Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2012 Proceedings

European Conference on Information Systems (ECIS)

5-15-2012

DEVELOPING A RISK MANAGEMENT PROCESS AND RISK TAXONOMY FOR MEDIUM-SIZED IT SOLUTION PROVIDERS

Alexander Herzfeldt
Technische Universität München

Marina Hausen
Technische Universität München

Robert O. Briggs
San Diego State University

Helmut Krcmar
Technical University of Munich

DEVELOPING A RISK MANAGEMENT PROCESS AND RISK TAXONOMY FOR MEDIUM-SIZED IT SOLUTION PROVIDERS

Herzfeldt, Alexander, Technische Universität München, Boltzmannstr. 3, 85748 Garching, Germany, alexander.herzfeldt@in.tum.de

Hausen, Marina, Technische Universität München, Boltzmannstr. 3, 85748 Garching, Germany, marina@hausen.org

Briggs, Robert O., San Diego State University, MIS Department, 15320 El Camino Real, Rancho Santa Fe, CA 92067, USA, rbriggs@mail.sdsu.edu

Krcmar, Helmut, Technische Universität München, Boltzmannstr. 3, 85748 Garching, Germany, krcmar@in.tum.de

Abstract

To differentiate from competitors, some organizations are transforming their business models from offering single products or services to providing IT solutions. In an IT solution, the provider and the customer co-operate in integrating hardware, software and service components to fulfil customer-specific needs. The new business model, however, presents new risks, for example, those engendered by operating the IT solution on behalf of the customer and by integrating modules from third-party providers. Also IT solution providers need to support the whole lifecycle from planning to end-of-life, and account for customer-specific risk profiles. It is therefore important that IT solution providers understand these additional risks, and that they adapt their risk management processes to account for and mitigate these risks.

In this paper, we present the results of a design science research project conducted in a medium-sized IT solution provider. We developed two artifacts. First, we developed a risk management process that could be generalized to IT solution providers of similar size. Second, we derived a taxonomy of IT solution risks to drive the risk management process. We describe process how the organization under study transformed its risk management processes and discuss implications for other medium-sized IT solution providers.

Keywords: IT solution, risk management, transformation, risk management process, risk taxonomy, design research

1 Introduction

To differentiate from competitors and to meet new customer expectations, some organizations are transforming their business models from offering a single IT product or service to providing IT solutions (Brady et al. 2005, Tuli et al. 2007). IT solutions integrate hardware, software and service components to fulfill customer-specific needs. The provider and the customer cooperate in developing and operating the IT solution over the whole IT solution lifecycle (Herzfeldt et al. 2011).

A business model based on IT solutions, however, presents new risk management challenges (Brady et al. 2005, Windahl et al. 2004). For example, providers frequently operate their IT solutions on behalf of their customers, and so need to cope with additional operating risks (Erkoyuncu et al. 2011)., IT solution providers sometimes do not themselves develop all the technologies underlying the IT solution, but acquire them from third-party organizations (Windahl et al. 2004). Thus, they face risks of value-added networks. Moreover, where developers of products tend to focus on risk management during development and marketing, IT solution providers must address risks that manifest over the whole solution lifecycle, from planning to end-of-life (Burianek et al. 2007). Further, IT solutions customers are involved with the provider continuously, and each customer may have a different risk profile (Windahl et al. 2004). New IT solution providers need to understand the additional risks engendered by their new business model, so they can change their risk management processes to account for and mitigate these risks (Brady et al. 2005).

In order to deepen understandings of these challenges and to understand how risk management for IT solutions differs from that of traditional product or service providers (as suggested, e.g., in ISO 30000, IT Infrastructure Library), we conducted a design science research project in a medium-sized German IT organization ALPHA AG. ALPHA started as a software and consulting organization and transformed into an IT solution provider. Our research yielded two artifacts that could be generalized to other solution providers of similar size. The first was a six-step collaborative risk management process for medium-sized IT solution providers. The process helped IT solution providers to identify and mitigate new risks. Validation cycles in the field, however, showed that new IT solution providers still overlooked many unanticipated risks. We therefore drew on the academic literature and worked with practitioners to synthesize a taxonomy of 182 IT solution risks to enhance the thoroughness of the risk discovery and mitigation process.

The remainder of the paper is organized as follows: In Section 2, we briefly elaborate the concept of IT solutions and examine some risks for IT solutions. Section 3 describes our research approach, the organization where the research was conducted, ALPHA AG, and our data collection methods. Section 4 reports our first design science cycle and derives a six-phases risk management process for medium-sized IT solution providers, and shows its implementation in ALPHA. Section 5 presents our taxonomy of IT solution risks. We end our paper with a discussion of our findings and conclude by showing implications for academics and practitioners.

2 Background

2.1 From products and services to IT solutions

IT solutions differ from traditional products or service in that: 1) IT solutions consist of bundles of hardware, software and service, 2) IT solutions are customer-specific, 3) IT solution components interact with each other and are highly integrated, and 4) both the customer and the provider enter a long-term business relationship (Burianek et al. 2007, Tuli et al. 2007). IT organizations that transform into IT solution providers thus need adapt their business model to account for these special characteristics.

