The Emergence of Information Infrastructure Risk Management in IT Services

Lars Öbrand
Umeå University
lars.obrand
@informatik.umu.se

Nils-Petter Augustsson
Umeå University
nils-petter.augustsson
@informatik.umu.se

Jonny Holmström
Umeå University
jonny.holmstrom
@informatik.umu.se

Lars Mathiassen
Georgia State
University
lars.mathiassen
@eci.gsu.edu

Abstract

Failure to understand, identify, and manage risk is often cited as a major cause of IT problems. While the project is the preferred level of analysis in most IT risk management research, IT is becoming increasingly infrastructural, and there is therefore a need to adapt risk strategies beyond the project level. In this paper, we explore how risk management practices in a successful IT service provider group emerged over time as the group coped with infrastructural dynamics and complexities. Drawing on Orlikowski's practice lens, we investigate actual practices and possible options related to risk management as rapid technological and organizational changes resulted in increased infrastructure management challenges for the IT service provider. Our research contributes to the IT risk management literature by applying risk theory to service management in the infrastructural domain and by moving beyond the project as level of analysis.

1. Introduction

Over the past several decades, information technology (IT) has become one of the most powerful factors shaping firm level processes and services and IT capability has therefore become both strategically and operationally essential to contemporary firms [1]. Following the increasing importance of IT in contemporary firms, there is growing consensus among researchers that IT strategy should be understood as cross-functional as it encompasses products, processes, and human resources, and is intertwined with corporate strategy [2].

Despite the strategic potential of IT, recent research shows how even the most proficient managers have difficulty handling IT as an organizational resource. They use decision milestones to anticipate outcomes, risk management technologies to prevent disasters, and sequential iteration to make sure everyone is performing according to plans. Still, a review of the IT risk management literature indicates how the factors affecting IT project outcomes have not been systematically examined [4]. To date, prior research has mainly focused on empirically categorizing the sources and types of risks associated with IT projects to better prioritize and assess the exposure and losses that may result (e.g., [3], [4]). Failure to understand, identify, and manage risk is often cited as a major cause of IT project problems such as cost and schedule overruns, unmet user requirements, and the production of IT systems that do not provide business value [3], [5]. While various risk checklists (e.g., [3]) and frameworks (e.g., [6]) have been proposed, the key dimensions associated with IT risk – including assessments of project performance on the one hand, and assessments of performance beyond the project timeline on the other hand – remain largely on the project level of analyses. There is thus little knowledge on how risks are managed in relation to contemporary infrastructure issues. However, it has become increasingly critical to understand how IT is intertwined with already existing systems, practices, mitigating and satisfying the diverse needs of a larger number of actors (see e.g., [7]).

For these reasons, this paper is focused on the emergence of side-effects, paradoxes, ambiguity and general difficulties in dealing with IT risks in the context of infrastructure management. Against this backdrop, our research question is: how do IT professionals identify and manage risks emerging from evolving IT infrastructures?

We have investigated these issues through a case study at Weilgo, a large IT consultancy firm. Using semi-structured interviews, documentation and workshops and drawing on Orlikowski's practice lens approach, we have explored the emergence of risk identification and management practices by a team of IT professionals over a period of ten years [8]. We also

investigate the formal project risk management method at Weilgo to understand it shaped the team's identification and management of risks. Weilgo is one of Sweden's largest IT consultancy firms with 37 offices throughout the country. At one of these, we studied a team that successfully has provided infrastructure services for over a decade. The team has faced technological, organizational and environmental changes impacting the ways in which it worked to ensure continuous success. As part of a consultancy firm, practically all work being done by the team is based on billable hours within the scope of management, maintenance or development projects. As a result, team members always have to contribute to the project at hand in the best possible way, making long term, cross-project issues difficult to manage.

The rest of the paper is organized as follows. The next section presents our research approach. This is followed by a section presenting relevant literature on software risk management, information infrastructure and Orlikowski's practice lens approach. We go on to present the enacted risk management practices by the Weilgo development team, divided in three phases in accordance with the evolving infrastructure. Finally, we discuss the results along with implications and conclusions.

2. Method

This is an interpretative case study with data collection in the form of semi-structured interviews and a workshop [9]. The study is hence based on the respondents' perceptions and the interpretation of the researcher [10]. The study involved five initial interviews with people at Weilgo, complemented by a total of six follow-up interviews with the three key members of the team. Furthermore we have accessed e-mail documentation spanning the ten year period, as well as other documentation in the form of agreements, presentations and project documentation (see table 1 below for more details). In addition, one of the researchers is an industrial PhD student working for Weilgo. We thus had dual goals for the research project; to contribute to research as well as to improve practice. To bridge these dual goals, we adopted Mathiassen's recommendation to organize projects as a loosely coupled system of agendas; as a shared space in which research efforts and practice initiatives can blend in a fruitful way [11]. We started the research process with a workshop, in order to make sure the dual goals were aligned, and after the interviews completed, we transcribed, analyzed, and reported back the findings to Weilgo, again to validate that the dual goals were met.

