Knowledge security risk management in contemporary companies – toward a proactive approach

Ilona Ilvonen
Tampere University of Technology
ilona.ilvonen@tut.fi

Jari Jussila
Tampere University of Technology
jari.j.jussila@tut.fi

Hannu Kärkkäinen
Tampere University of Technology
hannu.karkkainen@tut.fi

Tero Päiväranta
Luleå University of Technology
tero.paivarinta@ltu.se

Abstract
Although emerging organizational knowledge systems, such as social media, are widely researched, related knowledge security risks have received less attention. Traditional information security management models tend to concentrate on the technological viewpoint to secure existing information assets. However, the use of contemporary approaches for knowledge creation and sharing offer new important possibilities for making use of internal and external knowledge. Simultaneously, their implementation involves changes in technologies, as well as a change in work processes and communications. Hence, knowledge security risk management should be developed from the current focus on relatively static containers and information assets toward more proactive management of the potential future risks of knowledge sharing. This paper introduces a proactive process for managing knowledge security risks and reports experiences of its use by professionals with experience in various topics of information and knowledge security.

1. Introduction
Increasingly popular business approaches, such as open innovation, emphasize opening up organizational knowledge resources toward customers and other organizational stakeholders as well as utilizing knowledge resources residing outside company borders [1]. Due to the increasing use of the possibilities of, for instance, social media or social software, knowledge management in contemporary organizations is becoming less costly, more cloud-based, ubiquitous, standardized, and mobile [2]. Simultaneously, it has also become more personalized and more effective in meeting individual needs.

Therefore, there is simultaneously a strong need for understanding the types of potential risks related to increasingly open information and knowledge flows and relating these risks to the intended business benefits. However, many organizations lack an explicit or systematic knowledge protection strategy [3]. Because protecting knowledge is difficult, knowledge protection should not be marginalized or abandoned [4]. For example, risks resulting from social media-based knowledge environments and related protective measures are commonly neglected [5]. It can be very risky for a company to overemphasize knowledge protection, and thus, for instance, refuse to implement social media tools for knowledge sharing because competitors can simultaneously gain a knowledge-based competitive advantage by using them [2].

Regarding the existing studies that discuss risks and risk management related to information and, more specifically, the concept of knowledge, the majority of existing literature provides a plain technical view on information and technological assets [6]–[10], ignoring that knowledge is bound to people [7]–[9] [11], and as a consequence, people [8]–[13] and especially their communication [7] [11] are significant sources of security risks that are related to information and knowledge protection.

Novel forms of knowledge sharing and communication, such as various forms of social media, create both great opportunities and benefits for knowledge sharing, new knowledge creation, and as a result, significant competitive advantages. However, they also create new important challenges for information and knowledge risk management [2] [5] [14] [15]. For instance, they make knowledge sharing and resharing extremely easy and fast, but simultaneously, unselective and unpredictable. Additionally, it is virtually impossible to “undo” the action and results of knowledge sharing. The shared information can often be easily located by competitors and combined with other pieces of information by modern data analytics approaches. The above characteristics make the proactive management of knowledge risks essential.

An example of the risks related to the above type of fast sharing of information by contemporary means of social media is related to a recent incident in a Finnish Defense Forces meeting (employee cooperation negotiation), where one of the participants published confidential information in real time on his Facebook.
profile. He found out only minutes afterwards that all information discussed in the meeting was to be fully confidential and to be kept secret [16]. Similar types of incidents are also quite common in the business context, where confidential information concerning new product launches is revealed, for example, on Facebook or LinkedIn.

Knowledge sharing tools provide new containers for organizational communication that need to be identified (in the above example, it was expected that communication in a face-to-face meeting would take place only by traditional containers, mainly by slide presentations and discussions between people), but in addition, information can be communicated extremely fast in unexpected containers (Facebook) to an outside audience.

