

23 A STUDY OF THE RISKS IN AN INFORMATION SYSTEM OUTSOURCING PARTNERSHIP

Shabareesh Ajitkumar
Deborah Bunker
Stephen Smith
Donald Winchester
University of New South Wales
Sydney, Australia

Abstract

The objective of this paper is to report the findings of a case study into the risks involved in an information systems outsourcing partnership between a retail bank client and the vendor, an information technology service provider. By drawing on the case study, the paper proposes a theoretical development of shared benefits and shared risks in IT outsourcing partnerships. The paper argues that the longevity and success of the outsourcing partnership depends largely on managing shared risks and goals in the outsourcing partnership, which may gradually deteriorate over time without frequent, open interactions between partnership members. The outsourcing partnership contractual agreements alone may have limited scope in contributing to shared risk reduction in the IT outsourcing partnership if relationships deteriorate.

This research is based on an investigation of two organizations that used a formal contract to bind each partner's benefits, risks, roles, and responsibilities in an IT outsourcing partnership. Future research should seek to explore shared outsourced partnership benefits and risks across organizations in other sectors. Findings indicate that shared outsourced partnership risks need to be actively managed in order to reap the benefits. This paper argues that success in an IT outsourcing partnership relies on managing shared risks in the outsourcing relationship.

Keywords

Information technology, IT outsourcing, partnerships, shared risk

Please use the following format when citing this chapter:

Ajitkumar, S., Bunker, D., Smith, S., and Winchester, D., 2008, in IFIP International Federation for Information Processing, Volume 287, Open IT-Based Innovation: Moving Towards Cooperative IT Transfer and Knowledge Diffusion, eds. León, G., Bernardos, A., Casar, J., Kautz, K., and DeGross, J. (Boston: Springer), pp. 403-422.

1 INTRODUCTION

Information system outsourcing has experienced remarkable growth in recent years. The rapid growth of IS outsourcing has received extensive, on-going, worldwide business and information technology attention (Walker 1996). Information systems outsourcing deals have grown in size (Currie 2000), complexity (Marchand and Jacobsen 2001), and significance (Loh and Venkatraman 1992). This has resulted in an increased concern with the actual management of the outsourcing venture, and in particular with the issues of risk and risk management (Willcocks et al. 1999). Recent high profile outsourcing failures (e.g., Myers 1994) are further indicative of the lack of understanding of risk and risk mitigation practices that appear to be perpetuating within industry.

The next section discusses the literature review. Section three outlines the methodology. The fourth section overviews the outsourcing partnership. Section five interprets the case study. Section six sets the propositions for a proposed theory for the risks of IS outsourcing partnerships, briefly summarizing the main three propositions. The final section concludes and provides implications.

2 LITERATURE REVIEW

Several risks of IS outsourcing have been revealed in the literature, with most centered on the opportunistic behavior of the vendor, financial loss, service debasement, dependency, and loss of core competencies and skills (Ang and Toh 1998; Willcocks and Lacity 1999). Despite such revelation, several authors have claimed that research into outsourcing risk is still in its infancy and that there are “all too few systematic academic studies of the types of outsourcing risks, their salience and their mitigation” (Willcocks et al. 1999, p. 286). Outsourcing risk has only been investigated within the context of traditional buyer–seller type outsourcing, with no research to date examining risks salient in outsourcing partnerships.

Information system outsourcing partnerships are working relationships between client and vendor stakeholders that reflect a long-term commitment, a sense of mutual cooperation, shared risks and benefits and the presence of shared goals (Currie and Willcocks 1998; Lee 1998; Saunders et al. 1997). In recent years, much of the literature on IS outsourcing has focused on the emergence of the outsourcing partnership. Furthermore, several researchers claim that the nature of outsourcing has changed from a contractual to a partnership based relationship (Kern and Willcocks 2002). Lee et al. (2003) attribute the recent growth of outsourcing partnerships witnessed in industry to the maturity of outsourcing over time. Today, IS outsourcing involves a much greater depth and range of services, with companies now transferring entire IT functions, and in some cases even IT personnel, to their respective IT service providers. The apparent reverse in flow of IT resources “indicates a much more proactive role by today’s service providers, who assume more risk and investment than their counterparts in the past” (Lee et al. 2003, p. 87).

Despite the growing presence of IS outsourcing partnerships in both academic literature and in practice, no research to date has examined the risks pertinent to this form

of outsourcing. Currie and Willcocks (1998) investigated the risks inherent in different types of outsourcing arrangements and empirically found that each type presented a set of distinct risks. Although outsourcing partnerships were not examined, the study does, however, indicate that outsourcing partnerships may potentially pose unique risks that have yet to be identified by researchers. Furthermore, IS outsourcing partnerships are distinct from other forms of outsourcing given the underlying assumption that certain risks and benefits are shared by client and vendor partners (Lee and Kim 2005; Saunders et al. 1997). Consequentially, the risks of outsourcing identified within the literature may not apply to an IS outsourcing partnership, given its unique nature. Thus, there is an unequivocal need for exploratory and empirical research of the types of risks unique to an IS outsourcing partnership, their salience, and their interrelatedness. By conducting research of this nature, this study not only addresses a significant gap in the literature, but also provides practitioners with much needed insight into a highly critical area (risk) of a growing outsourcing discipline (partnership based outsourcing). The research problem is, *what are the risks entailed within an IS outsourcing partnership for both the client and the vendor?*

3 METHODOLOGY

The following research questions are formulated:

- Question 1. What risks are entailed within an IS outsourcing partnership for the client?
- Question 2. What risks are entailed within an IS outsourcing partnership for the vendor?
- Question 3. What risks are shared between the vendor and client in an IS outsourcing partnership?
- Question 4. How do these risks interrelate during the course of an IS outsourcing partnership?

To achieve the research objectives, an independent study was conducted. The interpretive approach has been selected as the theoretical perspective of choice, because the aims and purpose of interpretivist research are most suited to answering the research questions and are most reflective of the ontological and epistemological assumptions. Informed by the interpretivist theoretical perspective and its underlying assumptions, grounded theory has been selected with the aim of generating a descriptive and explanatory theory of the multiple perspectives of risk and risk management in the case companies involved in an IS outsourcing partnership.

