Association for Information Systems

AIS Electronic Library (AISeL)

ACIS 2016 Proceedings

Australasian (ACIS)

2016

The Multidimensionality of IT Outsourcing Risks

Anna Zaitsev
University of Sydney, anna.zaitsev@sydney.edu.au

Kenneth Stevens
The University of New South Wales, k.stevens@unsw.edu.au

Follow this and additional works at: https://aisel.aisnet.org/acis2016

The Multidimensionality of IT Outsourcing Risks

Anna Zaitsev
Business Information Systems
The University of Sydney Business School
New South Wales, Australia
Email: anna.zaitsev@sydney.edu.au

Kenneth J Stevens
Information Systems and Technology Management
The University of New South Wales Business School
New South Wales, Australia
Email: k.stevens@unsw.edu.au

Deborah Bunker
Business Information Systems
The University of Sydney Business School
New South Wales, Australia
Email: deborah.bunker@sydney.edu.au

Abstract

IT outsourcing is a complex endeavour with multiple sources of risks. The body of knowledge on the subject is vast but scattered. Our project aims to create an integrated risk and controls framework. This paper discusses the multidimensional nature of outsourcing risks that needs to be addressed when such framework is developed. This paper presents findings from two workshops where risks, their classifications and dimensions where discussed by a group of experienced risk practitioners. The results highlight that practitioners see strategy, stakeholders and the different phases of the outsourcing as important dimensions that create risk and need to be addressed when organisations are planning or running an outsourcing venture. This research confirms that there are a number of dimensions in IT outsourcing risk and it has provided depth to the understanding of these dimensions.

Keywords IT outsourcing, risk, multidimensionality, action research

1   Introduction

The risks associated with information systems outsourcing, and the managements of those risks is a topic that has drawn research attention in the information systems (IS) field since the first major outsourcing deal between Kodak and IBM in early nineties (e.g. Earl 1996; Willcocks et al. 1999; Herath and Kishore 2009; Yim 2014).

The lengthy history of the research in this topic has left us with a somewhat confusing assortment of categorisation schemes and taxonomies that classify these risks across a board range of dimensions from the purpose and approach of the outsourcing (e.g. Franceschini et al. 2003; Lacity and Rottman 2008) to the location of the outsourcing provider (Gandhi et al. 2012). The sources of risks are equally manifold (e.g. Gandhi et al. 2012), as are the theories used to explain them (Zaitsev and Bunker 2016). Similarly the suggested control mechanisms to the risks are also complex and multilayered (e.g. ISACA 2014; Protiviti 2015). Recent technological developments, for example cloud computing (Boyd 2014), can create novel risks, which require equally novel controls. With such complexity and diversity surrounding the way these risks, sources and controls are classified and discussed, it is little wonder that recent industry surveys show many organisations are failing to adequately address and manage these risk (Protiviti 2015).

These persisting issues with risk identification and management have motivated us into a research project focusing on the development of an innovative and integrated framework that can support business to effectively conduct sourcing risk assessments and implement appropriate mitigation strategies. Bunker, Hardy, Barber and Stevens (2015) describe a framework that could be applied by both outsourcing suppliers and customer in order to "1) decrease the rate of failure of sourcing arrangements by ensuring that the most cost effective controls are implemented and used, and 2) decrease the transaction costs for sourcing by limiting the use of inappropriate or ineffective controls and by encouraging the selection of controls that are appropriate and effective." (Bunker et al. 2015). A stream of this research is also focusing on development of an ontological representation of the risk and controls frameworks that will eventually form the basis for an interactive website in order to facilitate interactions between the academia and risk practitioners. The first steps towards the ontology are presented in Zaitsev and Bunker (2016).

A significant part of this project is the investigation of the multiplicity of the dimensions of outsourcing risks. In this paper we take a detailed look at the different perspectives on risk and controls, from the academic perspective and with the support of our empirical data.

This paper will briefly introduce the areas of IT outsourcing risks that are widely recognised and, through examples, outline the different dimensions and perspectives evident in the literature. The paper then describes action research workshops used to collect empirical data that explored these different dimensions. The paper then presents our results that highlight the need for multidimensional approach when discussing outsourcing risk and conclusions with a discussion of our next steps.

2   ITO perspectives and dimensions in literature

The multidimensionality of IT outsourcing risks stems from the complexity of IT outsourcing. Gonzales et al. (2006) have listed 22 different major outsourcing topic discussed in the academic literature. Each of these topics brings a new perceptive to the discussion of IS outsourcing and adds layers of complexity to the overall discussion. From within the literature, Gonzales et al. distil five main perspectives: outsourcing from the perspective of the client, perspective of the provider, perspective of the relationship, perspective of economic theories and other topics such as cultural issues, or industry related issues.

