Managing of Information Systems Risks in Extended Enterprises: The Case of Outsourcing

Bastian Schlaak
Chair of Information Management, Institute of Information Systems
University of Goettingen,
Germany
bschlaa@uni-goettingen.de

Scott Dynes
Center for Digital Strategies
Dartmouth College
Tuck School of Business,
USA
sdynes@dartmouth.edu

Lutz M. Kolbe
Chair of Information Management, Institute of Information Systems
University of Goettingen,
Germany
lkolbe@uni-goettingen.de

Ragnar Schierholz
ABB Switzerland Ltd.
Corporate Research
Switzerland
ragnar.schierholz@ch.abb.com

ABSTRACT

IT security issues and outsourcing of business processes are common but largely disjoint themes in the literature; common consideration is rare even though information security risk becomes a shared risk both through IS-based processes at outsourcing partners and potentially tightly-integrated IS systems. This paper explores this lack of an integrated model combining IT risk management view with the outsourcing process. Towards the development of an integrated model outsourcing and risk managing process phases are detailed; common phases of each serve as the basis for the introduction of an integrated model. Finally the paper suggests some points for future research.

Keywords

Risk Management, Outsourcing, Extended Enterprise.

INTRODUCTION

The increasing reliance of firms everywhere on the information infrastructure has raised questions regarding security and robustness at all levels of the economy, ranging from small firms who are dependent on the internet for select business communication to large multinationals that are extensively networked with their customers and suppliers. Today most companies are tightly integrated with and dependent on core suppliers, allies, customers, and possibly public authorities. Henceforth, we define this network of partners the "extended enterprise" (Johnson 2005) or "business network" (Alt, Fleisch and Österle 2001). One important example is the outsourcing of all kinds of tasks such as product development or production, application development or data processing to a service provider (Alt, Puschmann and Reichmayr 2001); this introduces operational and project risks arising from dependency on the service providers. A real-world example is MasterCard, which had problems when one of its data processing partners did not adhere to data retention rules; a security leak resulted in the inadvertent disclosure of millions of credit card records.

The level of concern around these risks has been evolving. Initially, efforts were focused on cybersecurity to prevent the spread of worms and viruses. Practitioners soon realized that the problem was more encompassing and consequential as demonstrated by the adoption of the term information security. Recently, more cognizant firms think not in terms of information security or information security management as laid out in ISO 27002, as but in terms of information risk management (Goetz and Johnson 2007).The latter view recognizes that firms face risks from loss of intellectual property as well as disruptions in the IT infrastructures that essentially run core business processes. Even though there is a broad awareness of IS risk, firms are taking different approaches to address this risk, ranging from denial ("I'm too small a player") through addressing issues internally to assuming complete responsibility for managing IS risk across their extended enterprise.

In this paper we set out to detail the types and maturity of information system (IS) risk management processes from the viewpoint of managing IS risk in outsourcing relationships, and to propose such a process based on industry best practices. The main research questions are:

(1) What are the challenges in identifying and managing IS risks with outsourcing partners, and what are the requirements for a descriptive as well as normative model?

(2) Is there existing literature or/and practices in the business world suggesting such a model?

(3) If not, what would such a model look like and are we able to detail certain aspects from information risk management field studies?

To answer these questions, we will present the drivers of IS risk management in the extended enterprise and analyze the related literature and assess existing frameworks, both on the risk management and on the outsourcing side. We will show that there is a lack of an integrated model that explicitly helps in managing IS risks in outsourcing relationships. We then derive requirements for such a model.

In the following section we describe the research methodology, data collection and data analysis from field studies of IT risk management practices at firms that work with outsourcing partners.

We then propose a model for developing outsourcing relationships that addresses IS risk as stated in the research questions (1) - (3) and we finish with a discussion of the proposed model in light of the requirements from literature and practice as stated before.

Finally we summarize the findings, highlight restrictions of the presented results and suggest areas for future research.

RELATED RESEARCH

Although IT outsourcing is a common business practice (e.g. Sparrow 2003) and IS-related risks are increasing, little research has been done to consider IS risk management in outsourcing processes. The basis for a risk oriented outsourcing model can be found in two related research areas: risk management process and outsourcing process.

Drivers for the IS risk management in the extended enterprise

Fleisch (2001) describes three important economic drivers, which lead to a more complex, integrated and interconnected IS. These are changes in the seller market, globalization and fast change. The more complex such a business network is, the more likely it fails (e.g. Westermann and Hunter 2007). The failure of any firm´s information network has an impact on the whole extended enterprise (Davis and Spekman 2003). Hence security incidents can result in high financial losses as well as in a loss of reputation (Satchell, Shanks, Howard and Murphy 2006). According to Westermann and Hunter business executives have to "understand the strategic importance of IT to their enterprises" to become aware of the IS risks. Without risk management, the effort to deal with incidents is higher than trying to avoid them (McKeen and Smith 2003).