Grounded theory is defined as a “general methodology for developing theory that is grounded in data systematically gathered and analyzed. Theory evolves during actual research, and it does this through continuous interplay between analysis and data collection” (Strauss and Corbin 1994, p. 273). The purpose of grounded theory is to inductively derive a theory by actively coding empirical data in such a way that categories, concepts, properties, and their interrelationships may be discovered. Within the grounded theory methodology, generating theory and conducting social research are,

conceptually, two parts of the same process (Glaser 1978). The Straussian approach has been employed in this study.

The data collection included semi-structured interviews with selected participants, organizational documents, and notes from direct observation. Fifteen semi-structured interviews were conducted, involving subjects from both the client and vendor organization. The number of interviews performed is within the suggested 15 to 20 interview range for qualitative research (Miles and Huberman 1984). Semi-structured interviews were used for a number of reasons. First, the nature of semi-structured interviews allowed answers evoked by initial questions to shape subsequent inquiries (Babbie 1992). Thus, the direction of the interview may be adapted according to issues and ideas raised by research participants. This allows researchers to uncover emergent issues and probe more deeply into issues of interest. This ability to uncover emergent issues is particularly appealing, given the earlier intentions of developing a substantive theory in the research area. Also, by only guiding conversation and not restricting participants in the type of information they could express, the semi-structured interview approach meets the demands of nondeterminism imposed by grounded theory (Charmaz 2000). Furthermore Rubin and Rubin (1995), also suggest that semi-structured interviews are advantageous in their ability to allow “questioning to be re-designed throughout the project” (p. 47). Thus, a greater understanding of the risks encountered during the partnership was developed, the semi-structured interview approach enabled refinement and redesign of the interview instrument to develop further insight into concepts or categories of interest. Participant subjects were interviewed face-to-face for the purposes of this study. The transcript of each participant was printed on a distinct color of paper so that they may be easily identified when placed on the “grounded theory wall.” Analysis of the interview transcript followed the coding (and categorizing) procedures prescribed by Strauss and Corbin (1990), which is open, axial, and selective coding.

4 OUTSOURCING PARTNERSHIP

The joint management infrastructure (JMI) project is a partnership between two organizations, namely, a large retail bank (First Bank) and Service Co., a global IT service provider (see Figure 1). Although the outsourcing arrangement took the form of a partnership, both organizations fundamentally assumed the role of either the client or the vendor. “*Before JMI the two companies were involved in a buyer-seller type agreement*” (Project Manager, Service Co.).

First Bank, the client organization in the partnership, requested Service Co. to provision numerous services within the bank’s infrastructure space, thereby subscribing Service Co. to the role of an outsourcing vendor or service provider.

Joint management infrastructure is an integrated solution of products (both hardware and software), architecture, and processes that offers a suite of delivery management technology enabling Service Co. to deliver its on-demand offering, which fulfils the promise of utility computing (i.e., the promise of “pay only for what is used”) in a shareable standardized environment. The result is a significant reduction in infrastructure costs for the client and an increase in the quality of services provisioned. Joint management infrastructure also provides Service Co. with a cost-effective mechanism to deliver

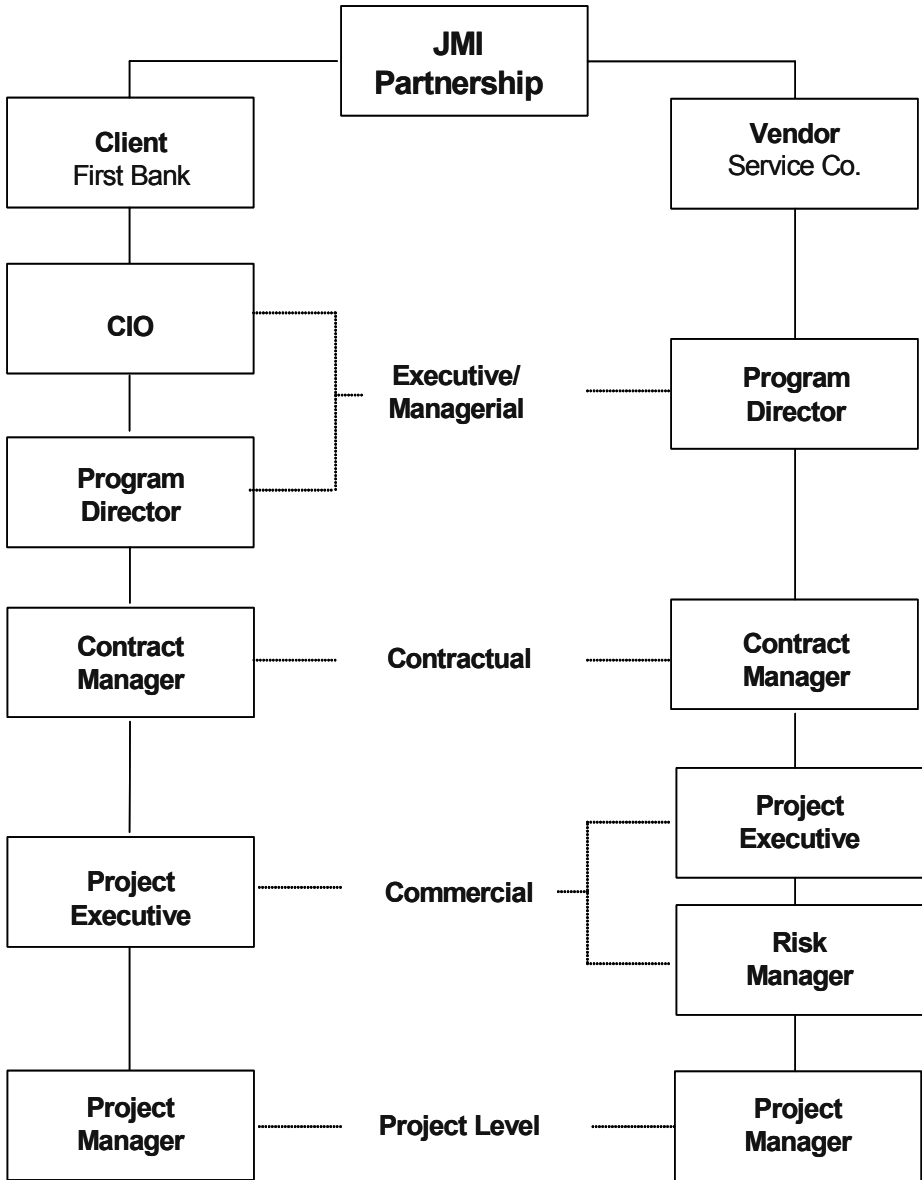


Figure 1. Overview of Interview Participants

infrastructure services for new on-demand services and new customer engagements, and to provide a platform to initiate movement of existing client accounts to an on-demand infrastructural suite. The JMI architectural model and its underlying technologies were developed by Service Co.'s technological innovation center in the United States and First Bank.

