

1-1-2008

IT offshoring risks and governance capabilities

Akemi T. Chatfield

University of Wollongong, akemi@uow.edu.au

Padmaharsha Wanninayaka

University of Wollongong, pw603@uow.edu.au

Follow this and additional works at: <https://ro.uow.edu.au/infopapers>



Part of the [Physical Sciences and Mathematics Commons](#)

Recommended Citation

Chatfield, Akemi T. and Wanninayaka, Padmaharsha: IT offshoring risks and governance capabilities
2008, 436-436.

<https://ro.uow.edu.au/infopapers/2468>

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

IT offshoring risks and governance capabilities

Abstract

IT offshoring or offshore outsourcing is a fast growing trend that is worldwide and continuing. Driven by the competitive pressure to reduce IT costs, firms in developed countries opt to buy IT services from offshore service providers in developing countries, which provide comparative advantage in lower labour costs and skilled workforce. While much has been written about its relative costs and benefits, there is a lack of comprehensive research on risks of IT offshoring. This research aims to identify IT offshoring risks based on a comprehensive review of the literature and content analysis. It also aims to map those risks to the extant IT outsourcing governance capabilities framework. The results show that the framework can be usefully extended to a different context of IT offshoring by including strategic management of risks and controls as a governance capability in order to address new and emerging risks in IT offshoring.

Keywords

capabilities, risks, offshoring, governance

Disciplines

Physical Sciences and Mathematics

Publication Details

Chatfield, A. T. & Wanninayaka, P. (2008). IT offshoring risks and governance capabilities. Hawaii International Conference on System Sciences (pp. 436-436). United states: IEEE Computer Society.

IT Offshoring Risks and Governance Capabilities

Akemi Takeoka Chatfield and Padmaharsha Wanninayaka
 School of Information Systems and Technology
 Faculty of Informatics, University of Wollongong, Australia
akemi@uow.edu.au

Abstract

IT offshoring or offshore outsourcing is a fast growing trend that is worldwide and continuing. Driven by the competitive pressure to reduce IT costs, firms in developed countries opt to buy IT services from offshore service providers in developing countries, which provide comparative advantage in lower labour costs and skilled workforce. While much has been written about its relative costs and benefits, there is a lack of comprehensive research on risks of IT offshoring. This research aims to identify IT offshoring risks based on a comprehensive review of the literature and content analysis. It also aims to map those risks to the extant IT outsourcing governance capabilities framework. The results show that the framework can be usefully extended to a different context of IT offshoring by including strategic management of risks and controls as a governance capability in order to address new and emerging risks in IT offshoring.

1. Introduction

Information technology (IT) offshoring or offshore outsourcing is a fast growing trend that is worldwide and continuing. According to an IDC market research report [12], the estimated market size of IT offshoring will reach US\$29.4 billion by 2010. IT offshoring is a business strategy that is (at least initially) focused on IT cost reduction by buying tradable services from offshore IT service providers in India, China or other developing economies who enjoy existing comparative advantage in lower labour cost and skilled labour, as shown in Table 1 below.

Offshoring as a business strategic option chosen by firms is not new. The manufacturing offshoring trend started in the 1960s in the U.S. and resulted in the paradigm shift from manufacturing toward services as the dominant GDP, and the same trend spread worldwide. Along the way manufacturing offshoring exerted both disruptive and transformative impacts on uneducated and unskilled factory workers. While IT offshoring will have similar or greater disruptive and transformative impacts on highly educated and highly skilled IT workforce in wealthy developed countries, this research will not address this much debated labour

issue. Rather, we address the research problem of identifying new and emerging risks of IT offshoring and evaluating which IT capabilities are core to successfully manage such risks, develop and sustain external vendor relationships that create business value to the client organization.

The process of IT offshoring involves the transfer of in-house IT functions and activities to offshore IT vendors, including business processes, non-core back office processing, software development and maintenance, consolidation of distributed IT infrastructure resources, and real-time management of IT assets such as customer database access control rights. Depending on the criticality of the services involved, IT offshoring arrangements will introduce operational and strategic risks, any of which will prevent firms from achieving their short-term profitability and/or long-term sustainability. Therefore, proper identification of the relevant risks, preventing the transfer of the existing risks and mitigating the negative impacts of the emerging risks are of paramount importance to the client firm.