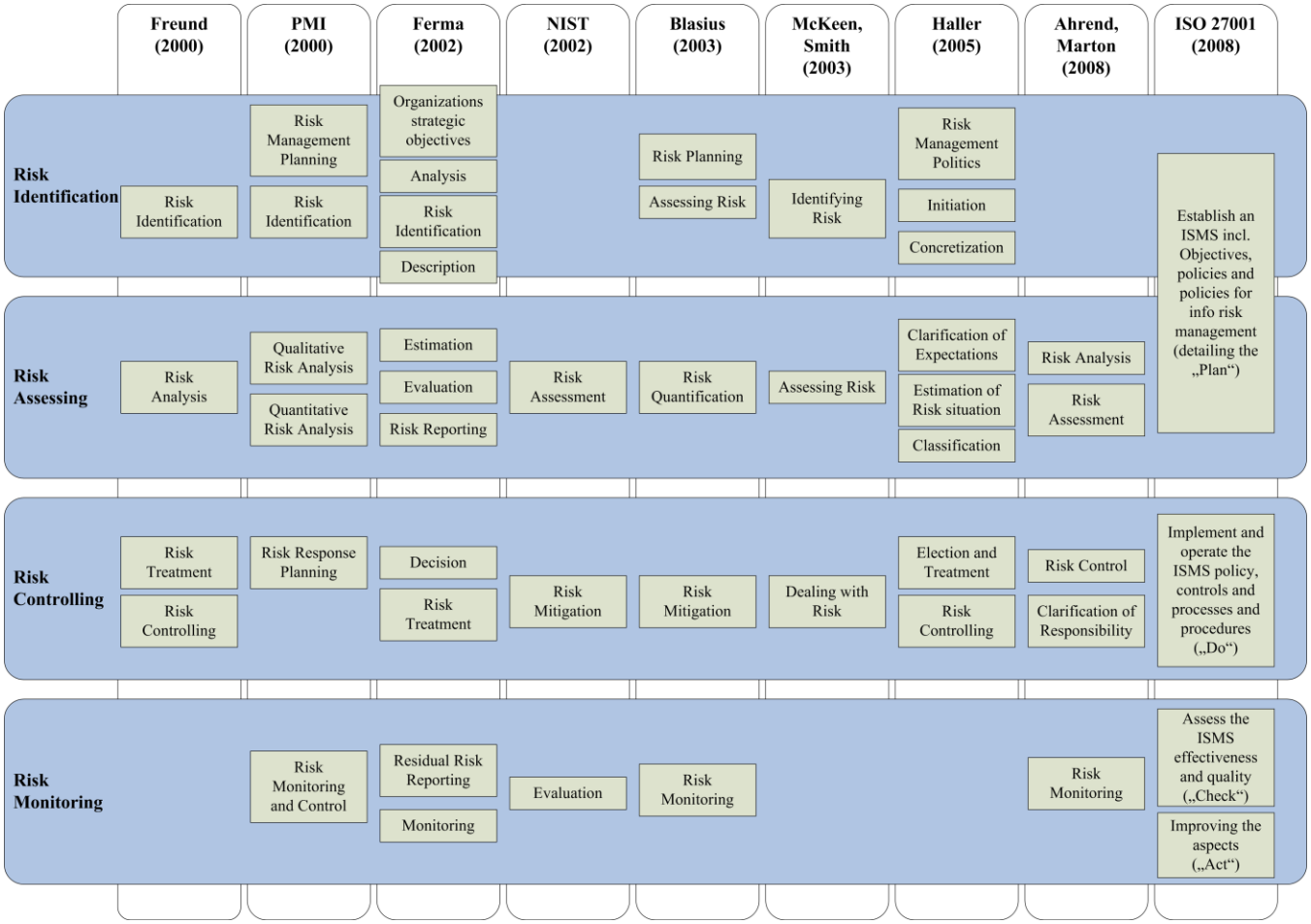

Figure 1. Overview of different Risk Management approaches

Risk management process

According to Simister (2000) the "risk management" concept was first used in insurance companies in the USA during the early 1950s. To this day, no standard definition for the term "risk management" exists (Simister 2000). According to Flaherty and Maki (2004) "enterprise risk management deals with risk and opportunities affecting value creation or preservation, defined as follows:

> *Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*"

A more IT oriented definition has been created by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce (NIST 2002). They define risk management as follows:

> *"Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organisations´ missions".*

Just as there multiple definitions, there are multiple risk management processes in the literature. A short overview is given in Figure 1.

Despite the differences in detail, the different risk management processes are based on a cycle model. Based on the tasks proposed by the different authors a generalized risk management model was developed which subsumed tasks into the

following four steps (indicated by the horizontal bars in Figure 1): identifying, assessing, controlling and monitoring. Figure 2 shows this general cycle of risk management that it is based upon these steps.