According to our review of existing literature on knowledge security risk management, there are some papers that acknowledge the above types of challenges [17] [8] [12] [18] [7]. The approaches generally bring forth the strong need for knowledge-based risk management, especially, as well as various approaches for dealing with some major challenges related to it. Several authors [7]–[9] [12] [17] emphasize the importance of identifying knowledge assets in the knowledge security risk management process and provide different approaches and tools for assisting in the identification of knowledge assets. However, only one of the discovered previous models included a method and a tool for identifying threats related to knowledge assets: the Octave Allegro method and its worksheets [7]. The model brings genre and container thinking to knowledge security risk management [7]. Genres can be described as “types” or “categories” of communications between people and organizations that are transmitted by means of “containers” (repositories and/or communication means).

However, the existing knowledge security risk management models [8] [9] [12] [17] [18], including Padyab et al.’s [7] genre-based approach, superficially discuss their perspective toward business, and they do not help in balancing the benefits and risks in a useful way. Rather, they concentrate on balancing the costs and benefits of individual risk mitigation means but neglect the view of the business benefits.

Putting the above together, contemporary knowledge sharing approaches, such as social media, provide new and useful means for knowledge sharing and inducing change in organizations. In situations involving change, knowledge protection needs to be emphasized [19]. Simultaneously, these situations firstly create a need for new knowledge security risk management approaches that help to identify and balance both knowledge sharing risks and benefits, and secondly, help to do this proactively, due to the aforementioned characteristics of contemporary knowledge sharing and communication means. Our aim is to build a knowledge security risk management model that can help to proactively identify the risks and costs, as well as the benefits, of contemporary forms of knowledge sharing. Social media is used as an example context for the use of our model in this paper because it well represents contemporary forms of knowledge sharing, and it is especially challenging from a risk-management perspective due to the characteristics mentioned above.

First, we briefly introduce the theoretical background for our work. After that, we introduce the proposed model, followed with an initial empirical evaluation. At the end of the paper, we discuss avenues for further research.

2. Key concepts and background theories

2.1 Knowledge

In our paper, the term knowledge is in a central role. We consider knowledge as an intangible asset that is created, shared, and held by people [20]. People create knowledge by thinking and interpreting [21] [22]. As a result of thinking, knowledge is embedded in people as tacit knowledge, but it is possible to communicate that knowledge to others in an explicit form in written or spoken language [20]. Knowledge as such can be valuable to the person that has it, but it creates value to an organization when it is used and shared among the employees for creating products, services, or processes. Knowledge can be seen as a key asset of a company [23] [24].

Although knowledge is bound to individual people, it is possible to transfer it from people to people [25]. This means that we concentrate on tacit knowledge that is externalized and needs to be secured in the process. We also acknowledge that new knowledge is created in organizations all the time, and decisions are made based on this new knowledge [26]. Knowledge is thus a highly dynamic asset, and securing something like that also requires dynamicity from the security processes.

2.2 Communication genres

According to Orlikowski [27], a “genre of organizational communication (e.g. a recommendation letter or a proposal) is a typified communicative action invoked in response to a recurrent situation.” To simplify, genres can be described as “types” or “categories” of communications between people, such as a project proposal that is usually communicated
repeatedly by using the same container (also referred to as communication medium), such as email, between the communicating parties. Genres are thus a means to identify how knowledge is shared between people and organizations and how this can put knowledge security at risk [7]. Most genre research (except for Yates and Orlikowski) has focused on genres transmitted through speech or print, whereas applying the genre theory to digital genres has received less attention [28]. However, genre theory has recently been applied to digital media as well [28] [29] and social media [30]. In information and knowledge security literature, genres are an emerging research area [7].

2.3 Knowledge security and knowledge risks

The concept of knowledge security [7] [31]–[33] is established in the information security management and knowledge management fields, but it does not yet have a commonly agreed-upon definition [8]. In this paper, knowledge security is understood as the managerial process and actions that are taken in organizations to identify threats toward important knowledge and to secure and protect the knowledge against those threats.

