An Integrated Risk Management Framework: Measuring the Success of Organizational Knowledge Protection

Research-in-Progress

Markus Manhart
University of Innsbruck
School of Management
Innsbruck, Austria
markus.manhart@uibk.ac.at

Stefan Thalmann
University of Innsbruck
School of Management
Innsbruck, Austria
stefan.thalmann@uibk.ac.at

ABSTRACT

In the underlying research- in- progress paper we propose an approach towards knowledge protection adapting existing approaches from IT security management. We argue that an organizational risk management framework should not only rely on protecting data but also on protecting knowledge which is underdeveloped in many cases and stops at the level of formulating abstract goals. We consider that a consistent translation from the organizational risk management goals to implemented controls is beneficial in particular to measure the success of the knowledge protection initiative. Further, the performance of organizational knowledge protection should be considered when assessing knowledge management success. The existence of controls for knowledge protection enables to measure how effectively controls implement the requirements and hence, indicate how well knowledge protection is actually pursued in an organization. This affects organizations' abilities to prove compliance to risk management standards, laws, guidelines, or frameworks and creates transparency throughout the whole knowledge protection processes.

Keywords

Knowledge protection, knowledge management, risk management, performance measurement, knowledge sharing, IT security management

INTRODUCTION

It is no secret that organizations heavily rely on information systems (IS) nowadays, paying increasingly attention to protecting them as consequences of security breaches are heavy (Rees, Bandyopadhyay and Spafford, 2003). Recently, companies take on great efforts to protect their data, spending a lot of money and resources to implement organizational frameworks such as COBIT and also engage with auditors to verify these frameworks. At the same time knowledge management (KM) literature proposes the sharing of knowledge and investigates how this sharing could be facilitated. However, even if organizations are aware of the negative impacts on the organizational performance, knowledge protection receives little attention in practice and KM literature so far (Väyrynen, Hekkala and Liias, 2013). Hence, it could happen that global organizational risk management goals are implemented rigidly for protecting data and processes, and that these goals are all along neglected or implemented in a non-systematic way from the knowledge perspective. Solid planning models for knowledge protection are missing even if they are needed in today´s world in which the importance of knowledge steadily increases as well as the amount of knowledge threats (Alstete, 2003).

This problem is exacerbated by recent developments in the field of social media and mobile technologies that seem promising to support organizations in their knowledge sharing (Bruck et al. 2012; Santos and Nagla 2012; Wang and Shen 2011), but creates challenges to protect knowledge for specific reasons: Knowledge sharing happens then when devices can be used at home, in the workplace, during transportation periods and during leisure activities (Wang and Shen 2011), blurring the boarders between work and leisure time as well as knowledge sharing for themselves and for the job (Väyrynen et al., 2013). Although, this implies many opportunities like contribution to an organization's performance and innovativeness (Easterby-Smith, Lyles and Tsang, 2008), this trend rises the need of establishing a knowledge risk framework.

Whilst the IT security management (ITSM) literature has already recognized the necessity to propose security frameworks, models or guidelines (Rees et al., 2003), KM literature widely neglected this topic so far. Rather, knowledge protection is considered to be a barrier to knowledge sharing (Khamseh and Jolly, 2008) even if empirical research shows that successful knowledge protection significantly enhances organizational performance (Mills and Smith, 2011). However neglecting knowledge protection can hinder innovation or cause replication of ideas by external organizations (Cheung, Ma, Wong and Tse, July 2012). We consider that finding a balance between protecting and sharing knowledge is crucial therefore.

Underestimating the importance of balancing protection and sharing of knowledge also impacts the performance measurement in KM. Recently the focus of performance measurement is almost exclusively on knowledge sharing and mostly neglects knowledge protection. As the evaluation of security controls based on KPIs has already been discussed in the ITSM literature (Demetz, Thalmann, Bachlechner and Maier, 2011; Sheldon, Abercrombie and Mili, 2008), similar efforts have been missing for measuring and quantifying the success of knowledge protection.