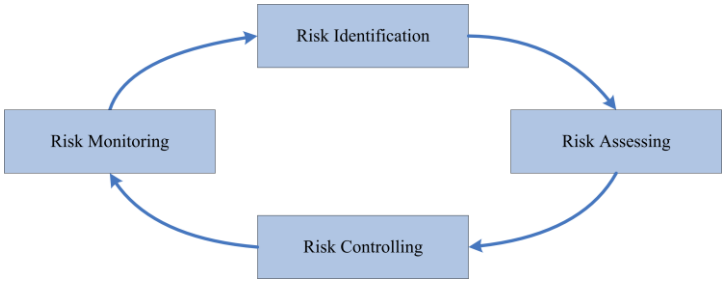

Figure 2. General Risk Management Cycle

Outsourcing process

Information Systems outsourcing is no new concept. It first appeared in 1963 with an agreement between Electronic Data Systems and Blue Cross (Dibbern, Goles, Hirschheim and Jayatilaka 2004). In 1989 Kodak made the first major outsourcing initiative with a cost of about $1 billion which received worldwide publicity (Sparrow 2003). The outsourcing market grew heavily in the past decades and Gartner (2008) predicts a market grow of 8.1 percent in 2008. Many different definitions for the term "outsourcing" exist in the IS literature; according to Dibbern et al. (2004) the term outsourcing "reflects the use of external agents to perform one or more organizational activities". Willcocks & Kern (1998) define IS outsourcing as:

> *"…the handing over to a third party management of IT/IS assets, resources, and/or activities for required results."*.

Important decisions regarding whether to outsource IS functions can be described in a process or lifecycle model. As before, no standard process exists in the IS literature. Figure 3 gives a short overview of processes found in the literature.

