Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2010 Proceedings

Americas Conference on Information Systems (AMCIS)

8-2010

Identifying Areas for Risk Sharing in IT Outsourcing

Kamalika Chakraborty
Infosys Technologies Ltd., kamalika.ch@gmail.com

Gerhard Schwabe
University of Zürich, schwabe@ifi.uzh.ch

Rajat Bhattacharya
ABB Information Systems Ltd., bhattacharya.rajat@gmail.com

Tom Philip
University of Zürich, philip@ifi.uzh.ch

Follow this and additional works at: http://aisel.aisnet.org/amcis2010

Recommended Citation
Chakraborty, Kamalika; Schwabe, Gerhard; Bhattacharya, Rajat; and Philip, Tom, "Identifying Areas for Risk Sharing in IT Outsourcing" (2010). *AMCIS 2010 Proceedings*. 415.
http://aisel.aisnet.org/amcis2010/415

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2010 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Identifying Areas for Risk Sharing in IT Outsourcing

Kamalika Chakraborty
Infosys Technologies Ltd.
kamalika.ch@gmail.com

Gerhard Schwabe
University of Zürich
schwabe@ifi.uzh.ch

Rajat Bhattacharya
ABB Information Systems Ltd.
bhattacharya.rajat@gmail.com

Tom Philip
University of Zürich
philip@ifi.uzh.ch

ABSTRACT

Risk management is of great importance to outsourcing deals. While the traditional outsourcing focuses on risk management by one partner (typically the outsourcer), this paper proposes a risk sharing approach. Such an approach requires the identification and prioritization of risks from both the outsourcer's and the service provider's perspective to identify areas of shared interest. The analysis then continues to define mitigation actions and map them to the most important areas. This paper reports on two cases of action research undertaken in large Swiss companies and their outsourcing partners, where this approach was successfully tested.

Keywords: IT outsourcing, Risk sharing, Action research

INTRODUCTION

The IT outsourcing (ITO) industry has grown tremendously (NASSCOM, 2009; Lamont, 2009) and undergone significant changes in last two decades, and especially in the last decade when organizations started looking at ITO not only as a means to reduce cost but also as a means to achieve a rapid, substantial and sustainable improvement in enterprise performance (Linder, 2004). Further, in the last decade there was a progressive increase in outsourcing of IT services to offshore locations (Crow and Muthuswamy, 2002).

The growth and change in nature of ITO during the last decade has not only brought benefit to organizations but also increased their risk exposure (Aubert et al., 2001). ITO by nature is prone to risks as IT services are not defined by any common standards (Rold, 2009). Further as organizations source IT services from different low-cost countries (King, 2007), and a number of different providers through complex service delivery models (Margevicius and Rold, 2007), the complexity and footprint of their ITO increase, so do their risk exposure. The risk exposure is not only limited to the organizations outsourcing IT services, but also to IT service providers providing them (Maurer, Scardino and Ridder, 2008). The challenge for IT service providers is to meet their clients' goals, while ensuring that their own, possibly differing, goals are also met. Clearly if an ITO arrangement is to be successful, while IT service providers must accept the transferred risks in projects and agree to the controls imposed by clients to manage the relationship, the providers must also stand to gain from the relationship, and its interests must also be met (Taylor, 2007). This is the underlying principle of risk sharing in ITO.

During the last two decades a lot of research has focused on how to identify, categorize and mitigate risks in both in-house and outsourced IT projects. However, the constantly changing nature of ITO has also meant that the types and nature of risks associated with ITO, and their probability and impact keep changing, and so the ways to mitigate these risks should also change.

The aim of this paper is to analyze all risks associated with ITO in terms of weightages (probability & impact) assigned to them by outsourcers and IT service providers, to prioritize the risks in terms of these weightages, and to list possible mitigation actions from the perspective of both parties, so as to clearly identify risks that can be shared between them. Further, this paper aims to identify similar types of mitigation actions (from both outsourcer and IT service provider perspective) for risks that can be shared and group them into a few risk sharing areas.

LITERATURE REVIEW

Risks in IT projects (with or without specific focus on ITO) have been widely defined, studied and categorized during the last two decades. A very comprehensive categorization of risks in IT projects was the 'Taxonomy of risks' defined by SEI in the early nineties (Carr et al., 1993; Gallagher, 2005), though this taxonomy made no distinction between risks in non-outsourced and outsourced IT projects. Subsequently, risks specific to ITO have been defined distinctly as an undesirable event, a probability function, a variance, and an expected loss, and categorized as Exogenous and Endogenous (Carr et al., 1993). All these definitions and categorizations are very generic (i.e. not specific to ITO). Other categorizations of risks in ITO as Financial, Technical and Business risks (Elitzur and Wensley, 1997) are also not specific enough, as they apply equally to any kind of outsourcing, and not necessarily ITO.