Different social media tools are created to support discussion and knowledge sharing between people, regardless of geographical distance [2]. From the point of view of knowledge security, these kinds of tools are repositories for knowledge [17], in addition to being channels for knowledge exchange, that is, containers in which different genres of communication take place [7]. A systematic way to identify and manage risks connected to knowledge would help in establishing a unified level of protection of knowledge, but research shows that this does not exist, at least not widely in organizations [6].

For the most part, discussions of social media risks in the literature focus on individual problems, such as losing control during stakeholder communication [34] or in providing insights from empirical examples [35]–[37]. Furthermore, the discussions are disparate, fragmented, and distributed in different outlets, such as academic articles, white papers, security threat reports, and news articles [38]. However, there has been work that consolidates the risk discussion, and we present two lists of different categories of social media risks in Table 1.

<table>
<thead>
<tr>
<th>Table 1 Social media risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>He [36]</td>
</tr>
<tr>
<td>Braun &amp; Esswein [37]</td>
</tr>
<tr>
<td>privacy invasion</td>
</tr>
<tr>
<td>loss of control</td>
</tr>
<tr>
<td>online threats</td>
</tr>
<tr>
<td>image damage</td>
</tr>
<tr>
<td>weak privacy settings</td>
</tr>
<tr>
<td>industrial espionage</td>
</tr>
<tr>
<td>malware</td>
</tr>
<tr>
<td>inefficiency</td>
</tr>
<tr>
<td>malicious apps</td>
</tr>
<tr>
<td>ineffectiveness</td>
</tr>
<tr>
<td>botnets</td>
</tr>
<tr>
<td>governance</td>
</tr>
</tbody>
</table>

The risks that we especially consider as knowledge security risks are presented in italics in Table 1. To be useful, the risk categories need to be broken down into individual threats, such as behavior that leads to the loss of control of knowledge or the release of knowledge that leads to image damage, so this kind of a risk listing is just the beginning of identifying the risks toward knowledge.

2.4 Risk management

Risk management is an area that has been widely researched and discussed in the literature. Generally, a security risk management process has at least four phases. These are for, example [39] [40]:

- asset and risk identification
- risk analysis
- risk-reducing measures, and
- risk monitoring.

The main steps are also illustrated in many different information security risk assessment models, with less emphasis on measures and monitoring [8] [41]. Although the steps of the process may be named differently, the contents of the steps essentially remain the same. What is common to the information security risk management process models is that many times the trigger for a risk management process comes from the need to meet information security management standards [18] [42]. We argue that instead of that, the trigger to the process should come from a business need. This argument is in line with project risk management literature [43], although the focus of project risk management is not on the security of the project, but rather on the overall success of the project.

3. A model for knowledge security risk management

In this paper, we argue that the knowledge security risk management (KSRM) process should start from the business need and the trigger that clarifies the need for the output of the risk management process. Knowledge is embedded into every organizational process, and thus knowledge security risks cannot be isolated from those business processes.
Knowledge security risk management is a continuous process that is triggered by a business goal, need, or problem that needs to be solved (step 1 in Figure 1). Typically, the process is connected to a development project in which some new activity or tool is evaluated and implemented into the organization. The context for analysis in this paper is the implementation of social media tools for communication. In the first step, the goals and benefits sought from the change and the people responsible for realizing them need to be identified [44]. Also, the people who are responsible for the assessment of the risks of the change need to be identified. The risk management process should be triggered by a business need, and there are always business expectations connected to a change. We argue that these expectations should also be an element in the risk analysis.