Moreover, Brady et al. (2005) stress the importance to consider business processes of IT solution providers from a lifecycle perspective. IT solution providers often engage in bidding processes to win a contract. These processes include a pre-bid phase, where potential new customers are identified, and a bid-phase, where the IT solution provider takes part in the bidding process of a potential customer. Not only must IT solution providers design, develop, and integrate an IT solution (project phase), but they oftentimes take over the operation of the IT solution they create (operational phase).

IT solution providers have to cope with a higher overall complexity then do the developers of commodity products (Herzfeldt et al. 2011, Tuli et al. 2007). Since IT solution providers often do not develop all the components of an IT solution themselves, but modularize the IT solution (Böhmann et al. 2007) to integrate components from third parties, they operate in complex networks of value-added relationships. Moreover, as IT solutions are customer-specific (Burianek et al. 2007), IT solution providers cooperate closely with customers to ensure the IT solution delivery. The close customer relationship may require IT solution providers to take over some of the customer's operational activities, a form of a selective outsourcing (Tuli et al. 2007, Windahl et al. 2004). Figure 1 gives an overview of the environment in which IT solution providers act. The complexity is magnified as IT solution providers offer multiple IT solutions and have multiple relationships with suppliers and customers.

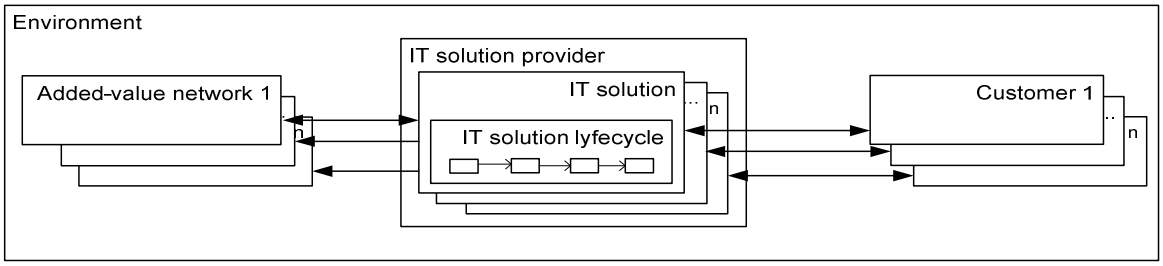

Figure 1. Environment of an IT solution provider

2.2 Risk management for IT solutions

Authors have advanced useful contributions to the field of IT solution risk management (Brady et al. 2005, Burianek et al. 2007). Nonetheless, risk management in the solution context is still nascent (Brady et al. 2005). In order to define the term *risk* for IT solutions, we refer to a definition from software engineering, proposed by Boehm (1991) and adapt it to the IT solution domain: Risks are uncertain events with negative impact on the IT solution objectives. Also, we find the following risk management process consisting of phases: risk identification, risk analysis, risk prioritization, risk management, and risk monitoring (Boehm 1991, Lyytinen et al. 1998) to useful for IT solutions, too. Similar processes are also described in the ISO 31000 or in the IT Infrastructure (ITIL) framework.

Due to the special characteristics of IT solutions, however, risk management for IT solutions needs to cover a wide range of aspects. We suggest researching neighboring domains of IT solutions in order to find more useful contributions: Those domains should include contributions on risk management in value-added networks, outsourcing, modularization, project management, operational management as well as software risk management and customer-provider relationship risk management.

3 Research design

3.1 Design science

The goal of Design Science Research is to create generalizable solutions to important classes of organizational problems. The goal of the design science process is to create an artifact, which has not existed before (Stahl 2008). March/Smith (1995) describe four types of artifacts: constructs, models, methods, and instantiations. The goal of this research was to explore what differentiates risk management for IT solution providers from risk management for commodity providers and to create a risk management method for medium-sized IT solution providers as well as a construct describing a risk taxonomy. Our research design matched well the process described by (Takeda et al. 1990) viewing design science research as a cyclic process consisting of awareness (problem identification), suggestion (suggestion of problem solving key concepts), development (implementation of a solution), evolution (artifact evolution), and conclusion (decision on artifact adoption).

3.2 Research Site

ALPHA AG was a useful site for this research because it is an exemplar for a typical medium-sized IT organization: ALPHA AG was founded in 1990 as a software and consulting organization and gradually changed its business model to provide IT solutions. In 2011, 60 employees generate revenue of about 4 Million € by serving customers in multiple industries, i.e., automotive, banking, trade, media, and public administration. ALPHA has about 50 customers per year. ALPHA pursues the concept of 'Integrating IT & Business', which stands for the integration of hardware, software, and service to fulfil the customer's business needs. To improve the efficiency of its business processes, ALPHA started a company-wide program to document and standardize processes in 2011. ALPHA leadership agreed to allow us to conduct this research with their personnel because they did not yet have a risk management process., and ALPHA practitioners were willing to work with us to develop a and validate a risk management process.

3.3 Data collection

The qualitative data were data were collected through interviews and observations in workshops with practitioners. Archival data came from bid proposals, project calculations, deal qualifications, risk assessments, design documents, user guides and contracts from several customer engagements. The data showed details of existing informal risk management activities (not formalized processes) and provide evidence of a number of risks across multiple cases. Interviews and workshops were conducted to deepen our understanding of risk management activities and to discover (new) risks.