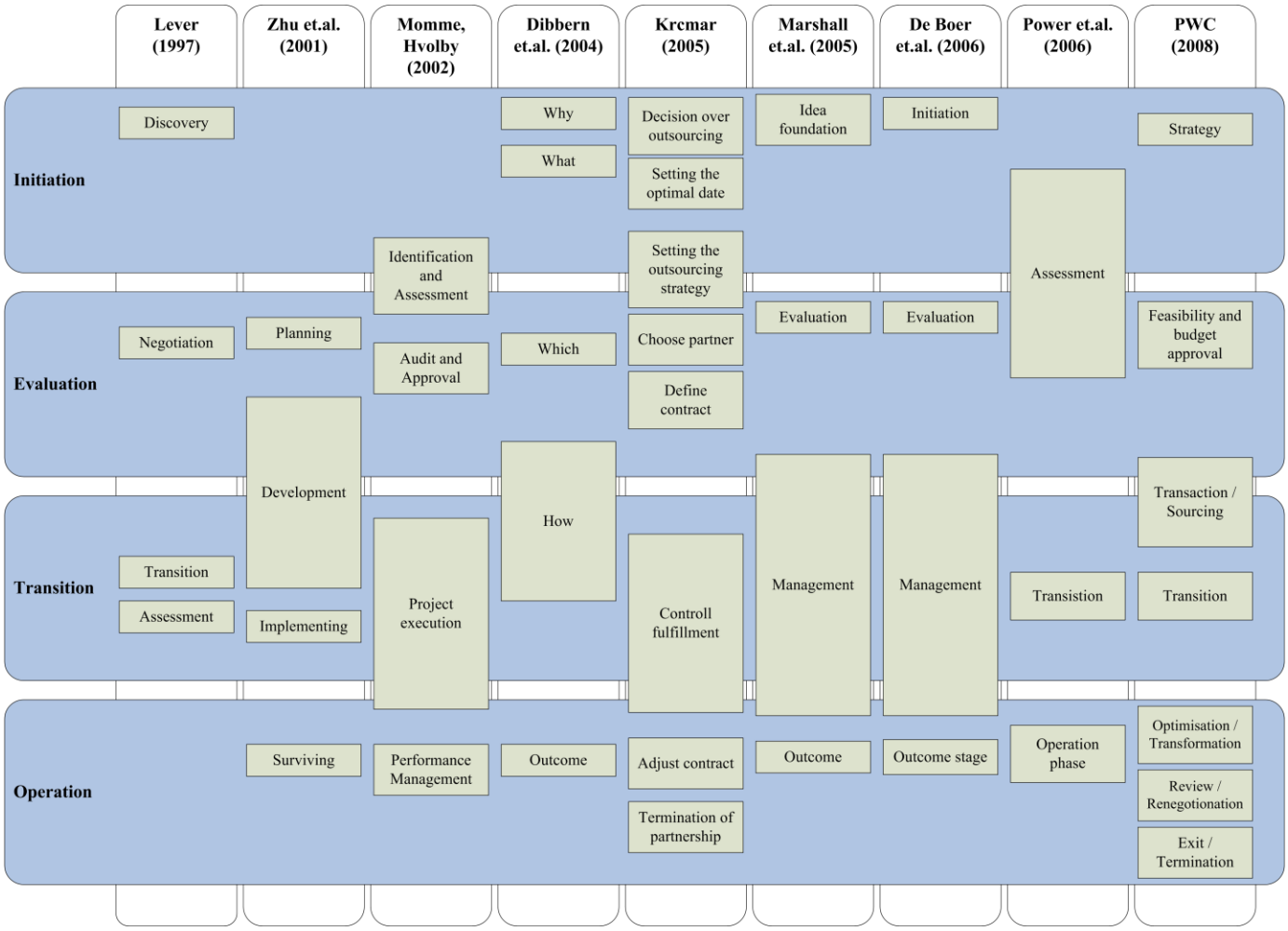

Figure 3. Overview of different Outsourcing approaches

The different models differ primarily in the number of stages. The model of Dibbern et al. is conceptually quite different, which might reflect its derivation from the Decision Making Model of Simon (1960) rather than a lifecycle model. Most of the models have three to four stages; more stages usually reflect a higher level of detail in a particular phase of a lifecycle model. In particular, the models from PWC and Krcmar are much more detailed due to their aim to be practice-oriented decision process guides. Though most of the models steps can be abstracted based on the tasks they represent to four elementary phases (initiation, evaluation, transition and operation, denoted by the horizontal shaded bars in Figure 3) their assignment is not as clear as it is in the risk management processes detailed above.

Integrated Models in the IS literature

While much has been written about outsourcing and risk management (Aron, Clemons and Redii 2005; Aubert, Dussault, Party and Rivard 1999; Aubert et al. 2005; Gouge 2003; Sparrow 2003), none of these consider IS risks in detail. Aron et al. (2005) divides risk into strategic, operational, intrinsic risks of atrophy and intrinsic risks of location. He handles the risks to outsourcing deals in general without providing a special model. Sparrow (2003) classifies the risks as follows: unrealistic expectations, inadequate contracts, poor relationship with your supplier, supplier lock in, loss of flexibility and loss of control. She also offers a risk management process but no integrated model.

Wong, Cheung, Hung, Kao, and Mamoulis (2007) researched security in outsourcing deals with a focus on data mining; this paper is too specialised to provide information to deduce an integrated model for managing IS risk in outsourcing processes.

RISK MANAGEMENT IN PRACTICE

Research methodology

The data presented in this paper are derived from two sources: field studies and CIO roundtables.

Field studies consist of a set of interviews with firms in a supply chain relationship. Typically a large Fortune 500 firm would be approached and be asked to serve as the 'host' firm for a field study; security and supply chain executives and managers would be interviewed at the host. The host would then introduce us to a few of its key suppliers; the same roles would be interviewed at these suppliers. In this way, insight was gained into the management of IT risk to the business at both the firm and supply chain level. Interviews were a combination of structured and unstructured questions. By asking the same questions of different interviewees in the same organization, we were able to look at the internal consistency of information provided in interviews and triangulated between the different data sources to arrive at a robust conclusion (Gubrium and Holstein 2002). Questions asked during the interviews centred on the identification and management of information security risks and business continuity risks the organization faced as a result of using technology to enable their services and supply chains. The data presented here is drawn from interviews with around 20 firms in the financial, manufacturing, health care, grocery and oil sectors.

The second source of information comes from chief information security officer (CISO) roundtables held by the Center for Digital Strategies at the Tuck School of Business. The most recent roundtable was titled 'Security Through Information Risk Management'; information risk officers from 23 firms discussed a broad range of information risk management issues (Goetz and Johnson 2007).

Insight into Information Risk Management

The results from our field studies and workshops indicate that while there has been a growing awareness of the risk to a business from the IT practices of business partners, IT risk management practices are still largely homegrown and based upon local knowledge and needs.

Field studies and a CISO roundtable held in 2004 (Dynes 2004) revealed that the majority of firms were not concerned with the information security practices of their business partners. For example, a manufacturing firm, while concerned with internal information security practices, did not have any requirements for information security practices at their business partners, counting on these partners to have a reasonable level of information security. A metal services firm, while having a relatively sophisticated view of business IT risk management, also did not assess the IT security practices of its business partners with the CISO stating that he could only justify worrying about things he had some control over, and he did not feel that he had control over supplier's IT security practices.

There were exceptions in 2004. A financial services information security director spoke of his firm taking complete responsibility for the IT security practices of their outsourcing partners, setting standards and auditing partners to assure they met those standards. There were examples of field study partners who had received questionnaires from large oil companies and manufacturers asking detailed questions about the IT security practices at the field study research partners; other interviews showed that the answers to such questionnaires did play a role in deciding which firms would be awarded a contract.