As ITO grew in volume during the last decade and risks specific to ITO were widely studied, most of the research looked at the topic through the lens of the Agency theory. This was also coupled with an emphasis on analysis of ITO risks from the principal's (outsourcer's) perspective (Nakatsu and Iacovou, 2009). Comparatively the research on the risks from an IT service provider's perspective has been limited. Further research on ITO risks from an IT service provider's perspective has mainly dealt with the benefits and the value adds that the IT service provider brings to the outsourcer (Levina, 2004), and not the risks the IT service provider is confronted with and has to manage. Also research on ITO risks has tended to focus heavily on outsourcing contracts (and pricing models) as ways to mitigate ITO risks (as opposed to other ways available). There exist many studies in identifying the determinants of contract choice which are meant to mitigate the risks related to ITO (e.g. Gopal et al., 2003). Research by Gartner analyzes how comprehensive and detailed contracts can significantly reduce operational, contractual, security and legal risks related to ITO (Huntley, 2006). Research by Gartner also looks at risk in the context of pricing models and compares the risk exposure of the outsourcers (as well as the IT service providers) for different pricing models (Maurer et al., 2005). Researchers have even developed mathematical models for analyzing and quantifying ITO risks and mitigating the same through incentive contracts (Osei-Bryson and Ngwenyama, 2005). Conversely research in the area of ITO contracts has suggested that optimal contracts can reduce the risk exposure for both outsourcers as well as the

IT service providers (Aubert et al., 2003).

Most academic research dealing with risk mitigation in ITO has tended to concentrate on either one of two categories of risks, namely sourcing or project risks. Sourcing risks are risks that are relevant at a sourcing level i.e. during contracting, or affecting an entire engagement or program, while project risks are risks relevant at an individual project level. All papers cited above focused on outsourcing contracts as a way to mitigate ITO risks and view ITO risks from a sourcing perspective. On the other hand research done at institutions like SEI focus exclusively on project (operational) risks. In scope of this literature review, no literature was found that discussed both these categories of risks simultaneously, and as distinct categories. The distinction was only observed in practice i.e. at one the companies (outsourcers) where this research was conducted.

The contract perspective focuses on defining responsibilities and consequences. This perspective is particularly important if there is a conflict of interest as assumed in the agency theory. However, other risk mitigation actions are possible, if both partners have an interest in hedging a risk. Here, partners can come to an arrangement to share risks in a fair and effective manner. As a precondition for such an arrangement the partners have to come to an understanding where they both see large risks and what mitigation actions can be taken.

Thus the primary research gaps identified in context of this paper are, (a) study of ITO Risks from IT service provider perspective, (b) detailed study on ways of mitigating ITO risks other than through outsourcing contracts, (c) study of sourcing and project risks as two distinct categories of ITO risks and, (d) study on sharing of ITO risks between outsourcers and IT service providers

The aim of this paper is to focus on the research gaps listed above and analyze ITO risks both from outsourcer and IT service provider perspective. The research questions that this paper aims to address are:

(a) Which ITO risks do both parties consider relevant for mitigation?
(b) How can the ITO risks that both parties consider relevant for mitigation be prioritized?
(c) Can both parties share the ITO risks they both find relevant, and if yes, which ones?
(d) Can a few risk sharing areas be determined based on the ITO risks found suitable for sharing?

RESEARCH METHODOLOGY, DATA COLLECTION AND RISK DATA

In order to address our research questions, we have followed the action research methodology, an appropriate methodology considering the real-life situations and the 'sustainable improvement' (Raurich, 2004) that could result from the research. This methodology introduced by Lewin (1946) analyzes real-world problems, undertakes research to increase the understanding of the researcher and participating parties, and takes action to bring about change in organizations (Dick, 1993). Following this approach, data collection was first done at one company (outsourcer) and its service providers, and an analysis was performed. This was followed by data collection at another outsourcer and its service providers, and analysis

performed earlier was validated. The first three research questions were addressed as follows with results as described. (a) A set of relevant ITO risks was defined based on available literature and interviews with practitioners. This set was called a risk sheet. (b) The risk sheet was then sent to multiple practitioners for them to quantify a probability and impact figure on each risk, based on which an average risk exposure value was calculated for each risk. The ITO risks were then prioritized based on their risk exposure value. (c) Mitigation actions from both outsourcer and IT service provider perspective were then defined for the higher priority ITO risks to identify which ITO risks could be shared between the two parties. The exact approach of quantifying a risk exposure value, and prioritizing risks based on it was co-defined by the authors and practitioners from the first outsourcer, and accepted by practitioners from the second outsourcer.