This paper aims to approach this lack of research by proposing a holistic organizational framework for risk management, incorporating the ITSM as well as the KM perspective. Furthermore, it aims at highlighting its contribution to performance measurement of security controls for KM. First we describe the related work of each of the concepts taking into account current efforts in the field of performance measurement and how they relate to our work. Second, we introduce our intended framework by means of a concrete example. Finally, we give an outlook on further steps of this ongoing research project.

BACKGROUND

IT Security Management

ITSM aims at satisfying the need to achieve, maintain and prove compliance to security requirements imposed by customers, regulations or other third parties, and to cost-efficiently manage IT security (Tracy, 2007). According to ITIL, ITSM is the alignment of security with the management organization (Höne and Eloff, 2002). Thus, ITSM cannot be seen apart from the business strategy (Cazemier, Overbeek and Peters, 1999). To achieve this aim, the translation of the high-level goals from organizational risk management (i.e. the security requirements) into operationalized controls as well as the final implementation needs to be traceable and testable. For the establihsment of this transparent translation, three major processes are performed in practice (Thalmann, Bachlechner and Maier, 2013):

Design of controls: Includes the translation of business security requirements into security controls, i.e. into mechanisms that effectively address identified security risks as well as taking the performance measurement perspective into account to mitigate identified risks (Dewri, Poolsappasit, Ray and Whitley, 2007).

Select control objectives: Aims at selecting risks to focus on within the scope of an audit as not each business process or service can be considered. Auditors define the audit scope by identifying business processes or services according to their relevance and measurability.

Verify control implementations: Controls implemented have to be assessed according to how they are generally able to satisfy a business security requirement and how effectively they are implemented. This is due to gain assurance about the own and the suppliers' compliance to laws, standards, etc.

Recent research addresses the challenges of establishing this top-down translation and proposes frameworks, models or guidelines therefore (Lakshminarayanan, Liu, Chen and Perry, 2006; Tracy, 2007).

Knowledge Sharing and Protection

KM literature strongly focuses on the barriers of knowledge transfer and its facilitation. The key assumption is that the successful knowledge transfer in organizations forms the basis for competitive advantages (Argote and Ingram, 2000; Bou-Llusar and Segarra-Cipre´s, 2006). Furthermore, effective knowledge transfer is seen as the ability of an organization to share knowledge and the task of KM is to facilitate this sharing (Goh, 2002). However, even if it is obvious that sharing all of organizational knowledge can as well have negative impacts on the organizational performance, knowledge protection got little attention from the KM literature so far and has widely been ignored as KM success factor (Jennex and Olfman, 2005). With respect to knowledge protection we share the view of (Bloodgood and Salisbury, 2001) according to which the concept can be defined as preventing knowledge from being altered, transferred to other organizations, lost, or becoming obsolete. Recently, literature rarely pays attention to this increased need for protecting knowledge, but knowledge protection should not be abandoned or marginalized (Gold, Malhotra and Segars, 2001). In today's distributed work environment knowledge transfer increasingly takes place through mediated channels of communication, in which sender and receiver are geographically disconnected (Fadel, Durcikova and Hoon, 2009). Several studies suggest that knowledge is exchanged through social software and Web 2.0 tools (Thalmann, Peinl, Hetmank, Kruse, Seeber, Maier, Pawlowski and Bick, 2012). Furthermore, knowledge workers are currently equipped with a wide range of different devices, such as tablet PC´s or smart phones which can be used to share knowledge. These trends are all positively associated with knowledge sharing. However, they imply additional risks from a knowledge protection point of view and lead to less control for the organization (Väyrynen et al., 2013). In the context of organizational networks the balance between sharing and protecting is particularly important (Marabelli and Newell, 2012). Here the framework for classifying knowledge risks proposed by (Trkman and Desouza, 2012) makes a first valuable step regarding a more systematic analysis. However, they neither recommend nor discuss concrete measures for each class of knowledge risks.