![Figure 1. The KSRM process](image)

Existing KSRM models only superficially discuss their perspective toward business and the actual business triggers that start the KSRM process. The few links to business that the models do provide include focusing on processes critical for business [8] [9] [17]; emphasizing stakeholders who are perceived important according to organizational strategic goals and objectives [7] [17]; supporting reduction of transaction costs in interorganizational collaboration by making explicit both risks and knowledge transfer benefits [12]; and ensuring that knowledge protection meets requirements forced by laws, standards, customers, or internal regulations [18]. In our model, all these elements are included in the business need step: knowledge security risks should be addressed to protect critical business processes so that strategic goals can be met. In addition to this, laws, standards, and regulations need to be met, but they should never be the primary reason for risk management.

The second step in the KSRM process is to identify important knowledge that may be at risk in the organization. Knowledge asset identification can be approached in many ways [7] [8] [12] [17] [45] [46] [47]. We consider knowledge to be bound to people, and all individuals possess a lot of knowledge. However, not all that knowledge is important to the organization that the individual works for. A business perspective is experienced to be a good way to direct information asset identification [9], and we argue that this applies to knowledge assets as well. Important knowledge exists both on the individual and collective level [48], and this should be acknowledged in the identification step.

The different knowledge identification models can be simplified to question sets that identify holders of important knowledge. For example, if the knowledge risk management process is connected to the implementation of new social media tools, identification can be performed by answering the following questions, for example:

- What knowledge will be shared with the tool?
- Who will be using the tool?
- For what purposes will different stakeholders use the social media tool?
- What is the importance of the knowledge that is shared within the social media tool?

The purpose of the knowledge identification step in this context is to gain an understanding of what knowledge will be shared (the genres of communication) over the chosen social media platform (new container) [2] [49], what the construction of the community is that will be using it [50], and what significance the knowledge holds for the company/companies that collaborate in the platform [50].

The third step of the KSRM process is threat identification. A threat is the potential of a negative event [41]. It can be further broken down into a vulnerability, an actor, or a threat agent that exploits that vulnerability, a motive that the actor has to the exploitation and the outcome of the event [41] [51]. Most existing models [7] [8] [12] [17] include threat identification either as an individual phase or as a part of the risk analysis phase in the KSRM process. We argue that separating threat identification as an individual task in the process helps to separate different kind of threat sources. In case of knowledge security risks, threat agents can be situated both inside and outside the boundaries of the organization. Knowledge may be lost due to technological threats, but information security functions cover most of those threats. Human threat agents should be identified, and identifying both vulnerabilities and motives to exploit them can be useful. Also, understanding the factors behind following or not following organizational rules is important [52].

In the example case of social media, understanding is needed of both the technical properties of the social media platform and the operations of the community.
that uses the platform to create understanding of the threat agents and threat scenarios. Customers, competitors, hackers, and employees are examples of threat agent groups that have different kinds of vulnerabilities to exploit and different kinds of motives. The concepts of threat agents and motives help break down the lists of knowledge risks presented in Table 1. Human error or benevolent mistakes are also threats that need to be taken into serious consideration. Even the smallest mistake can lead to big consequences very quickly. To identify as many threats as possible, the employees of an organization can be involved in the threat identification process. This also helps in the following steps, as the employees are already aware of the threats and threat agents.

The fourth step of the risk management process is risk analysis, in which the threats identified in the previous step are individually analyzed. The prioritization of the most important communication genres will be one way to identify the primary risks that need to be analyzed, since individually going through all the threats identified in the previous step may not be reasonable.

A risk is the combination of two elements: the consequences of a threat and the probability of it [53] [54]. Several existing models discuss risk analysis [7] [12] [17] as a process phase in KSRM. Aljafari and Sarnikar [17] include subphases of making assertions, providing evidence to support assertions, and calculating risk in the risk analysis process phase. They propose the Demspiter-Shaefer [55] [56] model as an approach for performing the risk analysis. Trkman and Desouza [12] introduce a framework that categorizes knowledge sharing risks and propose that managers can use the framework as a guide/sense-making device in identifying the main types of risk facing their organization. The Octave Allegro [41] method introduced in Padyab et al. [7] provides an approach and a tool for both identifying the threats and vulnerabilities and deciding on the risk mitigation actions. However, it is difficult to determine the monetary consequences of a threat or the exact probability of it [12] [17]. To simplify the risk analysis process, a 3x3 or 4x4 matrix (with threat consequences categorized from severe to minor and the probability categorized from certain to highly unlikely) can be used to assess whether the risks are major or minor [41] [53].