Figure 1 illustrates the main steps from data collection to analysis of results.

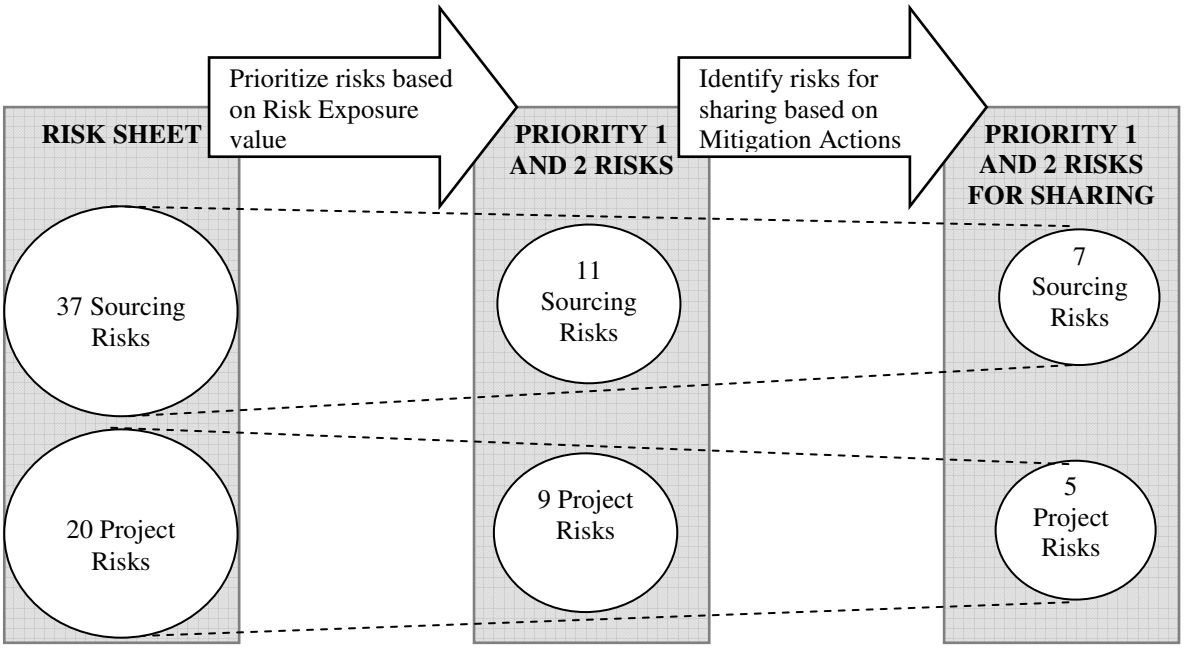

Figure 1: Data collection and analysis

Data were collected from personnel of two Global Fortune 500 companies (outsourcers) and eight of their IT service providers. The two outsourcers represent different industry domains i.e. reinsurance and electrical engineering, and being engaged in ITO for more than a decade have wide experience in this area. The eight IT service providers include three Global Fortune 500 companies from the US, three companies from India, representing both pure service and product plus service companies. The data collection covered twenty one respondents (eight mid-management personnel of the outsourcers with direct responsibility in ITO and thirteen engagement management personnel of the providers).

In the first step a set of relevant ITO risks was defined using information gathered from literature and individual face-to-face interviews (average duration sixty minutes) with fourteen respondents representing one outsourcer and five of its IT service providers. This set, titled the Risk Sheet consisted of 57 risks, belonging to one of two categories namely Sourcing Risks (37

risks) and Project Risks (20 risks). This categorization was validated in each interview. Each Sourcing Risk was sub-categorized as Intrinsic Sourcing Risk (17 risks), Partner Risk (9 risks) or Internal Risk (11 risks) as per definition followed by the outsourcer.

This Risk Sheet was then sent to the fourteen respondents to quantify a risk probability (1 to 4) and impact (1 to 4), where 1 is low and 4 high, for each Risk. Following this data collection, for each risk (for each respondent) a risk exposure was calculated as Risk Exposure (Aubert et al., 2001) = Risk Probability * Risk Impact. The Risk Exposure figures per risk, per respondent were then aggregated only per risk (as average of risk exposure figures from different respondents for the risk) i.e. Risk Exposure (consolidated) for Risk X = Average (individual Risk Exposures for Risk X). Two distinct sets of Risk Exposures were created, the first based on responses from the outsourcers' personnel, and the second from service providers' personnel. This distinction was made as the respondents represented two distinct sides of the ITO value chain, the outsourcers being the Principal (Aubert and Patry, 2005) and the service providers the Agent (Aubert and Patry, 2005).