In twelve interviews (09/2009-03/2010), we discussed five of ALPHA's IT solution engagements with the same executive vice president and an employee from a functional department in each interview. The foci of these discussions were the lifecycle and supporting processes of IT solutions, and the risks and problems that occurred in each engagement.

We conducted seven additional interviews and two workshops (05/2011-10/2011) to analyse existing risk management activities and to provide evidence of further risks. All of the interviews were held with the same executive vice president and the sales manager. In one interview, a third interviewee, an employee from the functional department participated. Participants of the two workshops were the same executive vice president, the sales manager, and two employees from the functional department (for each workshop). While interviews were conducted to understand the risk management activities, workshops were conducted to co-operatively develop the artefacts: In the first workshop, we developed the risk management process. In the second workshop, we developed the risk taxonomy. Details on the exact process will be given in chapter 4. The workshops were four weeks apart in time. In between those workshops, the practitioners addressed us with the concern that the process can help them with organizing their risk management but that they still overlooked many unanticipated risks, wherefore we synthesized a risk taxonomy in the second workshop. Except for the evaluation (cf. 5.4), interviews and workshops typically lasted between 1,5h and 3,5h.

4. Deriving a risk management process for IT solution providers

4.1 Awareness

When we started in October 2009, we discovered that risk management at ALPHA was not a formalized process and risk management activities were performed ad hoc. In interviews we found that employees are oftentimes even not aware of the existence of risk management. In order to gain an overview of ALPHA's activities and with our background from literature, we tried to match ALPHA's risk management activities to the general risk management process suggested in 2.2.

- In some cases, *risk identification* activities took place in the bid phase of a potential customer engagement. Those activities were performed in a brainstorming session and are supported by a basic checklist (nine risks divided including contract and technical risks). According to the practitioners, the main challenge at this point is the limited scope of the risk checklist.
- If the former activity was carried out, a *risk analysis* was occasionally performed next. In this activity, the probability of occurrence (low, medium or high) and the impact in terms of costs for

additional man-days that are required to fix the situation in case a risk occurs are estimated. We observed a high dependency of the risk assessment results on the personal opinions of the expert.

- We found that *risk management* would be another risk management activity. In this activity, the sales manager makes the decision whether to accept a risk or not. The practitioners told us that risk management is exercised ad hoc and often unconsciously. There existed no risk management plan and consequently no possibility to control the execution of risk management actions effectively.
- At ALPHA, the responsibility of *risk monitoring* is transferred from the sales manager to the project manager. However, if performed at all, only few risks are monitored in reality. A project manager decides himself on the priority of the risks. Status reports were communicated to the sales manager per email on an irregular basis and only in case a risk sharpens.

To sum up, we diagnosed that ALPHA performed risk management activities to some degree. We found the following immediate problem: Practitioners were unaware of the complete risk management process and there existed no documentation on how to perform risk management activities.

4.2 Suggestion

As a result form the diagnosis phase, the researchers reviewed literature on risk management processes for medium-sized IT solution providers. From neighboring disciplines (cf. 2.2) and with the help of the practitioners, we could derive the following requirements:

R1) The risk management process should consider the particularities of the medium-sized IT solution providers, i.e., scarcity of resources, short decision paths, multiple roles of employees (Knöpp 2005, Prautsch 2000, Taylor & Macfarlane 2006).

R2) The risk management should be described on an adequate level of detail to avoid misunderstandings when implemented in medium-sized organizations (Knöpp 2005, Taylor & Macfarlane 2006)

R3) The risk management process should be designed in such a process activities can be flexibly combined and altered (Knöpp 2005, Taylor & Macfarlane 2006).

R4) "The process should be easy to comprehend and implement" (From the field)

R5) "The risk management process should be accompanied by checklists to reduce complexity" (From the field)

R6) "The risk management process should be practicable and "livable" (From the field)

Implementing a risk management process fulfilling those requirements was seen by the researchers and practitioners as the desired future state. The plan was then to co-operatively develop a risk management process for ALPHA, which fulfills the above mentioned requirements.

4.3 Development

Based on existing risk management activities and literature, the team designed a risk management process for ALPHA in a workshop. The workshop procedure was as follows: We collaboratively sketched a process model as well as possible inputs and outputs of process phases.

The risk management process we derived in the workshop consists of six phases and is defined as a stage-gate process, where phases are followed by „gates". A gate is a filter based on which stakeholders decide whether to continue with the next process activity or not (Cooper & Kleinschmidt 2001). Also, the risk management process is circular, i.e., activities are repeated on a regular basis.

1) A *preliminary risk identification* phase takes place in the pre-bid phase. It serves as a first evaluation of risks and is mainly based on the invitation to bid. This activity is important since the bid process itself is resource- and time-consuming and should only be started when the preliminarily identified risks are considered acceptable. Since often very short deadlines are set for a bid response, this process step needs to be executed in short terms. The preliminary risk identification activity is followed by the first risk gate, which is only passed when the estimated overall risk is acceptable. The preliminary risk identification is executed by the sales manager.
2) The *risk identification* phase takes place in the bid phase. In contrast to the former activity, the risk identification is more detailed and a risk catalogue is developed by the management and functional departments. The risk catalogue development can be supported by a comprehensive risk checklist.