Knowledge protection is rarely addressed in scientific literature and, moreover, with diverse foci. First of all, knowledge itself is understood differently in the context of protection. Yodmongkon (2009) investigates knowledge from a society perspective, i.e. protecting cultural heritage. Other work focusses on privacy, i.e. knowledge of private consumers on security (Hui, 2010) or protection of knowledge about personal information (Yassine, Shirehjini, Shirmohammadi and Tran, 2012). However, the majority focuses on knowledge in an organizational context e.g. (Alstete, 2003; Norman, 2001; Olander, Hurmelinna-Laukkanen and Heilmann, 2011) which is also the perspective of this work. Another dimension in this context is the focus on knowledge *about* protection issues e.g. (Hui, 2010; Massingham, 2010). However, our focus is on knowledge *to be* protected as the top-down approach focuses on protecting knowledge of individuals but also organizations or organizational units. Considering the amount of literature that matches this scope of knowledge protection, some work focuses on protecting knowledge in a sense of defending it against attackers or industrial espionage (Norman, 2001, 2002; Olander et al., 2011) as well as in a sense of retention, i.e. knowledge loss related to leaving employees (Jennex, 2009; Jennex and Durcikova, 2013). Both views are in line with the definition of Bloodgood and Salisbury (2001) and are focus in our work. Last but not least, knowledge protection gains some attention in the context of organizational knowledge audits and intellectual capital. Here, the focus is primary on the identification of critical knowledge to subsequently develop a protection strategy (Chan and Lee, 2011). The development of such a strategy is, however, not in the focus of such work.

Performance Measurement in KM

Performance measurement is defined as the process of "quantifying the efficiency and effectiveness of action" (Neely, Gregory and Platts, 2005). It measures whether an organization achieves its goals defined in the business strategy (Neely et al., 2005). Yet, performance measurement in KM mainly focusses on the knowledge sharing capability (Zack, McKeen and Singh, 2009). As mentioned above, knowledge audits touch knowledge protection in terms of identifying critical knowledge to be protected. Beyond that, measuring the organizational ability to protect critical knowledge is mostly neglected. In the literature, knowledge audits are discussed as a means to assess what kind of knowledge is needed, how knowledge can affect the organizational culture, or how it contributes to address business needs (Liebowitz, Rubenstein-Montano, McCaw, Buchwalter, Browning, Newman and Rebeck, 2000). However, knowledge protection is necessary for effective functioning and control within organizations (Mills and Smith, 2011), therefore, knowledge audits measuring the performance of knowledge protection would be necessary to successfully manage knowledge protection. To measure whether and how well an organization achieves its goals, performance metrics need to be related to objectives, i.e. control objectives (Kueng, 2000). A performance metric quantifies the effectiveness or efficiency of an action, i.e. an implemented control (Neely et al., 2005). Therefore, a performance measurement framework should be closely related to the implementation of top level risk management goals. Assessing performance metrics by an internal (knowledge) audit for example, the performance of the knowledge protection could be assessed.

TOWARDS AN INTEGRATED FRAMEWORK

Nowadays, knowledge risk management heavily relies on the individual perception of human beings (Trkman and Desouza, 2012) and demands a solid planning model (Alstete, 2003). In this section we make a first step for such a solid planning model and we outline our knowledge risk framework as visualized in Figure 1. The figure shows that global risks impact ITSM as well as KM. Mitigating these risks demands a balanced recognition of securing data and knowledge simultaneously. Organizational risk management requirements should be translated stepwise into low-level security controls and subsequently into configurations and practices to protect knowledge. Organizational ITSM strives to protect data, information, as well as explicit knowledge. The latter can be stored in repositories in documented form (Maier and Thalmann, 2008) and is protected by technical controls of ITSM. However, a substantial and steadily increasing part of the (explicit) organizational knowledge is currently not stored in organizational repositories but stored in and exchanged via social software and social media. and thus is not protected by ITSM controls (Peinl, Hetmank, Bick, Thalmann, Kruse, Pawlowski, Maier and Seeber, 2013). Besides this challenge, implicit knowledge cannot be secured by such technical measures at all. Hence, organizations have to ensure that their explicit knowledge stored in organizational IT, the transference pipeline, as well as the implicit knowledge of their employees are properly protected (Alstete, 2003). Our approach strives to portray knowledge protection as a holistic approach taking these dimensions into account.