The Risk Sheet was then sent to the seven respondents representing the second outsourcer and three of its IT service providers, and face-to-face interviews were conducted with them to validate the risk sheet. All the risks listed in the Risk Sheet were verified as relevant in the ITO relationships of the second outsourcer as well. The Risk Sheet at this stage represented an answer to research question 1. The seven respondents were then requested to quantify the risk probability and impact in the same way as the first fourteen, and the two sets of risk exposures were consolidated based on all the twenty one responses. During this consolidation it was apparent that the risk exposure values from both the outsourcers had a very high similarity, proving that both companies had similar perception of probability and impact of the risks in the Risk Sheet.

The consolidated Risk Exposure values were then categorized into three categories High, Medium and Low as follows:

1. High – Risk Exposure value range 6.51 - 16
2. Medium – Risk Exposure value range 3.01 - 6.50
3. Low – Risk Exposure value range 1 - 3

Figure 1 lists the consolidated Risk Exposure for both Sourcing and Project risks from both outsourcer and service provider perspectives.

Sourcing Risk	Risk Exposure Outsourcer	Priority	Risk Exposure Provider	Priority
Geographical and geopolitical risks	4.06	Medium	3.19	Medium
Legal, Intellectual Property risks	3.66	Medium	4.81	Medium
Data security and data protection risks	5.44	Medium	6.39	Medium
Communication Gaps	7.13	High	5.67	Medium
Reputational risks	2.75	Low	3.99	Medium
Lack of Cultural fit	3.66	Medium	5.63	Medium
Lack of business continuity planning by the outsourcer	4.31	Medium	5.54	Medium
Personnel risks	7.13	High	6.00	Medium
Operational risks	7.19	High	6.22	Medium
Incorrect definition or choice of the scope of outsourcing	6.38	Medium	6.88	High
IT service provider performance measurement problems, definition of metrics, collection of data	5.25	Medium	3.35	Medium
Contracts not including clear IT service provider performance measurement criteria	5.91	Medium	4.79	Medium
Non Integration of IT service provider teams	4.92	Medium	5.60	Medium
Limited focus on Strategic partnerships with IT service providers	5.39	Medium	8.44	High
Inadequate knowledge about IT service providers cost model	6.25	Medium	6.08	Medium
Ad hoc sponsorship of outsourced IT projects	4.86	Medium	4.31	Medium
Lack of Trust between the outsourcer and all IT service providers	4.22	Medium	4.96	Medium
Specific IT service providers underperforming and failing to meet the SLAs	6.64	High	6.94	High
Eroding cost advantages with specific IT service providers	5.94	Medium	5.73	Medium
Financial Instability of specific IT service providers	4.38	Medium	4.13	Medium
Size of specific IT service provider company	2.58	Low	4.00	Medium
Lack of Cultural fit	4.25	Medium	4.83	Medium
Expertise and Experience risks	4.92	Medium	5.38	Medium
Technology Risks	3.44	Medium	3.97	Medium
Disputes & Litigation risks for specific IT service providers	2.81	Low	2.60	Low
Lack of Trust between the outsourcer and specific IT service providers	4.30	Medium	4.09	Medium
Non-optimal IT Service provider base	5.34	Medium	6.00	Medium
No formalized and/or well defined relationship management from the outsourcer	4.25	Medium	4.63	Medium
Lack of skills to manage IT service providers and execute IT outsourcing program	6.11	Medium	6.19	Medium
Loss of internal skills to be able to insource if needed	7.19	High	5.60	Medium
Loss of internal staff motivation	5.34	Medium	7.56	High
Technology risks	4.59	Medium	6.56	High
Transactional risks e.g uncertain requirements etc.	8.98	High	7.10	High
Uncertainty about the legal environment	3.94	Medium	4.69	Medium
Interdependence of activities impacting outsourced projects	7.56	High	4.31	Medium
Non consideration by the outsourcer of extra effort required to adapt to new models suggested by IT service provider	5.31	Medium	5.00	Medium
Unclear SLA definition at sourcing level company outsourcing IT projects	5.25	Medium	5.00	Medium

