6-2011

Managing risk in a failing IT project: A social constructionist view

Wee Kiat LIM
Singapore Management University, wklim@smu.edu.sg

Siew Kien SIA

Adrian YEOW

Citation

LIM, Wee Kiat; SIA, Siew Kien; and YEOW, Adrian. Managing risk in a failing IT project: A social constructionist view. (2011). *Journal of the Association for Information Systems*. 12, (6), 414-440. CMP Research.
Available at: https://ink.library.smu.edu.sg/cmp_research/2

Journal of the Association for Information Systems
JAIS

Research Article

Managing Risks in a Failing IT Project: A Social Constructionist View*

Wee-Kiat Lim
University of Colorado at Boulder
weekiat.lim@colorado.edu

Siew Kien Sia
Nanyang Technological University
asksia@ntu.edu.sg

Adrian Yeow
Nanyang Technological University
aykyeow@ntu.edu.sg

Abstract

Why do IT projects continue to stumble, despite the proliferation of risk management methodologies and a growing body of knowledge on project risk assessment and mitigation? In this paper, we propose an alternative theoretical perspective that views project risk as a social construction process shaped by the risk accounts of social groups and actors within an implementation context. Risk management is embedded in the social processes where risks are negotiated and contested, with some risk accounts amplified and some attenuated. Through the analysis of a large IT implementation in an Asian logistics firm and its trajectory of successive crises, we examine the process of the social construction of risk. Our findings highlight the inherent fragmentation and the challenge of building collectiveness in risk construction, and the need for risk managers to consider the influence of broader social structures and the reshaping dynamism of sudden focusing events in managing complex IT projects.

Keywords: *Risk Management, Process Model, IT Project Management, Social Construction, Case Study.*

* Kalle Lyytinen was the accepting senior editor. This article was submitted on 8th January 2010 and went through three revisions.

Volume 12, Issue 6, pp. 414-440, June 2011

Managing Risks in a Failing IT Project: A Social Constructionist View

1. Introduction

With IT systems becoming larger, more intertwined with operations, and involving multiple stakeholders from within and outside of organizations, the complexities of IT projects in organizations have escalated significantly. The challenge of managing such projects is evident in the dismal state of IT project success. Recent surveys conducted by Hewlett-Packard (HP) and Economist Intelligence Unit (EIU) echo similar depressing IT project success rates and reveal that outsourcing, changing user requirements, and poor coordination among managers are some of the key reasons driving project failure (BBC News, 2007). The latest CHAOS report offers a stark assessment of IT projects in the current bleak economic climate (Standish Group, 2009). Twenty-four percent of the projects failed, meaning they were canceled before completion or delivery, and never used. The failure rate increased 9 percent over six years, as shown in a comparison to an earlier survey (Standish Group, 2003).

High profile failures and a large number of "near-failures" have been well documented in IS research. For example, the London Stock Exchange's implementation of Project Taurus was cancelled after the exchange spent more than £80 million in five years (Drummond, 1996). The failed implementation of a new IT-based luggage management system at Denver International Airport is another case in point. It went over budget by US$2 million and was close to 16 months behind schedule before it was terminated (Montealegre & Keil, 2000). A more recent example is the Virtual Case File project commissioned by the U.S. Federal Bureau of Investigation (FBI). It was originally slated to turn operational in late 2003 but was ultimately terminated by early 2005 (Eggen & Witte, 2006; Goldstein, 2005). The additional cost to roll out the system would have been another US$50 million. According to the U.S. Office of the Inspector General (2005), the reasons for failure included poorly defined and slowly evolving design requirements, poor contracting practices, and lack of management continuity and oversight. These case studies point to the need for ongoing empirical research to understand how IT projects can be better managed to avoid project failures. In particular, risk control and risk reduction are essential elements in managing complex projects. IT project management should be structured in ways that address the major areas of risks (Shenhar & Dvir, 2007).

2. IT Project Risk Literature

IT project risk research, while accumulating a formidable body of knowledge over the years, is largely characterized by two main approaches: (1) the rational-choice and (2) the cognitive-behavioral approaches. The rational-choice approach is grounded in early research on IT project failures by McFarlan (1981), Davis (1982), Boehm (1991), and Alter and Ginzberg (1978). They focus on surfacing categories known as "risk factors," such as project novelty and complexity, and suggest related strategies to counter these factors. Subsequent work applied organizational theories such as socio-technical theory (Lyytinen, Mathiassen, & Ropponen, 1998), contingency theory (Barki, Rivard, & Talbot, 2001), and system theory (Alter & Sherer, 2004) to classify the identified risk factors into more formal risk categories. Critiques of this approach point out that it is difficult to draw a comprehensive laundry list of risk items at the start of the project or to maintain that list and manage the risk factors over the course of a project (Carlo, Lyytinen, & Boland, 2004). In their recent review of IT risk literature, Alter and Sherer (2004) noted that at least 228 risk items have been identified. Such a lengthy list is unwieldy, and it limits the efficacy of a "checklist-based" risk management approach. On the other hand, as noted by Carlo et al. (2004), risk management has to go beyond "controlling or mitigating the top ten risks" (p. 59). This is especially so with the increasing complexity of IT projects that make it impractical to apply the heuristics of the cause-effect chains in such a risk management approach (Lyytinen et al., 1998).

In contrast, the cognitive-behavioral approach to IT project risk is exemplified in the stream of research on project escalation (Keil, Mann, & Rai, 2000). This approach turns inward to consider how risks are perceived, which psychological factors influence these perceptions, and how these risk perceptions, in turn, govern their decisions. Keil and his associates (1995, 2007, 2000; Mähring & Keil, 2008) found that various cognitive theories such as avoidance theory and agency theory have high explanatory value as to why risk perceptions are distorted. They argue that these distorted perceptions explain why decisions and actions do not match the nature and severity of the actual risks. While this approach provides insights into the subjective nature of largely individual-based, and to some extent group-based, risk perceptions and how they relate to project failure, these risk perceptions are almost exclusively seen from a project manager's viewpoint. Other project stakeholders (e.g., users and vendors) are only considered nominally, as are the socialization dynamics in the project (Boehm, 1991; Schmidt, Lyytinen, Keil, & Cule, 2001).

Putting these two approaches together, the literature shows that IS failures can be minimized if project managers deploy more comprehensive checklists of risk factors and proactively reduce their cognitive-behavioral biases. Whether it attempts to create taxonomies of risk factors or attempts to uncover the perceptual inaccuracies and distortion surrounding project risks, both approaches conceptualize project risk as a value-neutral and observable construct that can be objectively assessed and analyzed (Lyytinen et al., 1998; Perrow, 1984). However, we argue that such conceptualizations of risk may be problematic on several fronts.

First, such conceptualizations may not sufficiently account for the social and organizational complexities of IT projects. Complex IT projects deal with a large number of tightly coupled and interactive systems and are, therefore, fraught with high uncertainty and ambiguity (Perrow, 1984). This uncertainty is further accentuated by the intangibility of the IT deliverables. They often involve multiple stakeholders working on complicated, interdependent functional requirements. These conditions point to a social context where many participants interact constantly to make sense of project uncertainty and ambiguity. How they encounter, experience, and subsequently communicate with one another what they understand as potentially deleterious to the project is important in developing a richer shared understanding of the project (Power, 2007). Cultural scholars such as Mary Douglas and Aaron Wildavsky have long argued that risks should be treated as "social processes rather than physical entities that exist independently of the humans who assess and experience them" (Bradbury, 1989, p. 389). Risks are, thus, not absolute, but local and contextual. They are to be defined and accepted by the relevant stakeholders in a particular social setting (Stahl, Lichtenstein, & Mangan, 2003).

Furthermore, these views of project risk often do not account for the temporal, emergent, and dynamic nature of project risks (Alter & Sherer, 2004; Mahring & Keil, 2008). Project risks change as the organizational and institutional conditions surrounding IT projects evolve (Berkun, 2005). It is an ongoing affair of risk identification, assessment, and mitigation, which goes beyond the well-bracketed episodic probes that characterize formal project risk management methodologies. The lack of dynamism in risk assessment is particularly salient when we consider the process by which IT projects fail, of how projects muddle along as conditions continually shift and signals of impending failure may appear and also quickly fade away.

Drawing our theoretical bases from both the social construction of risk in sociology (e.g., Tierney, 1999) and the social constructionist approach in IS (e.g., Orlikowski & Gash, 1994), we seek to offer a social constructionist view of project risk as an alternative theorizing of the process of risk management *in situ* in IT projects. In this light, we treat the multiple interpretations of risk in complex IT projects neither as wrongful readings of risks "out there," nor as embedded cognitive biases, but as situated accounts of risk that diverse stakeholder groups hold as they make sense of a disorderly world.

Consistent with risk researchers (e.g., Hansson, 2010; Tierney, 1999; and Renn, 2008), our position is that risks are both fact-laden and value-laden; they contain both objective and subjective elements. Yet, the state of IS project research has been preoccupied with existing risk management methods and has consequently ignored situated risk in the broader societal fabric. Wynne (1992) expressed similar concern that "the obsession with physical risk… deletes the deeper questions about institutional behaviors and social relations" (p. 755). What the social constructionist approach adds to the discussion is the interplay among the broader social structures and the interaction among the multiple stakeholder groups (e.g., users, IT departments, and vendors).

This is particularly relevant for complex IT projects, where multiple stakeholders are likely to come from different backgrounds, with different expertise and vested interests, to develop complex systems under complex project governance. Risks are likely to be perceived differently and deemed to be of varying degrees of criticality by different stakeholders. How the multiple interpretations of risk converge and diverge across the stakeholders is a question of interest to us. To this end, we believe that the social constructionist approach toward project risk is complementary to traditional risk approaches. It not only draws attention to the social interaction process through which risks are constructed but also widens the consideration to include the broader social structures that may perpetuate specific social orders, leading to the inclusion of some risks and the exclusion of others (Vaughan, 1996), with direct consequences on project outcomes.

In the next section, we detail how the literature on the social construction of risk, particularly from sociology, can enrich and extend our conceptualization of risk management in IT projects.

3. Social Construction of Risk

Discussions on the social construction of risk have their roots in the sociological literature on the social construction of reality and the scientific enterprise (Berger & Luckmann, 1966/1991; Latour & Woolgar, 1979; Pinch & Bijker, 1984), and the more specific field of natural hazards and disaster research (Clarke & Short, 1993; Renn, 1992, 2008; Tierney, 1999; Vaughan, 1996, 1999). Central to this view is that risk is a social construct that reflects how society deals with uncertainty (Otway & Thomas, 1982). This perspective goes beyond risks as externally quantifiable objects or as individual cognitive biases to conceive risks as products of social interactions, deeply embedded in social structures (Douglas & Wildavsky, 1982; Manning, 1989; Tierney, 1999). A social constructionist approach does not claim that risk does not exist. Rather, it seeks to understand the process through which "social agents create and use boundaries to demarcate that which is dangerous" (Clarke & Short, 1993, p. 379).

In trying to make sense of the uncertainties, different social groups come to define and attach meanings to a risk artifact (Douglas & Wildavsky 1982; Tierney, 1999). Their past experiences, knowledge differentials, vested interests, and value differences shape the way they construct their risk accounts (Orbuch, 1997). These accounts are verbal or written explanations about the likelihood of unanticipated events happening as individuals or groups profess understanding of their environment (Scott& Lyman, 1968). The risk accounts are subjected to a process of negotiation and contestation, with growing or diminishing degrees of stabilization toward consensus or conflict. Risk is, thus, conceived dynamically as being inter-subjective (i.e., shared among individuals and between groups), going beyond individuals' subjective perceptions (Berger & Luckmann, 1966/1991). Expressions of this inter-subjectivity are consolidated in the “accounts” that social groups create (Latour & Woolgar, 1979; Orbuch, 1997).