Organizations would also benefit from implementing controls for knowledge protection in terms of performance measurement. Transforming high risk requirements into concrete mechanisms allows organizations to measure performance on a very detailed level. The implementation of controls for knowledge protection also allows organizations to conduct meaningful audits. Then, audit results can be used to determine the performance of practices for knowledge protection, configurations of KM systems, or even the internal audit processes themselves. In the following, we outline our approach, using concrete examples.

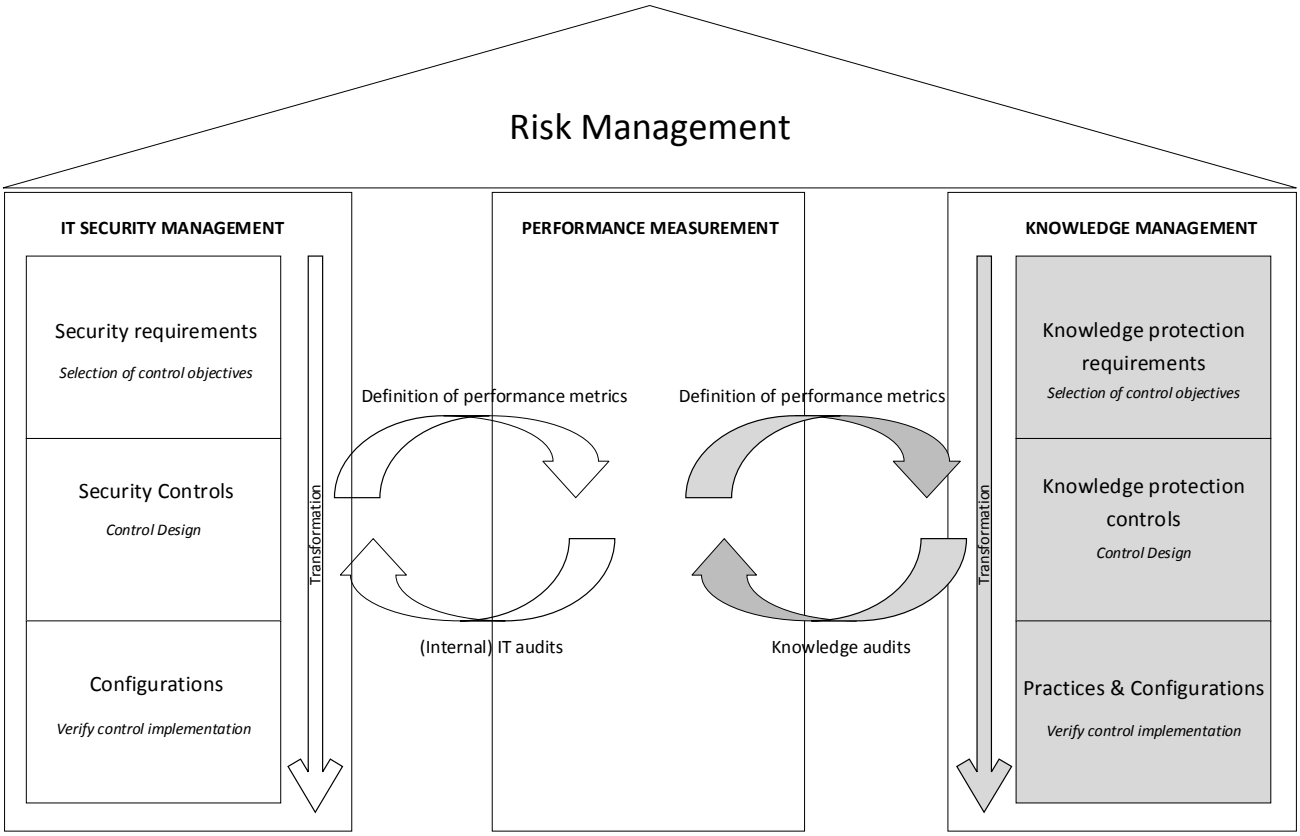

Figure 1: An Integrated Risk Management Framework

Design of controls: First, organizational risk management requirements have to be defined. The roots of such requirements are usually global risks that are relevant on a global level for organizational performance. Mitigation can be forced by laws, standards, customers, or internal regulations. Our example for such a high-level business security requirement is "protect customer affairs", occurring from the risk that disclosure of customer data would usually entail penalties from Service Level Agreements, for example. In the context of ITSM this would mean to protect customer data and all services in which these data are processed, in the context of KM to protect customer knowledge. These requirements are declarative, defining *what* should be protected, instead of *how* it is done. As a next step, requirements should be translated into a set of imperative controls. For ITSM this could be among others: "make the customer data base inaccessible from the internet", for KM: "no customer knowledge should be stored in public accessible parts of the organizational knowledge sharing platforms". With respect to the knowledge protection, this step is widely not considered by organizations. We recommend the definition of performance metrics for knowledge protection at this step. In the context of ITSM the coverage of access control could be one performance metric. In the case of knowledge protection, the number of fragments of customer knowledge in public accessible parts of the organizational knowledge sharing platforms could be one possible performance metric. Finally, the specified knowledge protection controls should be implemented by means of configurations of the knowledge management system as well as in instructions for knowledge protection. For ITSM, such an abstract configuration of the customer data base could be "block all traffic at the firewall between the internet and the customer data base". For knowledge protection an instruction could be "each employee has to attend at least one knowledge protection awareness training per year".