Project Risk	Risk Exposure Outsourcer	Priority	Risk Exposure Provider	Priority
Lack of proper project set-up by the outsourcer	6.00	Medium	6.69	High
Lack of proper Engagement Planning by the outsourcer	6.53	High	6.69	High
Unclear Communication & Escalation paths	6.88	High	6.01	Medium
Roles & Responsibilities not clearly defined	4.69	Medium	6.35	Medium
Lack of clear expectations of the outsourcer	5.25	Medium	6.75	High
Lack of clear specifications, lack of proper baseline definition by the outsourcer	9.84	High	7.72	High
Lack of proper knowledge transfer	6.11	Medium	8.70	High
Lack of appropriate QA & UAT Processes in the project	3.94	Medium	6.23	Medium
Lack of appropriate data, tools & processes	5.25	Medium	4.97	Medium
Mismanagement of On-site personnel of IT service provider	3.44	Medium	3.79	Medium
Cultural Differences between personnel of IT service provider & personnel of the outsourcer	3.52	Medium	4.44	Medium
Location of IT service provider	5.31	Medium	3.99	Medium
Insufficient skills/experience in outsourcing on part of the outsourcer	4.81	Medium	4.92	Medium
Inadequate resource planning and under utilization of resources either by the IT service provider or by the outsourcer	5.58	Medium	4.63	Medium
Inadequate forecasting information from the outsourcer (existing project releases etc.)	5.84	Medium	7.25	High
Inability of the outsourcer to completely adapt to new pricing, execution models practised by IT service providers	5.06	Medium	4.97	Medium
Lack of incentives on better than required performance by IT service provider	4.50	Medium	5.15	Medium
Lack of penalties on worse than required performance by IT service provider	5.31	Medium	5.59	Medium
IT service provider selection is impacted more by relationships than by actual performance	5.34	Medium	6.84	High
Lack of buy-in and support for outsourcing from employees of the outsourcer	5.50	Medium	6.79	High

Figure 2: Consolidated Risk Exposure for both Sourcing and Project risks

ANALYSIS OF RISK DATA

The analysis to prioritize ITO risks (research question 2) and identify the ones that can be shared (research question 3) was performed based on the Risk Exposure (calculated in the data collection step) for each risk in the Risk Sheet. The risks were prioritized based on the outsourcers' and service providers' joint perception of the Risk Exposure as follows.

1. IF Risk Exposure = "High" from both outsourcer and service provider perspective, THEN assign highest priority, *Priority 1*.
2. IF Risk Exposure = "High" from one perspective (either outsourcer or service provider) AND "Medium" from the other, THEN assign *Priority 2*.
3. IF Risk Exposure = "Medium" from both perspectives, THEN assign *Priority 3*.
4. IF Risk Exposure = "Medium" from one perspective (either outsourcer or service provider) AND "Low" from the other, THEN assign *Priority 4*.
5. IF Risk Exposure = "Low" from both perspectives, THEN assign lowest priority i.e. *Priority 5*.

The prioritization was performed for Sourcing and Project Risks separately, with results as summarized in Table 1:

No. of risks	Sourcing Risks	Project Risks
Priority 1	2	1
Priority 2	9	8
Priority 3	23	11
Priority 4	2	0
Priority 5	1	0
Total	37	20

Table 1: No. of Sourcing and Project Risks by Priority

In this prioritization, the higher priority risks (specifically Priority 1 and 2) signify that both outsourcers and service providers perceive the particular risk to have a higher probability of occurrence and a higher impact (on occurrence). Hence these risks are more relevant for sharing between the two parties, as sharing such risks would benefit both.

It was assumed that while ALL Priority 1 and 2 risks are relevant for sharing, it may not be possible for the outsourcers and the IT service providers to share ALL of them since SOME of these risks can be mitigated by only one party. This was validated by analysis where possible mitigation actions (for each Priority 1 and 2 risk) were listed from both perspectives, and consequently risks that can be shared were clearly identified. The results of the analysis, focusing on Priority 1 and 2 risks that can be shared are discussed below.

Priority 1 risks that can be shared

Risk 1: Specific IT service providers failing to meet SLAs (Risk Type –Sourcing Risk)

This risk includes under-performance or poor quality of deliverables from specific providers, and can be mitigated by both parties. The outsourcer can monitor performance of providers, escalate under-performance, and utilize penalty clauses in contracts, if necessary (Willcocks, Lacity and Kern, 1999). The providers can also monitor SLAs, and change/fine-tune delivery process to meet them. Even after changing processes if the SLAs are consistently difficult to meet, they can inform the outsourcer and if required re-negotiate these SLAs.