The idea of addressing the link between the evolving infrastructure and the ways in which risk management practices have evolved was triggered by the discussion in the workshop with Weilgo staff. Managers at the top level and functional level attended the workshops. The data collected in the interviews covered many different areas of interests as we strived to contribute to the team's solution of a real-world problem. The interviews were guided by the constructs of infrastructure and emergent risks and were conducted as an iterative process towards saturation.

Table 1 Description of the data sources

Data Sources	Description
Focus Group	One focus group session was conducted with 3 participants from the team. During this session the insider researcher and one of the outsider researchers (moderator) participated. The session was recorded and transcribed.
Formal interviews	Eight formal interviews were conducted. The interviews lasted for approximately one hour each. The interviews were recorded and transcribed.
Open-ended, semi-structured interviews	The insider role's daily informal discussions concerning the information infrastructure services allowed for insight in everyday practices at the company.
Projects proposals	Due to the insider role the research project had access to all project proposals. 10 proposals were collected from the time period, including approved and rejected proposals.
Project and maintenance contracts	The contracts during this time period were collected, in total 6 contracts.
Meeting Minutes	The formal meeting minutes from monthly and weekly meetings with the management group and internal team group were collected, in total 200 meeting minutes.
Email conversations	Email conversation between the project and maintenance manager (insider researcher) and internal and external stakeholders during the time

	period. Amounts to approximately 1150 emails.
Presentations	The various presentations used to describe the information infrastructures services to internal and external stakeholders during this time period, in total 40 presentations.

Data analysis was performed by first reflecting upon the respondents' answers and then clustering these into similar themes using atlas.ti software for coding purposes. Atlas.ti was also used to sort, search and code the documents. After results were reported back to Weilgo in the form of a report, a follow-up meeting was arranged where the results were discussed. The purpose with the report was to create understanding for whether or not the findings were correctly interpreted.

3. Risk Management

Risk management is about uncertainty regarding future events. Thus, risk management issues regarding the development and use of IT has been, and still is, a relevant topic in IS research and practice alike. There is a rich and differentiated literature on risk in our field, of which a large part is focused on software risk management and software development projects [3], [4], [5], [12], [13], [14], [15], [16], [17], [18], [19]. Most of the IS research on risk emphasize the adverse effects of risk and offer ways of identifying, and, ultimately, by the use of heuristics, techniques and tools to mitigate them. Carlo et al. note that most research has not gone beyond identifying risk factors to look at risk and control strategies at a behavioral level in socio-technical systems [20]. Furthermore, the project is the main level of analysis, considering external events, processes, and stakeholders as environmental factors [3], [4], [6], [19]. However, as IT becomes an increasingly infrastructural technology [7], [21] the relationship between IT and risk gets more complicated. Increased integration leads to more complexity, which in turn leads to new kinds of risks [22]. Hence, the need to go beyond the narrow system rationalism through a contingent, contextual and multivariate view on software risk management is recognized [14], [16]. The turbulence of business contexts, the diversity and multiplicity of stakeholders, and the evolution of information infrastructures invite researchers to reflect on the dynamics and complexities involved in the risk management approaches best suited for such complex and heterogeneous environments [16].

A useful approach to risk emergence in larger socio-technical networks has come from the work on infrastructure in IS research. Considering IT as information infrastructure rather than as information systems has become increasingly common in the literature (e.g. [23], [24], [25], [26]). In contrast to information systems, infrastructures are typically described as heterogeneous assemblages of technical and social components [25], [27]. In this research, risk plays an important part. Ciborra et al. discuss how the infrastructural character of IT contributes to new, surprising risks [24]. Also, the work of Beck [28] and Giddens [29] on risk is ushered in to the realm of IS research, and information infrastructure theory, by Hanseth (see e.g. [30]) where it is used to explain and understand side effects and unintended consequences challenging the efforts of gaining increased control and rationalization. This literature on risk in information infrastructure theory challenges the notion of risk predominant in IS research, and we share Hanseth's concern over the way in which risk is traditionally managed and agree that we need to reconsider risk as a whole [31]. This position is consistent with Carlo et al.'s call for IS researchers to look beyond the functional project level risks to carefully explain how risks emerge and are contained in larger sociotechnical networks [20].