However, IT offshoring practice, in comparison to IT outsourcing practice (to domestic IT vendors), is still new and emerging. In consequence, we do not have a full understanding of risks and controls in IT offshoring. Furthermore, relatively little research attention has been paid to understand which IT capabilities are core to IT offshoring risk management. Therefore, the aims of this research are to identify IT offshoring risks through a survey of research literature and to map them to the extant core information systems (IS) governance capabilities framework developed out of IT outsourcing field research [8, 30]. The framework represents a client firm perspective, and has identified nine core IS capabilities required for successfully managing IT outsourcing practice. What is particularly relevant to our research is its identification of leadership and informed buying as core IS capabilities that are necessary for outsourcing governance. In this paper, we argue that strategic management of risks and controls needs to be added to the governance capabilities in the extant framework in order to address new and emerging risks in IT offshoring.

Table 1. The appeal of IT offshoring

	Labour costs per hour (US\$)	Average annual salaries of computer programmers (US\$)	Predicted average annual salaries of computer programmers 2015 (US\$)	Current account balance (per cent GDP)	Population	Median age (years)
India	.74	6 350	20 000	+5.50	1.06b	24.4
China	.80	5 850	10 000	+2.86	1.3b	31.8
Malaysia	2.19	6 950	9 000	+12.50	23.5m	23.8
Australia	19.45	38 600	45 000	-6.30	19.9m	36.3
Britain	19.24	*69 748	-	-1.60	60.3m	38.7
US	21.83	74 500	85 000	-4.90	293m	36

Source: 'Labour costs per hour' are taken from *The Economist*, 'Country Briefings', available at: <http://www.economist.com/countries/>; and 'Annual average salaries of computer programmers' taken from Whitehorse Strategic Group Ltd., Table 3, *Study of ICT Outsourcing and offshoring in Australia*, p. 20. * Source: National Statistics (UK), *2004 Annual Survey of Hours and Earnings (ASHE)*, at http://www.statistics.gov.uk/downloads/theme_labour/ASHE_2004_exc/tab4_7a.xls 'Population' and 'median age' figures taken from the CIA World Factbook.

Source: [10]

The structure of this paper is as follows. The core IS capabilities framework is discussed in the next section, which is followed by research methodology employed to identify risks (section 3), results: IT offshoring risks (section 4), the risks mapped to the governance capabilities framework (section 5), and conclusion (section 6).

2. The Feeny and Willcocks Framework on Core IS Governance Capabilities

The Feeny and Willcocks Framework [8] was based on their field studies of successful IT outsourcing arrangements to identify core IS capabilities: leadership, informed buying, relationship building, making technology work, contract facilitation, contract monitoring, vendor development, business systems thinking, and architecture planning. The framework highlights leadership and informed buying as core IS capabilities that are necessary for outsourcing governance.

The nine core IS governance capabilities are grouped into three capability constructs, or "three faces" in the framework: business and IT vision; design of IT architecture; and delivery of IT services. The relationship between the outsourcing governance capabilities (leadership and informed buying) and the three capability constructs is shown in Figure 1 below. The first construct, Business and IT Vision, encompasses IT outsourcing governance (namely, leadership and informed buying), business systems thinking, (internal business-IT) relationship building,

and contract facilitation. Leadership capability is required to align IT outsourcing projects with business goals, strategies and activities to create business value. Informed buying is concerned with the initial stage of outsourcing through analysis of the external market for IT services. Business systems thinking in the IT organization is important to leverage IT capabilities to solve business problems, improve business processes, and facilitate business strategy formulation. Relationship building in this framework is essentially internally oriented, facilitating "the wider dialogue, establishing understanding, trust, and cooperation amongst business users and IT specialists. The task here is "getting the business constructively engaged in IT issues."" [30, p. 51] Contract facilitation capability is concerned with trouble-shooting of the problems and conflicts that arise within outsourcing relationships to ensure the successful delivery of IT services by external vendors.

The second construct, Delivery of IT Services, encompasses the outsourcing governance capabilities mentioned above, as well as three capabilities: vendor development, contract monitoring, and making technology work. Vendor development is concerned with the client firm's long-term investment in developing strategic buyer-supplier relationships that deliver business value to both parties. This capability is contrasted to contract facilitation mentioned above. While the former is long-term (including future relationships) and strategic, the latter is short-term during the contract period and, operational.