Risk 2 and 3: Transactional risk – Unclear/dynamic requirements specifications, no baseline definition, delayed/ contradictory clarifications from outsourcer (Risk Type – both Sourcing and Project Risk)

This is a common risk arising from outsourcers' lack of experience in outsourcing, inadequate understanding of the need for precise specifications, (Willcocks et al., 1999) and timely clarifications in outsourced projects. This risk can be mitigated by outsourcers by controlling the effect of requirement volatility on schedule and effort, and using outcome based contracts, which require clearly defined requirements. The provider can also help mitigate this risk by defining and following processes to minimize impact of high requirement volatility on schedule/effort (like iterative/agile development), collecting and sharing metrics on same with the outsourcer, ensuring sign-off on requirements, and constantly following up with outsourcer on required clarifications.

Priority 2 risks that can be shared

Risk 1: Personnel risks – Inadequate skill/knowledge level of the resources of the IT service providers (Risk Type – Sourcing Risk)

Skilled resources are key to the success of IT projects, and hence this is an important risk that needs mitigation at the sourcing level. Outsourcers using time and material contracts can mitigate this risk by clearly defining eligibility criteria for particular roles. They can also conduct assessments of personnel of providers, and additionally train them if required. Further, they can forecast requirement for specific skills early to the providers. Outsourcers can also utilize outcome based contracts to share this risk with providers. Providers can mitigate this risk by maintaining adequate bench strength, ensuring retention of skilled resources, and maintaining resource pools for important clients.

Risk 2: Operational risks – cost and schedule overruns (Risk Type – Sourcing Risk)

This is a risk which can jeopardize the goal of outsourcing which is often cost savings. Outsourcers can mitigate this risk by defining and monitoring KPIs (Willcocks et al., 1999) critical to cost and schedule adherence. Outsourcers must then maintain a repository of such KPI measurements for each provider, on a current and retrospective basis to be able to identify trends and forecast exception events with high probability. The provider can also monitor critical KPIs, share measurements of those KPIs with the outsourcer, and proactively forecast probable exception events to the outsourcer.

Risk 3: Technology risks – lack of expertise of IT service providers on specific technologies (Risk Type – Sourcing Risk)

This is also a common risk especially confronting outsourcers whose IT landscape is comprised of legacy/niche technologies for which skills are not easily available in the market. Outsourcers can mitigate this risk by training providers' resources if expertise is available internally. The outsourcer can also forecast requirements well in advance to providers, enabling them to find appropriate resources. Providers can mitigate this risk by investing in building expertise on such technologies, and by strengthening recruitment processes to meet client demands efficiently.

Risk 4: Interdependence of activities impacting outsourced projects (Risk Type – Sourcing Risk)

This risk is applicable to outsourcers having internal stakeholders in ITO distributed across multiple departments, or having multiple providers involved in the same project/program. Outsourcers can mitigate this risk by analyzing cost and schedule impacts of the complexity due to interdependence of activities between various departments and providers, determining the difference in cost, if project activities are split across different providers versus outsourcing a complete package to one provider, and awarding package based contracts whenever possible. Providers can mitigate this risk by offering competitive pricing if package-based contracts/end-to-end project implementations are awarded to them.

Risk 5: Lack of proper project set-up by the outsourcer (Risk Type – Project Risk)

This risk arises when outsourcers do not allocate adequate time for project setup due to internal pressures on achieving quick results. Outsourcers can mitigate this risk by including adequate time for project setup in project plans based on lessons learnt from previous projects. Involvement of the provider in the project setup can also mitigate this risk. Providers can mitigate this risk by proactively stating specific requirements to be fulfilled to start the project, supported by lessons learnt from previous projects.

Risk 6: Lack of proper knowledge transfer (Risk Type – Project Risk)

This is a common risk in ITO as outsourcers do not necessarily have all information required for project implementation documented and readily available. In many cases implicit knowledge available with internal resources is not documented. Outsourcers can mitigate this risk by including a knowledge transfer phase in the project plan, defining processes/artifacts for this phase, validating its effectiveness with reverse knowledge transfer, and maintaining repositories of relevant information. Providers can mitigate this risk by insisting on adequate knowledge transfer, maintaining knowledge artifacts and escalating issues with knowledge transfer to outsourcers in time.

Risk 7: Inadequate forecasting information from the outsourcer (Risk Type – Project Risk)

This risk often arises as the outsourcer cannot forecast project implementations accurately due to frequent changes in internal business demands, and uncertainty about financial approvals. To mitigate this risk outsourcers should define a process (involving relevant internal stakeholders) to plan, prioritize and bundle projects, to define clear forecasts that can be shared with providers well in advance. Providers can mitigate this risk by forecasting peak/lean periods based on past data, maintaining resource pools based on forecasts, and reviewing forecasts with outsourcers.

Risk 8 and 9: Communication gaps between outsourcer and providers, unclear communication/escalation paths (Risk Type – both Sourcing and Project Risk).