Select control objectives: The concept of knowledge audits is not completely new to organizations. However, it is often considered as related to assessing what knowledge is needed, culture assessments, or business needs assessment (Liebowitz et al., 2000). This view widely ignores knowledge protection. When translating the top-level risk management requirements into controls and configurations as it is done in ITSM, knowledge audits need to consider the audit from knowledge point of view as well. That is, the selection of control objectives, covering knowledge- related risks, knowledge processes, or the KM system, needs to be taken into account to define the scope of the knowledge audit.

Verify control implementations: In ITSM, the controls are assessed according to how they are generally able to satisfy a security requirement and how effectively they are implemented from an ITSM point of view. Knowledge audits do not cover the knowledge protection aspect. In our approach, the defined performance metrics are checked for example by internal

auditors. They assess whether the previously defined controls are properly designed and implemented. At that point, our approach contributes to enhance the measurability of performance in protecting knowledge. The level of knowledge protection would be transparent to decision makers and improvements could be made pointedly. With respect to the example above: In the context of ITSM the access to the customer database could be assessed by analyzing log files, for example. In the case of knowledge protection, auditors have to (regularly) scan the public accessible parts of the organizational knowledge sharing platform and its versioning history and calculate a value for this performance metric. To put it in a nutshell, organizations should make efforts towards the establishment of internal knowledge audits taking into account the assessment of whether measures for knowledge protection (configurations of KM systems and KM practices) are in place to implement the requirements from risk management.