4. Enacted Risk Practices

Drawing on Orlikowski's practice lens approach [8], we explore the risk identification and management enacted by a team over a ten year period, during which time the technology becomes increasingly infrastructural. Enactment is central to Orlikowski's approach to study technology in organizations [8]. Enactment refers to the practices of technology users as they appropriate specific technology features and produce structured patterns of action through repeated behaviors. Structures are embedded neither in organizations nor technology, and technological consequences are enacted by users rather than determined by features of the technology. Given that there are few if any causal effects [8], [32], IT is seen as an ingredient in social processes that may reflect dialectical forces operating both to promote and to oppose social change. The more malleable the technology, the greater the latitude enjoyed by users to enact social structures and work practices.

Weilgo is large IT consultancy firm with a considerable range of services, resources and products. The observed team belongs to the Application Management Department, which develops and

provides services and resources rather than products. As an IT service provider, the team can develop and manage an application code base to be adapted for different customer implementations. Keeping the implementations as standardized as possible allows for easier code base management. All development and management is carried out within the scope of projects. We describe the risks they have identified, and how they have managed them, since the formation of the team in early 2001. The risks and risk management approaches enacted by the team span three different phases, characterized by the technological and organizational context in which the team acted. We have organized the following description in accordance with these phases. For each phase, we discuss the enactment of risk management practices. We conclude the analysis by presenting the formal risk management scope and techniques offered by Weilgo as a tool to ensure project risk management.

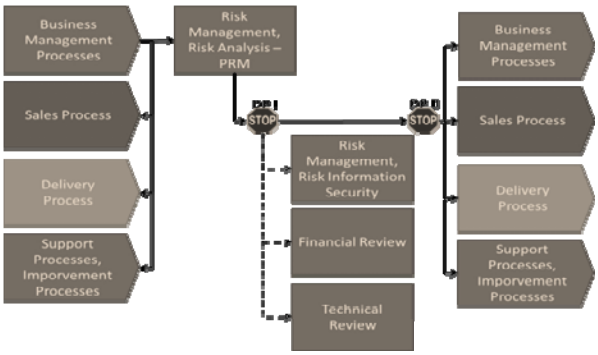

Figure 1 The risk management process at Weilgo

There is a standard for risk management at Weilgo. The risk management framework is divided into four processes. The prime process is focused on general business/assignment support, whereas the three additional sub processes focus on specific risk areas; Information Security Review, Financial Review and Technical Review. Every proposed project where Weilgo have some kind of delivery commitment goes through the same procedure in order to ensure project quality and success. The risk management process consists of six steps, each targeting phases in the delivery process - from bid to project delivery. Weilgo´s risk management framework does not stipulate the use of certain methods at all times, but give room for using various types of methods for risk assessment dependent on the type of assignment, size or risk exposure of the assignment. There are cases though when it is mandatory to use Weilgo's internal method (PRM).

Despite being detailed and thoroughgoing, the PRM documentation and questionnaires is concerned with and covers risks related to building new technology and does not cover if and how code in the project in question relates to previous or future projects. The PRM view of risk is primarily as financial risk, and its use in the organization is mainly to decide the project's price tag. The higher the financial risk for Weilgo, the higher the price. It does not help raise risk issues falling outside of the scope of the isolated project, nor does it cover issues that fall within Weilgo' s organizational borders. Furthermore, when agreed upon by a quality controller and the project group, the PRM is very seldom seen again by the project participants.

4.1. Phase 1: Tailor Made Technology

In early 2001, Weilgo was contacted by customer Alpha with a very specific idea about what kind of IT solution it needed. Alpha was a rapidly growing company, and most of the growth was a result of acquisitions, which resulted in a need for them to keep track of inventory and to find an efficient way to establish who had access to what in terms of information, systems, and processes. Alpha turned to Weilgo with an idea of using the Active Directory (AD) technology to address their challenges. Microsoft's AD is basically a catalogue which can structure and hold information, primarily about resources and security (access control). By using AD, Alpha hoped to come to grips with their information management problems. However, AD was a new technology and there was no readily available way of effectively managing the AD content. This was the major challenge for the team to tackle.

At the time, the Weilgo office consisted of only ten employees, of these two consultants were allocated as resources to this project. This was the starting point of the team. Over a period of five months they developed a console application for managing the AD using a beta version of Microsoft's .Net environment. They worked on the customer's site, in close contact the customer. The end result was an application called Tool which allowed the administrators at Alpha to manage the content of the AD. The application was tailor made in two respects. It was developed directly in accordance with the customers expressed needs, and it was developed with the sole purpose of managing AD catalogue objects.