Outsourcers and providers can jointly mitigate this risk by defining a clear management structure/communication path (Willcocks et al., 1999) for outsourced projects, and including communication plan in project plans. Outsourcers and providers can together define response times for clarifications. Finally both parties must align their objectives, processes and timelines and regularly review status versus plan.

While all Priority 1 risks were appropriate for sharing, some Priority 2 risks were identified as not appropriate for sharing as they can be mitigated only by the outsourcer. These risks are:

Sourcing Risks

1. Incorrect definition, or choice of the scope of outsourcing by the outsourcer
2. Limited focus on strategic partnerships with IT service providers
3. Loss of internal skills to be able to in-source if needed
4. Loss of internal staff motivation

Project Risks

1. Lack of proper Engagement Planning by the outsourcer
2. Lack of clear expectations from the outsourcer
3. IT service provider selection is impacted more by relationships than by actual performance
4. Lack of buy-in and support for outsourcing from employees of the outsourcer

RISK MITIGATION

In the previous sections the first three research questions were addressed and this section attempts to answer the final one. The various mitigation actions listed earlier can be grouped based on their similarity and broadly categorized (refer **bold** text) as follows:

The mitigation actions for Risk 1: 'Specific IT service providers failing to meet SLAs' can be grouped under one category i.e. **Continuous performance monitoring based on KPIs and SLAs** (Willcocks, Lacity and Fitzgerald, 1995). Risks 2 & 3: 'Transactional risk – Unclear/dynamic requirements specifications, no baseline definition, delayed/ contradictory clarifications from outsourcer' need two categories of mitigation actions namely **Well defined, comprehensive contracts** (Willcocks et al., 1999) AND **Clear scope definition, better requirement engineering and robust development process** (Willcocks et al., 1999). Risk 4: 'Personnel risks – Inadequate skill/knowledge level of the resources of the IT service provider' also needs two categories of mitigation actions i.e. **Well defined, comprehensive contracts** AND **Effective personnel sourcing, retention, development & training processes** (Bahli and Rivard, 2005). Risk 5: 'Operational risks – cost and schedule overruns' can be mitigated by the same category of mitigation actions applicable for Risk 1 i.e. **Continuous performance monitoring based on KPIs and SLAs** and Risk 6: 'Technology risks – lack of expertise of IT

service providers on specific technologies' by the one applicable for Risk 4 i.e. **Effective personnel sourcing, retention, development & training processes.** The mitigation actions for **'**Risk 7: Interdependence of activities impacting outsourced projects' can be grouped under the category **Effective data collection, data analysis and decision.** While Risk 8: 'Lack of proper project set-up by the outsourcer' can be addressed only by **Effective project planning**, mitigation of Risk 9: 'Lack of proper knowledge transfer' requires the same AND **Effective knowledge management** (Jensen and Szulanski, 2004). Three distinct categories of mitigation actions are required for **'**Risk 10: Inadequate forecasting information from the outsourcer' i.e. **Effective project planning** (Aubert et al., 2005), **Effective personnel sourcing, retention, development & training processes** AND **Effective external and internal communication**. Finally Risks 11 & 12: 'Communication gaps between outsourcer and providers, unclear communication/escalation paths' can be mitigated by **Effective project planning** AND **Effective external and internal communication.** Looking at the categories of mitigation action for each risk above, multiple cases are apparent where the same category of mitigation actions was applicable to more than one risk.

Thus while the twelve risks together require sixteen categories of mitigation actions, they require only eight DISTINCT categories of mitigation actions, i.e. the outsourcers and the IT service providers can share all the Priority 1 and 2 risks through eight categories of mitigation actions. This approach was presented to the Sourcing Strategy department of one of the outsourcers. After an hour's discussion, the six participants in the meeting agreed on a phased approach for risk sharing with the IT service providers. They decided to focus on sharing Priority 1 and 2 risks in the first phase followed by sharing of priority 3 and 4 risks in subsequent later phases. They also agreed to revisit the Risk Sheet periodically, to re-assess the weightages of the existing risks and to add new risks, if required. The second outsourcer also accepted the result and is implementing the same with its providers to jointly mitigate Priority 1 and 2 risks.

CONCLUSION

To conclude, the primary value of this paper is as a guide to researchers and practitioners to deal with a long list of potential ITO risks discussed in outsourcing literature and in practice. It is practically impossible to mitigate and share all these risks with the same priority all the time. This paper provides a framework to researchers and practitioners alike to

(a) Prioritize ITO risks to focus on the most important ones

(b) Identify those risks that are most appropriate for sharing

(c) Identify a small subset of all possible mitigation actions

The results presented in this paper are actionable by researchers and practitioners, since the paper

(a) Provides a comprehensive set of ITO risks

(b) Describes and then validates a methodology to select and prioritize the risks, and lists mitigation actions and categories. This methodology can be used with minor or no modifications, by other outsourcing networks for their own evaluations

(c) Provides data from two major companies and their outsourcing partners on their perception of ITO risks and mitigation actions.