From a review of the literature (Currie and Willcocks 1998; Henderson 1990; Lee 1998; Saunders et al. 1997), a definition of the term *outsourcing partnership* was developed. A partnership, for the purpose of this study, is defined as

An interorganizational relationship involving a long-term commitment between a client and vendor where both parties collaboratively work towards shared goals, while sharing both risks and rewards.

Based on this definition, it is clear that an outsourcing partnership is characterized by the presence of

- shared benefits (rewards)
- shared risks
- long-term commitments
- shared goals

The JMI partnership embodies these defining partnership characteristics in the case study.

Table 1 shows that the JMI partnership meets the criteria outlined in the definition of an outsourcing partnership based on the literature. The JMI partnership entailed several shared benefits and risks, many of which were formally reflected in a risk and reward sharing contract. The key benefits that were shared between both organizations include:

- **Competitive advantage.** Due to the infancy of the JMI offering, the two organizations stand to gain significant competitive advantage. Joint management infrastructure offers Service Co. the opportunity to commercially test the viability of its on-demand service offering prior to its full release to the global market. The service

Table 1. Criteria for JMI to Meet the Definition of an Outsourcing Partnership

Definition Criteria	How Are These Criteria Met by the JMI Partnership?
Presence of shared risks and rewards	The JMI project entails shared risks and rewards for both First Bank (the client) and Service Co. (the vendor). Both organizations have collaborated to develop a common environment to support First Bank's financial systems. Service Co. profits from this venture by leveraging this environment into a standard platform to be sold to other banks and financial institutions. Thus, both First Bank and Service Co. have vested significant resources and capital into the venture, which consequentially will entail shared risks.
Long term commitments	The JMI venture has progressed into its fourth year (of 10). Levels of commitment from Service Co. and First Bank have been consistently high for the life of the partnership.
Shared goals	Service Co. and First Bank share a number of common goals, namely <ol style="list-style-type: none"> 1. To develop an on-demand Infrastructural environment, 2. To drive down long-term costs in the infrastructure space, 3. To reduce complexity within the infrastructure space by means of consolidation and standardization, and 4. To optimize efficiency in the provisioning of infrastructure services.

offering is unique and unrivaled by any competitor, thus if the implementation is a success, Service Co. gains the opportunity to exploit a niche within the infrastructure market and reap much competitive advantage. Similarly, First Bank operates in an industry where competition is heavily driven by price. Joint management infrastructure will enable the bank to significantly drive IT costs down, thus gaining a competitive advantage over competing financial institutions.

- **Financial Benefits.** Joint management infrastructure offers financial benefits for both firms. Through such measures as performance bonuses and profit sharing initiatives, both firms stand to profit equally from the venture. Furthermore, JMI enables both firms to significantly drive costs down in the infrastructure space. Prior to JMI, Service Co. was making a substantial loss on the First Bank account while the bank received poor levels of service at far too high of a cost. With the implementation of JMI, Service Co. is able to make a reasonable profit from the deal while First Bank receives significant cost reductions for provisioned infrastructure services.
- **Greater efficiency.** Joint management infrastructure promotes greater efficiency in the management and provisioning of infrastructure services. Service Co. can utilize fewer resources to build servers and board applications as the JMI architecture demands use of Service Co. specific hardware and software, all of which Service Co. technicians are experienced in using. First Bank also profits from this enhanced efficiency as the bank is able to receive a built server in only 48 hours, which is much faster than the previous provisioning process.
- **Access to and development of expertise.** By outsourcing the infrastructure function, First Bank hope to gain access to and leverage Service Co.'s global expertise. Prior to the outsourcing venture, First Bank espoused an undisciplined approach to the management of infrastructure, with servers lacking the standardization required to be effectively managed. By outsourcing the infrastructure, First Bank hoped to tap into the vendor's expertise and make its infrastructure far more manageable by means of consolidation and standardization. The partnership also presented Service Co. with the opportunity to develop expertise and experience in implementing the JMI architecture.

The partnership also required both organizations to share many risks. Contractually, a specific risk sharing model was embedded into the contract. Aside from the shared financial risks reflected in the risk sharing model, several strategic and operational risks were also shared between the two organizations.

5 CASE STUDY

This paper presents the key risks that emanated during the course of the JMI partnership. The findings revealed over 80 risk factors. Through the use of iterative coding, six substantive codes emerged:

- client strategic risks
- vendor strategic risks
- shared strategic risks
- client operational risks
- vendor operational risks
- shared operational risks

These substantive codes represent the key theoretical concepts for understanding the risks associated with IS outsourcing partnerships and address the strategic risks discussed next in this paper.

5.1 Client Strategic Risks

Client strategic risks are defined as risks whose impact pervades beyond the boundaries of the partnership, risks that have a direct, adverse impact on the client organization's long-term business strategy, competitiveness, viability, and profitability. Several studies have proposed similar definitions of strategic risk (Aron et al. 2005; Clarke and Varma 1999; Collins and Ruefli 1995; Emblemssvag and Kjolstad 2002; Smith et al. 2001; Travis and Saldanha 1999).

Dependency is another key strategic risk for First Bank. By outsourcing its entire infrastructure function to a third party vendor, First Bank inherently forms a dependency on Service Co. for the provisioning of infrastructure services. "*We need JMI to survive—so there's definitely a dependency there*" (Project Manager, First Bank). This dependency resulted from the lack of internal capabilities, which the bank retained after outsourcing its infrastructure function. One of the significant corollaries of forming a dependency on Service Co. for the provisioning of all infrastructure services was the loss of control that eventuated. Once the infrastructure function had been outsourced, a gradual loss of control over the future direction of the infrastructure was noted. This precluded the bank's infrastructure function from serving its business needs, thus propelling a certain divide between IT and the business.