The negotiation and contestation of these risk accounts are influenced by broader social structures such as cultural norms, political power, economic interests, institutional pressures, and organizational agendas. Specifically, sociological research on disasters unravels how such forces shape the social understanding of risk (Tierney, 1999; Vaughan, 1999).[1] Several prominent sociological studies (though at the societal level of analysis) found that what constitutes risk, what type of risk models are employed, and how estimates of risk are constructed are the end results of economic and political negotiations as well as decisions influenced by existing organizational structures and their inter-relationships (Clarke & Short, 1993; Vaughan, 1996, 1999). Perrow (1984) and Shrader-Frechette (1985), for example, described how nuclear power risk assessments were influenced by organizational considerations, resulting in the exclusion of many potential causes of system failure. Others showed how factors such as culture and institutions (e.g., media and government agencies) amplify or attenuate specific interpretation of risk via a network of socially mediated communication channels (Kasperson et al., 1988; Masuda & Garvin, 2006).

The context of negotiation and contestation is also highly emergent, with the possibility of major unexpected events occurring that may tilt the underlying socialization dynamic in risk construction. This idea of prominent events shaping historical trajectories is also found in disaster research. In disaster

[1] As our aim is to highlight streams of research that are useful in building a theoretical framework of social construction of project risk, we do not provide an exhaustive survey of disaster research. Besides Tierney (1999), for a more detailed account of the social construction of risk in disaster research, refer to Tierney (2007) and Renn (1992).

research, "focusing events" refer to sudden, relatively uncommon social events that are harmful or reveal the possibility of greater future harms (Birkland, 1998; Tierney & Bevc, 2007). These events are often known to policy makers and the public simultaneously and serve as potential catalysts for policy change (Birkland, 1998). They are attention-grabbing (typically catastrophic) events that trigger social processes among actors or stakeholders to focus and call into question existing structures and understanding. They serve to open up a forum for the affected stakeholders to re-negotiate issues and examine taken-for-granted assumptions. Such social change dynamically modifies the construction of risk.

Extending the research in the social construction of risk into managing complex IT projects, we contend that the notion of IT risk is also a dynamic outcome of the social construction process. While the social constructionist perspective has been applied in the IS literature, such research tends to focus on how the meaning of IT is socially constructed during its adoption, design, and use, and not on the domain of IT risk management. These IS social constructionist studies are exemplified by the stream of research on technological frames (Davidson, 2006; Orlikowski & Gash, 1994). They conceive organizations as made up of different stakeholder groups (analogous to the distinct social groups in the society, writ large) and that each group holds different views or understandings of the focal technology. Such views are defined as a "technological frame" – a socio-cognitive construct that incorporates knowledge and expectations that guide actors' interpretations and actions related to IT (Orlikowski & Gash, 1994). The key contribution of such studies has been to demonstrate how the degree of incongruence of technological affects project outcomes, subsequent technological use, and related organizational outcomes (e.g., Davidson, 2002; Lin & Silva, 2005). Subsequent studies have extended the content of technological frames from technological attributes and use to systems development (Davidson, 2006) or IT's impact on organizational work practices (Wagner & Newell, 2006; Yeow & Sia, 2008).

Recent research has also begun addressing the sources of technological frames and the dynamics of frame construction and change. One stream of studies explores the role of negotiations, contestations, power and politics, and other social processes by which technological frames are socially constructed (Azad & Faraj, 2008; Lin & Silva, 2005; McLoughlin, Badham, & Couchman, 2000; Wagner & Newell, 2006; Yeow & Sia, 2008). Another stream of research looks at how emergent events such as "critical encounters" or "discrepant events" could lead to a series of significant social interactions that shift a group's technological frame (Majchrzak, Rice, Malhotra, King, & Ba, 2000; Newman & Robey, 1992; Tyre & Orlikowski, 1994). Finally, some research has also begun to consider how larger institutional and cultural influences permeate organizational boundaries to shape stakeholders' frames of technology (Barrett & Walsham, 1999). These insights from this ongoing IS constructionist research – ranging from the negotiation and contestation of locally situated organizational stakeholders, to the significance of emergent events, to broader institutional forces – mirror and resonate with some of the key concepts found in the social constructionist study of risk reviewed above.

By grounding our research in the social constructionist view of risk, we expand this stream of social constructionist research in IS beyond the core technology artifact to the domain of IT risk management. How are notions of risks in IT projects constructed? Why are some project risks accepted as key project risks while others are rejected or trivialized? Drawing on concepts from the social construction of risk in sociology (e.g., risk accounts, social interaction, social structures, focusing events) and relevant ones from the social constructionist research in IS, we seek to see how these factors play out in the context of a failing IT project. Specifically, the aim of the study is to create a process model (Pettigrew, 1990; Van de Ven & Huber, 1990) in illuminating the social construction process of risk in IT projects – a complex process that, in the view of Latour & Woolgar (1979), "involve(s) the use of devices whereby all traces of production are made extremely difficult to detect." We show the utility of introducing these concepts in clarifying the process of social construction of risk in IT projects through an in-depth case study of a large IT project implementation in an Asian logistic firm. The IT project underwent several major disruptions and suffered major slippages, but was launched, albeit belatedly. The complex project dynamics over time provided an ideal context for us to examine the processes of risk construction. In the next section, we present the case site and research methodology.

4. Research Method

4.1. Background of case site

Leveraging an opportunity to track and analyze the trajectory of IT implementation issues and challenges, we conducted a case study of a major IT project slippage in a large Asian logistic firm. It is a large and established organization, in business for over 40 years and employing more than 10,000 people. The firm has three major lines of business, each dedicated to a particular transport means – Air, Land, and Sea Logistics. A key strategic business niche is in the warehousing and transportation of hazardous materials (e.g., combustible goods). Each hazardous materials business unit (HMBU) functions autonomously under its respective larger transport-centric business unit. Figure 1 presents the organizational structure of the logistics firm.

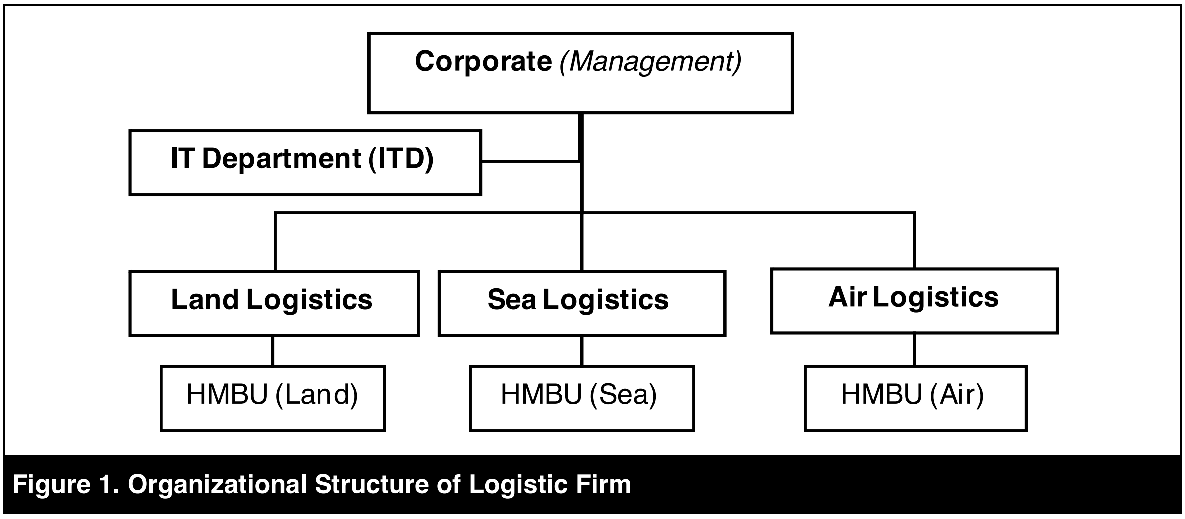

Figure 1. Organizational Structure of Logistic Firm

In 2001, the firm embarked on a strategic IT project to improve its competitive edge in the hazardous materials business. The project ("Project Alpha") consisted of (1) a sophisticated IT system that would automate its storage warehousing and transporting operations and (2) a novel "containerization" concept that would radically streamline and expedite the warehousing, transfer, and delivery of hazardous goods using standard size containers. The system would enable seamless logistic integration across its land, sea, and air businesses. Through consolidated and centralized planning, it would substantially enhance inventory visibility, safety, security, and accountability in managing the hazardous materials. The old logistic management system was largely transactional, comprising a few stovepipe standalone systems. There was limited inventory information to manage across the multiple warehouses. Planning, control, and management of warehousing and logistic activities (e.g., storage allocation, safety audit, fleet management, job scheduling, and replenishment planning) were non-standardized and carried out manually, using only simple spreadsheets. The jump in sophistication in its operations was substantial. The new system comprised 20 highly inter-dependent modules; of which half were intelligent modules consisting of complex planning and scheduling engines. Figure 2 provides the overview of the key modules in the new IT system.

The IT Department (i.e., ITD) was in charge of Project Alpha. ITD was part of an IT shared service organization that managed the full range of IT services -- system acquisition, development, and operation -- for the firm. Given the management's decision to structure Project Alpha as a fixed-price "turnkey"[2] project, ITD coordinated the outsourcing of the project implementation. The outsourcing vendor was *"to be solely responsible for the design, development and implementation of the new system"* (as per contract specification). The vendor, in turn, subcontracted the intelligent system component to another IT specialist firm.

[2] ITD was a mature shared service organization, having developed many of the mission-critical applications for users in the past. Project implementations typically followed a well-established in-house system implementation methodology. The "turnkey" development approach was, at that point in time, a recent addition and emphasized careful vendor and contract management.

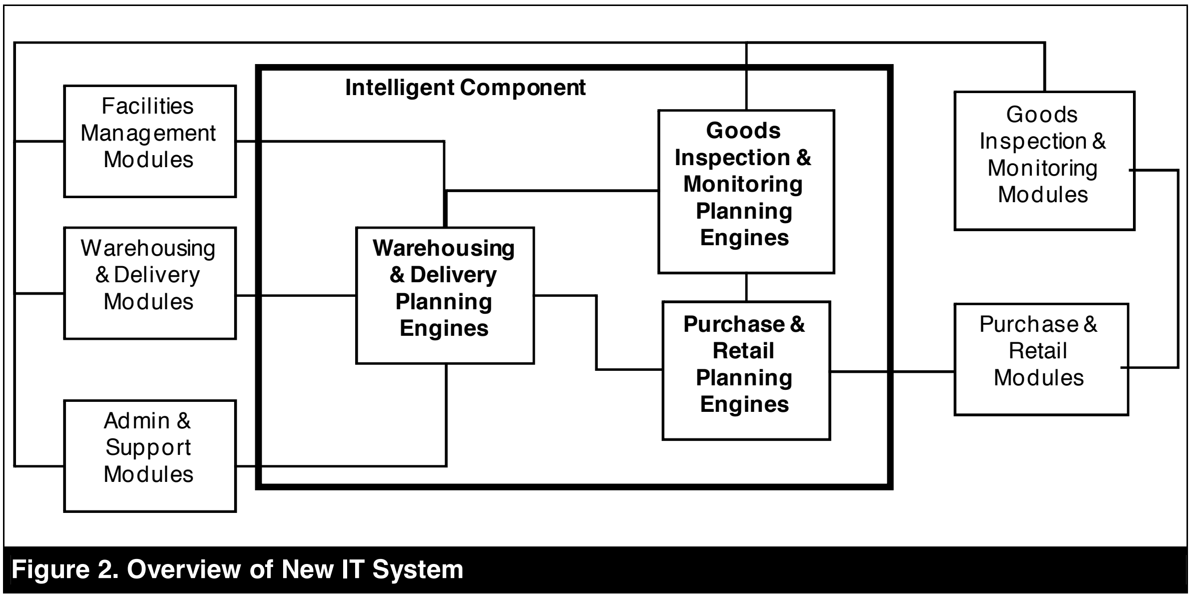
Intelligent Component
Facilities Management Modules
Warehousing & Delivery Modules
Admin & Support Modules
Warehousing & Delivery Planning Engines
Goods Inspection & Monitoring Planning Engines
Purchase & Retail Planning Engines
Goods Inspection & Monitoring Modules
Purchase & Retail Modules

Figure 2. Overview of New IT System

In terms of project management, an ITD manager was designated as the Corporate Project Manager *"to monitor the progress of the project, conduct checkpoint reviews and ensure the timely and quality delivery of the system"* (as per contract specification). An experienced manager from Land HMBU was appointed as the Operations (Ops) Manager *"to coordinate all users for the requirement specification, user training, and system operations"* (as per contract specification). Both the Corporate Project Manager and the Ops Manager co-chaired the project management team. The Vendor Project Manager, who was under the Corporate Project Manager's charge, was responsible for the subcontractor. Above the project management team were two committees: (1) the working committee and (2) the steering committee. The working committee was initially chaired by the Head of HMBU only and was later co-chaired with a senior management representative from ITD in early 2005. The steering committee was helmed by the Head of Operations from Corporate Unit, who was responsible for all three land, sea, and air B.U.s. Although the committee was the highest level of project oversight, because its members had responsibility largely for the general management of the hazardous materials business, it was not fully dedicated to Project Alpha. Figure 3 illustrates the project management structure.