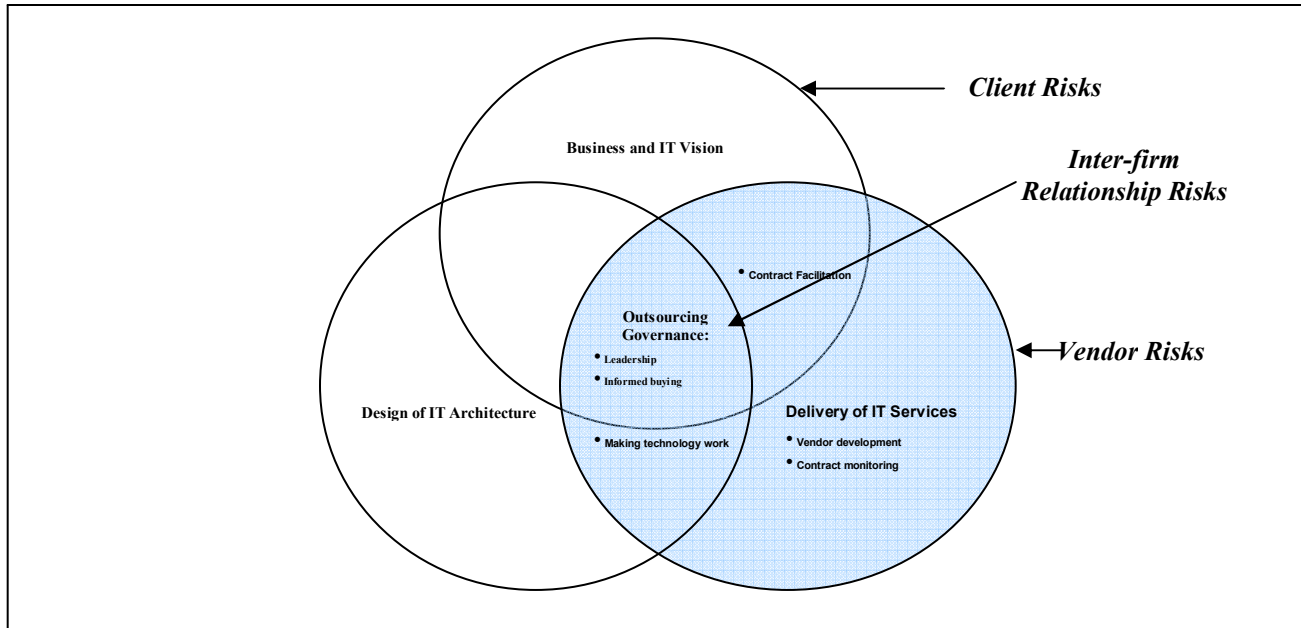


Figure 1. Nine outsourcing governance capabilities and three capability constructs

Contract monitoring is concerned with “holding suppliers to account against both existing service contracts and the developing performance standards of the service market” [30, p. 51]. Making technology work capability is to align IT enterprise architecture with external delivery of IT services through outsourcing options.

The third construct, Design of IT Architecture, encompasses the governance capabilities, (internal business-IT) relationship building, making technology work, and architecture planning. Architecture planning capability is concerned with developing a flexible IT enterprise architecture that meets present and future business needs and that aligns with the client firm’s business and IT vision.

In Figure 1 above we show new italicized terms that are not found in the framework: client risks, vendor risks and inter-firm relationship risks. These terms refer to three different sources of risks that are used in the process of mapping risks in section 5. Client risks are those risks that are primarily originated in the client firm’s internal resources or lack thereof. Similarly, vendor risks are those risks that are primarily related to the vendor firm’s internal resources. In contrast, inter-firm relationship risks refer to those risks that arise as a result of IT offshoring relationships.

3. Research Methodology

This section discusses research questions and literature review and content analysis as the research

methodology adopted in this paper to identify IT offshoring risks. We then discuss a sample of the relevant academic literature selected for content analysis, and content analysis applied to the sample: level of analysis and procedural rules adopted in this research. Next, we discuss how we have identified IT offshoring risks in the research sample. Finally, we discuss how the risks identified in this research were mapped to the extant core IS governance capabilities framework.

3.1 Research Questions

We address two related research questions from a perspective of the client firm that offshore outsources its IT functions: (1) What are risks of IT offshoring as identified in the academic research literature? (2) Does the extant core IS capabilities framework [8, 30] hold when it is extended to a different context of IT offshoring governance capabilities for managing offshoring risks?

3.2 Content Analysis

Content analysis is defined broadly by Holsti [11, p. 14] as “any technique for making inferences by objectively and systematically identifying specified characteristics of messages”. Content analysis as a research methodology has been used in social sciences in general and by information systems (IS) researchers in the diverse contexts. Content analysis is used to identify whether or not certain words or concepts are present within texts or sets of texts. The presence,

meanings and relationships of such words and concepts can be quantified and analysed to make inferences about the message within the texts [5].