When implementing new social media tools and performing risk analysis connected to them, business need and business case are important inputs for risk analysis. In case a threat connected to the use of social media is realized, the loss of benefits that were aimed for by using that tool is an element in the monetary consequences of the threat. However, the consequences may be a lot bigger than the benefits, if the trust of customers is lost due to the risk, for example. This is why reputation risks and loss of control are the kinds of knowledge risks that especially need to be carefully considered and analyzed.

The fifth step of the KSRM process, cost-benefit-analysis, is our most obvious addition to the traditional risk management models. Manhart and Thalmann [18] address cost-benefit analysis in connection with risk mitigation from the perspective of assessing the performance of knowledge protection, but not for evaluating or balancing the costs and benefits of knowledge sharing and knowledge protection. Also, Padyab et al. [7] argue that the output from risk assessment will help organizations to conduct a cost-benefit analysis based on current controls and countermeasures as to whether they mitigate, transfer, avoid, or accept the risks, but they do not consider balancing the costs (of mitigation) with business benefits. Cost-benefit analysis as such is not new, but the broader scope of it is the contribution of our paper.

Elements of cost-benefit analysis are performed throughout the risk management process, yet it needs to be acknowledged as an individual step in the process in order to emphasize the most essential location of the activity. This is because the risk analysis step provides major inputs to cost-benefit analysis in the form of estimated value of risk realization. The other steps of the process also provide input, especially the expected benefits of the implementation of knowledge sharing with the social media tool. In the cost-benefit analysis, all costs that are connected to the implementation and use of the social media tools need to be considered, including the estimated costs of risk realization. These are then compared to the expected monetary and other benefits brought by the knowledge sharing and risk mitigation.

The sixth step is risk mitigation. The implementation of risk mitigation controls adds to the costs, but diminishes risks, on the other hand, and thus affects the balance between costs and benefits. In addition to the direct costs of mitigation, knowledge protection has indirect costs, such as administration costs and the cost of loss of communication [57]. Risk mitigation controls need to be selected after a careful consideration of which risks are worth addressing and when mitigation is reasonable [58]. Risk mitigation is addressed in several KSRM models [7] [8] [17] [18], and in the case of security policies [17], the SECI model [8] [20] and internal audits [18] are mentioned as mitigation means.

Our example case of social media tool implementation is no different from other change situations in an organization: if the change is too risky or too costly, it may be abandoned, in which case
mitigation is unnecessary. Cost-benefit analysis may also affect the choice of mitigation means when the costs of mitigation are contrasted with the risk that is being mitigated and the benefits of the mitigated activity. This way, the most cost-effective mitigation means can be identified. In addition to the above-mentioned mitigation means, training and risk awareness of employees in the case of social media are keys to knowledge security. Technical controls may be able to mitigate some risks connected to knowledge sharing in social media, but the focus of risk mitigation should be more on managerial and administrative controls to handle knowledge security threats originating from communication between people [59]. An organization also has to accept that some knowledge risks, such as sharing knowledge with personal professional networks, cannot be mitigated with policies and rules [52].

The last step in the KSRM process is monitoring. Although this is identified as one of the key phases in the general risk management literature [39], it is partly missing from the existing knowledge risk management models. Manhart and Thalmann [18] propose conducting knowledge audits to monitor knowledge security risks. The monitoring step remains active for a long time after a change has taken place. If the use, users, or technological qualities of the original system change, risks connected to it should be reevaluated. Also, the success of mitigation activities should be constantly monitored.