Project Alpha formally kicked off in April 2001 and was initially scheduled for rollout by the land B.U. by mid-2004. The project's progress, however, was constantly disrupted. Two major crises that nearly crippled the project deserve mention. First, the vendor's subcontractor went bankrupt early in the project. A second subcontractor was found, which was followed by a series of antagonistic client-vendor interactions that led to the second crisis, when the vendor mutinied and staged a dramatic stand-off in late 2004. Through management intervention, the project managed to hobble on and was eventually completed at the end of 2007. The project slippage was close to three years, after six revisions of the commissioning date for the IT system. Figure 4 shows the timeline for Project Alpha.

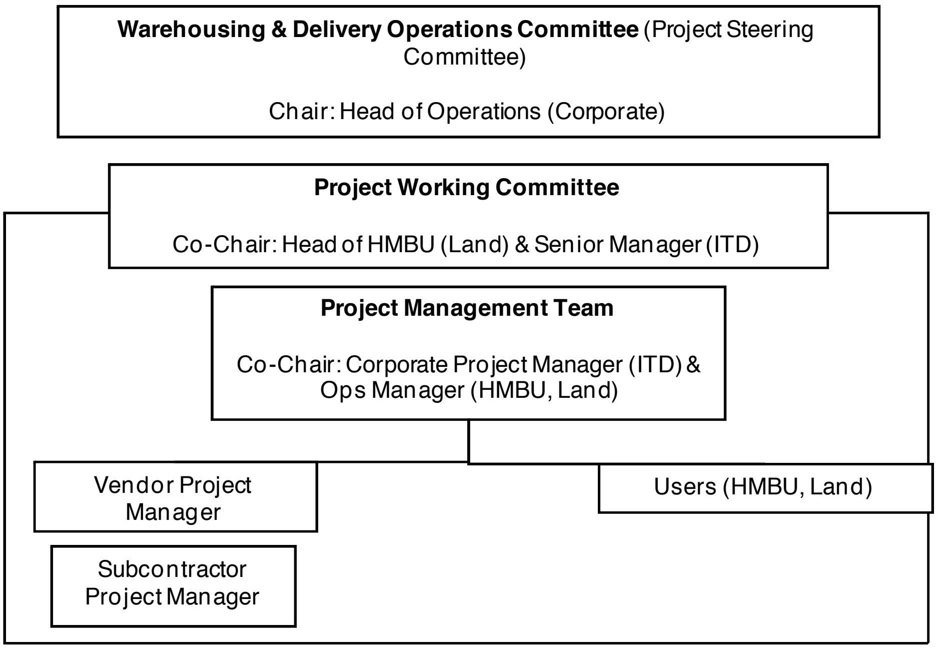
Warehousing & Delivery Operations Committee (Project Steering Committee)
Chair: Head of Operations (Corporate)
Project Working Committee
Co-Chair: Head of HMBU (Land) & Senior Manager (ITD)
Project Management Team
Co-Chair: Corporate Project Manager (ITD) & Ops Manager (HMBU, Land)
Vendor Project Manager
Users (HMBU, Land)
Subcontractor Project Manager

Figure 3. Project Management Structure

2001	2002	2003	2004	2005	2006	2007
April 2001 Project kicked off.	**Late 2002** Subcontractor went bankrupt.	**March 2003** New subcontractor joined Project **Late 2003** Additional containerization study completed	**Late 2004** Vendor mutiny –"information blackout."	**Early 2005** Senior ITD Mgr appointed as co-chair of Project Working Committee.	**Early 2006** Researchers entered project site for interviews **Mid 2006** First transactional module rolled out.	**Late 2007** Full commissioning of IT System.

Figure 4. Project Alpha Timeline

4.2. Data Collection and Analysis

We were invited by ITD in the later stage of the project (i.e., early 2006) to provide an independent report of the key events, issues, and lessons derived from this project. As neutral observers, we did not intervene with any project decisions. We collected our data from two main sources. First, we examined online and offline archival data, including project proposal reports, tender specifications, contracts, official correspondence (e.g., emails, letters), project progress reports, project management plans, minutes of meetings, and presentation slides. These materials were especially useful for us to trace the sequence of actions and events that occurred between 2000 and 2006. Specifically, they helped us construct or validate the risk accounts for different stakeholders.

Second, we conducted 14 interviews with the key actors in Project Alpha. Table 1 shows the breakdown of the interviews by stakeholder group. Although the number of interviews was relatively low, we covered all the stakeholder groups involved, i.e., ITD, HMBU users, vendor, and

Subcontractor, and targeted all key individuals who had significant influence over the construction of risk accounts by the respective stakeholders.

Reflecting Myers and Newman's (2007) call to situate the researchers within their interviews, we entered the field as "known" investigators (Lofland & Lofland, 1995), and our interviewees were aware that our intent was to understand their views on the trajectory of the project. We also deployed a "portfolio" of roles and identities that was contingent on the situations we encountered. For instance, we demonstrated "acceptable incompetence" (Lofland & Lofland, 1995) to draw out elaboration from our interviewees. This quintessential student role encouraged them to flesh out their arguments, such as providing concrete examples to illustrate their more abstract ideas. On other occasions, we also displayed "selective competence" (Lofland & Lofland, 1995) to enhance our credibility as IT project management researchers.

Table 1. Breakdown of Interviews by Stakeholder Groups

Stakeholder	# Interviews	# Distinct Interviewees
ITD	**7**	**5**
Senior Executives	3	2
Project Manager	3	1
Project Team Leads	1	2
HMBU Users	**4**	**6**
Head of HMBU	1	1
Ops Manager	2	1
User Representatives	1	4
Vendor	**2**	**2**
Senior Executive	1	1
Project Manager	1	1
Subcontractor	**1**	**2**
Senior Project Consultants	1	2
Total	14	15

Each interview lasted between 1 and 1.5 hours, with one researcher doing most of the inquiry and the other focused on note-taking. We conducted most interviews one-to-one, but for those at the lower level, we conducted group interviews, as these group sessions provided a familiar and less threatening environment to generate richer discussion in the context of a failing IT project (Nahar, Lyytinen, Huda, & Muravyov, 2006). We did not use a tape recorder, as interviewees were more comfortable discussing issues without one. We consolidated our notes for each interview and typed them within 24 hours. We promptly resolved differences in the interview notes through discussion and clarification.

We conducted these interviews over a seven-month period toward the end of the project, i.e., from April to October 2006. Recognizing the limitation of recall biases in retrospective accounts, we actively corroborated the events, issues, and themes noted in these interviews with intensive archival data analysis and field observations at case sites. Where appropriate, we cued the interviewees on key events that they had omitted, or challenged them on inconsistencies that we could identify.

Given that our data are process data (i.e., sequences of events that were contextual and of variable temporal embeddedness (Langley, 1999), we adopted a process approach to analyze how project risk is socially constructed. In line with extant process studies, we adopted the definition of "process" as "the sequences of interactions and activities that unfold over the duration of the entity being studied in context" (Van de Ven, 2007, p. 197). As such, we followed Langley's (1999) idea of combining narrative strategy and temporal bracketing strategy in our data analysis. The narrative strategy essentially involves the construction of a detailed story from the raw data using time as its main anchor point. Accordingly, we crafted an in-depth and chronological narrative of the entire implementation process. It formed the base document for summarizing the vast amount of information available in the primary dataset of archival and interview data. We also used it as a validation tool (Eisenhardt, 1989). First, as part of the deliverables, we asked various key actors to verify the 40-page case report (i.e., ITD, users, and vendor) before we formally submitted it to corporate management. Second, we used the report for case discussion and reflection within the firm's in-house project management training. We were subsequently invited to facilitate a case discussion on the project, with a joint panel of representatives from various stakeholder groups, namely, the ITD Project Manager, HMBU Ops Manager, and Vendor Project Manager. These events solidified our confidence that our analysis and reporting were authentic and credible (Golden-Biddle & Locke, 1993).

Next, we used the narrative as the basis to identify phases, following the temporal bracketing strategy (Langley, 1999, p. 707). In essence, the temporal bracketing strategy attempts to surface activities or interactions within a certain period that have certain continuity and are "bracketed" by discontinuities. Each continuous period is referred to as a phase, though not in a predictable sequential sense. This approach is widely adopted within IS process studies, e.g., Newman and Robey's (1992) encounter-episode framework. In our analysis of phases, we focused on the risk accounts that were held by the various key stakeholders. From the project archives (e.g., project minutes and email correspondence) and the interviews, we analyzed the initial risk accounts of the three main stakeholder groups (i.e., ITD project management, Land HMBU users, and vendor/subcontractor).

We then sought to understand how antecedent conditions such as their historical backgrounds, the way they perceived their roles and responsibilities, how they viewed the new IT system, and the main challenges they saw in implementing it influenced the initial risk accounts. Next, we analyzed the social interaction events as the different stakeholders engaged each other in the project, i.e., how the respective risk accounts were (or were not) communicated to the other stakeholders and the responses from others. We also sought to surface the social structures that shaped the social interaction events. For example, the initial gap between the dominant risk account and the individual risk accounts of users and vendors was attributed to the dominant position of ITD in the project structure. The resultant dominant risk accounts were derived from the actual risk management decisions and risk mitigating actions taken at the project level (e.g., non-escalation decision despite the withdrawal of first subcontractor, the appointment of ITD senior manager to co-chair Project Working Committee). Finally, we surfaced specific discontinuities, i.e., focusing events, which interrupted the path of interactions. Thus, each set of social interaction and risk mitigation actions formed our phases, while focusing events marked the start and end of these phases.

The first and second authors conducted the process data analyses, while the third author played the devil's advocate, asking clarification questions or offering alternative interpretations. In essence, he ensured that the team did not conclude the analysis prematurely (Eisenhardt, 1989).

5. Project Alpha's Failing Trajectory

5.1. Project kick-off: Initial enthusiasm and optimism

Project Alpha started when the senior management at the logistics firm was planning various organizational transformation initiatives. There was substantial enthusiasm and excitement for the strategic change. Although HMBU users were not heavy users of IT and, hence, generally not technologically savvy, they were enthusiastic about the potential benefits the new IT system would bring. Project Alpha was hailed as a quantum leap that would sharpen the firm's competitive edge. It was expected to significantly maximize operating efficiency, reduce cycle time, and enhance the quality of inspection and surveillance for hazardous materials.