Content analysis begins with identifying research questions and selecting a sample of texts. Once selected, the text must be coded into manageable content categories. The process of coding is basically one of selective reduction. For this paper, first we searched for the words “offshoring”, “global sourcing” and the combination of words “outsourcing” “India” as the search arguments in three separate rounds of searching, using citation and the abstract provided by the on-line databases: ProQuest 5000, ACM Digital Database and Emerald. In the third round of searching we substituted the word “India” with words “offshore” “overseas” “international” “global” “cross border”, in order to more accurately capture and include the relevant literature in the sample. Once we identified the collection of articles that satisfied the above criteria, we further searched the full text of these articles for the words “information technology” and “risk” in an attempt to select the articles that focused on IT offshoring risks. We have not coded for frequency of the words as content analysis is deployed to identify comprehensively the relevant literature on IT offshoring risks.

During the search it was observed that while most of the IS/IT journals contained an abstract some of the business journals did not. Certain instances were observed where there were discrepancies between the abstract in the article and the abstract provided by the database. The conference proceedings were searched using the search facilities within the respective websites which did not allow specifying which part of the article to be searched. (i.e. citation and abstract or full text). Due to some of these procedural challenges in conducting content analysis, the set of articles selected for this study should be considered as a representative sample of the relevant literature and not as an exhaustive collection.

3.3 Research Sample

After the three rounds of searching we identified a total of 55 articles from academic IS/IT journals, corporate/ business journals and conference proceedings as relevant research sample for the content analysis. However, for this study only the papers published in the academic IS/IT journals are selected and therefore, a total of 25 articles from corporate/business journals and conference proceedings were excluded from further analysis. We also excluded 5 articles published in the academic IS/IT journals that made references to IT offshoring in the context of book reviews, editor’s letters/comments or commentaries on articles published by other

researchers. Since our aim was to select the research journal articles that focused on identification of risks related to IT offshoring, the exclusion of these 30 articles was appropriate. Therefore, a total of 25 articles were selected for further interpretive content analysis. The IS/IT journals included in this study and the number of articles selected from each journal are listed in Table 2.

Table 2. Academic journals selected for content analysis

IT/IS Journals	No. of Articles
Information Systems Management	5
Journal of Global Information Management	4
MIS Quarterly Executive	3
Communications of the ACM	2
Journal of Information Technology	2
Journal of Management Information Systems	2
MIT Sloan Management Review	2
Information & Management	1
Information Management Journal	1
Information Management & Computer Security	1
Journal of Strategic Information Systems	1
Management Science	1
Total number of articles	25

3.4 Risk Identification and Coding Method

Our first research question was concerned with IT offshoring risk identification from the perspective of the client firm. This phase of research was conducted as follows. First, in a pilot study two researchers read all the selected articles and discussed whether or not the IT governance framework discussed in Section 2 could be applied to a new context of IT offshoring, beyond its original outsourcing context. In other words, our aim was to decide if the nine constructs identified in the framework were sufficient and useful for our purpose of identifying and classifying risks reported in the 25 articles. We read the articles again and applied the nine constructs systematically to perform a grounded search of risks in the research sample. Second, we coded independently all the risks identified and discussed in the sample. In coding risks, we adopted the author’s descriptive label (e.g. “heavy start up costs”) whenever possible in order to capture and represent its original message as accurately as possible. However, when its meaning was not immediately clear

to us, we reworded the risk description. Hence, the two researchers coded the risks independently and produced a set of two lists of all the risks reported in each article. Finally, we compared the lists systematically, having achieved high level inter-judge agreement (over 95%) for the most of the risks. Where we disagreed or discovered coding errors, we revisited the articles to reconcile the disagreements. We then compiled a comprehensive list of all the risks across the sample.

3.5 Risk Mapping Method

Our second research question was concerned with whether or not the extant core IS governance capabilities framework holds when it is extended to a different context of IT offshoring governance capabilities for managing offshoring risks. In order to explore this question, we first identified the three sources of risks as briefly discussed in Section 2. At the initial round of mapping the risks, we did not straightaway classify the risks into the governance framework. Rather, we classified each risk into one of the three sources of IT offshoring risks: client, vendor or inter-firm relationships. This classification code (“C”, “V” or “R”) was added to the comprehensive list of all the risks identified earlier. We found the Figure 1 useful in mapping all the risks on the list against the nine core capabilities of the governance framework. The IT offshoring risks identified in the 25 journal articles are discussed in the next section and the mapping results are presented in Section 5.