Today firms are in general much more sophisticated in their approach to information system risks. There are a few themes that commonly occur in both our field studies and CISO roundtables:

- The conversation is moving from security to risk. Information security has largely been viewed as an add-on activity that happens in addition to 'normal' business and IT processes. Firms are quickly evolving to think about information security as addressing a risk to the business and are starting to talk about information risk as an element of business control in the same conversation as other business risks. This conversation means that information systems risk identification and management is becoming a standard part of business, particularly when looking at new business processes form a risk/reward standpoint. That said, managers say that information systems risk is not yet a first-class risk. One manager noted that information system risks will rise to a certain level in the organization, but never quite to the top, where there is always a bigger issue to tackle.
- Conversations around information risk are moving from IT speak to business speak. This is being driven by the fact that the conversation is becoming more risk-based, and that CISOs find they get more traction in the organization if they speak in business terms. This places a premium on CISOs who understand business in general and their business in particular as well as the technology side. In order to develop such expertise, some interviewed firms will send some of their best

information security folks out into the business – not to do information security or IT, but to do the work of a business unit. This could be viewed variously as planting information risk management seeds in the business, or getting information risk folks deep business experience. Either way, these firms feel they will have a more robust information systems risk management stance.

- While formal processes for identifying information system risk are increasingly being used, there is no standard process. The development and adoption of a standard process would drive increased transparency of firm's information system risk and risk environment – i.e. it would be easier for firms to communicate threats and vulnerabilities with one another. This lack of information sharing is a key barrier to the adoption of rational levels of information security at the level of business sectors (Dynes Goetz and Freeman 2007). The processes that have been talked about have one consistent theme: prioritizing information system risk by likelihood and impact. The processes range from quite structured, where there is an explicit series of questions to ask about each business process to heuristic: one manager was talking about his process and saying, 'Once you've done this for a while, the risks are obvious'. While there does not seem to be a strong set of standard methodologies for identifying or categorizing information systems risk, there does seem to be a widely-used standard for prioritizing risk: the probability/impact magic quadrant. In our experience, all firms used an "educated gut" to estimate the probabilities for various attacks. The most advanced process included looking at the effectiveness of past information risk decisions and taking those learnings back into the risk management process.
- Firms are concerned with protecting their business when outsourcing, particularly intellectual property (IP) with outsourcing partners in other countries. Firms are starting to require certain information security practices of their outsourcing partners, in some cases subjecting these partners to periodic audits. Companies have to realize that better business outcomes are possible by assisting their partners with these information risk efforts by giving the partners access to information risk consultants. As the outsourcing partner chain may involve smaller companies that do not have the proper IT resources, this helps both parties achieve their goals. Another path to addressing outsourcing risk is to reduce the number of outsourcing partners. IP concerns range from the ease of reproducing digital intellectual property to the different legal and cultural landscapes in common outsourcing countries such as China, India and Russia. Managers talked about having to appreciate the cultural differences among countries to effectively gauge information risk when outsourcing. IP laws and traditions are non-existent in some countries, and thus tighter or stronger levels of control may be justified. Other managers noted that firms may be able to mitigate their business risks, the political environment is largely beyond the firm's control.

The data from practice demonstrate the growing awareness of IS risk management in outsourcing deals and a lack of standard process as well. To solve these problems an integrated model is required.

Challenges in managing outsourcing IS risk

Typical challenges derive from different fields such as organizational or technical matters. The first challenge is creating a risk management culture in the outsourcing firm, which is a prerequisite for an effective risk management program. Processes for identifying risks have to be adapted and implemented. All this needs to be done in an environment where the view of IT risk to the business is shared by both IS and business executives. Another challenge in outsourcing is concern about the potential loss of intellectual property; understanding the cultural and legal environment of potential outsourcing partners is important to addressing this issue, and in general.

DISCUSSION: TOWARDS AN INTEGRATED MODEL

Requirements for an integrated model

The requirements derive from two fields: research and practice. An integrated model has to be literature based and it must be amenable to validation. A model should also make clear, reasoned connections between the outsourcing and risk management processes described above. A model should be neither too abstract nor too detailed, it should be specific enough to provide clear guidance but not so specific that it cannot be easily applied to a good majority of situations. Adopting these to the processes in the related research section leads to the following requirements:

- *Risk Management Process*
  The identification, assessing, controlling and monitoring steps are essential and have to be considered in the integrated model. Another important demand is the cycle idea that represents the fact that risk management in business is an ongoing process.

- *Outsourcing Process Model*
  The elementary steps in the outsourcing process are initiation, evaluation, transition and operation; each has to be included in the integrated model.

According to the presented results in the previous section, the requirement from practice can be specified as the following:

- Risk management has to be focused on the business mission instead of dealing strictly with IT security issues.
- To achieve acceptance among business executives and managers the integrated model has to speak to business drivers and results.
- The model should be able to serve as a standard model to drive and assess alternatives for better inter-firm communication.
- Processes resulting from the model should be such that they can be easily implemented by firms with smaller IS resources or that operate in different cultures.