In the case of social media, monitoring knowledge security risks includes following and monitoring the use of the social media tool and enforcing the security policies that are connected to its use. In addition, the technical security of the tool needs to be constantly monitored. It is especially important to constantly monitor what kind of knowledge is shared and created in the social media tool, that is, what kind of communication genres take place in it so that any changes in the threats can be identified and properly mitigated. The monitoring step makes our KSRM process responsive and proactive to the ever-changing threats created by contemporary communication means.

4. Expert evaluation and discussion

In this section, we present expert evaluation of our proposed KSRM model and a discussion of the changes that were made on the basis of the empirical material. In Figure 2, we present a revised version of the KSRM model.

We presented the KSRM model illustrated in Figure 1 to a group of five IT professionals in a social media-related education and training course. The participants were asked to apply the model to the context of their choice, the focus being on some use case of social media in a company. The participants were asked to reflect on the usefulness of the model to the context they chose to examine, and these varied from the use of social media tools for marketing to the use of social media for communication in a product development project. The participants had experience on risk management in companies, including program and project risk management, information systems risk management, and information security consultancy. The first participant was a program manager (hereafter PROGMAN) in a global telecommunications company, with more than 10 years of experience on project management and program management. The second participant was a system administrator (hereafter SYSADMIN) in an IT-service company, with one year of experience in information system risk management. The third participant was a sales manager (hereafter SALESMAN) at a software company, with one year of experience in mobile software development, sales, and social media communications. The fourth participant had less than a year of experience in information security consultancy (hereafter INFOSEC) at a transportation company, and the fifth participant was an experienced software engineer (hereafter SWENG) with more than seven years of experience at global ICT companies.

The experiences and reflections were captured from a) oral presentations that were recorded and transcribed or b) written assignments. In this section, we present the main reflections and feedback of the participants on the KSRM process. Overall, the participants felt that the KSRM model is a useful tool for managing the new kinds of challenging knowledge risks that contemporary communication means create. In their case, the context for analysis was the implementation of social media tools and approaches for knowledge sharing for different purposes. In this section, we concentrate on the main suggestions for improvement that the qualitative analysis of the empirical material brought up.

Cost-benefit analysis

The participants identified components related to the cost-benefit analysis of the KSRM model as central contributions of the model. The strength of the (KSRM) model is in its ability to identify both the potential business benefits of social media use and the associated risks (SALESMAN).

Also, suggestions were made in terms of how to better highlight the importance of cost-benefit analysis and in which phases of the model it should be performed.
The KSRM model supported and made it easy to proceed logically in carrying out the risk analysis in a product development project communication. However, the important novelty of the model, the cost-benefit analysis, is not given enough attention during the whole process, as cost-benefit analysis is only presented at the late phase (phase 5) of the model...cost-benefit analysis could be done as a second phase in the model or alternatively be included in the knowledge identification (phase 2) as a new supporting sub-phase of estimating benefits against costs that would be either accepted or rejected in this phase before moving to actual risk analysis. (PROGMAN)

The framework was a good and balanced tool. However, we feel that risk mitigation should be done before cost-benefit phase, because risk mitigation affects cost-benefit analysis (INFOSEC).

The price of mitigation of each risk is different depending on how the risk is mitigated (SWENG).

Risk mitigation was perceived as an important element in knowledge security management. For instance, it was seen as a strength of the KSRM model that it supported building the capability to be prepared and to respond to for example accidental leaks of knowledge by employees (SYSADMIN).

The participants mentioned several examples of mitigation actions that can be used to mitigate risk of employee knowledge leakage, for example, leakage of release date or technical details of new product: access control, information security policies, training, and trust-based approaches (SWENG, INFOSEC).