4. Results: IT Offshoring Risks

A total of 48 unique risks were identified and reported in the sample of 25 journal articles. These risks were classified, based on the point of origin, into one of the three categories: client risks, vendor risks or inter-firm relationship risks. Table 3 lists the summary statistics of all the risks according to the point of origin. There were 22 client risks identified as originated at the client’s end that included loss of organizational capabilities and competencies, vendor lock-ins and high/increasing transaction costs. A total of 20 vendor risks were identified that included service debasement, lack of critical knowledge/expertise on client’s domains and functional areas. A total of 6 inter-firm relationship risks that were identified included lack of communication and coordination, risks related to cultural and language differences and lack of trust.

Table 3. Summary statistics of risk categories

Risk’s Point of Origin	Frequency	%
Client risks	22	45.8
Vendor risks	20	41.7
Inter-firm relationship risks	6	12.5
Total	48	100

Table 4 shows the comprehensive list of all the risks and their codes we used in this research. Citations for the journal articles that identified specific risks are shown within the square brackets in the table with the numbers corresponding to references listed at the end of this paper. The Table is broken down by the risk’s point of origin: client, vendor or inter-firm relationships.

Table 4. Classification of IT offshoring risks

Client Risks	Code
Loss of organizational capabilities/ competencies [1; 6; 14; 17; 18]	C.1
High turnover of the client's workforce [22]	C.2
Low morale of the client's workforce [22]	C.3
Resistance to change [14; 25]	C.4
Low awareness of offshore location/vendor capabilities [3]	C.5
Inability/inexperience in managing vendor activities from a distance [1; 3; 25]	C.6
Incomplete/poorly drafted contracts [14; 25]	C.7
Vendor lock-ins/risks of increasing control of the service providers [1; 4; 6; 13; 14; 26]	C.8
Increased switching costs [6; 13; 14]	C.9
Wrong type of service outsourced/ offshored [25]	C.10
Heavy start up costs [31]	C.11
High/increasing transaction costs [4; 6; 7, 14; 16; 18; 22; 23; 26]	C.12
Hidden contract costs: costs and implications related to unexpected changes to contracts [6]	C.13
Cost incurred due to non-performance of the vendor (disputes and litigation) [4; 6]	C.14
Increasing charge rates and decreasing cost advantage [17; 20; 26]	C.15
Lack of clarity in requirements [10; 26]	C.16
Project size and complexity [1;10]	C.17
Risk of business failure/ uncertainties [6]	C.18
Restrictive regulations imposed by the client's country [3; 25]	C.19
Loss of domestic jobs/ employment opportunities [16; 19; 20; 22; 28; 29]	C.20
Downward pressure on domestic salaries [29]	C.21

Threat to national security [4]	C.22
Vendor Risks	Code
Service debasement [1; 6]	V.1
Scope creep and change management [31]	V.2
Use of outdated technologies and products by the service provider [14]	V.3
Lack of critical knowledge/ expertise on clients domains and functional areas [1; 3; 4; 25]	V.4
Lack of resources availability/ mobilization [2; 4; 10; 17, 23; 25]	V.5
High staff turnover of the vendor’s workforce [3; 10; 25]	V.6
Poor quality and errors [2; 20; 23]	V.7
Risks associated with disaster recovery operations at offshore destination [6]	V.8
High cost of training/long learning curves [10; 26]	V.9
Geographical / natural disaster risks [1, 4; 15; 18; 28]	V.10
Political risks [4; 15; 16; 25]	V.11
Lack of basic communication infrastructure facilities [1, 2; 3; 4; 16; 18; 24; 25]	V.12
Currency rate fluctuation and weak local currency [1, 27]	V.13
High taxes/tariffs and complications [25]	V.14
Trade barriers and restrictive business environment for foreign companies at the offshore destination [25; 27]	V.15
Lack of intellectual property safeguards [2; 4; 14; 22; 23; 24; 25; 26; 27]	V.17
Legal risks [18]	V.18
Corruption at offshore destination [4]	V.19
(Limited) access to recruitment networks [4]	V.20
Inter-firm Relationship Risks	Code
Project overruns/mismatches between expectations and deliverables [6; 14; 22; 26; 27; 31]	R.1
Lack of communication and coordination [3; 4; 18; 25; 26]	R.2
Lack of trust between the vendor and the service provider [3; 6]	R.3
Communication and coordination difficulties due to time zone differences [3; 4; 24; 25; 28]	R.4
Cultural differences [3; 18; 23; 24; 25]	R.5
Language differences [3; 23; 24]	R.6

5. The Risks Mapped to the Framework

All 48 risks listed in Table 4 were mapped against the extant core IS governance capabilities framework

discussed in Section 2, using its nine constructs to guide us in the process of mapping. Table 5 below shows the summary statistics. It shows that 28 risks out of a total of 48 risks found in the sample could be mapped against either of the nine constructs 1) leadership, 2) informed buying, 3)contract facilitation, 4) vendor development, 5) contract monitoring, 6) making technology work, 7) business systems thinking, 8) (internal business-IT) relationship building, and 9)architecture planning. This means that the extant core IS governance capabilities framework is sufficient and useful in mapping nearly 60 per cent of the risks reported in the 25 journal articles.