All these requirements have to be considered in an integrated model to fill the lack mentioned before.

IS risk oriented outsourcing model

In general there are two paths that lead to an integrated model. The first is to integrate a risk management process into an outsourcing process. The second is the other way round. The objective is to consider IS-related risks in outsourcing relationships; the outsourcing decision is the driver. Therefore we propose a model based on the four elementary steps in the outsourcing process. While melding the cyclical risk model to a predominantly non-cyclical outsourcing model would not seem natural, there are important elements from IT risk models that would serve to inform outsourcing efforts at every stage.

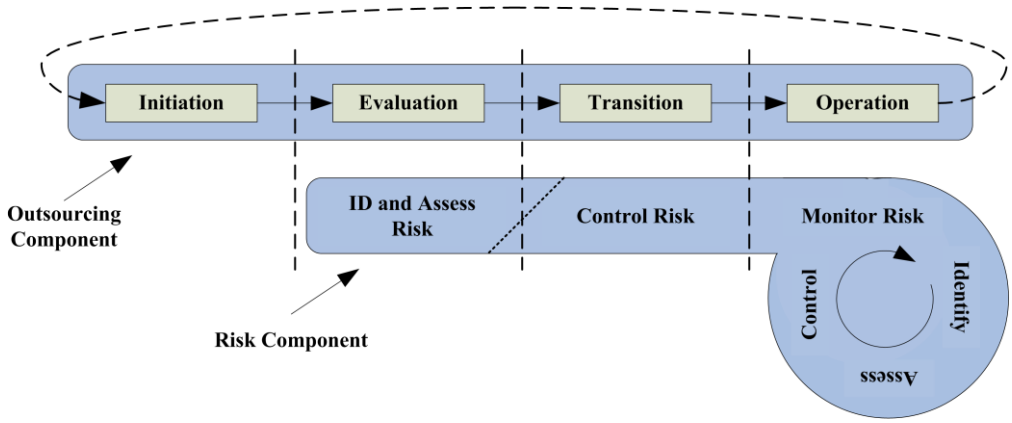

Figure 4. Proposal for an integrated model of outsourcing and risk management.

Following the overview of outsourcing models as shown in Figure 3, there are four key phases to outsourcing: Initiation, Evaluation, Transition, and Operation. The proposed model binds zero or more stages of the risk management cycle (Figure 2) to each phase of the outsourcing model. While outsourcing is most likely a cyclic procedure as well, the cycle times and drivers of the outsourcing cycle are very different than those for IS risk management. As a result we are not going into any detail regarding the outsourcing cycle. The Initiation stage does not have an IS risk management component; in this stage the idea of outsourcing a business process is being discussed; the details are deferred to the next stage, the Evaluation stage. In this stage, it is important to assess the complete range of business risks, not just from the perspective of the balance sheet, but also from the standpoint of potential information asset risk. This would include business continuity risk, and the risk that a potential outsourcing partner would be unable to manage a level of IS risk management required to protect its operations and the firm's other information assets such as customer data or intellectual property. Here, the Identify and Assess IS Risk stages of the risk management cycle would be utilized to develop an understanding of these risks. The next stage in the outsourcing model is Transition, making the organizational changes that realize the business process outsourcing. This is the appropriate stage to enact IS risk controls: at the very start of the outsourcing engagement. In this fashion, IS risk management is 'baked in' rather than 'bolted on'. The final stage is the Operational stage. Here, the correct IS risk approach is to enact the full IS

risk management cycle, using the risks identified, assess and controlled for in the previous stages at the starting point. The risk cycle should be operated as required based upon technical, regulatory, auditing or other changes in the operating environment. At this stage, the outsourcing engagement should be viewed as another business process.

Outsourcing processes starts with the initiation phase. First off all firms have to decide whether to outsource an activity or process. Setting the degree and distance of outsourcing comes up next followed by finding the optimal date for starting the outsourcing. At this phase it is not necessary to deal with IS risk management.

Choosing the vendor and setting up the contract are the core activities in the evaluation step. Appropriate IS risk management activities focus on identifying the risks associated with outsourcing. At first it is necessary to identify the risks that can occur on handing over resources, and/or activities to third parties. If a company wants to out source its IS infrastructure, a typical IS risk can be an increased danger of network breakdowns, or a decreased response to such breakdowns. Understanding these risks will influence the decision of whether to outsource; in general the outsourcing decision is highly dependent on the risk appetite of the enterprise. Another focus lies on assessing the different offers and the possible vendors. To make offers and vendors comparable, it is necessary to adopt a standard of measuring. Measuring the security level of a company is very complex and until security ratings from specialised firms, comparable to the investment ratings of Moody's or Standard and Poor's are available the effort for this can easily be underestimated. One possible system for measuring security are maturity models as provided by the Fraunhofer Institute (Fraunhofer Institute 2002). Part of the 'controlling risk' phase takes part here as well; developing the contract is an important step in Evaluation but is a central tool in influencing risks, particularly the Service Level Agreement of the contract, which can be used to define baseline levels of service and penalties for missing those levels. At this phase the effort for risk management can be very high.