Another strategic risk that was realized by the client organization was the loss of innovative capacity within the infrastructure space. Service Co., by owning all of the infrastructure and its constituting components, assumed responsibility of all infrastructural maintenance and enhancement related activities. This presented First Bank with a significant risk as it was unable to assume immediate control of JMI's innovative and technological progression.

First Bank was also posed with significant financial risks during the course of the partnership. Such risks relate not to the loss of investments made into the partnership, although they are the wider financial repercussions of partnership failure. The costs associated with recovering from failure are quite significant for First Bank as substantial investments would be required to bring the infrastructure function back in house or to establish a new outsourcing arrangement with an alternate service provider.

5.2 Vendor Strategic Risks

Vendor strategic risks are defined as risks whose impacts go beyond the boundaries of the partnership, that is, risks that have a direct and adverse impact on the vendor organization's long-term business strategy, competitiveness, viability, and profitability.

A key strategic risk for Service Co. was the market failure of their JMI service offering. The JMI partnership presented Service Co. with the opportunity to test the commercial viability of their JMI offering. Significant investments were made to design the JMI architecture and its surrounding processes.

The JMI partnership also entailed a significant reputation risk for Service Co. *"If we don't get this implementation of JMI right, then we could lose the interest of other banks around the world"* (Risk Manager, Service Co.). Given the fact that the partnership was highly publicized, many of Service Co.'s existing and potential clients eagerly followed the progress of the partnership to gauge whether JMI could really deliver the benefits that it promised. This high degree of transparency presented Service Co. with the forbidding risk of losing potential business had the venture failed.

Dependency is a risk commonly associated with the client organization (Aubert et al. 2002; Hoecsht and Trott 2006). However, the JMI case indicates that this is a risk also experienced by the vendor. Respondents interviewed from Service Co. acknowledged that the vendor formed a dependency on the client. *"It is a big account for Service Co.; First Bank is one of our biggest clients accounting for about a fifth of our business"* (Program Director, Service Co.). The nature of this dependency was two-fold: first, a financial dependency existed as Service Co. relied on First Bank as a stable and continuous source of income, and second, a dependency of advocacy was also ingrained in the outsourcing relationship between the organizations.

By entering into the JMI partnership, Service Co. assumed a series of financial risks. Such risks do not necessarily pertain to the direct loss of capital invested into the partnership (e.g., financial risks), although they are the indirect financial implications associated with partnership failure. These include loss of future business, failing to make a return on investments in developing the JMI service offering, costs incurred in business transformation and retransformation, and the opportunity costs associated with the time and resources invested in developing and marketing the JMI service offering and on-demand business strategy.

5.3 Shared Strategic Risks

Shared strategic risks are defined as risks whose impacts go beyond the boundaries of the partnership, that is, risks that have a direct, adverse, and mutual impact on the organizations' long-term business strategy, competitiveness, viability, and profitability. Despite several studies acknowledging the presence of shared risks in outsourcing partnerships, no research to date has been able to provide any insight into the types of risks that are shared between the vendor and client. An analysis of the findings confirms that risks are indeed shared between the client and vendor and further reveals that such risks are of a strategic nature.

The JMI venture required both organizations to invest heavily into the partnership. Such investment came in the form of capital, time, and labor resources. Thus, the partnership posed a shared financial risk for both organizations. The risk–reward sharing contract also encouraged both organizations to share financial risks. Additionally, an element of profit sharing was also reflected in the contract, which aligned the two organizations financially.

Unlawful disclosure of trade secrets and confidential information was another risk to which both Service Co. and First Bank were alert. The JMI partnership demanded a high level of transparency to be established across both organizations. Thus, each organization had access to highly confidential materials belonging to their respective partner. This was indeed an alarming risk for both organizations as disclosure of such confidential materials may directly affect their respective competitive positions.

First Bank’s concerns pertained more so to the disclosure of confidential customer data and the entailing legal repercussions. The design of JMI specified that all virtual servers provisioned would reside physically on Service Co.’s premises. Furthermore, several personnel from the vendor organization required access to all data managed by the infrastructure. Several cases of information leakage and disclosure have been presented in the literature (Khalfan 2004; Peltier 1996), although no studies have acknowledged that this is a risk that is also carried by the vendor.

Partner financial instability is another shared strategic risk that was noted in the case study. Given the dependencies between the two organizations, a significant risk emerges if one of the partner companies was to collapse financially, consequentially resulting in the ultimate failure of the partnership and placing the other partner further at risk. The risk of partner instability is also pertinent to Service Co., who, in the event of First Bank financially collapsing, will fail to make a return on their investment and ultimately lose a substantial source of continued income. Sullivan and Ngwenyama (2005) found that “vendor financial instability will lead to a willingness to shirk under the terms of the contract—a vendor with nothing to lose is more willing to walk away from the contract and declare bankruptcy” (p. 76).

Severance of the business relationship between First Bank and Service Co. was another shared strategic risk that emerged during the course of the JMI partnership. “*We were both conscious of the fact that if JMI did not work then that would mean the end of our working relationship*” (Project Manager, Service Co.). Both organizations came to the realization that JMI signified one final attempt to sustain their business relationship. The severance of the business relationship presents significant consequences for both the client and vendor.

5.4 Client Operational Risks

A client operational risk is a risk whose potential impact is contained within the boundaries of the partnership (i.e., at the project level), that is, a risk that has a direct and adverse impact on

- the client’s ability to carry out its roles and responsibilities as defined in the partnership
- the client’s ability to realize expected goals and benefits as defined in the partnership

Several client operational risks emerged during the course of the JMI partnership.

Perhaps the most significant client operational risk was the debasement of service that eventuated as a result of First Bank adopting the JMI service model. One of the goals that First Bank had set prior to entering into the partnership was to greatly improve the quality of infrastructural services through the implementation of JMI. This goal, however, was not entirely achieved as a result of Service Co.'s failure to meet established service levels.

The debasement of service that occurred during the JMI case clearly limited First Bank's ability to achieve its goal of enhancing the efficiency and quality of processes within the infrastructure space. Furthermore, the expected benefit of gaining a competitive advantage through the implementation of JMI was also not realized as a result of Service Co. failing to meet numerous service level targets.