Table 5. Summary statistics of risks identified

Risks in the Sample	Frequency	%
Governance framework	28	58.3
Environmental uncertainty – client risks	4	8.3
Environmental uncertainty – vendor risks	11	22.9
Inter-firm relationships risks	5	10.4
Total	48	99.9

However, the remaining 20 risks cannot be so easily mapped against the governance framework. Table 5 above shows that, of the 20 risks that do not fit into the framework, 4 client risks are related to the client firm’s environmental uncertainty and 11 vendor risks are also associated with the vendor firm’s environmental uncertainty. In addition, 5 risks are inter-firm relationship risks that result from IT offshoring practice. In other words, the extant core IS governance framework does not provide core IS governance capabilities explicitly to manage and control these new environmental risks and inter-firm relational risks that are uniquely associated with IT offshoring practice, but not with IT outsourcing. Perhaps, these risks did not show up on client firms’ radar and hence the corresponding governance capabilities were not considered as important in the extant framework due to its central focus on the IT outsourcing environment (to domestic IS service providers).

Table 6 below shows IT offshoring risks that were mapped well against the nine core IS governance capabilities. The Table shows that a great majority of IT offshoring risks that were identified and reported in the sample were also commonly recognized as IT outsourcing risks; for example the client firm’s loss of organizational capabilities/competencies, requirements uncertainty, hidden contract costs, vendor lock-ins/risks of increasing control of the IT vendors, and uncertainty associated with large-scale IT projects such as scope creep and change management.

Table 6. IT offshoring risks mapped against the nine core governance capabilities

Risk	Code
1. Leadership	
Loss of organizational capabilities/competencies	C.1
Risk of business failure/uncertainties	C.18
2. Informed Buying	
Low awareness of offshore location/vendor capabilities	C.5
Wrong type of service outsourced/ offshored	C.10
3. Contract Facilitation	
Inability/inexperience in managing vendor activities from a distance	C.6
Heavy start up costs	C.11
4. Vendor Development	
Vendor lock-ins/risks of increasing control of the service providers	C.8
Increased switching costs	C.9
5. Contract Monitoring	
Incomplete/poorly drafted contracts	C.7
High/increasing transaction costs	C.12
Hidden contract costs: costs and implications related to unexpected changes to contracts	C.13
Cost incurred due to non-performance of the vendor (disputes and litigation)	C.14
Increasing charge rates and decreasing cost advantage	C.15
Service debasement	V.1
Scope creep and change management	V.2
Project overruns/mismatches between expectations and deliverables	R.1
6. Making Technology Work	
High turnover of the client's workforce	C.2
Lack of critical knowledge/expertise on clients domains and functional areas	V.4
Lack of resources availability/mobilization	V.5
High staff turnover of the vendor's workforce	V.6
Poor quality and errors	V.7
High cost of training/long learning curves	V9
7. Business Systems Thinking	
Lack of clarity in requirements	C.16
Project size and complexity	C.17
8. (internal business – IT) Relationship Building	
Low morale of the client's workforce	C.3
Resistance to change	C.4
9. Architecture Planning	
Use of outdated technologies and products by the service provider	V.3
Risks associated with disaster recovery operations at offshore destination	V.8

Three tables below list those IT offshoring risks in the sample that do not map well in the core IS governance capabilities framework. Table 7 lists client risks that are environmental uncertainty in nature. Table 8 identifies vendor risks that are also environmental uncertainty in nature. Finally, Table 9 shows neither client risks nor vendor risks, but rather are inter-firm relational risks that originate from the offshoring transactions, coordination and interactions between the client and the vendor during the contract duration.