The transition phase is characterized by handing over the resources to the outsourcing partner to start the delivery process of the vendor. Controlling the identified and measured risks is now the main function of the integrated risk management effort. Decisions over security arrangements, policies or the level of risk that a company would take have to be done now.

In the Operation phase the vendor is delivering the output and contract adjustments can be necessary. In this phase monitoring the IS related risks is the main risk management activity. Therefore in the operational state all of the risk management phases are important. Starting with Monitoring the whole General Risk Management Cycle takes place here. This is caused by the fact that new risks can occur, which have to be identified, assessed, controlled and monitored again.

Implications for Practice and Research

By using the proposed model in outsourcing processes companies can be sure to act methodically with risks in outsourcing deals. It is based upon different models which provide proven approaches either for risk management or outsourcing processes. In practice the model should be used considering the companies strategy regarding to risk taking and general outsourcing strategies. Doing this should lead to a higher awareness of risks in outsourcing and it would probably help to get people managing and controlling these as it can help to improve the inter-firm communication between business people and other employees. As shown in the second section there was a lack of an integrated outsourcing/risk management model. By integrating these two approaches into one model the paper tried to fill this gap.

CONCLUSION

The paper showed that the main challenges for managing IS risks with outsourcing partners are related to identifying and creating awareness of the associated business risks. Requirements for a model can be derived from the basic steps of the models shown in the overviews and from particular demands from practice. As the IS literature does not suggest a model that fits with these requirements, this paper proposes an integrated model where risk management is an embedded part of the outsourcing process.

As the model is based upon abstractions of outsourcing and IS risk management models as well as best practices for information risk management, the proposed combined model is not an outsourcing IS risk management best practices model, although we hope that future research will show that it is. Another limitation lies in the differing definitions of terms such as Risk Management and function in the different models surveyed. Depending on the point of view single tasks can be addressed in more than one phase. With the objective of creating a clear and good understandable model the paper addressed single tasks to one phase ignoring the fact that an assignment can not always be clear.

The proposed model can serve as a basis for a standard model in the future or as the outline for a set of best practices. In any case it should serve as a starting point for further research and might motivate practitioners to deal systematically with IS risk management in outsourcing processes. Further activities in research might be a comprehensive study or a closer look into the different task and phases of the appointed outsourcing and risk models.