The verification of whether measures are implemented effectively can improve the performance of KM in several ways. Verifying whether protection requirements are enforced would demand much more effort for internal auditors. To take the example from above: Under the assumption that no controls are in place, the auditor can only refer to check whether "customer affairs" are protected. This high level requirement is very difficult to assess and the responsibility to identify which KM systems, practices, or processes etc. are affected by this requirement. By implementing concrete controls, practices and configurations for knowledge protection, the internal auditor could save a lot of time and resources to verify whether requirements are satisfied. Last but not least, the implementation of controls itself reduces the probability that a requirement is not satisfied. That is, when there is no concrete control "no customer knowledge should be stored in public accessible parts of the organizational knowledge sharing platforms" then employees are not aware when breaching a requirement.

DISCUSSION AND OUTLOOK

In this research- in- progress paper we highlighted the current imbalance of implementing organizational risk management. It turned out that this implementation is currently rigidly performed in ITSM and rather superficial in KM. To ensure an overarching and consistent risk management approach, both perspectives need to be aligned. Therefore, we propose to adapt the already established procedures from ITSM to the domain of knowledge protection. Our framework recommends to translate high level risk management requirements into knowledge protection goals, finally resulting in concrete measures. This translation process also includes the definition of performance measurement metrics to assess the success of the knowledge protection campaign. We further propose to include this performance measurement framework focusing on knowledge protection into an overarching KM risk framework.

A stronger focus on knowledge protection in times of increased product piracy and patent rows seems to be an important aspect for KM as well. Especially current empirical evidence, on the fact that successful knowledge protection significantly enhances organizational performance, underlines this development (Mills and Smith, 2011). This domain is also promising as the measurement approach in form of audit reports is already known to controllers and accountants responsible for the budgets. Here, the measurement is much more direct and traceable for them compared to measuring the more indirect success of knowledge sharing, for example. However, this paper is an initial sketch for this promising research domain which needs further attention from the KM research side.

In our future research we first want to investigate the current practices of knowledge protection in an explorative field study. Here our focus will be on organizational networks as the balance of knowledge sharing and protecting is particularly challenging in this context (Trkman and Desouza, 2012). Building up on that, we will check current measures and practices in knowledge protection in a focus group interview with KM practitioners. Further, we want to contrast the known approaches from the area of ITSM with the current organizational practices to get more information on the barriers and also motivational aspects related to an integrated risk management framework.

Following, a revised and more detailed framework should be developed on the basis of the results from the focus group interviews. Thereby, a technical-oriented part building up on KM systems and repositories of knowledge resources and a non-technical part building up on KM practices is planned. Our current expectation is that technical solutions known from ITSM could be adapted to the needs of knowledge protection in KM systems. In a third step we plan to continue this research by accompanying an implementation project of a KM system. Here, the technical-oriented part of the framework should be implemented and evaluated.

ACKNOWLEDGMENTS

The research leading to the presented results was partially funded by the European Commission under the 7th Framework Programme (FP7) through the PoSecCo project (project no. 257129) and LEARNING LAYERS (contract no. 318209).