3) In the *risk analysis* phase, the probability of occurrence and impact are assessed for each identified risk item. Risks interdependencies and interactions are further assessed as compound risks. Because of the resource scarcity of medium-sized organizations, we opt for an expert-based technique for the risk analysis activity. Experts from the management and functional departments are supposed to evaluate the probability of occurrence of each risk on a three-level scale: "low" corresponding to a probability inferior to 15%, medium corresponding to a probability between 15% and 30% and "high" corresponding to a probability of occurrence higher than 30%. For every risk experts are then supposed to estimate costs of additional man-days required to deal with the consequences in case a risk occurs. The next gate will be passed when the overall risk level of a bid is acceptable.
4) In the *risk prioritization* risks are classified into three classes ("A", "B" and "C") according to their exposure (probability of occurrence multiplied by impact). "A"-risks are the most critical risk that must be continuously monitored. "B"-risks represent probable risks and should also be monitored. "C"-risks might be neglected in the further risk activities due to reasons of efficiency.
5) In the *risk management* phase, a plan for addressing each risk item is created. Possible risk management strategies include procuring extra information, risk avoiding, risk transferring, risk mitigation, or risk acceptance (Boehm 1991). According to practitioners risk transferring to the customer is the most frequent strategy employed. In one project, for example, ALPHA identified a risk related to the specification of software interfaces from a third party. The interfaces were not yet specified and ALPHA could not guarantee the timely go-life of the IT solution. Thus, as the customer was a large car-manufacturer, ALPHA had the car manufacturer exert pressure on the third-party software provider. Moreover, as a result of the risk management phase, a risk plan is developed. The risk plan includes a prioritized list of the risks with management strategies for each risk (or at least for each "A"-risk) as well as the current and the target risk exposure. The risk management strategies are then implemented.
6) The *risk monitoring* phase begins with the actual project phase, where the IT solution is designed and developed, and is continued during the integration and operation phase. It ends with the end of the lifecycle of the IT solution. Risk monitoring involves tracking changes in the risk exposure of at least the "A"-risks, tracking the progress toward resolving risks and taking corrective action where needed. Status reports about at least the "A"-risks should be made in a standardized form which would contain the name of the risk factor, the initial, current and target risk exposure, and, when necessary, comments of the project manager on actions taken to resolve this risk items.

A graphical overview of the risk management process as well as its integration into the lifecycle phase of the IT solution is given in Figure 3. We see the risk management process as a circular activity. Risk identification, prioritization, and analysis activities should be carried out on a regular basis during the project and operational phases.

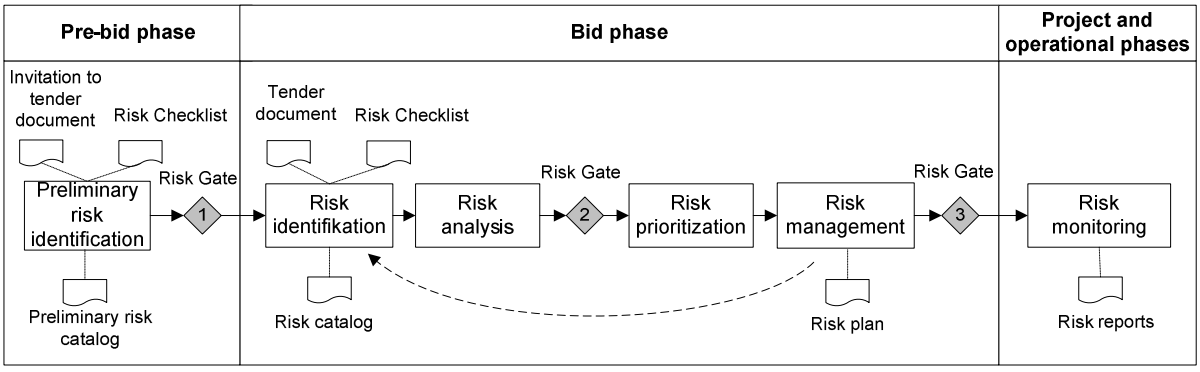

Figure 2. A risk management process for medium-sized IT solution providers

In the following, we briefly describe some adaptations we made for the implementation of the risk management process at ALPHA. Those adaptations were performed due to particular characteristics of ALPHA's organization, which we do not find useful to generalize. The general schema of the risk management process is the same. However, the preliminary preliminary risk identification phase was subdivided into two subphases due to organizational reasons: At ALPHA, the sales department and the functional department separately identify business risk and technical risks in two subphases. Only when both departments come to the conclusion that low risk is involved with an invitation to tender

independently, a tender document is analyzed in more detail in the actual risk identification phase. Other than described above, the risk management phase is followed by three risk gates instead of one since the sales department, the functional department and managment approve the risk plan independently before the contract negotiation begins at ALPHA.