During the implementation phase, Alpha was bought by a large, multi-national company, and the requirements changed to include a demand for any user to be able to interact with the AD. This coincided with Exchange server, and Outlook, increasingly becoming the standard solution for managing address information

in many organizations. Since Microsoft integrated AD and Exchange, the team made the decision to widen the scope of the Tool to include management of address information. This allowed them to market the Tool to a wide variety of organizations, provided they used Microsoft Exchange. At the time, the Weilgo office operated at a local level, making it important for the team to cater to a wide variety of potential customers. During the two years that followed, the two members of the team focused on selling the Tool by spending a lot of time at sales meetings with potential customers. The successful sale of Tool ensured that the members of the team survived layoffs at Weilgo in the wake of the recession in the Swedish economy.

The main risks in this phase were technological since AD was relatively new and Microsoft did not at this point offer an application for managing AD objects. By closely monitoring Microsoft's development and use of AD and related technologies, the team was able to adapt the scope of Tool at an early stage to encompass address information management. This was an important step in developing a more generic solution, thus increasing the number of potential customers. To extend their reach beyond a local level, the team also started to market Tool internally at Weilgo, actively looking to be part of projects initiated and run by other Weilgo offices.

4.2. Phase 2: Building Infrastructure Services

In 2004 a further decoupling from AD was made when the team decided to use a MIIS server (Microsoft Identity Integration Server) as a layer between Tools and the underlying systems, thus connectivity was increased. This version of Tool was chosen as the interface and workflow engine between a new internal service and the central Weilgo services offered to the firm's customers. The internal service functioned as a back-end service offering e.g. Service Desk resources, administration of mailbox accounts, access management. Tool was established as an integration technology internally at Weilgo. The use of the MIIS server increased flexibility, and although still basically a console application it was adapted to function in a larger, more heterogeneous, environment. There were competing products offering similar functionality, and the choice of Tool hinged to a large extent the team's relationship with Weilgo actors in strategically important positions. These relationships had been established while the team members promoted Tool internally. Since Weilgo is a multi-national company, this was a larger project than the group was used to. The focus on external sales gave way for setting up the roll-out and maintenance schemes for the new service. Members of the team also secured positions in the support and maintenance organization. Although Tool offered functionality initial acceptance by end users at Service Desk was relatively low due to the application interface. During this time a new team member arrived, and team roles were articulated. The new member assumed the role of project manager, and one of the original members was appointed IT architect. These roles helped focus the team's efforts as a need to manage the relationship with central services became important.

In the wake of the internal Weilgo project the team decides to rethink and redesign Tool. New generations of AD and connected technologies had opened up for new possibilities. The team made use of vision documents from Microsoft in their efforts and some important development decisions were made in accordance with those visions. The team focused on the possibility to support organizational processes. Building the application from a process support point of view entailed focus on connectivity and configurability. To mark this shift the application was renamed "Primus". The application focused on efficient integration of all systems depending on an AD or a meta-catalogue. The team marketed Primus as an integration platform, and the new interface was designed to be configurable to the needs of the end users to a much larger extent than before, the end users being a more heterogeneous category than was the case before.

All previous development had been accomplished within development projects paid for by customers, but the initial development of Primus was paid for by the team themselves, with small resources allocated by their local Weilgo office. This allowed them to develop the application free from outside requirements. Before Primus was completely developed financial issues at the office forced the team to turn their attention to other projects. To keep developing Primus the team followed the same strategy as with Tool. With every Primus implementation they tried to keep the code base as standardized as possible, making incremental changes in accordance with their initial ideas about the application properties.

4.3. Phase 3: The Portfolio Approach

By 2008 the customer base for the team has shifted. Although still working towards external customers, the team focuses mainly on being part of larger deliveries by Weilgo on a central level. To establish Primus as

the standard integration platform in Weilgo central service deliveries was seen as essential in order to ensure continuous project opportunities for the group. By participation at sales meetings and through Primus presentations at meetings and workshops internally at Weilgo the team works hard at establishing contacts with key players in the large projects. Team put effort in convincing other Weilgo departments that Primus is a better choice than the other, competing, technologies found on the market as well as within the Weilgo organization, thus becoming the go to technology in major service deliveries.

The need to establish good relationships within other departments became increasingly important. Primus's functionality made it useful in different kinds of projects, a lot of them initiated by the Infrastructure Management department as they were a key actor in large-scale outsourcing project deliveries. As part of a larger project the team is not in control over the relationship with the external customer. In these circumstances the team worked with two different sets of requirements, one from the central service and another from the external customer. As a consequence the project manager's role as representative in the larger project group became increasingly important, as well as the inclusion of new team members to manage the dual sets of requirements.