REFERENCES

1. Alstete, J. (2003) Trends in corporate knowledge asset protection, *Journal of Knowledge Management Practice*, 4.
2. Argote, L. and Ingram, P. (2000) Knowledge Transfer: A Basis for Competitive Advantage in Firms, *Organizational Behavior and Human Decision Processes*, 82, 1, 150-169.
3. Bloodgood, J.M. and Salisbury, D. (2001) Understanding the Influence of Organizational Change Strategies on Information Technology and Knowledge Management Strategies., *Decision Support Systems*, 31, 1, 55-69.
4. Bou-Llusar, J.C. and Segarra-Cipre´s, M. (2006) Strategic Knowledge Transfer and its Implications for Competitive Advantage: An Integrative Conceptual Framework, *Journal of Knowledge Management*, 10, 4, 100-112.
5. Cazemier, J.A., Overbeek, P.L. and Peters, L.M. (1999) Security management, The Stationery Office.
6. Chan, P.C.W. and Lee, W.B. (2011) Knowledge Audit with Intellectual Capital in the Quality Management Process: An Empirical Study in an Electronics Company, *The Electronic Journal of Knowledge Management*, 9, 2, 98-116.
7. Cheung, C., Ma, R., Wong, W. and Tse, Y. (July 2012) Development of an Organizational Knowledge Capabilities Assessment (OKCA) Method for Innovative Technology Enterprises, *World Academy of Science, Engineering and Technology*, 67, 54-65.
8. Demetz, L., Thalmann, S., Bachlechner, D. and Maier, R. "Performance Measurement in Cross-Organizational Security Settings," in: *International Workshop on Security Measurements and Metrics*, IEEE, Alberta, Kanada, 2011.
9. Dewri, R., Poolsappasit, N., Ray, I. and Whitley, D. "Optimal security hardening using multi-objective optimization on attack tree models of networks," in: *Proceedings of the 14th ACM conference on Computer and communications security*, ACM, Alexandria, Virginia, USA, 2007, 204-213.
10. Easterby-Smith, M., Lyles, M.A. and Tsang, E.W. (2008) Inter-organizational knowledge transfer: Current themes and future prospects, *Journal of Management Studies*, 45, 4, 677-690.
11. Fadel, K.J., Durcikova, A. and Hoon, S.C. (2009) Information Influence in Mediated Knowledge Transfer: An Experimental Test of Elaboration Likelihood., *International Journal of Knowledge Management* 5, 4, 26-42.
12. Goh, S.C. (2002) Managing Effective Knowledge Transfer: An Integrative Framework and some Practive Implications, *Journal of Knowldge Management*, 6, 1, 23-30.
13. Gold, A.H., Malhotra, A. and Segars, A.H. (2001) Knowledge Management: An Organizational Capabilities Perspective, *Journal of Management Information Systems*, 18, 1, 185-214.
14. Höne, K. and Eloff, J.H.P. (2002) Information security policy — what do international information security standards say?, *Computers & Security*, 21, 5, 402-409.
15. Hui, W. (2010) Brand, knowledge, and false sense of security, *Information Management & Computer Security*, 18, 3, 162-172.
16. Jennex, M. and Olfman, L. (2005) Assessing knowledge management success, *International Journal of Knowledge Management (IJKM)*, 1, 2, 33-49.
17. Jennex, M.E. "Assessing knowledge loss risk," in: *Americas Conference on Information Systems*, San Francisco, California, 2009, Paper 446.
18. Jennex, M.E. and Durcikova, A. "Assessing Knowledge Loss Risk," in: *46th Hawaii International Conference on System Sciences, HICSS46*, IEEE Computer Society, Hawaii, 2013.
19. Khamseh, H.M. and Jolly, D.R. (2008) Knowledge transfer in alliances: determinant factors, *Journal of Knowledge Management*, 12, 1, 37-50.
20. Kueng, P. (2000) Process performance measurement system: A tool to support process-based organizations, *Total Quality Management*, 11, 1, 67-85.
21. Lakshminarayanan, V., Liu, W.Q., Chen, C.L. and Perry, D.E. (2006) A Case Study of Architecting Security Requirements in Practice: Initial Analysis, University of Texas.
22. Liebowitz, J., Rubenstein-Montano, B., McCaw, D., Buchwalter, J., Browning, C., Newman, B. and Rebeck, K. (2000) The knowledge audit, *Knowledge and Process Management*, 7, 1, 3-10.
23. Maier, R. and Thalmann, S. (2008) Institutionalised Collaborative Tagging as an Instrument for Managing the Maturing Learning and Knowledge Resources, *International Journal of Technology Enhanced Learning*, 1, 1/2, 70-84.
24. Marabelli, M. and Newell, S. (2012) Knowledge Risks in Organizational Networks: The Practice Perspective, *The Journal of Strategic Information Systems*, 21, 1, 18-30.
25. Massingham, P. (2010) Knowledge risk management: a framework, *Journal of Knowledge Management*, 14, 3, 464-485.
26. Mills, A.M. and Smith, T.A. (2011) Knowledge Management and Organizational Performance: A Decomposed View, *Journal of Knowledge Management*, 15, 1, 156-171.