Risk monitoring

Monitoring was seen as an important element that addressed the changes inside the company or its business environment, which should trigger actions in

---

**Figure 2. A revised KSRM process**

Risk mitigation

Mitigation was perceived as an important element in knowledge security management. For instance, it was seen as a strength of the KSRM model that it supported building the capability to be prepared and to respond to for example accidental leaks of knowledge by employees (SYSADMIN).

The participants mentioned several examples of mitigation actions that can be used to mitigate risk of employee knowledge leakage, for example, leakage of release date or technical details of new product: access control, information security policies, training, and trust-based approaches (SWENG, INFOSEC).

Risk monitoring

Monitoring was seen as an important element that addressed the changes inside the company or its business environment, which should trigger actions in
the knowledge security management of the company. As an example, one of the professionals mentioned:

*The end of an employee’s work contract can be a significant trigger for access control and administrators to remove all access rights (to information systems) from the (old) employee.*

(INFOSEC)

According to this participant, violating company information security policies is an example of another trigger that should lead to actions of the IT department and also to consequences for the employees. Additionally, different information system logs can be used to trigger alarms. For example, the system can monitor and recognize delete commands to certain files.

**Ease of use of the model**

The participants also discussed the KSRM model from the vantage point of ease of use. For the most part, the participants were able to follow the KSRM process and felt that it is useful. However, they felt that without clarifying examples, the process model as such was a little difficult to understand and use.

*The weakness of the high [abstract] level of the [KSRM] model is how to fit the model in a specific use case. We understood the model, but only after looking at the lecture slides and sub questions [of an example application of the model] we were able to find solutions to the different parts.*

(SYSADMIN)

The participants experienced the process to be on quite an abstract level; that is, the theoretical explanation of each step was a little difficult to understand. They suggested that the model could be complemented with illustrative examples of each step and also suggested that the KSRM model could be modified into a web-based tool that could include different kinds of worksheets that would be easier to work with.

**5. Conclusions and suggestions for future research**

The knowledge security field is still a relatively new one, and this paper adds to the discussion on how knowledge security risks should be managed in organizations, especially when contemporary forms of knowledge sharing are considered and implemented. We argue that our model provides a useful approach for KSRM, supporting the evaluation of and decision making about what knowledge is important, how it should be shared, and what should be taken into consideration when securing that knowledge.

To improve the model and take the feedback from the evaluators into consideration, as well as to better include the perspective of proactive identification of the risks and costs of knowledge sharing, our KSRM model could be complemented with Padyab et al.’s [7] knowledge risk management approach. In their paper, Padyab et al. [7] present a hybrid GBM-OA method for knowledge risk management. This method combines the genre-based method for managing communication and the Octave Allegro approach for risk management. Our KSRM model has similar elements but a fundamentally different approach to knowledge risk management. In our model, we emphasize that knowledge risk management should be more business driven, balancing business risks and benefits, and should be connected to all business processes. This corresponds to the first steps of the hybrid GBM-OA method [7], but the KSRM model emphasizes two things that are not evident from the GBM-OA method: business trigger and change.

In the initial evaluation of the KSRM, the location and execution of the cost-benefit analysis component in the process received attention and reflection. For example, by applying the GBM-OA method [7] to the KSRM model, the cost-benefit analysis could be easier for managers to conduct. They could identify different genres of communication that will take place in the new social media tools and thus compare the risks, costs, and benefits of both the old and new way of communication. This genre-based analysis would also help identify new communication genres of important knowledge that the social media tool elicits. In practice, this genre-based cost-benefit analysis would require that the cost-benefit analysis stage is added to the GBM-OA model or that the KSRM and GBM-OA models are merged together. Future research should concentrate on the next step of development of our model: the development of a combined KSRM-GBM-OA model and testing it in real-life scenarios.

The initial evaluation provides encouraging support for our arguments, but evaluations should be done in the future in practical case scenarios, where preferably, observation and follow-up are added to the selection of empirical data gathering methods.

**References**