During a large implementation project in early 2009 the customer requested an end user portal in addition to the use of Primus as administrative interface for the internal Weilgo service delivery. The team was appointed to develop the end user portal which was to become the interface used by customer's employees, thus work on the Portal began in the spring of 2009. They decided to treat this as a separate project and not as a part of the Primus service delivery project. This was not an obvious choice since the Portal essentially consisted of a new interface to Primus without its own logic. By decoupling the interface from the Primus application logic it became highly configurable to the end user's preferences and needs without the constraints of the underlying layers. The Portal project ran parallel to the Primus project in what had now become an implementation programme.

After passing the test period the Primus project was suddenly terminated by the programme management. In an unrelated project the internal Service Desk at Weilgo decided to go with a competing technology for their administration of employee information and access control. Since Service Desk was an important part of the central service delivery, and organizationally situated in the same company that owned the programme, Primus was out. The Portal project, although building on the Primus workflow and integration logic, was unaffected.

For the Team, the risks in this phase are mainly of organizational character. The technology was established and they had an installed base of applications and code that was flexible enough to be adapted to different contexts with only minor development efforts. The key for the team was being able to anticipate and respond to project and central service requirements, even in projects that they were not part of. The organizational context became increasingly heterogeneous, dynamic and complex. Project decisions had ramifications well beyond the scope of the actual project, departmental interests played a part in the projects and the needs and requirements of large customers affected the standard services at Weilgo. By decoupling the layers of technology they created a portfolio of applications allowing them to be agile in a dynamic environment.

5. Discussion

Drawing on Orlikowski's (2000) practice lens framework, we have investigated the actions of the team in terms of risk management, rather than starting with viewing these practices as appropriation of formal risk management strategies. This allowed us to analyze how the team enacted emergent structures through recurrent interaction with the evolving infrastructure. The practice lens approach also allowed us to go beyond the project level of analysis. Scant attention has been directed beyond the project level in the IT risk management literature, and our effort is therefore an effort to do so. The formal risk management procedure at Weilgo, although rigorous, did not help capture the whole range of risk management practices enacted by the team over the three phases. As the infrastructure evolved through technological, organizational and social changes, so did the risks the team identified, and as complexity increased so did the divergence between the enacted risk practices and the formal ones. Looking at the actual risk practices, they were influenced by actors, events, and technologies far beyond the scope of the traditional risks emerging from single, isolated projects.

In the first phase, risks were mainly technological as the technology they worked with (AD) was new and immature in the sense there was no readily available way to meet customer requirements. Keeping close track of Microsoft's development of AD and related technologies was a vital strategy for the team to ensure

long term sustainability of the Tool. During this phase the risk management method at Weilgo (PRM) offered considerable support as it helped the team to identify technological risks. One premise behind PRM is that the technology in the project is new to Weilgo, which clearly was the case for the team in this phase.

By encompassing address information management, the team broadened the potential customer base, keeping the team safe from layoffs in the wake of the economic recession. Marketing Tool internally at Weilgo' s other offices and departments in order to further widen their market and project participation was an important strategy, which later on also paved the way for the choice of Tool in Weilgo' s internal back-end service. This kind of risk management however, was not covered in the PRM but played an important role in the trajectory of the team and their technology. It supports the view by Carlo et al (2004) that risk and control strategies at a behavior level in socio-technical systems are important.

The second phase focused on building infrastructure services and increasing connectivity through standardization and a focus on application flexibility. The team redesigned their application with support for organizational processes in mind, developing it as an infrastructure gateway with increased integration capabilities. If the service in phase one was closely connected to technology, it was now built and marketed as an integration application servicing organizational processes much more independent of the systems and technologies it interconnected. Although the IT in this phase was more mature, a close eye on the trajectory of Microsoft's technology development was important for the team as they continued to develop their code base, and services, in a way that made them competitive both within Weilgo and with external customers

As the character of the technology shifted towards the infrastructural new kinds of risks were identified and managed by the team. These, however, fell outside of the scope of the PRM. The complexity increased further as the team became part of large scale projects competing internally at Weilgo to establish Tool and Primus. Securing positions in support and maintenance between projects also contributed to the team's trajectory. Furthermore, Primus was developed outside the scope of customer projects. This supports the claim by Carlo et al that we need to look beyond the functional project level of analysis to address questions of how risks emerge in larger socio-technical networks [20]. It is also in contrast with the idea that external events, processes and stakeholders are viewed as environmental factors [3], [4], [6], [19].