27. Neely, A., Gregory, M. and Platts, K. (2005) Performance measurement system design: A literature review and research agenda, *International Journal of Operations & Production Management*, 25, 12, 1228-1263.
28. Norman, P.M. (2001) Are Your Secrets Safe? Knowledge Protection in Strategic Alliances, *Business Horizons*, 44, 6, 51-60.
29. Norman, P.M. (2002) Protecting knowledge in strategic alliances: Resource and relational characteristics, *The Journal of High Technology Management Research*, 13, 2, 177-202.
30. Olander, H., Hurmelinna-Laukkanen, P.I.A. and Heilmann, P.I.A. (2011) Do SMEs Benefit From HRM-Related Knowledge Protection In Innovation Management?, *International Journal of Innovation Management*, 15, 3, 593-616.
31. Peinl, R., Hetmank, L., Bick, M., Thalmann, S., Kruse, P., Pawlowski, J.M., Maier, R. and Seeber, I. (2013) Gathering Knowledge from Social Knowledge Management Environments: Validation of an Anticipatory Standard in *Proceedings of the 11th International Conference on Wirtschaftsinformatik (WI2013)*, Leipzig, Germany, 753-767.
32. Rees, J., Bandyopadhyay, S. and Spafford, E.H. (2003) PFIRES: A Policy Framework for Information Security, *Commuications of the ACM*, 46, 7, 101-106.
33. Sheldon, F.T., Abercrombie, R.K. and Mili, A. "Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission," in: *Cyber Security and Information Intelligence Research Workshop*, ACM, Oak Ridge, Tennessee, 2008.
34. Thalmann, S., Bachlechner, D. and Maier, R. "Security Management in Cross-Organizational Settings: A Design Science Approach," in: *International Conference on Information Systems 2012*, Orlando, 2013.
35. Thalmann, S., Peinl, R., Hetmank, L., Kruse, P., Seeber, I., Maier, R., Pawlowski, J.M. and Bick, M. (2012) Ontology-based Standardization on Knowledge Exchange in Social Knowledge Management Environments in S. Lindstaedt and M. Granitzer (eds.) *Proceedings of the 12th International Conference on Knowledge Management and Knowledge Technologies*, Graz, Austria, ACM.
36. Tracy, R.P. (2007) IT Security Management and Business Process Automation: Challenges, Approaches, and Rewards, *Information Systems Security*, 16, 2, 114-122.
37. Trkman, P. and Desouza, K.C. (2012) Knowledge Risks in Organizational Networks: An Exploratory Framework, *The Journal of Strategic Information Systems*, 21, 1, 1–17.
38. Väyrynen, K., Hekkala, R. and Liias, T. (2013) Knowledge Protection Challenges of Social Media Encountered by Organizations, *Journal of Organizational Computing and Electronic Commerce*, 23, 1, 34-55.
39. Yassine, A., Shirehjini, A.A.N., Shirmohammadi, S. and Tran, T.T. (2012) Knowledge-empowered agent information system for privacy payoff in eCommerce, *Knowledge and information systems*, 32, 2, 445-473.
40. Yodmongkon, P. and Chakpitak, N. (2009) Applying Intellectual Capital Process Model for Creating a Defensive Protection System to Local Traditional Knowledge: the Case of Mea-hiya Community, *Electronic Journal of Knowledge Management*, 7, 4, 517-534.
41. Zack, M., McKeen, J. and Singh, S. (2009) Knowledge management and organizational performance: an exploratory analysis, *Journal of Knowledge Management*, 13, 6, 392-409.