REFERENCES

1. Ahrend, F. and Marton, A. (2008) IT-Risikomanagement leben!, Wirkungsvolle Umsetzung für Projekte in der Softwareentwicklung, Springer, Berlin, Heidelberg.
2. Alt, R., Fleisch, E. and Österle, H (2001) Business Networking in der Praxis, Springer, Berlin, Heidelberg.
3. Alt, R., Puschmann, T. and Reichmayr, C. (2001) Strategien zum Business Networking, in Alt, R., Fleisch, E. and Österle, H (Ed.) Business Networking in der Praxis, Springer, Berlin, Heidelberg, 77-101.
4. Aron, R., Clemons, E. K. and Redii, S. (2005) Just Right Outsourcing: Understanding and Managing Risk, Proceedings of the 38th Hawaii International Conference on System Sciences, 3-6 January 2005, Big Island, Hawaii, USA, 37-55.
5. Aubert, B. A., Dussault, S., Party, M. and Rivard, S. (1999) Managing the Risk of IT Outsourcing, Proceedings of the 32nd Hawaii International Conference on System Sciences, January 5-8, 1999, Maui, Hawaii. IEEE Computer Society.
6. Aubert, B. A., Party, M. and Rivard, S. (2005) A Framework for Information Technology Outsourcing Risk Management, The DATA BASE for Advances in Information Systemes, 36, 4, 9-28.
7. Blasius, I. (2003) Risikomanagement in Projekten zur Implementierung integrierter betrieblicher Standardsoftware (Risk management in implementation projects of integrated operational standard software), University of Siegen.
8. Davis, E.W. and Spekman, R.E. (2003) The Extended Enterprise: Gaining Competitive Advantage through Collaborative Supply Chains, Financial Times Prentice Hall Books.
9. De Boer, L., Gaytan, J. and Arroyo, P. (2006) A satisfying model of outsourcing, Supply Chain Management – An International Journal, 11,5 444-55.
10. Dibbern, J., Goles, T., Hirschheim, R. and Jayatilaka, B. (2004) Information Systems Outsourcing: A Survey and Analysis of the Literature, in: The DATA BASE for Advances in Information Systems, 35, 4, 6-102.
11. Dynes, S. B. C. (2004) Security and Privacy: At Odds With Speed and Collaboration?, http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/SecurityAndPrivacy/Overview2.pdf, accessed 18 Feb 2008.
12. Dynes, S., Goetz, E. and Freeman, M. (2007) Cyber Security: Are Economic Incentives Adequate?, in: Critical Infrastructure Protection (IFIP International Federation for Information Processing) (IFIP International Federation for Information Processing), Goetz, E. and Shenoi, S. (Ed.), Springer, New York.
13. Flaherty, J. J. and Maki, T. (2004) Enterprise Risk Management – Integrated Framework, Executive Summary, Committee of Sponsoring Organizations of the Treadway Commission.
14. Federation of European Risk Management Association - Ferma (2002) Der Risikomanagament-Standard, http://www.ferma.eu/Portals/2/documents/RMS/RMS-German.pdf, accessed 16 Feb 2008.
15. Fleisch, E. (2001) Das Netzwerkunternehmen, Springer, Berlin, Heidelberg.
16. Fraunhofer Institute (2002) SMM - Assessing a Company's IT Security, http://www.ercim.org/publication/Ercim_News/enw49/kurrek.html, accessed 19 Feb 2008.
17. Freund, D. (2000) Risk Management als Projektmanagement Disziplin. Immer noch die große Unbekannte?, in: projectMANAGEMENT aktuell, 04/2000.
18. Gartner (2008) Gartner Says Worldwide Outsourcing Market to Grow 8.1 Percent in 2008, http://www.gartner.com/it/page.jsp?id=578307, accessed 03 Mar 2008.
19. Goetz, E. and Johnson, M.E. (2007) Security through Information Risk Management: A Workshop for Information Security Executives – Overview. http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/CISO2007/Overview.pdf, accessed 18 Feb 2008.
20. Gouge, I. (2003) Shaping the IT organization, Springer, London.
21. Gubrium, J.F. and Holstein, J.A. (2002). Handbook of Interview Research, Sage Publications, London.
22. Haller, M. (2005) Der managementorientierte Umgang mit Risiko - Grundlagen eines integrierten Konzeptes, Risikomanagement und –kommunikation, Institut für Versicherungswirtschaft, University of St. Gallen.
23. ISO (2008) The ISO27001 Certification Process, http://www.27000.org/ismsprocess.htm, accessed 03 Mar 2008.
24. Johnson, M.E. (2005) A Broader Context for Information Security, Financial Times, September 16th 2005, 4.
25. Krcmar, H. (2005) Informationsmanagement, Springer, Berlin, Heidelberg, New York.

26. Lever, S., An analysis of managerial motivations behind outsourcing practices in human resources, Hum. Resource Planning, 1997, 20, 37-48.
27. McKeen, J.D. and Smith, H.A. (2003) Making IT Happen, Critical Issues in IT Management, Wiley, Cichester.
28. Marshall, D., Lamming, R., Fynes, B. and De Búrca, S. (2005) The development of an outsourcing process model, International Journal of Logistics, 8 4, 347-359.
29. Momme J. and Hvobly, H-H. (2002) An outsourcing framework: action research in the heavy industry sector, in: European Journal of Purchasind & Supply Chain, 8, 4, 185-196.
30. NIST (National Institute of Standards and Technology) (2002) Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-30, Gaithersburg.
31. Project Management Institute - PMI (2000) A Guide to the Project Management Body of Knowledge, PMBOK Guide, Newton Square, Pennsylvania.
32. Power, M.J., Desouza, K. and Bonifazi, C. (2006) The Outsourcing Handbook, Kogan Page, London.
33. Satchell, C., Shanks, G., Howard, S., Murphy, J. (2005) Beyond Security: Implications for the Future of Federal Digital Identity Management Systems, Proceedings of OZCHI 2005, ACM International Conference Proceedings Series, ACM , Sydney November.
34. Simon, H.A. (1960) The New Science of Management Decision, Harper, New York.
35. Simister, T.(2000) Risk management: the need to set standards, in: Balance Sheet, 8 4, 9-10.
36. Sparrow, E. (2003) Successful IT outsourcing, Springer, London, 2003.
37. Westermann, G. and Hunter, R. (2007) IT Risk, Turning Business Threats into Competitive Advantage, Harvard Business School Press, Boston.
38. Willcocks, L.P. and Kern, T. (2008) IT Outsourcing as Strategic Partnering: The Case of the UK Inland Revenue, in: European Journal of information Systems, 7, 1, 29-45.
39. Wong, W.K., Cheung, D.W., Hung, E., Kao, B. and Mamoulis, N. (2007) Security in Outsourcing of Association Rule Mining, Proceedings of the 33rd international conference on Very large data bases, 11-122.
40. Zhu, Z., Hsu, K. and Lillie, J. (2001) Outsourcing – a strategic move: the process and ingredients for success. Mgmnt Decision, 39, 373-378.