First Bank's limited understanding of the JMI technology was another operational risk that precluded the client from meeting its responsibilities under the terms of the outsourcing contract. From an analysis of the findings, it is clear that personnel from the client organization did not have a sound understanding of JMI in terms of how the infrastructure set-up works, the nature of its underlying technologies, or the scope of its functionality.

The somewhat limited understanding of JMI conveyed by members of First Bank's project teams is a cause for concern. When assessing the progress of the JMI partnership, it is clear that such a lack of understanding precluded First Bank from meeting several of its assumed responsibilities. First Bank's internal project team was unable to adequately modify a significant proportion of the bank's applications and systems as part of the application refresh initiative. This may be attributed to the team's failure to achieve a satisfactory level of understanding of JMI's technical specifications.

Given the infancy of the JMI solution, it was evident during the course of the partnership that Service Co. was highly inexperienced with its delivery. Several respondents, surprisingly from both organizations, conveyed their concerns over the vendor's inexperience with the outsourced technology. It is evident from the case that the vendor's lack of experience with the outsourced technology is indeed an operational risk for the client. Service Co.'s inexperience with JMI limited First Bank's ability to achieve its goals of improving efficiency within the infrastructure space and the quality of infrastructure services.

The implementation of the JMI architecture and its surrounding processes required First Bank to undergo extensive internal changes, particularly in relation to the way in which IT teams approached system development and maintenance related projects. Prior to JMI, all server design, development, and implementation related activities were performed by system architects assigned to project teams. With the onset of JMI, all servers were now centrally provisioned and managed by Service Co. Due to large numbers of users refusing to adopt the JMI service offering, several in-house servers needed to be maintained in order to support the systems and applications of noncompliant users. The maintenance of such additional servers extends the terms of the outsourcing contract, thus presenting further costs for First Bank.

To facilitate the JMI venture, a substantial number of First Bank's system architects were permanently transferred to Service Co. Somewhat surprisingly, not all of the transferred staff were assigned to the JMI project, with many being assigned to other client engagements. Respondents interviewed from First Bank were highly critical of

Service Co.'s management of the transitional employees, conveying that the knowledge these employees had of the bank's applications, systems, and processes could not be leveraged if they weren't directly involved in the project.

A corollary of losing internal capabilities, as stated in the literature, is the gradual tendency of the client to offload complete responsibility of the outsourced function (Lacity and Willcocks 1998; Willcocks et al. 1999). This was evident in the case, with Service Co. having assumed ownership of the entire infrastructure function by the end of the implementation phase. Offloading responsibility of the management and operation of infrastructure is a prominent risk for First Bank as, in doing so, the bank had no direct control over the quality of service that it received.

5.5 Vendor Operational Risks

A vendor operational risk is a risk whose potential impact is contained within the boundaries of the partnership (i.e., at the project level), that is, a risk that has a direct and adverse impact on

- the vendor's ability to carry out its roles and responsibilities as defined in the partnership
- the vendor's ability to realize expected goals and benefits as defined in the partnership

Several vendor operational risks emerged during the course of the JMI partnership. It must be noted that the literature offers no insight into the types of risks encountered by the vendor during an outsourcing venture. Thus, this study addresses a significant gap in the literature through its identification, analysis and discussion of vendor operational risks.

This study's findings have clearly shown that the vendor's lack of experience is indeed a risk to the client at an operational level. However, an analysis of the findings further indicates that this is in fact an operational risk for the vendor as well. Service Co.'s inexperience with JMI led the partner to miss several key service level targets. This resulted in the vendor being penalized financially and further prevented the vendor from acquiring the performance bonus. It was essential for Service Co. to achieve the performance bonus in order to recover the investments made in purchasing all of the equipment required to implement JMI.

The client's lack of understanding of the outsourced technology also presented a risk for Service Co. The vendor was unable to achieve its goal of developing a truly standardized infrastructural environment due to First Bank's incessant requests to customize infrastructural components. Respondents from Service Co. attribute this to First Bank's failure to understand the nature JMI and the capabilities that it offers.

First Bank's lack of understanding of JMI also prevented the bank from adequately managing the vendor. In light of the events presented by the JMI case, it is evident that the client's lack of understanding is indeed a risk for the vendor as well. One may be inclined to classify this risk as a vendor operational risk as it clearly limited Service Co.'s ability to deliver the JMI infrastructure on time and within budget.

Another operational risk which was evident in the case was the lack of demarcation of duties between Service Co. and other subcontractors such as TelCo. TelCo. was responsible for all networking and connectivity related tasks during the course of the partnership. This included laying the network cables and installing all the network devices such as switches, routers, and hubs. The JMI infrastructure operated through the physical infrastructure implemented by TelCo. This difficulty in determining accountability for infrastructure failures further limited Service Co.'s ability to deliver JMI within the scheduled time frame as much time was needed to uncover the source of problems.

Service Co. may have been in a better position to meet service levels and prevent many of the network failures if the vendor had direct control over TelCo. and was accountable for the subcontractor's performance. This was not the case during the partnership as the subcontractor was directly managed by First Bank. This arrangement was somewhat ineffective as First Bank had little knowledge of the network design and JMI's network requirements. Service Co. would have been in a far better position to manage TelCo. due to the corporation's thorough understanding of JMI's physical design and the infrastructure's network requirements. Thus, by limiting the vendor's ability to meet its responsibilities as defined in the partnership agreement, the risk of lack of control over subcontractors can be clearly classified as a vendor operational risk.

According to respondents from Service Co., First Bank failed to provide the vendor with adequate forecasts of expected capacity. Such forecasts were essential to Service Co.'s capacity provisioning process as the vendor needed sufficient time to scale the infrastructure to support First Bank's future capacity needs. The contract specified that First Bank was to establish a capacity pipeline that provided forecasts of capacity spanning for a period of one year. However, the bank was unable to meet this requirement, instead providing forecasts for only a period of eight months. Thus, it is clear from the events in the case that the client's inability or unwillingness to meet commitments is indeed a vendor operational risk. The reason for this is because the risk limited Service Co.'s ability to meet certain responsibilities (i.e., deliver JMI on time, provision required levels of capacity and board the required applications) and achieve specific goals (maximize efficiency and drive down costs within the infrastructure space).