In the third phase, the technology was standardized and established and the team had developed an installed base of code allowing them to make customer adaptions with only minor development efforts, the team's focus turned to manage organizational risks. As the organizational context at Weilgo became increasingly heterogeneous and dynamic, and central service deliveries became increasingly important, the team needed to adapt their risk management strategies. By decoupling the layers of technology they created a portfolio of applications, thus enabling them to act with agility as conditions changed. The main risks in this phase fall outside of the scope of single, isolated projects. The formal risk management at Weilgo is in this phase insufficient to offer any support in the identification and management of these risks.

This highlights the claim by Schmidt et al that researchers need to reflect on risk approaches in heterogeneous environments [16]. It also contrasts an approach to risk management that aims to provide ex ante risk checklists and mitigation methods. The need to move beyond the project level of analysis is further highlighted by the risks management practices enacted in this phase. This support the view of risk offered by literature on information infrastructures [24], [30], [31], but also extends risk management literature it by examining risk practices enacted in such an environment rather than using risk as a means to investigate and explain side effects and unintended consequences.

While providing infrastructure services for, and in, a heterogeneous and dynamic context, the team managed the risks they identified within the scope of more or less isolated projects. These projects were units with their own requirements, resources, actors and clearly defined borders. More often than not, these project were not set up or controlled by the team, even so, they constituted the main vehicles through which the team realized their management strategies for all risks – including those not concerning the project as such. As service providers, the team develops and manages application code bases rather than developing products, and the only way for the team to do that is through projects in which they always have to focus on customer's requirements. This being the case, long term direction and development of the applications will almost always be incremental and challenging.

A key challenge in infrastructure adaptation is balancing user value while maintaining a stable standard in infrastructure adaptation (Rönnbäck et al.,

2007). In order to keep the application code base manageable and in line with their visions, the team strove for a high degree of standardization in implementation, at the same time they were obliged to meet customer requirements in order to get the order in the first place. Meeting these dual goals affected the way in which they work within projects, requiring on-going balancing of project value with long term application and service development. In this way, by moving beyond the project as the level of analysis for risk management, we extended IT risk management theory by showing how risks not concerned with projects have important consequences for the way in which project participants work. In this sense, project external stakeholders, events and processes cannot be regarded as environmental factors [3], [12], [19]. Instead, they are part of an evolving information infrastructure with an installed base of technology and social actors all impacting the way in which projects are played out in practice. In fact, managing risk on an individual project level can lead to diffusing rather than containing risk [33]. In the case of Weilgo, the lack of cross-project risk management shows how decisions made (e.g. technological) in one project can have serious impact on other projects, the termination of the Primus project being a case in point. As it turned out, Weilgo had no risk management tools in place to identify or manage such effects.

Even though most research on IT risk focus on the adverse effects of risks, it is known that risk-taking is one of the competitive advantages of an organization [34]. Innovating necessarily entails a number of more or less unavoidable risks such as losing key personnel [35], financial risks [36], and technological risks [37]. The close link between risk and innovation is well illustrated in the Weilgo case with its forward-looking activities closely related to uncertainty and change. We could therefore observe that in order to realize an innovative potential, risk-taking was an unavoidable necessity.

Drawing on this analysis, the primary way of dealing with risks for Weilgo is by having consultants proactively making processes agile over time. During all three phases in the evolution of the infrastructural services, we saw how Weilgo rather than seeking to reduce risks continuously explored different opportunities and entertained a number of alternative routes of action. Through an active exploration of a range of possible ways forward, the innovation process was kept agile. The evolution towards a portfolio approach enabled agility – as the portfolio presented Weilgo with options to choose between and also sometimes avoid business risks.

This process of enabling agility while also reducing risk is related to the locally oriented and adaptive view of risk and innovation as proposed by Wynne (1996). In this view, the innovator is aware that the existing evolution of a particular venture is but one of many ways in which the process can be developed, and the innovator is therefore always ready to move swiftly in several possible directions. These findings support a human agency view of technology use in an organizational context, specifically supporting Orlikowski's, [8], [38] argument that technology's consequences for organizations – such as risks – are enacted in practice rather than merely embedded in risk management models.

The way in which the team identified and managed risks emerging from the evolving IT infrastructure suggests that Weilgo as a service provider organization adopted a focus oriented less toward project oriented planning and more toward cross-functional and cross-project flexibility and learning. At Weilgo, the infrastructure did not facilitate effective learning between projects or functions. In effect, the focus on projects contributed to further increase the uncertainty while inhibiting the flexibility and learning needed to systematically manage the new risks.

We argue that such understanding of the interactions between technology and organization is the foundation for managing information infrastructures. The case illustrates the continuously evolving infrastructural technology and how it evolved over the three phases – along with the events, people and processes that all together constitute a challenge from a risk management perspective. The team's strategy thus resembles Ciboria's idea of 'cultivation' where information infrastructure is understood as an organic process in which technology is allowed to drift [39]. Indeed, the infrastructure drifted over time, and so did the associated risk management practices, while the formal risk management models remained stable and hence with little consequence.