4.4 Evaluation

Following the first field trials of the new risk management process, we interviewed practitioners about their experience with and attitude towards the new process, paying particular attention to the requirements we had previously derived. The practitioners reported that the process is suited to ALPHA's organizational culture, and can be performed readily within ALPHA as a medium-sized IT solution provider (R1). With regard to R2, the practitioners appreciated the "straight-forwardness" of the process and found it easy to understand and implement. With the additional supporting documents we wrote for the process (not included here due to reasons of space), practitioners have a detailed documentation at their fingertips (R3). Giving the example of the adaptation of the process to the organizational characteristics of ALPHA, the process reveals itself flexible to be adapted for medium-sized IT solution providers (R5).

However, we could not meet R4 and not fully meet R6 in the first cycle. Although the practitioners appreciated our work, they constantly asked us to provide them with information on "which risks really occur in IT solutions" and demanded a risk checklist: Without a checklist, "the process would only be half as useful as with a checklist as foundation". As literature proved that a risk checklist is a core element of a risk management approach (Boehm 1991, Lyytinen et al. 1998), we decided to work with the practitioners to derive a taxonomy of risks for IT solutions in the second research cycle.

4.5 Conclusion

The pilot tests of the new risk management process at ALPHA demonstrated how medium-sized IT solution providers could transform the risk management processes to support the IT solutions business model. However, we failed to fulfill R4 and R6 in the first design science cycle: a) we could not answer the question of which risks IT solution provider must address; and b) practitioners claimed that our process could be more "livable" and "useful" if a checklist were derived.

Other findings include: Five of the phases included in our process can be found in literature on general risk management or in neighboring disciplines. However, we find that in a setting where providers take part in bidding processes, a preliminary risk identification is required to decide from a risk perspective whether to answer to an invitation to tender or not. Another finding is that risk management does not start with the beginning of a project, but already in the (pre-)bid process. To be more concrete, risk management phases 1-5 should already be performed before the project begins.

5. Developing a taxonomy of IT solution risks

5.1 Awareness

As we already knew the goal of the design science cycle (deriving a risk checklist for IT solutions to make the risk management process more "livable" and "useful"), we focused on the characteristics and the environment of IT solutions to find important domains risks stem from. From two interviews and from analyzing six of ALPHA's IT solution engagements, we could identify the following domains relevant in IT solution risk management: value-added network risks, outsourcing risks, modularization risks, project risks, service risks, and customer risks.

5.2 Suggestion

As a result form the awareness phase, the researches performed an intense literature review on IT solution risks. The literature review was carried out according to the guidelines by Webster and Watson (2002). To make the risk taxonomy holistic, we analyzed multiple domains to include risks for all components of an IT solution, all lifecycle phases of an IT solutions as well as special

characteristics, e.g., risks stemming from operations, value-added networks, and the customer-provider relationship. Due to the multitude of domains covered, we did not focus on specific journals but made use of databases. Five major databases were included in our research: Science Direct, Emerald, Springer, Google Scholar and the Software Institute Database. Search words were: "risk", "integrated solution risk", "it solution risk", "customer solution risk", "service engineering risk", "product service system risk", "value-added network risk", "modularization risk", "it project risk", "contract risk", "modularization risks", "service risks" and "customer risks". For each search word, we read the titles of the first 100 results (sorted by numbers of citations). If the title was promising, we read the abstract and when the abstract was promising the full paper. From fruitful articles, we made a backward research to find prior articles (cf. Webster & Watson 2002). Moreover, we included articles we knew beforehand (mainly German articles). In sum we drew on 182 abstracts and 90 full papers. Sources included in the taxonomy are, e.g., Boehm (1991), Brady et al. (2005), Erkoyuncu et al. (2011), and Ward & Chapman (1995), Windahl et al. (2004).

From the literature review, we could identify 179 risks (after elimination of duplicates). We added risks if the pertained to any component, the lifecycle or a special characteristic of IT solutions. We then categorized the identified risks into groups. Our idea was to make the categorization taxonomic to avoid confusion due to multiple occurrences of risks in different categories. A taxonomy is a classification scheme of artifacts where artifacts are attributed to one and only one category (White & Edwards 1995). We started with the following categories: Value-added, outsourcing, modularization, project, service, and customer risks. However, as the number of risks was highly unequal from category to category, we enlarged the result groups to market risks, financial risks, technological risks, business risks, value-added network risks, modularization risks, project management risks, pre-project risks, project risks, operational risks, contract risks and customer risks. Then, based on the idea of IT solutions as described 2.1 and after two more iterations, we finally came to a taxonomy of four top categories, namely, environmental risks, provider risks, it solution risks, and customer risks, including 13 sub categories. An extract of our taxonomy can be found in Table 1.