Service Co. was unfairly assessed on a number of occasions during the course of the partnership, which resulted in the company suffering financially. One such example was Service Co. enduring numerous penalties for outages experienced during the implementation phase. It was established that the cause of these outages was TelCo.'s implementation of an unstable network. Despite this fact, First Bank continued to penalize Service Co., even though the contract negates any liability on the part of the vendor in the event that an outage occurs due to faults in the physical network. As a result of such unfair assessments, Service Co. was unable to gain any real recoverability on investments made into the partnership.

5.6 Shared Operational Risk

A shared operational risk is a risk whose potential impact is contained within the boundaries of the partnership (i.e., at the project level), that is, a risk that has a direct and adverse impact on

- the abilities of the client and vendor to carry out their roles and responsibilities as defined in the partnership arrangement
- the abilities of the client and vendor to realize expected shared goals and benefits as defined in the partnership arrangement

Several researchers have theorized that outsourcing partnerships entail risks that mutually affect both client and vendor partners (Currie and Willcocks 1998; Lacity and Willcocks 1998; Lee and Kim 1999; McFarlan and Nolan 1995). However, no study has exposed the types of risks that are indeed shared between the client and vendor. This study addresses this gap. Six main areas of shared operational risks were identified from the events in the case and are now briefly discussed.

Relational risks refer to risks that inhibit collaboration between the vendor and client, thus preventing them from working effectively to achieve shared goals and fulfil shared responsibilities. The lack of trust between the two organizations led to several conflicts emerging during the course of the partnership. Furthermore, because the organizations did not trust each other, conflicts could not be resolved on a relational level and were often escalated to the contract managers. This greatly impeded both organizations from performing their respective responsibilities as they were constantly disputing the terms of the contract.

The requirements also posed several risks that precluded both the client and vendor from meeting their shared responsibilities. Respondents described the requirements prepared by First Bank as incomplete, unclear, and poorly specified.

The nature of the JMI technology itself posed several risks for the two organizations that potentially limited their abilities to achieve shared goals and realize planned technological benefits. One of the primary technology risks which the case revealed was the uncertainty of the technological direction taken by both organizations. It is important to note that JMI is by no means a stand-alone solution; instead it is a discipline that demands both the client and vendor to follow a specific technological direction. This direction has a diverse impact, affecting all of First Bank's operations within the infrastructure space and shaping Service Co.'s management of the bank's infrastructure.

The contextual environment in which the partnership took place also presented risks for the two organizations. Such risks had a direct and adverse impact on their ability to achieve shared goals and fulfil shared responsibilities. The Reserve Bank of Australia (RBA), a regulator within the banking industry, exerted much pressure on both organizations during the course of the JMI partnership. All infrastructure designs, business continuity plans, and disaster recovery plans were required to be submitted to the RBA for approval before the project could transition to the build and implementation phase. A comprehensive review of the literature revealed only one study (Willcocks et al. 1999) that considered environment risks.

Several risks emerged as a result of inadequate management practices. Such risks have been classified as shared operational risks as they inhibited both organizations from fulfilling their shared responsibilities of managing the outsourcing partnership. Senior management's failure to communicate the partnership presented a clear risk for both organizations. The partnership emanated from a series of negotiations between senior managers from both organizations, with personnel involved at the implementation level having no visibility of the nature of the partnership arrangement.

The use of a long-term contract posed a risk to both organizations. Traditionally, outsourcing contracts have taken the form of short term engagements. By signing a 10 year deal, Service Co. was presented with the opportunity to truly develop JMI as a global, on-demand service offering and stood to reap significant financial benefits. However, given that the partnership was driven by a risk–reward sharing contract, Service Co. was also at risk of suffering a long-term financial loss as a result of poor service provisioning or the JMI technology failing to meet expectations. Perhaps the most significant contractual risk revealed in the case was the contract’s failure to represent the intent of both parties. “*We needed to communicate more...especially how we were progressing*” (Project Manager, Service Co.).

6 THE RISKS OF IS OUTSOURCING PARTNERSHIPS: A THEORY PROPOSAL

An analysis and interpretation of the JMI case study presented in section 5 suggests six substantive codes: *client strategic risks*, *vendor strategic risks*, *shared strategic risks*, *client operational risks*, *vendor operational risks*, and *shared operational risks*. It is clear that these risks are not independent, but are interrelated. At the heart of the substantive theory are the *shared operational risks*. These risks have been identified as the core risks of an outsourcing partnership. It is proposed that shared operational risks exert an influence (that is, increase the likelihood) on all of the other five types of risks. *Vendor operational risks* are also proposed to increase the likelihood of *vendor strategic risks*. Similarly, it is proposed that *client operational risks* increase the likelihood of *client strategic risks*.

Three main propositions have been put forward as part of the substantive theory and for brevity are briefly summarized as

1. Increased *shared operational risks* increase the likelihood of all *strategic risks* (*shared strategic risks*, *client strategic risks*, and *vendor strategic risks*).
2. Increased *shared operational risks* increase the likelihood of *client* and *vendor operational risks*.
3. Increased *client/vendor operational risks* increase the likelihood *client/vendor strategic risks*.

The three propositions and the directions of their interactions with the six risk categories are shown in Figure 2.

Figure 2 illustrates several minor propositions, listed below, for each main proposition (these are not discussed due to word limitations).

- Proposition 1.1: Increased shared operational risks increases the likelihood of shared strategic risks.
- Proposition 1.2: Increased shared operational risks increases the likelihood of vendor strategic risks.
- Proposition 1.3: Increased shared operational risks increases the likelihood of client strategic risks.

Proposition 1: Increased *shared operational risks* increase the likelihood of all *strategic risks*.

Proposition 2: Increased *shared operational risks* increase the likelihood of all *client and vendor operational risks*.

Proposition 3: Increased *client operational risks* increase the likelihood of all *client and vendor strategic risks*.