6. Conclusion

In IT risk management literature the project is the preferred level of analysis, and there is little knowledge on how risks are managed in relation to contemporary infrastructure issues. To this end we have examined how IT professionals identify and manage risks emerging from an evolving IT infrastructure by investigating the enacted risk management practices of an IT service provider team over a period ten years. Our theoretical lens allowed us to in detail examine

how risk management was enacted and related to the increased infrastructural capabilities of the technology.

The divergence between the project oriented formal risk management at the IT service provider increased as the team managed risks emerging from the information infrastructure impacting the way in which projects are played out. Risk Management is about uncertainties regarding future events. As the infrastructure evolved, becoming increasingly heterogeneous and complex, new risks emerged. The identification and management of these built on the team's ability to maintain a cross-project and cross-functional perspective.

Furthermore, as shown in the above, risk and innovation are intimately intertwined; both on an analytical as well as on an empirical level. Through bringing the concepts of risk and innovation together in an exploration of how risks are enacted by Weilgo consultants, we have been able to able to draw tentative conclusions about how different risks are encountered and dealt with on the micro level of innovation. Such a mapping of risk and risk practices may begin to fill an important gap in existing knowledge.

7. References

[1] Sambamurthy V, Bharadwaj A, Grover V. Shaping agility through digital options: Reconceptualizing the role of information technology in contemporary firms. MIS Quarterly. 2003;27(2):237–263.

[2] Bharadwaj AS. A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. MIS Quarterly. 2000;24(1):169-196.

[3] Lefebvre AL, Mason R, Lefebvre E. The influence prism in SMEs: The power of CEO's perceptions on technology policy and its organizational impacts. Management Science. 1997;43(6):856–878.

[4] Boehm BW. Software risk management: Principles and practices. IEEE Software. 1991;8(1):32-41.

[5] McFarlan WF. Portfolio approach to information systems. Harvard Business Review. 1981;59(5):142–150.

[6] Barki H, Rivard S, Talbot J. Toward an assessment of software development risk. Journal of Management Information Systems. 1993;10(2):203– 225.

[7] Keil M, Cule P, Lyytinen K, Schmidt R. A framework for identifying software project risks. Communications of the ACM. 1998;41(11):76–83.

[8] Tilson D, Lyytinen K, Sørensen C. Digital Infrastructures: The Missing IS Research Agenda. Information Systems Research. 2010;1:(December 2010):748 - 759.

[9] Orlikowski WJ. Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations. Organization Science. 2000;11(4):404-428.

[10] Walsham G. Interpretive case studies in IS research: nature and method. European Journal of Information Systems. 1995 74-81.

[11] Klein HK, Myers MD. A set of principles for conducting and evaluating interpretative field studies in Information Systems. MIS Quarterly. 1999;23(1):67-94.

[12] Mathiassen L. Collaborative practice research. Information Technology and People. 2002;15(4):321-345.

[13] Alter S, Ginzberg M. Managing Uncertainty in MIS Implementation. Sloan Management Review. 1978 23-31.

[14] Charette RN. Software Engineering Risk Analysis and Management. New York: McGraw-Hill; 1989.

[15] Lyytinen K, Mathiassen L, Ropponen J. Attention Shaping and software risk: A categorical analysis of four classical risk management approaches. Information Systems Research. 1998;9(3):233.

[16] Iversen JH, Mathiassen L, Nielsen PA. Managing Risk in Software Process Improvement: An Action Research Approach. MIS Quarterly. 2004;28(3):395-433.

[17] Smith HA, McKeen JD, Staples DS. Risk Management in Information Systems: Problems and Potentials. Communications of the Association for Information Systems. 2001;7.

[18] Persson JS, Mathiassen L, Boeg J, Madsen T. Managing Risks in Distributed Software Projects: An Integrative Framework. IEEE Transactions on Engineering Management. 2009;56(3):508-532.

[19] Keil M, Robey D. Turning Around Troubled Software Projects: An Exploratory Study of the Deescalation of Commitment to Failing Courses of Action. Journal of Management Information Systems. 1999;15(4):63.

[20] Ropponen J, Lyytinen K. Components of Software Development Risk: How to Address Them? A Project Manager Survey. IEEE Transactions on Software Engineering. 2000;26(2).

[21] Carlo JL, Lyytinen K, Boland Jr RJ. Systemic Risk, IT Artifacts, and High Reliability Organizations: A Case of Constructing a Radical Architecture. Sprouts: Working Paper on Information Environments, Systems and Organizations. 2004;4(2).