Table 7. Environmental uncertainty – client

Risk	Code
Legal Risks	
Restrictive regulations imposed by the client's country	C.19
Economic Risks	
Loss of domestic jobs/employment opportunities	C.20
Downward pressure on domestic salaries	C.21
Political Risks	
Threat to national security	C.22

Table 8. Environmental uncertainty – vendor

Risk	Code
Technical Risks	
Lack of basic communication infrastructure facilities	V.12
Legal Risks	
Low data security and information privacy safeguards	V.16
Lack of intellectual property safeguards	V.17
Legal risks	V.18
Economic Risks	
Currency rate fluctuation and weak local currency	V.13
High taxes/tariffs and complications	V.14
Trade barriers and restrictive business environment for foreign companies at the offshore destination	V.15
Political Risks	
Political risks	V.11
Social Risks	
Corruption at offshore destination	V.19
(Limited) access to recruitment networks	V.20
Geographical Risks	
Geographical / natural disaster risks	V.10

Table 9. Inter-firm relationship risks

Risk	Code
Lack of communication and coordination	R.2
Lack of trust between the vendor and the service provider	R.3
Communication and coordination difficulties due to time zone differences	R.4
Cultural differences	R.5
Language differences	R.6

6. Conclusion

Much has been written about the benefits of IT offshoring such as large IT cost savings, access to new technological capabilities, and flexibility in delivering IT services. However, despite the growing IT offshoring practices worldwide, little research attention has been directed to comprehensively identify the risks associated with IT offshoring. As a result, we do not have a full understanding of strategic and operational risks client firms may face when they opt to offshore IT functions. Importantly, this means that these firms may face the risk of failing to develop new IT governance capabilities that are required to identify, manage and control these risks. In light of this knowledge gap, this research has made two significant contributions to both the IT governance and IT offshoring risk research.

The first research contribution is towards the development of a better understanding of the risks involved in IT offshoring, through IT offshoring risk literature review and content analysis. We have also categorized these risks reported in the research journals into risk categories based on the source of origin: client risks, vendor risks and inter-firm relationship risks that arise within IT offshoring arrangements. Client risks, such as loss of firm's capabilities and competences and increased switching costs, have been identified in the IT outsourcing literature and not new. Similarly, vendor risks such as lack of critical knowledge/expertise on client's business domains and functional areas and vendor service debasement were also reported in outsourcing literature. However, new and emerging IT offshoring risks that are unique to IT offshoring practice include inter-firm relationship risks such as greater difficulty in communicating and coordinating with offshore vendors whose cultures, languages, national law enforcement practices radically differ from those of the client firm. Furthermore, new and emerging IT offshoring risks also include risks associated with environmental uncertainties such as lack of intellectual property safeguards and corruption at offshore destination.

The second research contribution this study has made is towards the theoretical extension to the extant core IS governance framework. In this research, we found that nearly sixty per cent of the risks identified in the IT offshoring literature could be mapped against the core IS governance capabilities framework. However, further analysis of the results indicates the need to revise the governance capabilities identified in the core IS capabilities framework, which was originally developed in the IT outsourcing context. In addition to the two capabilities of leadership and informed buying that comprise the outsourcing governance in the framework, we suggest that the third capability, namely strategic management of risks and controls, needs to be added to the extant governance capabilities in order to address new and emerging IT offshoring risks in a different offshoring context.

This paper has focused on the IT offshoring risk literature. Future research directions should include the expansion of the research scope to include software development risk literature as well as further analysis of the conference papers that were excluded in this paper. Validation of our findings is required through case studies of client firms that have opted to offshore IT functions.

References

- [1] Aron, R., Clemons, E. K., and Reddi, S. "Just Right Outsourcing: Understanding and Managing Risk," *Journal of Management Information Systems* 22(7), 2006, pp. 37-55.
- [2] Bhatnagar, S. C., and Madon, S. "The Indian Software Industry: Moving towards Maturity," *Journal of Information Technology* 12(4), 1997, pp. 277-288.
- [3] Carmel, E., and Agarwal, R. "The Maturation of Offshore Sourcing of Information Technology Work," *MIS Quarterly Executive* 1(2), 2002, pp. 65-77.
- [4] Carmel, E., and Nicholson, B. "Small Firms and Offshore Software Outsourcing: High Transaction Costs and Their Mitigation," *Journal of Global Information Management* 13(3), 2005, pp. 33-54.
- [5] Chatfield, A., and Wanninayaka, P. "IT Governance Silo in the Firm: An Analysis of IT Governance Research Literature," *Proceedings of 2006 IT Governance International Conference*, Auckland, New Zealand, 2006.
- [6] Dhar, S., and Balakrishnan, B. "Risks, Benefits, and Challenges in Global IT Outsourcing: Perspectives and Practices," *Journal of Global Information Management* 14(3), 2006, pp. 39-63.
- [7] Dutta, A., and Roy, R. "Offshore Outsourcing: A Dynamic Causal Model of Counteracting Forces,"