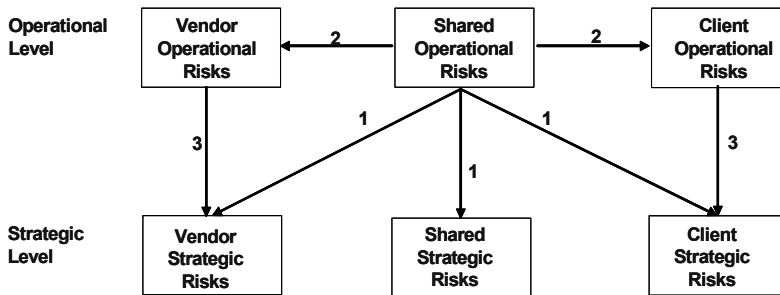


Figure 2. Three Propositions and Directional Interactions between Six Coded Risk Categories

- Proposition 2.1: Increased shared operational risks increase the likelihood of client operational risks.
- Proposition 2.2: Increased shared operational risks increase the likelihood of vendor operational risks.
- Proposition 3.1: Increased vendor operational risks increases the likelihood of vendor strategic risks.
- Proposition 3.2: Increased client operational risks increases the likelihood of client strategic risks.

6.1 Proposition 1 Summary

It is proposed that increased shared operational risks increase the likelihood of shared strategic risks, client strategic risks, and vendor strategic risks.

The likelihood is that all strategic risks increase as shared operational risks are realized by the client and vendor. The fundamental reason for this is because shared operational risks directly threaten the success of the partnership. As the case has shown, in line with the literature on outsourcing partnerships, the inability of both organizations to meet shared responsibilities and realize shared goals and benefits will ultimately drive the partnership to failure.

6.2 Proposition 2 Summary

The findings of this study revealed that increased shared operational risks increase the likelihood of client and vendor operational risks. Not meeting shared goals and shared responsibilities further limits the achievement of individual goals and the fulfillment of individual responsibilities. A shared goal, which the two organizations failed to

meet during the course of the partnership, was to develop and implement a standardized infrastructure environment.

6.3 Proposition 3 Summary

Failure to achieve individual goals and fulfil individual responsibilities promotes risks, which directly impact the organization's strategy, viability, profitability, and competitiveness (i.e., vendor/client strategic risks).

7 CONCLUSION AND IMPLICATIONS

The theoretical framework reveals six key types of risks: vendor strategic risks, shared strategic risks, client strategic risks, vendor operational risks, shared operational risks, and client operational risks, and their interrelationships. Shared operational risks have been identified as the central risks in an IS outsourcing partnership, influencing all of the other five risk types. Additionally, it was found that client operational risks increase the likelihood of client strategic risks. Similarly, an analysis of the findings revealed that vendor operational risks increase the likelihood of vendor strategic risks.

Development of this substantive theory has contributed to the IS outsourcing research literature by addressing two key gaps within the research domain. First, a review of the literature indicated that no study of risk in the context of IS outsourcing partnerships has been conducted. Second, no research to date has examined risk from the perspective of both client and vendor stakeholders. In addressing these areas overlooked in the research field, this study presents several important implications for theory and practice. Finally, no studies of outsourcing risk have considered risk from the vendor perspective. Thus, the literature provides no insight into the types of risks experienced by the vendor during an outsourcing engagement. This study, by analyzing the empirical data gathered from the case, has uncovered several risks that are pertinent to the vendor. In doing so, this study has addressed a significant gap in the outsourcing literature.

For practitioners, the substantive theory developed in this research study offers much insight into the main areas of risk deserving management attention during an IS outsourcing partnership arrangement. In developing an awareness of the six key risk areas and their interrelatedness, practitioners will be better prepared to manage many of the risks entailed in IS outsourcing partnerships. The theoretical contribution of this research lies in its proposal of a substantive theory of risk. This theory contributes to a better understanding of the risks of IS outsourcing partnerships. A limitation of this study is the single-case study methodology employed. Further research in this area from both a theoretical and empirical nature is ongoing.

References

- Ang, S., and Toh, S. K. 1998. "Failure in Software Outsourcing: A Case Analysis," in *Strategic Sourcing of Information Systems*, L. P. Willcocks and M. C. Lacity (eds.), Chichester, UK: John Wiley and Sons Ltd., pp. 351-368.

- Aron, R., Clemons, E. K., and Reddi, S. 2005. "Just Right Outsourcing: Understanding and Managing Risk," *Journal of Management Information Systems* (22:2), pp. 37-56.
- Aubert, B., Patry, M., Rivard, S., and Smith, H. 2001. "IT Outsourcing Risk Management at British Petroleum," in *Proceedings of the 34th Hawaii International Conference on System Sciences*, Maui, HI, January 3-6, Los Alamitos, CA: IEEE Computer Society Press.
- Babbie, E. 1992. *The Practice of Social Research Methods for Social Work* (6th ed.), Belmont, CA: Wadsworth Publishing Company.
- Charmaz, K. 2000. "Grounded Theory: Objectivist and Constructivist Methods," in *Handbook of Qualitative Research* (2nd ed.), N. K. Denzin and Y. S. Lincoln (eds.), Thousand Oaks, CA: Sage Publications, pp. 509-535.
- Clarke C. J., and Varma S. 1999. "Strategic Risk Management: The New Competitive Edge," *Long Range Planning* (32:4), pp. 414-424.
- Collins, J. M., and Ruefli, T. W. 1995. *Strategic Risk: A State-Defined Approach*, Boston: Springer.
- Currie, W. 2000. "The Supply-Side of IT Outsourcing: The Trend towards Mergers, Acquisitions and Joint Ventures," *International Journal of Physical Distribution and Logistics Management* (30), pp. 238-254.
- Currie, W. L., and Willcocks, L. P. 1998. "Analyzing Four Types of IT Sourcing Decisions in the Context of Scale, Client/Supplier Interdependency and Risk Mitigation," *Information Systems Journal* (8:2), pp. 119-143.
- Emblemsvag, J., and Kjolstad, L. E. 2002. "Strategic Risk Analysis: A Field Version," *Management Decision* (40:9), pp. 842-852.
- Glaser, B. 1978. *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory*, Mill Valley, CA: Sociology Press.
- Henderson J C. 1990. "Plugging into Strategic Partnerships: The Critical IS Connection," *Sloan Management Review* (31), pp. 7-18.
- Khalfan, A. M. 2004. "Information Security Considerations in IS/IT Outsourcing Projects: A Descriptive Case Study of Two Sectors," *International Journal of Information Management* (24:1), pp. 29-42.
- Kern, T., and Willcocks, L. 2000. "Exploring Information Technology Outsourcing Relationships: Theory and Practice," *Journal of Strategic Information Systems* (9), pp. 321-350.
- Lacity, M. C., Willcocks, L. P. 1998. "An Empirical Investigation of Information Technology Sourcing Practices: Lessons from Experience," *MIS Quarterly* (22:3), pp. 363-308.
- Lee, J. N. 1998. "Partnership Quality in IS Outsourcing: Social Theory Perspective," paper presented at the Doctoral Consortium of the 19th International Conference on Information Systems, Helsinki, Finland.
- Lee, J. N, Huynh, M. Q., Kwok, R. C-W., and Pi, S-M. 2003. "IT Outsourcing Evolution—Past, Present, and Future," *Communications of ACM* (46:5), pp. 84-89.
- Lee, J. N, and Kim, Y. G. 2005. "Understanding Outsourcing Partnership: A Comparison of Three Theoretical Perspectives," *IEEE Transactions on Engineering Management* (52:1), pp. 43-58.
- Loh, L., and Venkatraman, N. 1992. "Determinants of Information Technology Outsourcing: A Cross-Sectional Analysis," *Journal of Management Information Systems* (8), pp. 7-24.
- Marchand, N., and Jacobsen, H. A. 2001. "An Economic Model to Study Dependencies between Independent Software Vendors and Application Service Providers," *Electronic Commerce Research* (1:3), pp. 315-334.
- McFarlane, F. W., and Nolan, R. L. 1995. "How to Manage an IT Outsourcing Alliance," *Sloan Management Review* (36:2), pp. 9-23.
- Miles, M. B., and Huberman, A. M. 1984. *Qualitative Data Analysis: A Sourcebook of New Methods*, London: Sage Publications.
- Myers, M. D. 1994. "A Disaster for All to See: An Interpretive Analysis of a Failed IS Project," *Accounting Management and Information Technologies* (4:4), pp. 185-201.

