Case No. BAB102. Wellesley, MA: Babson College.

Sarvary, M. & Chard, A. M. (1997). Knowledge Management at Ernst & Young. HBS No. M291-PDF-ENG. Cambridge, MA: Harvard Business School Publishing.

References – Research employed to elaborate the initial list of risk factors and undesirable outcomes but not cited in the text

Alavi, M., & Leidner, D. E. (1999). Knowledge management systems: Issues, challenges and benefits. Communications of the Associations for Information Systems, 1(2), 1-36.

Benbya, H. (2006). Mechanisms for knowledge management systems effectiveness: Empirical evidence from the Silicon Valley. Paper presented at the 2006 Academy of Management Conference. Atlanta, GA.

Butler, T., Heavin, C., & O'Donova, F. (2007). A Theoretical Model and Framework for Understanding Knowledge Management System Implementation. Journal of Organizational & End User Computing, 19(4), 1-21.

Chua, A. (2004). Knowledge management system architecture: A bridge between KM consultants and technologies. International Journal of Information Management, 24, 87-98.

Cooper, L. P. (2003). A research agenda to reduce risk in new product development through knowledge management: A practitioner perspective. Journal of Engineering and Technology Management, 20(1), 117-140.

Davenport, T., De Long, D., & Beers, M. (1998). Successful knowledge management projects. Sloan Management Review, 39(2), 43-57.

Davenport, T., & Prusak, L. (1998). Working Knowledge: How Organizations Manage What They Know. Cambridge, MA: Harvard Business School Press.

Garud, R., & Kumaraswamy, A. (2005). Vicious and Virtuous Circles in the Management of Knowledge: The Case of Infosys Technologies. MIS Quarterly, 29(1), 9-33.

Gray, P. & Durcikova, A. (2006). The role of knowledge repositories in technical support environments: Speed versus learning in user performance. Journal of Management Information Systems, 22(3), 159-190.

Grover, V., & Davenport, T. (2001). General Perspectives on Knowledge Management: Fostering a Research Agenda. Journal of Management Information Systems, 18(1), 5-21.

Hahn, J., & Subramani, M. (2000). A Framework of Knowledge Management Systems: Issues and Challenges for Theory and Practice. Paper presented at the 21st International Conference on Information Systems, Brisbane, Australia, 302-312.

Hasanali, F. (2002). Critical success factors of knowledge management. [online] ://www.providersedge.com/docs/km_articles/Critical_Success_Factors_of_KM.pdf.

Jennex, M. E., (2008). Exploring System Use as a Mesure of Knowledge Management Success. Journal of Organizational & End User Computing, 20(1), 50-63.

Jennex, M., & Olfman, L. (2006). A Model of Knowledge Management Success. International Journal of Knowledge Management, 2(3), 51-68.

Lee, S.M., & Hong, S. (2002). An enterprise-wide knowledge management system infrastructure. Industrial Management and Data Systems, 102, 17-26.

Marks, P., Polak, P., McCoy, & S., Galleta, D. (2008). Sharing Knowledge. Communications of the ACM, 51(2), 60-65.

Markus, M. L., Majchrzak, A., & Gasser, L. (2002). A Design Theory for Systems that Support Emergent Knowledge Processes. MIS Quarterly, 26(3), 179-212.

Massey, A. P., Montoya-Weiss, M. M., & O'Driscoll, T. M. (2002). Knowledge Management in Pursuit of Performance: Insights from Nortel Networks. MIS Quarterly, 26(3), 269-289.

McDermott, R., & O'Dell, C. (2001). Overcoming cultural barriers to sharing knowledge. Journal of Knowledge Management, 5(1), 76-85

Poston, R., & Speier, C. (2005). Effective Use of Knowledge Management Systems: A Process Model of Content Ratings and Credibility Indicators. MIS Quarterly, 29(2), 221-244.

Sambamurthy, V., & Subramani, M. (2005). Special Issue on Information Technologies and Knowledge Management. MIS Quarterly, 29(2), 193-195.

Wing, L., & Chua, A. (2005). Knowledge management project abandonment: An exploratory examination of root causes. Communications of AIS, 16, 723-743.

Wong, K. Y. (2005). Critical success factors for implementing knowledge management in small and medium enterprises. Industrial Management and Data Systems. 105(3), 261-279.

Zack, M. (1999a). Developing a Knowledge Strategy. California Management Review, 41(3), 125-145.

Zack, M. (1999b). Managing codified Knowledge. Sloan Management Review, 40(4), 45-58.