Five established IT consulting firms were invited to submit their tender proposals for the project. However, only two firms responded.[3] Facilitated by ITD, the users went through a rigorous assessment using the Analytic Hierarchy Process (AHP) to select the eventual vendor for Project Alpha. The AHP was a well-established risk management process instituted by the organization for vendor evaluation and selection. The process separated evaluation of tender by allocating price and technical/performance assessment to different teams. The technical/performance assessment was based on an index of one vendor's scores against the other in terms of 19 factors including company profile, development experience, domain expertise, project management, qualification/certification, management commitment, and compliance with functional specifications. The price quotes were then provided to a separate team for a cost effectiveness calculation after the technical/performance evaluation was completed and approved by senior management. The proposal with the best benefit-cost ratio was selected. The rigorous process was to ensure that ITD and HMBU selected the most worthy and qualified vendor. The vendor, too, projected a confident image, and its partner subcontractor had won various accolades in the industry.

> *Initially when we started we had a lot of optimism and from the tender, the vendors gave us an impression that they could do anything.* (Interview with Ops Manager)

5.2. Short-lived optimism – ITD's risk account emerging as dominant

The initial optimism was short-lived. Within the first six months of project initiation, there were already indications that the implementation of Project Alpha would be rough, with increasing grousing from various parties about vague user requirements, complex technical interfaces, poor progress updates, inadequate documentation, etc. Driven by their different roles in the project, the ITD, users, and vendor were evidently concerned with different problems and issues. Table 2 shows the different risk accounts we reconstructed from the project archives (e.g., project minutes and email correspondence) and the interviews.

The users' risk account was concerned with technical risk where the new system may fail to provide required functionalities and performance. Their risk account was about managing innovation complexity. Users were concerned mainly with ensuring that all their requirements would be captured and accommodated in the new system, especially with respect to the design of the relatively novel and unfamiliar containerization solution for hazardous logistics. This was also reflected in their skimpy requirement specifications, as the specifications were spelled out only in terms of expected system capabilities but had few details on how such solutions could be devised and built. On the other hand, from the vendor and its subcontractor, the risk account was focused on risk of scope creep; it was largely described as controlling the changing user requirements and preventing scope creep. They were particularly conscious of the fixed-price nature of the contract.

The risk account of ITD was also different. Driven by the mentality of a "turnkey approach," ITD saw its role primarily as a vendor manager. Their risk account was centered on vendor management risk in that the vendor might not deliver Project Alpha based on the agreed contractual terms of reference. They were careful to monitor the delivery schedule and progress reports, holding bi-weekly progress meetings and expecting the production of a monthly report. They were insistent on compliance, e.g., the adherence to technical architecture, software development, and documentation standards. Outstanding issues and performance metrics were closely tracked.

[3] The lack of tender interest by three other established IT firms was not picked up by ITD as a potential risk indicator. The second subcontractor (who was involved in the drafting of the tender document), however, noted the lack of response was probably indicative of the project complexity, which should have triggered a reassessment of risk by ITD.

Table 2. Key Stakeholders' background, roles and risk accounts

	ITD	HMBU Users	Vendor
Background	- Strong IT culture: part of a large IT shared service organization (separate legal entity) - Physically located in a separate building from users - Deep technical IT expertise, with established system development methodologies - Limited understanding of HMBU operations, as ITD had no prior application development experience with HMBU	- Strong business culture: high responsiveness to customers - Deep logistics operations knowledge - Limited IT skills: prior logistics handling and planning largely manual, relying only on simple spreadsheet analysis - Traditionally rely on ITD to manage all IT matters	- Strong professional IT consulting culture - Among the top three vendors locally - Expertise largely in IT system implementation - Had prior working experience with ITD but not with HMBU - Limited expertise in logistics operations optimization: Dependent on subcontractor for specialized expertise in logistics planning
View of New IT System	- Viewed new IT system as a structured IT project to be delivered completely by vendor as a finished package	- Viewed new IT system as a novel and innovative IT project that would tap the specialized expertise of the vendor to leapfrog their competitors	- Viewed new IT system as an IT consulting engagement to develop system to cater to the ways users wanted to transform their logistic operations
Project Roles and Responsibilities	- Corporate Project Manager, in charge of the overall implementation of Project Alpha - With the "turnkey" approach, ITD saw its role more specifically as vendor manager - Co-chaired Project Management Team	- Operations Manager, tasked with ensuring user requirements were adequately addressed and captured - Co-chaired Project Management Team	- Vendor Project Manager, tasked with designing, building, and delivering system in the "turnkey" approach, through a fixed price contract
Risk Account	- Vendor Management: Vendor might not deliver new system based on the contractual terms of reference	- Innovation Risk: Vendor could not design and implement their requirements, especially in applying the novel and unfamiliar containerization solution	- Scope Creep: Users would supply vague or changing user requirements with possible scope creep
Risk Mitigating actions	- To tighten vendor management: exerting tighter control on vendor, scrutinizing contract, and demanding adherence to planned milestones and detailed documentation	- To manage innovation complexity: clarifying and understanding the complex design of the containerization solution in meeting their requirements	- To manage and control user requirements: delineating clear decision authority and enforcing timely and proper sign-offs

Among the various accounts, however, ITD's risk account dominated, given its advantageous position as the formal corporate project manager for Project Alpha. Although both ITD and users co-chaired the Project Management Team (PMT, see Figure 3), the "real" formal authority of the project was with ITD, as users, historically, had been passive and left most IT matters to ITD. As a result, the risk account of ITD was amplifying the vendor management risk, while the risk accounts of the users (in managing innovation complexity) and vendor (in controlling user requirements) were attenuated. Accordingly, the Corporate Project Manager and his lieutenants read the various negative project signals that arose not as innovation complexity or user requirement management issues, but rather as indications of a vendor management problem. An illustrative example was that ITD had repeatedly brushed aside suggestions that Project Alpha entailed a high level of experimentation and prototyping due to its innovation novelty and the complex interdependency involved. Instead, ITD saw the Project Alpha project as "just another project" and expressed puzzlement at the difficulties the vendor faced in building the new logistic system.

> *(It is normal that) Every system has their peculiar and unique functions. I really don't see why [Project Alpha] should be different (and therefore difficult to manage).* (Interview with ITD Senior Manager)

Yet, evidence of such novelty and complexity were frequently articulated in the interviews with the other stakeholders. In particular, the second subcontractor, being most knowledgeable about hazardous materials logistics operations, unreservedly recognized these challenges of Project Alpha:

> *People always think that it is just another logistic or warehousing system. [Project Alpha] is not just transactional. The planning engines drive the whole system. They involve complex concepts and optimization algorithms…There are a lot of combinational possibilities. The organization needs to have an accurate feel of the technical challenges. [Project Alpha] is not another IT project!*
>
> *You need to chop up [Project Alpha] into smaller pieces to specify the requirements. But each piece is still a "monster." You need to chop further. For example, in designing [one of the intelligent component modules], there are thousands of tasks when it comes to delivery during peak period, but during the lull period, the number is in the low hundreds. You need to decide at what level to configure the tasks. If the task units are too minute, the planning model will be too big to solve. Once the peak period kicks in, you will be dead (i.e., the system will fail). Unfortunately, not everyone understands this kind of complexity.*

The risk accounts of the users and vendor were not totally "muted," but their emergence was constrained by the limited social interaction with ITD during the course of the project. Physically, even though ITD had allocated workstations in a separate building with the vendor consultants, they stayed mainly in their own office and, hence, had limited visibility into the vendor's work activities. In particular, ITD's "I-manage-the-vendor" orientation and "us-against-them" mentality inhibited a two-way interaction between ITD and the vendor. The resulting risk mitigating actions followed largely from the dominant ITD's risk account.

As such, ITD was very diligent in chasing the vendor (typically over email). They sent multiple reminders to ensure tight adherence to project milestones and provide detailed documentation. They were keen only on doing vendor control tasks but showed little interest in understanding the actual operational challenges on the ground. ITD was keen to maintain its role as the controller, reluctant to get its hands dirty, and afraid that "*if I do it, it will become my job.*"

> *If we help them (the vendor) more, those tasks will gradually become our job. Coordinating with users in arranging or changing requirement meetings was one example. After a while, they just expected us to do it.* (Interview with Deputy ITD Project Manager B)

As explained by the ITD Project Manager himself using a river metaphor, ITD was not the river that directed the water flow, but *"the bank that prevents the water from flooding."* ITD's focus on tight supervision and persistent requests for formal reports and constant updating resulted in a defensive stance by the vendor. The vendor was careful and selective in information sharing for fear of raising unnecessary alarms, which could invite immediate reprimands from ITD.

5.3. First crisis: ITD shaking off doubts about its dominant risk account

In late 2002, the first subcontractor suddenly withdrew from Project Alpha due to bankruptcy. The users were shocked. ITD, too, had been kept in the dark. However, it had suspected problems as early as mid-2002 when the vendor's deliverables were falling behind schedule, and the vendor started to give evasive reasons.

> *We had some sensing when things were behind schedule then, and (our vendor) was very evasive…The writing was on the wall, but could it be just graffiti?* (ITD Project Manager)

Without conducting a deeper investigation to understand the extent of the problem, ITD quickly interpreted the issue as the "vendor's problem"[4] and demanded that the vendor seek a new partner without delay. Within three months, the vendor recruited a new subcontractor with expertise in hazardous materials in early 2003.

Despite the relatively quick replacement of the sub-contractor, the incident had cast some doubts on ITD's dominant risk account. Picking up some weak indication of project complexity (e.g., a reassessment by the new subcontractor that only 5 percent of the containerization solution designed by the old subcontractor was deemed usable), the users became more skeptical of ITD's risk account that it was merely a vendor management problem. Through a now more vocal and interactive Ops Manager, for example, users began raising issues about the clarity of the innovative containerization solution in the new system. Instead of working more closely with the vendor and the new subcontractor to understand more about the solution complexity, ITD again adopted a hands-off approach, showing a general lack of interest in understanding the users' risk account. However, to appease the users, ITD took to the commissioning of an independent review to study the feasible containerization solution. The commissioned study was, unfortunately, superficial and remained "*too high level to be useful,*" in the opinion of the users and the new sub-contractor.

Similarly, the vendor was becoming frustrated with its inability to enact risk mitigating actions to contain user requirements, given its lack of authority and the lack of support from ITD project management (e.g., the unexpected planning requirements of having to incorporate staging areas and sampling policies for safety check). The vendor also began raising questions and seeking clarification about its roles and authority in a turnkey development approach, in its attempt to dispute the dominant risk account that Project Alpha needed to deal with expanding user requirements.

However, ITD was quick to produce counter-evidence to reinforce its risk account. For example, the ITD Project Manager carefully archived the trails of correspondences and could quickly produce a binder of email correspondence to the users and minutes of meetings that showed the "incompetence and lack of professionalism" of the vendor, affirming its risk account that vendor management was the risk to be managed. An excerpt in the binder read as follow:

> *Any update? (Sent: early August, 2004)… Any update? (Sent: mid-August, 2004)… [blank forwarded e-mail with two previous e-mails enclosed] (Sent: mid-October, 2004), [Vendor Project Manager] pls assist to expedite. This item has been long outstanding (Sent: late November, 2004) [Vendor Project Manager], status [please]? This problem has been outstanding for very long. This was raised again during yesterday's meeting with [Ops Manager]. Pls expedite the process (Sent: end December, 2004)*

The vendor's complaint about vague user requirements was rebutted as the vendor's incompetence, as these requirements were "*common-sense requirements that good consultants should have anticipated*" and that "*some things are obvious - how can you build a toilet without the water pipe?*"

[4] This was ITD's interpretation, even though some interviewees felt that the solution design for Project Alpha was "too big for (the old subcontractor) to solve," and that they "finally surrendered after one and a half years."