LITERATURE

1. Aubert, B., Patry, M. and Rivard S. (2001) Measuring and Managing IT Outsourcing Risk: Lessons Learned, CIRANO, 2020 University, 25th floor, Montréal, Canada H3A 2A5.
2. Aubert, B., Patry, M. and Rivard, S. (2005), A framework for information technology outsourcing risk management, *The DATA BASE for Advances in Information Systems*, 36, 4, 9-28.
3. Bahli B. and Rivard S. (2005) Validating measures of information technology outsourcing risk factors, *The international journal of management science*, 33, 175-185.
4. Carr J., Konda L., Monarch, I., Ulrich C., Walker, F. (1993) Taxonomy-Based Risk Identification, June 1993, Software Engineering Institute, Carnegie Mellon University, Technical Report, CMU/SEI-93-TR-6, ESC-TR-93-183.
5. Crow Galen B. and Muthuswamy, B. (2002), International Outsourcing in the Information Technology Industry: Trends and Implications, *Communications of the International Information Management Association*, 3, 1, 25-34.
6. Da Rold, C. (2009), Three Golden Rules of Cost and Risk Reduction in Outsourcing, 15 January 2009, ID Number: G00164226, Gartner Research.
7. Dick, B. (1993), You want to do an action research thesis? http://www.scu.edu.au/schools/gcm/ar/art/arthesis.html, Last viewed on 24th February 2010.
8. Elitzur R. and Wensley A. (1997), Game theory as a tool for understanding information services outsourcing, JIT. *Journal of information Technology*, 12, 1, 45-60.
9. Gallagher, B., A Taxonomy of Operational Risks, Software Engineering Institute, Carnegie Mellon University
10. Gopal A., Sivaramakrishnan K., Krishnan M. S. & Mukhopadhyay T (2003), Contracts in Offshore Software Development: An Empirical Analysis, *Management Science*, 49, 12, 167-1683.
11. Jensen, R. and Szulanski G. (2004) Stickiness and the Adaptation of Organizational Practices in Cross-Border Knowledge Transfers, *Journal of international business studies*, 35, 6, 508-52.
12. King R. (2007), The Outsourcing Upstarts, Business Week, July 31, 2007.
13. Lamont, J. (2009), India to keep top spot in outsourcing, says report, 2 December 2009, Financial Times.
14. Levina, N and Ross J.W (2003)., From the Vendor's Perspective: Exploring the Value Proposition in IT Outsourcing, New York University, Stern School of Business., *MIS Quarterly (27:3),*331-364
15. Lewin, K. (1946), Action research and minority problems, *Journal of social issues,* 2, 4, 34-46.
16. Linder, Jane C. (2004) Transformational Outsourcing, *MIT Sloan Management review*, 45, 2, 52-58.
17. Margevicius, Mark A. & Da Rold, C. (2007), Alternative Delivery Models: 14 New Ways to Deliver IT, 27 September 2007, Gartner Research, ID Number: G00149805.
18. Maurer W., Scardino L., Doering K. & Ridder F. (2008), Pricing Model Definitions, Benefits and Risks for IT Services and Outsourcing Contracts, Gartner, Publication date 20 April 2008.
19. Nakatsu Robbie T. & Iacovou Charalambos L. (2009) A comparative study of important risk factors involved in offshore and domestic outsourcing of software development projects: A two-panel Delphi study, *Information & Management,* 46, 1, 57–68.
20. NASSCOM, McKinsey & Co. (2009), Perspective 2020: Transform Business, Transform India, published May 2009.

21. Raurich, V. (2004) Integrative innovation planning in technology based companies, Dissertation at the Swiss Federal Institute of Technology Zurich, Switzerland.
23. Taylor, H. (2007), Outsourced IT Projects from the Vendor Perspective: Different Goals, Different Risks, *Journal of Global Information Management*, 15, 2, 1-27.
24. Willcocks L., Lacity M. and Fitzgerald G. (1995) Information technology outsourcing in Europe and the USA: Assessment issues, *International journal of information management*, 15, 5, 333-351.
25. Willcocks, L., Lacity, M. and Kern, T. (1999) Risk mitigation in IT outsourcing strategy revisited: longitudinal case research at LISA, *Journal of strategic information systems*, 8, 285-314.