- Journal of Management Information Systems* 22(2), 2005, pp.15-35.
- [8] Feeny, D. F., Willcocks L.P. "Core IS Capabilities for Exploiting Information Technology," *Sloan Management Review* 39(3), 1998, pp. 9-21.
- [9] Gopal, A., Sivaramakrishnan, K., Krishnan, M. S., and Mukhopadhyay, T. "Contracts in Offshore Software Development: An Empirical Analysis," *Management Science* 49(12), 2003, pp. 1671-1683.
- [10] Grant, R. *Offshoring jobs: US and Australian Debates*, Parliament of Australia - Department of Parliamentary Services, Australia, 2005.
- [11] Holsti, O. *Content Analysis for the Social Sciences and Humanities*. Reading, Mass., 1969.
- [12] IDC. *IDC Executive Market Watch Market Research*, July 26, 2006 (available online at http://cdn.idc.com/uk/downloads/events/idc_executive_market_watch.pdf).
- [13] Kaiser, K. M., and Hawk, S. "Evolution of Offshore Software Development: From Outsourcing to Cosourcing," *MIS Quarterly Executive* 3(2), 2004, pp. 69-81.
- [14] Karyda, M., Mitrou, E., and Quirchmayr, G. "A Framework for Outsourcing IS/IT Security Services," *Information Management & Computer Security* 14(5), 2006, pp. 402-415.
- [15] King, W. R. "Outsourcing Becomes More Complex," *Information Systems Management* 22(2), 2005a, pp. 89-90.
- [16] King, W. R. "Innovation in Responding to the "Threat" of IT Offshoring," *Information Systems Management* 22(4), 2005b, pp. 80-81.
- [17] King, W. R. "Offshoring Decision Time is at Hand," *Information Systems Management* 23(3), 2006, pp.102-103.
- [18] King, W. R. "The IS Organization of the Future: Impacts of Global Sourcing," *Information Systems Management* 24(2), 2007, pp.121-127.
- [19] Mann, C. "What Global Sourcing Means for US IT Workers and the Economy," *Communications of the ACM* 47(7), 2004, pp. 33-35.
- [20] Matloff, N. "Globalization and the American IT Worker," *Communications of the ACM* 47(11), 2004, pp. 27-29.
- [21] Meadows, C. J. "Globalizing Software Development," *Journal of Global Information Management* 4(1), 1996, pp. 5-14.
- [22] Niederman, F., Kundu, S., and Salas, S. "IT Software Development Offshoring: A Multi-Level Theoretical Framework and Research Agenda," *Journal of Global Information Management* 14(2), 2006, pp. 52-74.
- [23] Qu, Z., and Brocklehurst, M. "What Will it Take for China to Become a Competitive Force in Offshore Outsourcing? An Analysis of the Role of Transaction Costs in Supplier Selection," *Journal of Information Technology* 18(1), 2003, pp. 53-67.
- [24] Rao, M. T. "Key Issues for Global IT Sourcing: Country and Individual Factors," *Information Systems Management* 21(3), 2004, pp. 16-21.
- [25] Rottman, J. W., and Lacity, M. C. "Twenty Practices for Offshore Sourcing," *MIS Quarterly Executive* 3(3), 2004, pp. 117-130.
- [26] Rottman, J. W., and Lacity, M. C. "Proven Practices for Effectively Offshoring IT Work," *MIT Sloan Management Review* 47(3), 2006, pp. 56-63.
- [27] Smith, M. A., Mitra, S., and Narasimhan, S. "Offshore Outsourcing of Software Development and Maintenance: A Framework for Issues," *Information & Management* 31(3), 1996, pp. 165-175.
- [28] Swartz, N. "Offshoring Privacy," *Information Management Journal* 38(5), 2004, pp. 24-26.
- [29] Venkatraman, N. "Offshoring without Guilt," *MIT Sloan Management Review* 45(3), 2004, pp. 14-16.
- [30] Willcocks L.P., Feeny, D. F. "IT Outsourcing and Core IS Capabilities: Challenges and Lessons at Dupont," *Information Systems Management* 23(1), 2006, pp. 49-56.
- [31] Zviran, M., Ahituv, N., and Armoni, A. "Building Outsourcing Relationships across the Global Community: The UPS–Motorola Experience," *The Journal of Strategic Information Systems* 10(4), 2001, pp. 313-333.