Moreover, Lacity et al. (2010) conducted a review of the dependent and independent variables used in IT outsourcing literature and found 36 dependent variables and 138 independent variables that have been used to investigate forces affecting the IT outsourcing. They categorised the dependent variables into two categories: IT outsourcing decisions and outcomes. The independent variables were split into thirteen categories, ranging from motivation to supplier characteristics. Each variable could be seen as potential source of risk, not only the variables that are clearly labelled with "risk" in their names.

Both extensive literature reviews by Gonzales et al. (2006) and Lacity et al. (2010) confirm that the subject of IT outsourcing has been studied from multiple perspectives but not all of the aspects of outsourcing are recognised as potential sources of IT outsourcing risks. Thus, we decided to investigate literature that would especially discuss risks from temporal, theoretical or organisational perspectives.

It is apparent that perspective on risk taken depends on the phase the IT outsourcing endeavour is in. For example, Gewald and Hinz (2004) classify operational risk by four stages: the pre-deal phase, the contractual phase, the transition phase and the delivery phase. For each of these phases, there are different risks involved, with some risk extinguishing and others arising as a project progresses along its phases.

So what are the causes for the risks in the different stages of an IT outsourcing project? The key underlying theories provide some basis for an explanation. Agency theory has been used to explain opportunistic behaviour (Sharma 1997) and other undesired behaviours (Gonzales et al. 2010) and controls that can be put in place via careful contracting (Eisenheardt 1989). The resource-based view (RBV) assists in understanding uncertainty, complexity and cost-related risks (Duncan 1998). Risks related to vendor-customer relationship, such as the risks arising from different cultural and political aspects, are usually related to transaction cost theory (e.g. Jurison 1995: Aubert et al. 2004: Elango and Chen 2010; Jain and Thietart 2013). Unfortunately, while the extant literature does provide an adequate theoretical explanation for some risks, they represent only a small proportion of the identified risks (Zaitsev and Bunker 2016).

Organisational roles and their relationship with risks also lack coverage in the academic literature. While some studies have identified that there are multiple factors that could be related to different roles, such as trust, contracts and HR capabilities (Lacity et al. 2010), and the different groups of stakeholders, such as employees, shareholders, customers and vendors have been identified (e.g. Gandhi et al. 2012), they have not been pursued in any particular depth.

Another aspect of outsourcing is the destination of the outsourced services. Offshoring, especially when it involves crossing continents, is discussed as one of the major risk factor in IT outsourcing (e.g. Dibbern et al. 2008; Herath and Kishore 2009). Offshoring, onshoring and nearshoring, the commonly used geographical categories of outsourcing (Gandhi et al. 2012), are seen to be undertaken for either traditional cost cutting purposes or strategic and reasons (Franceschini et al. 2003), however the changing business and political landscape in which these different outsourcing arrangements operate mean that the various risks associated with the arrangements are evolving and hence in need of further investigation.

The different perspectives identified and discussed in academic literature are summarised in Figure 1. While the literature does cover different aspects of the phenomena, a holistic and integrated view, which would combine all the different facets, is yet to be created.
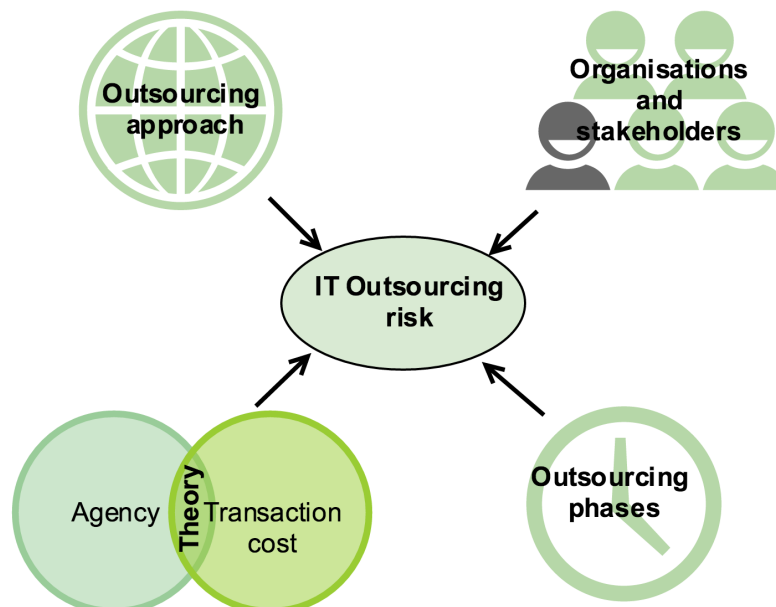

Figure 1 Risk dimensions discussed in literature

3   Research Design

Understand the different dimensions in IT outsourcing is the first step towards overall research objective of developing and implementing an IT outsourcing risk and control Framework. To better understand these dimensions, and other aspects of the research, series of stakeholder workshops were held. Bunker et al. (2015) stated the objectives of the workshop were to determine: "how practitioners identify and manage risk complexity through their patterns of control within their sourcing arrangements and the technical, social and institutional influences embedded in their risk perceptions."