Despite the setback of the first crisis, ITD soon steered the project risk account back to the theme of vendor management. The risk mitigating actions by ITD were, thus, on the "right" track and the situation was "in control." A review of the email correspondence between ITD and the vendor during this period revealed the continuation of a strong vendor management flavor, focusing largely on chasing progress updates, compliance to technical IT standards for the user interface, database design, component architecture, etc., but with little discussion of issues relating to innovation complexity or user requirement management.

Moreover, being the only party that would interact with all key stakeholders (including relevant higher authority in the Corporate Unit), ITD wielded not just formal authority but also substantial "informational" advantage over others, even in shaping the risk picture before senior management. The regular updates to the steering committee (comprising senior management of ITD, users, and vendor) were often smooth and non-eventful. However, the interviews and the documents suggest that the senior management did not get the complete picture, reflective of the actual project realities. In fact, between November 2002 and March 2005, there was only one documented case of meeting minutes sent to the Project Steering Committee. Even then, the update slides to the steering committee did not convey the gravity of the concerns of the users or vendor at various stages. One of the steering committee members reflected subsequently on such reluctance of ITD to engage senior management:

> *[ITD] sits through all the meetings and they are supposed to be on top of things. They need to do active monitoring, active participation and the guts to tell management bad stories and take (issues) by the hook. They cannot hide the bad news.*

As the deadlines for the project deliverables slipped, ITD exerted even more pressure on the vendor by demanding more frequent reporting and intermediate deliverables (e.g., design documentation). The vendor resisted, as it saw ITD's actions as counter-productive, since ITD imposed more administrative burdens on the vendor's project team, further draining its resources. The exasperation on both sides eventually led to open hostility between ITD and the vendor during meetings. The vendor, for example, complained about the lack of "respectful" interaction, which had led to many of its staff resigning, going on no-pay leave, or requesting transfers.

> *We need our customers to be reasonable. We all have our self-esteem, our self-worth - not big egos. There's no need for them (ITD) to hurl verbal abuse and "whip" the consultants upside down in the meetings.* (Interview with Vendor Vice-President)

ITD, on the other hand, was adamant. In fact, it believed the high staff turnover was simply due to "poor project management" on the part of the contractor in "over-relying on key personnel and failing to institute adequate succession planning." To them, building good relationships with the vendor was unnecessary:

> *We are not the best of buddies and we don't go drinking together, that's fine with me. Good relationship is immaterial to the project. We should concentrate on getting the deliverables.* (Interview with Corporate Project Manager)

The tight control of ITD in vendor management led to the deterioration of the relationship with the vendor. There were various occasions of heated exchanges, as noted by a senior manager in ITD.

> *Both sides were very defensive. [Vendor] felt that users wanted more and more and [ITD] always sided with the users. On the user end, they felt that [Vendor] tried to avoid everything they asked. Instead of finding the workable solutions together, they were busy guarding each other's interests…*

Such hostility perpetuated a divisive mindset. There were indications of one party picking up and highlighting signs of risk for the other party, yet these signs were ignored. For example, the vendor insisted on using its development approach and internal project structure, disregarding ITD's attempts to raise concern of worsening integration complexity in Project Alpha.

> *[The vendor] structured their development teams this way: the requirement analysts talked to users…there were also the developers and testers, and the testers did nothing but testing…there were gaps between analysts and developers – what the developers interpreted and implemented might not be congruent with the analysts, as they had made their assumptions without consulting the users. For the testers, if they did not have the knowledge from the rest, they could not come up with the test specs, and they took too long… the test days kept postponing as the test cases were not ready yet.* (Interview with Corporate Project Manager)

Similarly, the vendor and the subcontractor had sensed that Project Alpha "*in the leaders' minds was a transformation, but the ground people (in Land HMBU) feel that it's only a migration*," and tried to communicate the need for careful change management. However, ITD felt that it had done enough and did not respond sufficiently to their concern about engaging the users more actively.

> *There will be a monstrous transformation of [Land HMBU] community, so they must have change management. It's not giving a talk here and there. You need to actively involve those people to change their mindset, and some people you need to chop (i.e., retrench)… We keep telling [Ops Manager] about change management and BPR (business process re-engineering), but [ITD] didn't like us doing that and said, "Don't tell me I miss this out."* (Interview with Subcontractor Project Manager)

5.4. Second crisis – User/Vendor taking active roles in renegotiating dominant risk account

In late 2004, the vendor mutinied unexpectedly by declaring what ITD referred to as an "information blackout," abruptly cutting off all interactions between its consultants and ITD and the users. All pre-planned requirement meetings with the users were cancelled. ITD and the users were caught completely off-guard.

> *At first, we tried to clarify with them (regarding the sudden cancellation). The [vendor] analysts told us that it was a top management decision to churn out the requirements and they were not to have any meeting.* (ITD Manager)

Claiming that they had incurred a loss of a few million, their argument was that the user requirements should have been closed by early March 2002, as originally planned in the contract. The stand-off left the fate of Project Alpha hanging in limbo for several weeks. The vendor only returned to the discussion table after it had gained the commitment of the firm's senior management to finalize and close all project requirements – the risk account that they had been trying to surface thus far.

As the vendor returned, ITD still held onto its risk account and again attempted to actively manage the vendor by instituting a military-like emergency "operations center" at the project office to track the resolution of user requirements more closely. The occurrence of these unexpected events, however, substantially eroded the credibility of ITD's dominant risk account.

Unhappy with such developments, some users expressed their displeasure with the ITD for its inability to mitigate risks despite noticing "*the same old routine of [the] vendor promising to get out of uncomfortable situations.*"

> *[ITD] was supposed to monitor and control the vendor. We saw a lot of monitoring but no control… [ITD] was not recovering fast enough to take grasp of the situation.* (Interview with Deputy Ops Manager)

The "operations center" soon lost its efficacy, as project charts and tables were not updated, ending up simply, as one project member noted ironically, as cosmetic "Chinese couplets"[5] on the walls. The "operations center" was closed down in early 2005 after just three months.

[5] Chinese couplets are auspicious verses written on red paper and typically displayed during the Chinese Lunar New Year.

Users began taking a more active role to renegotiate the dominant risk account and the related project priorities. User senior management raised a formal alert with the corporate management. The Head of Land HMBU pressured the ITD director to issue a formal memo to the corporate COO to reflect the dire state of Project Alpha, implicitly requesting an ultimatum for project closure. Through high-level senior management intervention between the vendor, ITD and the users, a more regular dialogue was instituted to keep track of the progress of Project Alpha. This process of dialogue brought about a more balanced context where inputs from all three parties were considered. Users, for example, also began acknowledging the issue of requirement management raised by the vendor.

> *They (the project team members) don't have the higher management focus… and are too bogged down at the tactical level. They don't realize the importance of fixing the user requirements.* (Interview with Head of Land HMBU)

As a result, the project risk accounts that addressed tight requirement management (vendor) and innovation complexity (users) were now given higher priority. At the same time, the vendor management (ITD) risk account was attenuated with an agreement by all parties that there would be relatively less emphasis on sticking strictly to formal project documentation and procedures for the time being. A more "vendor-friendly" ITD senior manager (above the ITD corporate project manager) was also brought in to mediate interaction between ITD and the vendor. He co-chaired the Project Working Committee with the Head of HMBU. Users also pushed for open, frank, and truthful reporting in tracking the progress of Project Alpha instead of "*waiting too late before raising it.*" Careless promises from the vendor, for example, were frowned upon by the users.

> *In some of the meetings, if the gut feel of the vendor is that they need nine months to complete a deliverable, they will put down nine months straight away! Can they stop being so optimistic? In one of the meetings, I told them upfront not to present the optimistic picture. They need to be realistic of what's coming ahead.* (Interview with Head of Land HMBU)

It was also agreed that any major issues identified by ITD, users, or the vendor should be immediately brought to the others. Such facilitated interactions helped the various stakeholders to develop a more sophisticated understanding of the project requirements and the common appreciation of the complexity in the novel warehouse planning system. Accordingly, a more "sequential roll-out" approach was adopted. Project Alpha was divided into two components, with delivery efforts emphasizing the implementation of the transactional component first while taking a "small-win" approach toward delivering the more complex planning engine component. Such a prototyping approach required ITD and the users to be actively involved with the vendor to learn and agree on the acceptable design solutions.

> *The (earlier) aggressive approach might not be the best. Our approach now is different, not big bang but through prototyping. Dynamic sorting, for example, is being experimented through a standalone system with a department. We practice first to get familiar with the concept. If it is ok, we will expand the solution to other processes.* (Interview with Ops Manager, Land HMBU)

The greater interactions among ITD, the users, and the vendor seemed to have enabled a more comprehensive understanding of risk, triggering the appropriate risk mitigating actions. Project Alpha was finally recognized as a "*complex and large system with complex engine formulation and workflow*" (as per project meeting minutes). Setting the algorithms and the underlying assumptions was "*more complex than expected.*" A key risk factor agreed upon was the lack of experience in domain expertise. Mitigation measures put in place included agreeing on the verification checklists of the planning engines upfront, instituting multiple trials and parallel runs, and extensive testing with good data sets to verify planning engines. The iterative and more concrete verification of planning engines enabled ITD, users, and vendor to sort out differences in requirement specifications and put the project back on course.

In mid-2006, the first transactional component was rolled out, followed by the containerization modules in early 2007. The full system (with its various planning modules) was finally completed at the end of 2007.

6. Discussion

The case of Project Alpha recounts the trajectory of a troubled project that is characterized by disruptions and multiple encounters of disagreement and conflict. Our close analysis reveals a dynamic social construction process. Figure 5 summarizes our observations as a process model that includes successive phases of risk construction, risk negotiation, and risk mitigating actions. As different stakeholders came to define and attach meanings to the critical risk in Project Alpha, their knowledge differentials (e.g., competencies/expertise, past experiences), vested interests (e.g., project roles and responsibilities), and value differences (e.g., IT - business - professional consulting culture) shaped the way they constructed their risk accounts. These factors are considered in our process model to be the "basis for risk construction." They do not stay static in the course of IT projects, but are affected by various events that occur. For example, the fragmented access to and the uneven distribution of information created disparity in knowledge among ITD, the vendor, and the users in perceiving the risk of innovation complexity for Project Alpha. It was only later when the information flow became more balanced, that such complexity became evident. Other factors (e.g., the vested interests related to specific project roles) are, however, more stable and have a pervasive influence throughout the project.

Similarly, the negotiation and contestation of risk accounts also manifested different degrees of intensity across phases. In the initial dominant phase, these risk accounts were passively negotiated. Given ITD's superior position in the project management structure, its account was largely accepted as given and became the dominant risk account. The first focusing event – the bankruptcy of the first subcontractor – jolted the basis of risk construction by exposing new information or information privy to one party, creating an opportunity for reconstruction as competing risk accounts of the users and vendor sought to be heard. The intensity of contestation grew as ITD had to address these concerns and actively repair its risk account during the repair phase. With its superior authority and control of information flow, it (consciously or unconsciously) filtered contextual cues or edited "social reality" to present risks in ways that accentuated its risk account while discounting other risk accounts and superficially addressing their concerns (e.g., in commissioning an independent study). Finally, with the second focusing event, i.e., the vendor's unexpected staging of an "information blackout," the context for negotiation and contestation was radically altered in the collective phase. With a revamped project management structure and a more balanced information flow, users now took charge in pushing a new order for the risk agenda. The continuous flux of negotiation and contestation and the uncertainties of their outcomes suggest a highly fluid and dynamic existence of IT project risk accounts.