[22] Carr NG. IT? Does it Matter? Network Magazine. 2003;18(7):6.

[23] Hanseth O. Introduction: integration-complexity-risk-the making of information systems out of control, in Risk, Complexity and ICT. Cheltenham: Edward Elgar Publishing Ltd; 2007.

[24] Braa J, Hanseth O, Heywood A, Mohammed W. Developing Health Information Systems in Developing Countries: The Flexible Standards Strategy. MIS Quarterly. 2007;31(2):381-402.

[25] Ciborra C, Braa, K, Cordella A, Dahlbom B, Failla A, Hanseth O, Hepsø V, Ljungberg J, Monteiro E, Simon K. From Control to Drift. The Dynamics of Corporate Information Infrastructures. Oxford University Press; 2000.

[26] Hanseth O, Monteiro E, Hatling M. Developing Information Infrastructure: The Tension Between Standardization and Flexibility. Science, Technology and Human Values. 1996;2(4):407-426.

[27] Star SL, Ruhleder K. Steps toward an ecology of infrastructure: design and access for large information spaces," (7:1), 1996, pp. 111-34. Information Systems Research. 1996;7(1):111-134.

[28] Hanseth O, Monteiro E. Inscribing Behaviour in Information Infrastructure Standards. Accounting, Management & Information Technology. 1997;7(4):183-211.

[29] Beck U. World Risk Society. Cambridge: Polity Press; 1998.

[30] Giddens A. The Consequences of Modernity. Polity Press; 1990.

[31] Blechar J, Hanseth O. From Risk Management to "Organized Irresponsibility"? Risks and Risk Management in the Mobile Telcom Sector. In: Ciborra CU, Hanseth O. Complexity, Integration and Risk. Elgar Publishing.; 2007.

[32] Hanseth O, Braa K. Globalization and 'Risk Society'. In: editors CUCaA, editor. From Control to Drift: the dynamics of corporate information infrastructures. Oxford University Press; 2000.

[33] Robey D, Boudreau MC. Accounting for the Contradictory Organizational Consequences of Information Technology: Theoretical Directions and Methodological Implications. Information Systems Research. 1999;10(2).

[34] Rönnbäck L, Holmström J. Running to Stand Still: Examining the Role of Information Technology in Industrial Risk Management. In: 16th European Conference on Information Systems; 2007.

[35] Singh JV. Performance, slack, and risk taking in organizational decision making. Academy of Management Review. 1986;29(3).

[36] Bevan S. Quit stalling. People Management. 1997;3(23):32-35.

[37] Souder WE, Bethay D. The risk pyramid for new product development: An application to complex aerospace hardware. The Journal of Product Innovation Management. 1993;10(3):181-195.

[38] Hartmann GC, Lakatos AL. Assessing technology risk – a case study. Research Technology Management. 1998;41(2):32-39.

[39] Orlikowski WJ. Improvising Organizational Transformation Over Time: A Situated Change Perspective. Information Systems Research. 1996;7(1):63-92.

[40] Ciborra C. The Labyrinths of Information: Challenging the Wisdom of Systems. Oxford: Oxford University Press; 2002.

[41] Ciborra C, Osei-Joehene D. Corporate ICT Infrastructures and Risk. In: Proceedings of the European Conference of Information Systems; 2003; Naples.

[42] Hanseth O, Lyytinen K. Design theory for dynamic complexity in information infrastructures: the case of building internet. Journal of Information Technology. 2010 1-19.

[43] Keil M, Lei L, Mathiassen L, Guangzhi Z. The influence of checklists and roles on software practitioner risk perception and decision-making. The Journal of Systems and Software. 2008 908–919.

[44] Lyytinen K. A Taxanomic Perspective of Information Systems Development: Theoretical constructs and recommendations. In: Boland JR, Hirschheim AR. Critical Issues in Information Systems Research. John Wiley & Sons Limited; 1987.

[45] Rönnbäck L, Holmström J, Hanseth O. IT-adaptation Challenges in the Process Industry: an Exploratory Case Study. Industrial Management and Data Systems. 2007;107(9):1276-1289.

[46] Schmidt, R., Lyytinen, K., Keil, M. & Cule, P. (2001) "Identifying Software Project Risks: an International Delphi Study. Journal of Management Information Systems. 2001;17(4):5-36.

[47] Walsham G. Doing Interpretive Research. European Journal of Information System. 2006;15:320-330.

[48] Wynne B. May the sheep safely graze? A reflexive view on the lay-expert divide. In: Lash S, Szerszynski B, Wynne B. Risk, Environment and Modernity. London: Sage; 1996. p. 44-83.