1. Environmental risks	
1.1. Market	e.g. lack of market acceptance; new market entrants
1.2. Financial	e.g. uncertainty in discounting and inflation rates
1.3. Technology related risks	e.g. emerging technologies; disruptive innovations
2. Provider risks	
2.1. Business risks	e.g. long time-to-market; high degree of novelty
2.2. Modularization	e.g. cherry-picking by customers/competitors; unbundling
2.3. Supplier/ Value-Added Network	e.g. supplier's failure to deliver; no cooperation between vendors
2.4. Structural risks	e.g. lack of experience with IT solutions
3. IT solution risks	
3.1. Project Management risks	
3.1.1. Management risks	e.g. improper definition of roles and responsibilities; poor control
3.1.2. Requirement volatility	e.g. instable/ incomplete/ unclear/ uncertain requirements
3.1.3. People-related risks	e.g. internal resistance to change; inertia and fear of innovations
3.2. Pre-project risks	
3.2.1. Tendering	e.g. wrong choice of negotiations partner; poor bid quality
3.2.2. Contracting	e.g. inflexible/ incomplete/ immeasurable contracts
3.3. Project risks	
3.3.1. Analysis	e.g. market dynamics not understood; incorrect offer definition
3.3.2. Conceptualization	e.g. unfeasible requirements; unrealistic project objectives
3.3.3. Design and Development	e.g. lack of know-how; little flexibility for design changes
3.3.4. Integration/ Introduction	e.g. lack of user cooperation
3.4. Operational and end of lifecycle	
3.4.1. Operation and Maintenance	e.g. load increase in maintenance service systems; external failure
3.4.2. Evolution	e.g. no evolution or improvement process planned
3.4.3. Disposal/ Renewal	e.g. uncertainty of future environmental/ data security legislations
4. Customer risks	
4.1. Customer organisation risks	e.g. opportunistic customer behavior; lack of client trust
4.2. Customer relational risks	e.g. tardiness in transmitting information; loss of customer input

Table 1. A taxonomy of risks for IT solutions (excerpt)

Providing the practitioners with an IT solution risk taxonomy to make the risk management process more "livable" and "useful" was seen as the desired future state. Having derived a taxonomy of IT solution risks from literature, the plan was to co-operatively validate the taxonomy in practice and to add/ identify those risks that were of relevance for ALPHA's business model.

5.3 Development

In a workshop, we presented the taxonomy of risks to the practitioners. With the practitioners we analyzed the risks one by one with regard of its relevance for ALPHA's business model. After having analyzed about 40 risks items the team, however, came to the conclusion that all risks items were of relevance in some way. We then restarted and attributed an importance flag to the risks items. Those risks that were pivotal for ALPHA were attributed "A", risks that needed to be monitored in every IT solution project were attributed "B". All other risk items were attributed "C". In a next step, we asked the practitioners to add additional risks they could think of and mark them analogously.

The practitioners added three new risks items. The whole list then summed up to 182 risk items. Among these 182 risks were 33 found to be "B"-risks and six to be "A"-risks (All "A" and "B" risks can be found in the appendix). Among the "A"-risks were the following: (1) failure to manage end-user expectations, (2) insufficient documentation of post-contract arrangements between customer and provider; (3) inaccurate estimates of needed resources; (4) no planning or inadequate planning of the project; (5) high level of project complexity; (6) risks caused by a high intensity of customer integration and involvement. Risk 2 was not found in literature but was identified by the practitioners.

5.4 Evaluation

ALPHA now performs risk management according to the process reported above using the taxonomy synthesized during this research. After the revised process was carried out for a little less than a month, we interviewed the practitioners about their experiences with and attitudes about the process. We conducted three unstructured interviews (15, 20, and 30 minutes respectively). The opening question was about advantages of the new process and taxonomy. One practitioner stated, "The process would only be half as useful as without a checklist as its foundation." Several practitioners reported that risk identification in the pre-bid phase could be performed more quickly (with regard to expensed time) when they used the taxonomy than when they did not, so ALPHA could scan and respond to more invitations to tender in the same time. The executive vice president reported that, with the structured process and the taxonomy, he could give some risk identification and assessment tasks to a less experienced co-worker as he was more confident in the results derived with our process than before with no structured process. Also, one practitioner stated that the structured process would avoid communication misunderstandings.

More evaluation results with regard to the taxonomy are as follows: All interviewees acknowledged that the taxonomy (the version consisting of 39 risk items) is "complete" and "covers all important risks for [ALPHA]". One interviewee, who was a project member not previously involved in our research, could not think of additional risk items important to ALPHA either. More comments from the interviewees were "A taxonomy that is too detailed is not useful, as it would consume too many resources to work through all of the risk items" and "the taxonomy is especially useful as we now have for the less experienced employees examples of the risk that are important to us". With regard to the process derived in the first design science cycle, the taxonomy serves as input in the preliminary risk identification phase (phase 1) in the pre-bid phase and in the risk identification phase (phase 2).

5.5 Conclusion

Our intervention was called "successful" in terms of applicability as practitioners now perform risk management for each (potential) customer and as practitioners have a structured risk management process and documentation at their fingertips. As practitioners report that risk identification can be performed more quickly, that less communication misunderstandings occur, and that the executive vice president gave some risk identification and assessment tasks to a less experienced co-worker, we conclude that the risk management process is carried out at ALPHA.