Finally, the legitimacy of risk-mitigating actions followed from the contestation outcomes among the risk accounts. In this case, we saw initial mitigating actions to address vendor management risks, moving toward even more intensive efforts to address such risks, before radically switching to deal with the risks of innovation complexity and controlling user requirements. It was interesting to observe that ITD was not lacking in its efforts to exert control over the project. ITD was tenaciously trying to mitigate risks throughout the course of Project Alpha, exerting tremendous pressure on the vendor. It was not true that controls were not present, but these controls were rendered according to a specific risk account and, hence, did not address the concerns articulated by risk accounts that emphasized other critical risks. The social constructionist perspective, thus, helps us to understand why we still see projects failing despite the application of seemingly heavy controls or risk mitigating actions. Moreover, these risk-mitigating actions were dynamic. While they followed from a specific risk account, the dissonance resulting from the increasing misalignment between the mitigating actions and the risk realities did not necessarily dissipate but precipitated into focusing events that altered the basis for the risk (re)construction (e.g., the information blackout staged by the vendor). Such an interpretation, i.e., the possible self-correcting nature of risks through a focusing event, hints at the limit of social construction. It reaffirms the complementary risk management approach that we adopt here, i.e., while the social constructionist perspective is insightful, we cannot deny the objective realities of unmitigated risks.

The process model we propose from the analysis of Project Alpha illuminates the process of risk construction in an IT project. In the following discussion, we highlight a few noteworthy aspects of the process of social construction of risk:

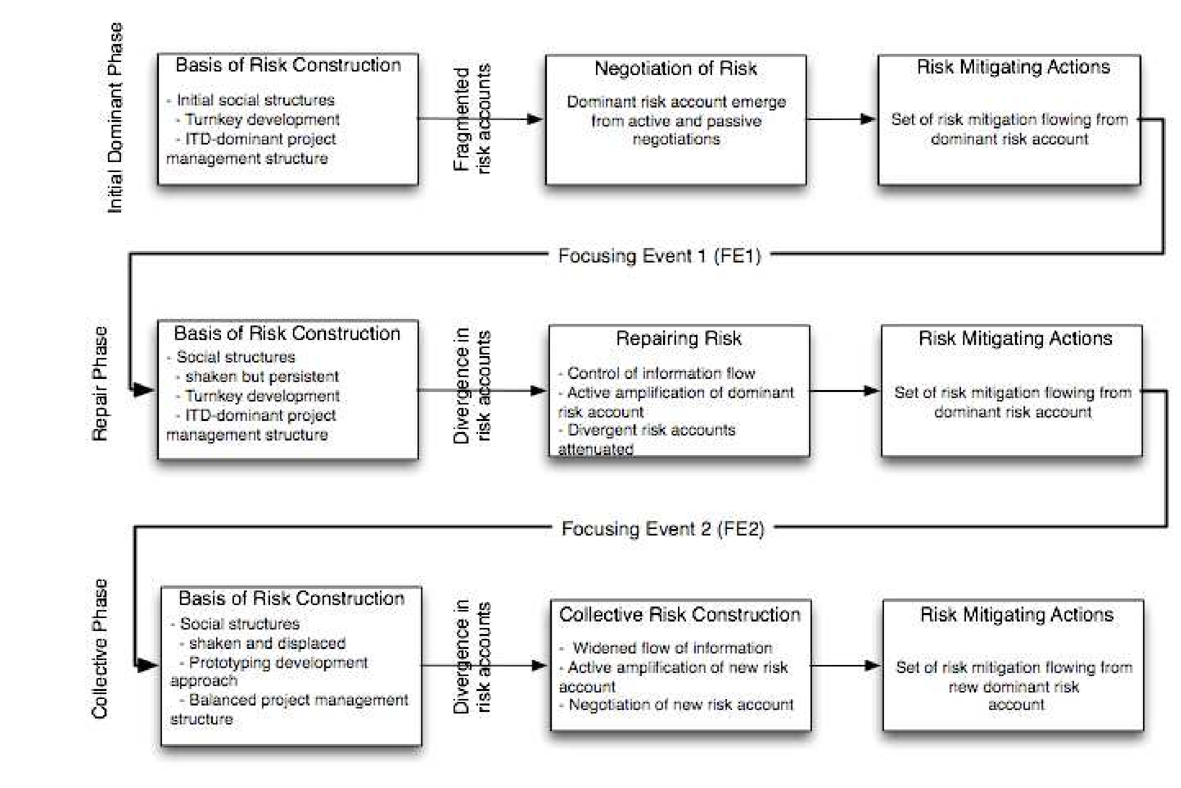
Initial Dominant Phase
Basis of Risk Construction
- Initial social structures
- Turnkey development
- ITD-dominant project management structure
Fragmented risk accounts
Negotiation of Risk
Dominant risk account emerge from active and passive negotiations
Risk Mitigating Actions
Set of risk mitigation flowing from dominant risk account
Focusing Event 1 (FE1)
Repair Phase
Basis of Risk Construction
- Social structures
- shaken but persistent
- Turnkey development
- ITD-dominant project management structure
Divergence in risk accounts
Repairing Risk
- Control of information flow
- Active amplification of dominant risk account
- Divergent risk accounts attenuated
Risk Mitigating Actions
Set of risk mitigation flowing from dominant risk account
Focusing Event 2 (FE2)
Collective Phase
Basis of Risk Construction
- Social structures
- shaken and displaced
- Prototyping development approach
- Balanced project management structure
Divergence in risk accounts
Collective Risk Construction
- Widened flow of information
- Active amplification of new risk account
- Negotiation of new risk account
Risk Mitigating Actions
Set of risk mitigation flowing from new dominant risk account

Figure 5. Key Phases in the Process of Social Construction of Risk in Project Alpha

6.1. Social construction of risk is inherently fragmented and subject to a process of negotiation and contestation

Unlike extant literature that assumes a homogeneous and objective set of project risks, we found that different stakeholders in Project Alpha held onto differing accounts that identified different aspects of the project as risk. Stakeholders in the project came from diverse backgrounds, played unique roles, and harbored divergent vested interests. Hence, their accounts of where the risks were and how to solve them were different. These risk accounts constituted what the different stakeholder groups understood as potential causes of project failing, as they made sense of the ambiguity and uncertainty surrounding the project. ITD saw the risk in managing the vendor. Users saw the risk in managing innovation complexity, and the vendor saw the risk in controlling user requirements. However, as the different risk accounts were brought together, they were subject to a process of negotiation and contestation (active or passive) in constructing overall risk perceptions. As different stakeholders took control, different accounts of risk and the related mitigating actions were amplified or attenuated (e.g., the consistent amplification of vendor management as the “real issue” by ITD, and ITD’s repeated brushing aside of the vendor’s concern about requirement management as an “irritant but not show-stopper”). The consequence was a fragmented view of risk, as weak signals from other risk accounts were ignored or discounted. The lack of a big picture view, for example, was noted by a senior manager in the user group in reflecting on lessons learned:

> *We were not fast enough to recover quickly to take grasp of the situation. There is no one to watch the bigger picture, to watch out for key areas….* (Interview with Head of Land HMBU)

As we saw in Project Alpha, the consequence was severe. The fragmented risk accounts by different stakeholders, which were not reconciled until very late in the project, had a significant negative impact on the project and jeopardized its completion.

6.2. Broader social structures predispose the risk construction in specific directions

Moreover, the negotiation and contestation of the risk accounts among the different stakeholders do not develop in a vacuum, but are shaped by broader social structures. These structures perpetuate specific social orders that amplify some risk accounts but attenuate others, having direct consequences on risk-mitigating actions. In Project Alpha, the broader social structure took the form of project governance, i.e., the turnkey development approach. The turnkey approach imposed a significant bearing on the process of risk construction, triggering a specific "fixated" response from ITD from its well-established repertoire of system development methodologies (though the turnkey development approach had been a relatively new addition). ITD saw it as a redistribution of project risk to the vendor and, thus, defined its role narrowly as vendor manager, instead of taking the broader ownership of project management responsibility that it would assume in other system development projects. Such a mindset was not limited to ITD alone. In a way, the users contracted ITD to deliver their IT system; ITD then contracted with the vendor to design, implement, and deliver; the vendor, in turn, outsourced the analytical engines to the subcontractor. The way the turnkey contracting approach was executed perpetuated a divisive "you-versus-me" mindset. Such a mindset inhibited the construction of a larger and richer picture of risk. The hands-off approach compartmentalized the roles and responsibilities and set the stage for a divided ITD-Users-Vendor project team. As each of them acted on their roles over the course of the project, their different interests and narrow motivations led naturally to the divergent construction of project risk from their own perspectives.

Such fragmentation was further reinforced by the project management structure that favored a specific balance in power. The formal authority vested upon ITD as the corporate project manager gave ITD an upper hand in shaping the construction of risk (e.g., its informational advantage, resource access to enact mitigating actions). Its risk account of tight vendor management arising from the turnkey contracting approach dominated the others. Murmurs of concerns from the other risk perspectives were voiced but not heard. The construction of the risk account and the related mitigating actions for the Project Alpha remained in the hands of a very small team of ITD managers. Their advantageous position in the project enabled them to construct a specific risk account and yet retained an air of rationality that "can be argued against but not rejected as being irrational" (Hansson 1989, p.108). Manning (1989, p.366) noted such maneuvers to justify and repair risk accounts as "the editing" or bracketing of cues and events for socially constructing reality and representing it to the organization. Until a later stage of Project Alpha when signs of trouble became glaringly obvious, the risk account of ITD was largely left uncontested. The finding, thus, suggests that the dominant risk account could possibly converge and be perpetuated with little or no need for explicit negotiation, due to the presence of a power imbalance embedded within the governance structure of such complex projects. It also explains why some stakeholders have a much greater ability than others to shape the social construction of risk.

6.3. Focusing events trigger the social re-construction of risk

Although ITD had an upper hand in pushing its agenda, the dominance of its risk account could not be taken for granted and needed careful defending and continuous "repair" to align with the surrounding events. The finding reaffirms that "closure" (in resolving multiple risk accounts) is a matter of degree (Pinch & Bijker, 1984). ITD's dominant risk account was unstable and had to be continuously defended, i.e., through systematic reasoning (Renn, 2008). The dominant risk account, however, may be "jolted" by specific crises or major events that are incongruent with such a risk account, casting doubts on the current position and triggering a renegotiation of the social order in constructing a new risk account. Such events may precipitate internally or surface entirely from external sources. These focusing events are interesting, as they provide the ingredients for multiple interpretations by the various stakeholders to reorganize their risk accounts. They afford the occasion to challenge taken-for-granted assumptions in the project, and often destabilize the dominant risk account and trigger fundamental shifts in the risk agenda (Birkland, 1998; Majchrzak et al., 2000).

However, such challenges may or may not be successful. For example, while ITD had to repair its account of risk after the first crisis, the broader social structures inherent in the turnkey development approach and the ITD-dominant project management structure were weakened but did not change; ITD as the Corporate Project Manager continued to enjoy a privileged position in the project management structure. Vendor management as a risk continued to be amplified while the risk accounts of others were attenuated. In contrast, these social structures were shaken and successfully displaced in the second crisis. The ITD-dominant project management structures were changed as the User Ops Manager assumed more control and the corporate unit introduced new oversight authority (ITD Senior Manager) over the ITD Project Manager to facilitate interaction with the vendor. Users and the vendor could now surface, package, and substantiate their risk accounts, legitimatizing their amplification. Similarly, the turnkey development approach became more incremental and participative as a prototype development approach was adopted. These findings suggest that the process by which a dominant risk account is re-opened for negotiation is more challenging. It involves substantial efforts to change the governance structure, shift the power balance, and leverage elements of emergent focusing events to support a different risk account. The possible occurrence of such focusing events and their reshaping uncertainties suggests that the process of risk construction is more dynamic than expected, as these events (endogenous or exogenous) can radically alter the attention on competing risk accounts or even create new risk accounts.