- Peltier, T. 1996. "The Risk of Allowing Outside Staff Access to Your Information Systems," *Information Security Technical Report* (1:3), pp. 18-28.
- Rubin, H., and Rubin, I. 1995. *Qualitative Interviewing: The Art of Hearing Data*, Thousand Oaks, CA: Sage Publications.
- Saunders, C., Gebelt, M., and Hu, Q. 1997. "Achieving Success in Information Systems Outsourcing," *California Management Review* (39:2), pp. 63-79.
- Smith H. A., McKeen J. D., Staples D. S. 2001. "Risk Management in Information Systems: Problems and Potentials," *Communications of the Association for Information Systems* (7:13), pp. 1-29.
- Strauss A. L., and Corbin, J. M. 1990. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*, Newbury Park, CA: Sage Publications.
- Strauss, A. L., and Corbin, J. M. 1994. "Grounded Theory Methodology: An Overview," in *Handbook of Qualitative Research*, N. K. Denzin, and Y. S. Lincoln (eds.), Thousand Oaks, CA: Sage Publications, pp. 273-285.
- Sullivan, W. E., and Ngwenyama, O. K. 2005. "How Are Public Sector Organizations Managing Is Outsourcing Risks? An Analysis of Outsourcing Guidelines from Three Jurisdictions," *Journal of Computer Information* (45:3), pp. 73-87.
- Travis, J., and Saldanha, M. 1999. "An Investigation of IS/IT Project Risk Analysis and Management Practices in Western Australia," in *Proceedings of the 10th Australasian Conference on Information Systems*, Wellington, New Zealand, December 1-3.
- Walker, C. 1996. "Giant Contracts Boost UK Outsourcing Growth," *ComputerWeekly*, July 20, p. 12.
- Willcocks, L. P., and Lacity, M. 1999. "IT Outsourcing in Financial Services: Risk, Creative Contracting, Business Advantage," *Information Systems Journal* (9), pp. 163-183.
- Willcocks, L. P., Lacity, M., and Kern, T. 1999. "Risk Mitigation in IT Outsourcing Strategy Revisited: Longitudinal Case Research," *Journal of Strategic Information Systems* (8:2), pp. 285-314.

About the Authors

Shabareesh Ajitkumar is a management consultant with the leading Australian consultancy Portland Group. He recently completed his First Class Honours thesis on risk management in the context of IS outsourcing partnerships with the School of Information Systems, Technology and Management at the University of New South Wales. He can be contacted by e-mail at SAjitkumar@portlandgroup.com.

Stephen Smith is the Executive Officer of Emergency Management Operations in the Office of the Government Chief Information Officer, Department of Commerce, in the New South Wales State Government. He holds a Ph.D. and Master's of Commerce degree from the University of New South Wales in information systems and a Bachelor of Science in Engineering. Stephen is a casual lecturer in IS security at the School of Information Systems, Technology, and Management, University of New South Wales. His publications include articles in *Information Systems Management Journal*, *The International Journal of Knowledge, Culture and Change Management*, and various refereed national and international conference proceedings in IS/IT. He can be contacted by e-mail at Stephen.Smith@commerce.nsw.gov.au.

Deborah Bunker is a senior lecturer at the School of Information Systems, Technology and Management at the University of New South Wales. She holds a Ph.D. in Information Systems Management. Her research interests are in IS philosophy, IS management, IS adoption and diffusion, and e-Commerce/e-Business. She has published widely in these areas. Deborah is a founding member and the Vice-Chair of IFIP TC 8 WG 8.6 on the adoption and diffusion of IT. She can be reached at d.bunker@unsw.edu.au.

Donald Winchester is a research fellow in SEAR (Security, E-Fraud, Assurance, and Risk) within the School of Information Systems, Technology and Management, Australian School of Business, University of New South Wales. He is a Ph.D. candidate (finance) in the Australian School of Business, University of New South Wales. He holds a BCM (Lincoln University), MBA (Massey University), and MBS (Massey University), all in finance. Current research interests are in information systems security, identity crime, risks in financial institutions, outsourcing, and international financial flows. His work has been published in international journals and referred conference proceedings. Donald can be contacted by e-mail at d.winchester@unsw.edu.au or don_winchester@yahoo.com.