Findings with regard to the taxonomy include: IT solutions cover a large number of domains (e.g. value-added networks, outsourcing, modularization) and consequently are particularly risk-prone. Nonetheless, we find that large risk taxonomies such as our original risk taxonomy consisting of 182 risks are not useful in a practical context. Practitioners need manageable checklists consisting of the most important risks which let them allow performing tasks efficiently and without large resource expenditure. Also, a large number of important risks for IT solution providers stem from customer-integration. Thus managing the customer seems to be critical in IT solutions. We also discovered a new pivotal risks not found in literature (to the best knowledge of the authors), namely "insufficient documentation of post-contract arrangements between customer and provider". Moreover, we find that a checklist can provide less experienced employees with practical examples on which lists are important and that checklists make risk identification "more efficient and transparent overall".

6 Discussion

The proposed risk management process was informed by the academic literature on risk management, and was adapted in cooperation with practitioners to fulfill the requirements of medium-sized IT solution providers. Both a scarcity of contributions on risk management for IT solutions in literature (Brady et al. 2005, Windahl et al. 2004) and practitioners demanding for risk management approaches in the IT solution context show that we tackle an important class of problem.

From our research, we came to the following main findings: First, where developers of commodity products tend to focus on risk management during development and marketing, IT solution providers must perform risk management activities over the whole IT solution lifecycle, from planning to end-of-life. Importantly, risk management does not start with the beginning of the project phase as often claimed in literature, but already in the pre-bid phase. Second, although medium-sized organizations have few resources in place, process standardization and documentation can be useful and is even asked for by practitioners. Nonetheless, processes have to be "simple", "livable", and "well-documented". Third, customer-related risks belong to the top risks for IT solution providers. The findings lead us to the conclusion that risk management for IT solutions is similar to risk management as described in existing standards and guidelines (e.g., ISO 30000, ITIL) however, that some special characteristics have to be accounted for to implement existing guidelines in the solution context and to adapt them to medium-sized organizations.

In this research, we present two artifacts: a risk management process consisting of six phases, including preliminary risk identification, risk identification, risk analysis, risk prioritization, risk management, and risk monitoring as well as a taxonomy of IT solution risks consisting of 182 risk items. From our knowledge of other IT solution providers, we argue that ALPHA is an exemplar for a typical medium-sized IT organization and that our risk management process and risk taxonomy derived cooperatively with ALPHA is a generalizable solution for medium-sized IT solution providers.

With regard to the validation of our results we find that both the risk management process and the taxonomy are in use at ALPHA. Moreover, we found the following advantages from interviews: The pre-bid risk identification can be performed more quickly (with regard to expensed time) and more invitations to tender can be scanned in the same time. The executive vice president reported that he gave some risk identification and assessment tasks to a less experienced co-worker as he is more confident in the results derived with our process than in results derived with no structured process.

For academics, our research has several implications. First, we proposed a risk management process for medium-sized IT solution providers transforming from product or service organizations to IT solution providers. This is a major contribution since existing approaches in literature are not adapted to the special IT solutions characteristics. Also, existing approaches do not consider risk management activities in the pre-bid and bid phases. Second, we derived an IT solution risk taxonomy filling in a gap in literature where a unified taxonomy has been lacking.

Managerial implications of our research are the following: First, we provide a risk management process and an IT solution risk taxonomy readily applicable for practitioners. Second, we show how the transformation process from a product or service organization to an IT solution provider can be

performed for the risk management. Third, we find that process standardization can also be useful in medium-sized organizations for multiple reasons: Process standardization helps to increase process efficiency, avoids communication misunderstandings and allows less experienced employees to perform otherwise too complex tasks.

That said, there are also some limitations to our research: With regard to the IT solutions risks taxonomy, more research is needed to determine to what extent the proposed structure is taxonomic. Also, we introduced a change in ALPHAs organization and measured the successfulness in terms of applicability of our new risk management process in interviews. It might be useful to quantitatively validate our results. Future directions for research include more exemplar instances in other organizations and industries. It would be interesting to research if the process is also applicable for small or large IT solution providers. Moreover, a design theory to guide practitioners to successfully design their own risk management processes for their particular IT organization would be useful.

7 Conclusion

We performed two design science cycles to develop a risk management process for medium-sized IT solution providers as well as a taxonomy of risks which serves as checklist in the risk identification phases. The risk management process consists of six phases, including preliminary risk identification, risk identification, risk analysis, risk prioritization, risk management, and risk monitoring. Our original taxonomy of IT solution risks consists of 182 risk items, which we reduced into a manageable 39 risk-items list for ALPHA. Top-level risk categories included in the taxonomy are environmental risks, provider risks, solution risks, and customer risks.

This paper contributes a novel single expression of the risk management process for medium-sized IT solution providers as well as taxonomy of IT solution risks. We showed how the transformation process for a commodity provider to an IT solution provider can be performed and how the desired future state might look like. The risk management process and the taxonomy are in use at ALPHA.

This contribution is intended to fill in a gap where a risk management process for medium-sized IT solution providers has been lacking. We hope that practitioners can use our results for their organizations. However, we also point out that more rigorous research might be useful to further explore the risk management process' acceptability in other organizations. Researchers might use our contribution as a starting point to open up the new field of risk management for IT solution providers.

References

Boehm, B. W. (1991). Software Risk Management: Principles and Practices. IEEE Software, 8 (1), 32-41.