7. Contributions to Research and Practice

7.1. A social constructionist perspective of IT risk management

The case illustrates the usefulness of a social constructionist perspective in understanding risk management in a complex IT project. Recognizing risk as a social construction suggests that risk outcomes are inseparable from the process that produces them. Our analysis does not suggest that IT projects can do away with conventional technical risk assessments, but it does suggest that behind the facade of objectivity, there is a deeper socialization process that has a strong bearing in shaping the eventual definition of IT risks in complex projects. Understanding the socialization process addresses the question of why certain aspects of a project are identified, amplified as risk factors, and mitigated against, while others are ignored or brushed aside, with direct consequence on project outcomes.

For example, the large and established ITD had employed various risk management artifacts and methodologies in Project Alpha, e.g., the use of AHP in vendor selection, software quality assurance, project documentation standards, and the formal setup of an IT command center in managing critical operations. But these artifacts and methodologies were employed from the perspective of a single risk account of tightening vendor management. While they provided ITD with an inflated sense of security and confidence, they were limited in efficacy in addressing the other problems. The selection process for what constitutes a risk and what does not is not arbitrary, but tightly intertwined with the underlying social processes. The social constructionist perspective, thus, changes the questions we ask in IT risk management research. It helps to shift the IT risk management perspective toward a stronger process orientation. Greater emphasis should be placed on the risk assessment process and not just on the outcome (e.g., better risk calculation, more comprehensive methodologies), risk conversation and not just a checklist, risk culture and not just risk technology. This process-centric view means that the construction of risk is not a one-time exercise, but a continuously evolving effort as the socialization dynamic changes over time. Thus, treating risks as social constructs offers an important complementary perspective to theorize about IT risk management.

7.2. A process model of the social construction of IT project risk

We also propose from our analysis a process model that illustrates the social construction of risk in the management of complex IT projects. First, the process model highlights the role of social structures within the project context (e.g., institutionalized project governance and project management structure) in shaping the ensuing interaction within each phase. This is consistent with one of the precepts of process studies – that social processes are "embedded in the contexts that produce and are produced by them" (Pettigrew, 1997, p. 340). Second, by bracketing the IT project temporally, our process model draws attention to the socialization dynamics (e.g., the need for negotiation and contestation, the reshaping dynamism of focusing events) in risk construction. We show how these factors in one phase influence the subsequent basis of risk construction, the negotiation and contestation of risk accounts, and the legitimacy of risk-mitigating actions taken in future phases (Langley, 1999). Together these two features of the process model show why risk construction cannot be divorced from the broader social structures, e.g., the political decision-making process. Finally, it also shows that dominant risk accounts, while difficult to challenge and reopen for negotiation, can be displaced through dramatic focusing events. These focusing events, like critical encounters (Cho, Mathiassen, & Nilsson, 2008; Newman & Robey, 1992) or critical incidents (Lyytinen & Newman, 2008) discussed in IS process studies are necessary, but not sufficient, conditions for change in existing constructions of project risk.

The notion of project risk is, thus, dynamic, a tentative product of and ingredient for social interaction that is open to new definitions, solutions, and terms (Douglas & Wildavsky, 1982; Manning, 1989). The process model brings together the consideration of the social agents (multiple stakeholders), the external and more persistent social structural factors, and the internal and more emergent socialization dynamism factors to provide a holistic picture for us to understand the ongoing process through which risk is socially constructed and reconstructed. As such, our process model extends the growing stream of IS literature that has used the process approach in analyzing IS projects (e.g., Azad & Faraj, 2008; Cho et al., 2008; Lyytinen & Newman, 2008) into the domain of IT project risk management.

7.3. Implications for IT Risk Management Practices

In terms of contribution to practice, this research also highlights the need to manage the risk accounts from multiple stakeholders given the inherent fragmentation in complex projects. Different stakeholder groups are alert to different risks and new risks at different points in time (but never quite at the same time) as they enact different roles and as different trajectories of events occur. In other words, the relationship between stakeholders and IT project outcomes is more nuanced and complex than previously understood (Lyytinen et al., 1998; Schmidt et al., 2001). Our study shows that project management must manage the risk accounts of key stakeholders. Such a diversity of risk accounts is natural in complex projects and should be tapped to stimulate knowledge exchange to enlarge the risk picture, given that risk perceptions are often externalized to other stakeholders (Keil, Tiwana, & Bush, 2002). At the same time, project managers should be conscious of their own potential biases or blind spots arising from their roles and project expectations. They may need to rethink the top-down, authoritative approach, since this may unintentionally mute or remove important alternative views. Left unmanaged, the risk construction process and the related risk mitigating actions may only be done or decided by a “selected few” who hold dominant positions (including themselves), leading to dysfunctional risk management. It explains how individual preferences, political power, and private information get translated through the risk construction process into critical project decisions.

Project managers, thus, need to be more sensitive to the socialization dynamics underlying risk construction. In particular, a useful perspective follows from the notion of “collective mindfulness” (Weick & Roberts, 1993). Through their work with high-reliability organizations, Weick and Roberts have found that a successful approach to risk is built on a demanding social regime that is sensitive to multiple viewpoints of risk and encourages “perceptual malleability” (Langer, 1989; Weick & Roberts, 1993). It requires the fostering of social processes that are preoccupied with failures, reluctant to simplify observations, sensitive to operations, committed to resilience, and structurally under-specified for fluid decision making. This collective perspective collates and integrates various risk accounts to give meaning to “weak signals,” thus triggering the appropriate risk mitigating responses. It supplies the dynamic discerning capability for project members to doubt, ask about, and update their mental picture of risk continuously (Weick, Sutcliffe, & Obstfeld, 1999). In the case of Project Alpha, such interventions in social context did come, albeit belatedly, e.g., through the establishment of regular dialogue among ITD, users, and the vendor, and the appointment of a more vendor-friendly ITD senior manager to mediate between ITD and the vendor. The change in the socialization dynamic (i.e., more frequent, more fluid, two-way communication) facilitated the social reconstruction of risk.

Project managers should be reminded that a key role they play is to structure “critical dialogue” among key stakeholders. Focused efforts may be required to engineer the social context to enhance “collectiveness,” e.g., correcting imbalance in project authority, co-locating client-vendor work teams, promoting team building activities, instituting forums for knowledge sharing, and realigning joint incentives. Project managers should work toward facilitating healthy social processes to enable a richer and more comprehensive risk construction for greater effectiveness in risk mitigation.

7.4. Limitations and future research

As our research is an early attempt to understand the social construction of risk within the context of IT projects, additional research should be conducted to shed further light on this area. Given our research question, we conducted an in-depth case study of a single failing IT project using narrative and temporal bracketing strategies to inductively build our process model. While these strategies provide relatively high accuracy and richness, they necessarily lead to tradeoffs in terms of limited generalizability of the process model and our theoretical insights (Langley, 1999). In our case, the process model may be specific to complex projects with multi-vendor arrangements. Further research should be done to explore the applicability of the proposed process of social construction of risk within other IT projects of varying complexity and different governance structures. On the other hand, our process model may serve as a heuristic for critique and reformulation (Van de Ven & Poole, 1990, p. 532) and an initial theoretical foundation for more empirical research within the domain of IT project risk.

Another limitation of our research, as indicated earlier, is that it is principally based on archival data and retrospective accounts. We attempted to mitigate this with active triangulation of archival and interview data, but future studies should consider other data collection methods such as direct observations or extended interviews of participants at regular intervals to "capture reality in flight" (Pettigrew, 1997, p. 347) and thereby enrich and extend the findings of our research (Van de Ven, 2007).

Finally, this research extends IT risk research by explicating the nature of IT risks as products of social interactions and social structures. As we have discussed, we believe that our approach (social construction process) is complementary to traditional risk approaches that focus mainly on the objective aspects. Future research may adopt an integrated approach that includes elements from the rational-choice, cognitive-behavioral, and social-constructionist approaches. One potential research question may be to extend the current single process analysis to multiple processes as proposed by Pettigrew (1997) and recently highlighted in Lyytinen and Newman's socio-technical change model (2008). For example, we could study how the social construction process interacts with the cognitive-behavioral escalation process (Mähring & Keil, 2008). Researchers could explore the interactions between these two processes e.g., whether they are evolving in parallel or in overlapping sequence or if specific social interactions influence both the intersubjective perspective of risk and the individual level perception of risk.

8. Conclusion

To conclude, research has shown many IT projects exceed their budget, hobble past their scheduled delivery date, or deliver systems that fail to meet user requirements. These challenged projects continue to drain valuable organizational resources, and could ultimately end in a painful and protracted demise. This study demonstrates the relevance of a social constructionist perspective to enrich existing rational-choice or cognitive-behavioral approaches in managing IT risk for complex projects. Such projects often contain many risk signals, coming from different parts of the project, picked up by different stakeholders in the process. Understanding the notion of risk as a social construction is, thus, useful in clarifying why some signals constitute risks while others do not. Specifically, our study shows how risk is socially constructed through a process of articulating, negotiating, and contesting by various stakeholders in the project. The directions of the interaction are influenced by the broader social structures and can be dynamically reshaped by sudden focusing events. The process is highly emergent, demanding continuous management attention to the underlying social dynamics. Treating project risk as a social construct offers another perspective to theorize about project risk management, not just in understanding how stakeholder sense-making is related to risk construction, but also in broadening the project risk considerations to include the influence of social structures and processes. This heightened awareness of social structures and processes should also help to enhance the effectiveness of IT managers in deploying traditional risk management approaches.

References

Alter, S., & Ginzberg, M. (1978). Managing uncertainty in MIS implementation. *Sloan Management Review, 20*(1), 23-31.

Alter, S., & S. A. Sherer (2004). A general, but readily adaptable model of information system risk. *Communications of the Association for Information Systems, 14*, 1-28.

Azad, B., & Faraj, S. (2008). Making e-Government systems workable: Exploring the evolution of frames. *Journal of Strategic Information Systems, 17*(2), 75-98.

Barki, H., Rivard, S., & Talbot, J. (2001). An integrative contingency model of software project risk management. *Journal of Management Information Systems, 17*(4), 37-69.

Barrett, M., & Walsham, G. (1999). Electronic trading and work transformation in the London insurance market. *Information Systems Research, 10*(1), 1-22.

BBC News. (2007, 4 June 2007). *Complacency 'rife' in IT projects*. Retrieved 6 June 2007, from http://news.bbc.co.uk/1/hi/business/6720547.stm

Berger, P. L., & Luckmann, T. (1966/1991). *The social construction of reality: A treatise in the sociology of knowledge*. New York: Penguin Books.

Berkun, S. (2005). *The art of project management*. Sebastopol, CA: O'Reilly.

Birkland, T. A. (1998). Focusing events, mobilization, and agenda setting. *Journal of Public Policy, 18*(1), 53-74.

Boehm, B. W. (1991). Software risk management: principles and practices. *IEEE Software, 8*(1), 32-41.

Bradbury, J. A. (1989). The policy implications of differing concepts of risk. *Science, Technology, & Human Values, 14*(4), 380-399.

Carlo, J., K. Lyytinen, & Boland, R. J. (2004). Systemic risk, information technology artifacts, and high reliability organizations: A case of constructing a radical architecture. *Sprouts: Working Papers on Information Environments, Systems and Organizations, 4*(2), 57-73.

Cho, S., Mathiassen, L., & Nilsson, A. (2008). Contextual dynamics during health information systems implementation: an event-based actor-network approach. *European Journal of Information Systems, 17*(6), 614-630.

Clarke, L., & Short, J. F. J. (1993). Social organization and risk: Some current controversies. *Annual Review of Sociology, 19*(1), 375-399.

Davidson, E. J. (2002). Technology frames and framing: A socio-cognitive investigation of requirements determination. *MIS Quarterly, 26*(4), 329-358.

Davidson, E. J. (2006). A technological frames perspective on information technology and organizational change. *Journal of Applied Behavioral Science, 42*(1), 23-39.

Davis, G. B. (1982). Strategies for information requirements determination. *IBM Systems Journal, 21*(1), 4-30.

Douglas, M., & Wildavsky, A. (1982). *Risk and culture: An essay on the selection of technological and environmental dangers*. Berkeley, CA: University of California Press.

Drummond, H. (1996). The politics of risk: Trials and tribulations of the Taurus project. *Journal of Information Technology, 11*(4), 347-357.

Eggen, D., & Witte, G. (2006). The FBI's upgrade that wasn't. In *The Washington Post*. Washington, D.C.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review, 14*(4), 532-550.

Golden-Biddle, K. & Locke, K. (1993). Appealing work: An investigation of how ethnographic text convince. *Organization Science, 4*(4), 595-616.

Goldstein, H. (2005). Who killed the virtual case file? *IEEE Spectrum, 42*(9), 24-35.

Hansson, S. O. (1989). Dimensions of risk. *Risk Analysis, 9*(1), 107-112.

Hansson, S. O. (2010). Risk: Objective or subjective, facts or values. *Journal of Risk Research, 13*(2), 231-238.

Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R.,...Ratick, S. (1988). The social amplification of risk: A conceptual framework. *Risk Analysis, 8*(2), 177-187.

Keil, M. (1995). Pulling the plug: Software project management and the problem of project escalation. *MIS Quarterly, 19*(4), 421-447.

Keil, M., Depledge, G., & Rai, A. (2007). Escalation: The role of problem recognition and cognitive bias. *Decision Sciences, 38*(3), 391-421.

Keil, M., Mann, J., & Rai, A. (2000). Why software projects escalate: An empirical analysis and test of four theoretical models. *MIS Quarterly, 24*(4), 631-664.

Keil, M., Tiwana, A., & Bush, A. (2002). Reconciling user and project manager perceptions of IT project risk: A Delphi study. *Information Systems Journal*, 12(2), 103-119.

Langer, E. J. (1989). *Mindfulness*. Reading, MA: Addison-Wesley.

Langley, A. (1999). Strategies for theorizing from process data. *Academy of Management Review, 24*(4), 691-710.

Latour, B.,& Woolgar, S. (1979). *Laboratory life: The social construction of scientific facts*. Vol. 80. Beverly Hills, CA: Sage Publications.

Lin, A., & Silva, L. (2005). The social and political construction of technological frames. *European Journal of Information Systems, 14*(1), 49-59.

Lofland, J., & Lofland, L. H. (1995). *Analyzing social settings: A guide to qualitative observation and analysis* (3rd ed.). Bermont, CA: Wadsworth Publishing Company.

Lyytinen, K., Mathiassen, L., & Ropponen, J. (1998). Attention shaping and software risk - A categorical analysis of four classical risk management approaches. *Information Systems Research, 9*(3), 233-255.

Lyytinen, K., & Newman, M. (2008). Explaining information systems change: a punctuated socio-technical change model. *European Journal of Information Systems, 17*(6), 589-613.

Mähring, M., & Keil, M. (2008). Information technology project escalation: A process model. *Decision Sciences, 39*(2), 239-272.

Majchrzak, A., Rice, R. E., Malhotra, A., King, N., & Ba, S. (2000). Technology Adaptation: The case of a computer-supported inter-organizational virtual team. *MIS Quarterly, 24*(4), 569-600.

Manning, P. K. (1989). Managing risk: Managing uncertainty in the British nuclear installations inspectorate. *Law and Policy,* 11(3), 350-369.

Masuda, J. R., & Garvin, T. (2006). Place, culture, and the social amplification of risk. *Risk Analysis, 26*(2), 437-454.

McFarlan, F. W. (1981). Portfolio approach to information systems. *Harvard Business Review, 59*(5), 142-150.

McLoughlin, I., Badham, R., & Couchman, P. (2000). Rethinking political process in technological change: Socio-technical configurations and frames. *Technology Analysis & Strategic Management, 12*(1), 17-37.

Montealegre, R., & Keil, M. (2000). De-escalating information technology projects: Lessons from the Denver International Airport. *MIS Quarterly, 24*(3), 417-447.

Myers, M., & Newman, M. (2007). The qualitative interview in IS research: Examining the Craft. *Information & Organization, 17*(1), 2-26.

Nahar, N., Lyytinen, K. Huda, N., & Muravyov, S. V. (2006). Success factors for information technology supported international technology transfer: Finding expert consensus. *Information and Management, 43*(5), 663-677.

Newman, M., & Robey, D. (1992). A social process model of user-analyst relationships. *MIS Quarterly, 16*(2), 249-266.

Orbuch, T. L. (1997). People's accounts count: The sociology of accounts. *Annual Review of Sociology, 23*, 455-478.

Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: Making sense of information technology in organizations. *ACM Transactions on Information Systems, 12*(2), 174-207.

Otway, H. J., & Thomas, K. (1982). Reflections on risk perception and policy. *Risk Analysis, 2*, 269-82.

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. New York: Basic Books.

Pettigrew, A. M. (1990). Longitudinal field research on change: Theory and practice. *Organization Science, 1*(3), 267-292.

Pettigrew, A. M. (1997). What is a processual analysis? *Scandinavian Journal of Management, 13*(4), 337-348.

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science, 14*(3), 399-441.

Power, M. (2007). *Organized uncertainty*. New York: Oxford University Press.

Renn, O. (1992). Concepts of risks: A classification. In S. Krimsky & D. Golding (Eds.), *Social theories of risk* (pp. 53-79). Westport, CT: Praeger.

Renn, O. (2008). "Concepts of risk: An interdisciplinary review part 1: Disciplinary risk concepts. *GAIA - Ecological Perspectives for Science and Society, 17*(1), 50-66.

Schmidt, R. C., Lyytinen, K., Keil, M., & Cule, P. E. (2001). Identifying software project risks: An international Delphi study. *Journal of Management Information Systems, 17*(4), 5-36.

Scott, M. B., & Lyman, S. M. (1968). Accounts. *American Sociological Review, 33*(1), 46-62.

Shenhar, A. J., & Dvir, D. (2007). Project management research – the challenge and opportunity. *Project Management Journal, 38*(2), 93-99.

Shrader-Frechette, K. S. (1985). *Risk analysis and scientific method: Methodological and ethical problems with evaluating societal hazards*. Dodrecht: D. Reidel.

Stahl, B. C., Lichtenstein, Y., & Mangan, A. (2003). The limits of risk management – A social construction approach. *Communications of the International Information Management Association, 3*(3), 15-22.

Standish Group. (2003). *Latest Standish Group CHAOS Report shows project success rates have improved by 50%*. Retrieved from http://www.standishgroup.com/

Standish Group. (2009). *Standish Group report shows more projects failing and less successful projects*. Retrieved July 8, 2009, from http://www.standishgroup.com/newsroom/chaos_2009.php

Tierney, K. J. (1999). Toward a critical sociology of risk. *Sociological Forum, 14*(2), 215-242.

Tierney, K. J. (2007). From the margins to the mainstream? Disaster research at the crossroads. *Annual Review of Sociology, 33*, 503-525.

Tierney, K. J., & Bevc, C. (2007). Disaster as war: Militarism and the social construction of disaster in New Orleans. In D. L. Brunsma, D. Overfelt & J. S. Picou (Eds.), *The sociology of Katrina: Perspectives on a modern catastrophe* (pp. 35-50). Maryland: Rowman & Littlefield Publishers, Inc.

Tyre, M., & Orlikowski, W. (1994). Windows of opportunity: Temporal patterns of technological adaptation in organizations. *Organization Science, 5*(1), 98-118.

U.S. Office of the Inspector General. (2005). *Statement of Glenn A. Fine Inspector General, U.S. Department of Justice before the Senate Committee on Appropriations Subcommittee on Commerce, Justice, State and the Judiciary concerning The Federal Bureau of Investigation's Trilogy Information Technology Modernization Project*. Washington, D.C. Retrieved from http://www.justice.gov/oig/testimony/0502/final.pdf.

Van de Ven, A. (2007). Designing process studies. In A. Van de Ven (Ed.), *Engaged scholarship: Creating knowledge for science and practice* (pp. 194-231). Oxford, UK: Oxford University Press.

Van de Ven, A., & Huber, G. (1990). Longitudinal field research methods for studying processes of organizational change. *Organization Science, 1*(3), 213-219.

Van de Ven, A., & Poole, M. S. (1990). Methods for studying innovation development in the Minnesota Innovation Research Program. *Organization Science, 1*(3), 313-335.

Vaughan, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. Chicago, IL: University of Chicago Press.

Vaughan, D. (1999). The dark side of organizations: Mistake, misconduct, and disaster. *Annual Review of Sociology, 25*(1), 271-305.

Wagner, E., & Newell, S. (2006). Repairing ERP: Producing social order to create a working information system. *The Journal of Applied Behavioral Science, 42*(1), 40-57.

Weick, K. E., & Roberts, K. H. (1993). Collective mind in organizations: Heedful interrelating on flight decks. *Administrative Science Quarterly, 38*(3), 357-381.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. In R. I. Sutton & B. W. Staw (Eds.), *Research in organizational behavior* (pp. 81-123). Connecticut: JAI Press.

Wynne, B. (1992). Carving out science (and politics) in the regulatory jungle. Social *Studies of Science, 22*(4), 745-758.

Yeow, A., & Sia, S. (2008). Negotiating "best practices" in package software implementation. *Information & Organization, 18*(1), 1-28.

About the Authors

Wee-Kiat LIM is a Ph.D. student in the Department of Sociology at the University of Colorado at Boulder. He is also a graduate research assistant at the Natural Hazards Center in the Institute of Behavioral Science, University of Colorado at Boulder. His research interests include IT project management, the relationships between technology, organizations, and society, as well as how organizations respond to extreme events. Wee-Kiat has also published in *MIS Quarterly Executive* and in top refereed conferences, such as the International Conference of Information Systems (ICIS) and the Academy of Management Meeting. Previously, he was a research associate at the Information Management Research Center (IMARC) in Nanyang Business School, Nanyang Technological University. He holds a Bachelor of Communication Studies (Second Upper Honors) from Nanyang Technological University. He has also held research and planning positions in Singapore's telecommunications and national defense sectors.

Siew Kien SIA is an Associate Professor and the Director of the Information Management Research Center (IMARC) at Nanyang Business School, Nanyang Technological University. His main research interests focus on process redesign and integration, enterprise systems implementation, and global IT governance. Siew Kien has published in international journals such as *Decision Sciences*, *Communications of ACM*, *Journal of Management Information Systems*, *Journal of the Association for Information Systems*, *MIS Quarterly Executive*, *European Journal of Information Systems*, *Information and Organization*, *Journal of Strategic Information Systems*, *Journal of Information Technology*, and *Database*. He has over 18 years of research and consulting experience in private and public-sector organizations, as well as in global and Asian MNCs.

Adrian YEOW is an Assistant Professor in the Division of Information Technology and Operations Management at Nanyang Business School, Nanyang Technological University. He received a PhD in Information Systems from University of Maryland, College Park and a Bachelor of Communications Studies (First Class Honors) from Nanyang Technological University. Adrian's research focuses on how information technologies, institutions, and organizations interrelate with each other in organizational processes such as complex IT implementations and ongoing daily coordination practices. His works have been published in *Journal of the Association for Information Systems*, *Information & Organization* as well as in top refereed conferences such as International Conference of Information Systems (ICIS) and Academy of Management. Prior to entering academia, Adrian was a Manager of Product Development for a major Singapore communications company and has extensive product development and project management experience in telecommunications and software development.