Böhmann T., P. Langer, and M. Schermann. Systematische Überführung von kundenspezifischen IT-Lösungen in integrierte Produkt-Dienstleistungsbausteine mit der SCORE-Methode. Wirtschaftsinformatik, 50 (3), 197-207.

Brady, T., A. Davies and D. M. Gann (2005). Creating value by delivering integrated solutions. International Journal of Project Management, 23 (5), 360-365.

Burianek, F., C. Ihl, S. Bonnemeier and R. Reichwald (2007). Typologisierung hybrider Produkte. Ein Ansatz basierend auf der Komplexität der Leistungserbringung. Working Paper 1, Technische Universität München, München, 2007.

Cooper, R. G. and E. Kleinschmidt (2001). An investigation into the New Product Process: Steps, Deficiencies, and Impact. Journal of Product Innovation Management, 3 (2), 71-85.

Erkoyuncu, J. A., R. Roy, E. Shehab and K. Cheruvu (2011). Understanding service uncertainties in industrial product-service cost estimation. International Journal of Advanced Manufacturing Technology, 52 (9-12), 1223-1238.

Herzfeldt, A., R. O. Briggs, A. Read and H. Krcmar (2011). Towards a Taxonomy of Requirements for Hybrid Products. 44th Hawaii International Conference on System Sciences, Kauai, HI, USA, 1-10.

Knöpp, M. D., H.-J.; Altwasser, V. (2005). ITIL im Mittelstand einfach erfolgreich umsetzen. WEKA MEDIA, Kissing, Germany.

Lyytinen, K., L. Mathiassen and J. Ropponen (1998). Attention shaping and software risk-A categorical analysis of four classical risk management approaches. Information Systems Research, 9 (3), 233-255.
Prautsch, W. (2000). IV-Controlling in kleinen und mittleren Unternehmen (KMU). In IV-Controlling: Konzepte, Umsetzungen, Erfahrungen. (Ed, Dobschütz, L. v.; Barth, M.; Jäger-Goy, H.; Kütz, M.; Möller, H.-P.) Gabler, Wiesbaden, Germany, p. 723-746.
Stahl, B. (Ed.) (2008). The Ideology of Design: A Critical Appreciation of the Design Science Discourse in Information Systems and Wirtschaftsinformatik. Physica Verlag, Heidelberg, Germany.
Takeda, H., P. Veerkamp, T. Tomiyama and H. Yoshikawa (1990). Modeling Design processes. AI Magazine, 11 (4), 37-48.
Taylor, S. and I. Macfarlane (2006). ITIL small-scale implementation. Stationery Office, Norwich, UK.
Tuli, K. R., A. K. Kohli and S. G. Bharadwaj (2007). Rethinking Customer Solutions: From Product Bundles to Relational Processes. Journal of Marketing, 71 (3), 1-17.
Ward, S. C. and C. B. Chapman (1995). Risk-management perspective on the project lifecycle. International Journal of Project Management, 13 (3), 145-149.
Webster, J. and R. T. Watson (2002). Analyzing the past to prepare for the future: Writing a Literature Review. MIS Quarterly, 26 (2), 13-23.
White, S. and M. Edwards (1995). A Requirements Taxonomy for Specifying Complex Systems. 1st International Conference on Engkineering of Complex Computer Systems, Southern Florida, USA, p. 373-376.
Windahl, C., P. Andersson, C. Berggren and C. Nehler (2004). Manufacturing firms and integrated solutions: characteristics and implications. European Journal of Innovation Management, 7 (3), 218-228.

Appendix 1 Checklist for IT solution risks (for categories refer to 5.2)

Level A-risks:
- Failure to manage end-user expectations
- Insufficient documentation of arrangements with customer
- Inaccurate estimates of needed resources
- No planning or inadequate planning
- High level of project complexity
- High degree of user involvement

Level B-Risks
- Volatility of the labor market
- Volatility of market prices
- Lack of reputation
- Lack of credibility
- Utilization of new/ immature technologies
- Long time-to-market
- Cherry-Picking by customers/competitors
- Difficulties in management of the increasing level of organizational complexity
- Lack of experience with IT solutions
- New partnering and consulting competencies required
- Lack of technical personnel and support personnel
- Lack of effective project management skills
- Poor or nonexistent control/ poor risk management
- Important project resources not available
- Insufficient/inappropriate staffing
- Instable requirements
- Incomplete requirements
- Unclear requirements
- Uncertain requirements
- Changing project scope or objectives
- Lack of required project knowledge skills
- Lack of training and education of the project personnel
- High staffing volatility
- Incomplete contract
- Immeasurable contract
- Failure to identify all stakeholders
- Customer's inability to express needs and wishes
- Customer's inability to express requirements
- Lack of management involvement from the customer side
- Invalid/ incorrect requirements
- Lack of know-how

- Underestimated development time
- Not foreseen development costs
- Lack of effective development process or methodology
- Insufficient testing
- Uncertainties in the characteristics of the failure process
- Unjustified customer expectations with regard to cost and quality
- Customer bargaining power
- Non respect of deadlines
- Low quality information flow from the customer to the provider
- Challenges with information sharing and transparency
- Loss or a distortion of customer input

The full taxonomy including categories and explanations including all sources is available upon request from the authors.