Our research project consists of four research stages. In the first stage we developed sourcing risk identification and classification with the data gathered in the workshops. The next step is focused on developing control patterns and third stage concentrates on integrating the sourcing risk and classifications as well as the sourcing controls. Finally we plan to apply and test the framework in situ in order to identify risks and controls. In the application and test stage we will also measure control effectiveness in order to inform better decisions and improve the risk and controls framework.

This paper describes the findings of the first stage. The research data was collected in series of workshops where industry representatives were invited to share their knowledge of ICT sourcing risks with the research team consisting of academics with industry background. We designed the workshops in order to provide us better understanding of risks in organisational sourcing arrangements, risks that are impacting the effective decision making on outsourcing by organisations.

This approach is aligned with our action research methodology, which consists of exploration and action research cycles, forming a reflective, iterative and rigorous process (Baskerville and Wood-Harper 1998). The workshops were designed to facilitate the identification of main issues regarding the phenomena of IT outsourcing risks and also to provide intervention opportunity to the workshop participants, a chance to take part in design and redesign of the tools that would help to solve the issues. The three key generic components of Discovery and Action Research methodologies, as in Bunker et al. (2015), are:

- Workshops –The *diagnostic* component, involving researchers and key industry representatives in developing a shared interpretation of the Sourcing Risk and Control Framework objectives, assumptions, information, processes and support practices; diagnosis also involves problems related to implementation of a particular framework design and achievements of the framework objectives;

- Workshops – The *intervention* component (also called therapeutic), involving the design and re-design of the Sourcing Risk and Control Framework objectives, assumptions, information, processes and support practices, based on diagnosis; and

- Organisational Case Studies – The *learning* component, involving distinct, ongoing processes of reflection on consultative practices underway and learning from observations of changes in these practices in the design of the Sourcing Risk and Control Framework. This will be undertaken in the context of the critical argument theory.

The canonical form of action research, the design we are following in our research project, is presented in *Figure 2*, specifying cycles that involve diagnosis, action planning, evaluating and specifying learning is presented (Baskerville and Wood-Harper 1998).
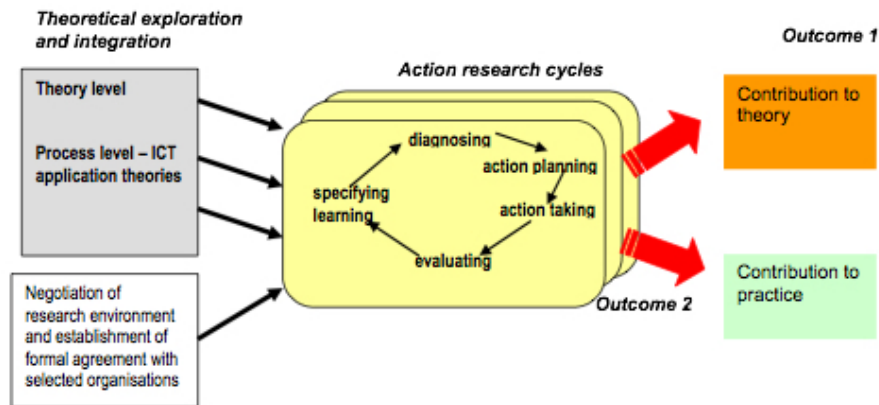
Figure 2 Research design (Bunker et al. 2015)

The research data is collected in each cycle of cyclical Discovery and Action Research. The project team recorded all the workshops as well as other reflection and learning phases of the research. The workshop participants consisted of a mix of practitioners and academics, all of who had experience in outsourcing and risk management in IT industry.

Practitioners	Count	Academics	Count (discipline)
Director	4	Professor	1 (IS)
Information security manager	1	Senior lecturer	3 (IS, computer science)
Legal council	1	Lecturer	2 (IS, accounting)
Project manager/technical lead/practice lead	4		
	10		6

Table 1 Workshop participants

Overall three workshops were held with the same participants, with only first two relevant for this topic. The research workshops were facilitated with Quality Function Deployment (QFD) method (e.g. Crow 1994; Akao 2004). This facilitation technique aided the collection of detailed qualitative data within the workshop's time constraints and discussed in further detail in Bunker et al. (2015). A overview of workshop activities is outlined in *Table 2 Workshop activities and outcomes*

Workshop	Workshop activities	Workshop outcomes
First workshop: introduction and risks	• Gathering requirements for the risk ontology ("If you had a risk ontology, what would you use it for?") • Mapping the requirements under different requirement categories	• Requirements for the ontology • Initials risks written on PostIT notes • Transcript of the workshop discussion
Second workshop: risks analysis	• Additional risks written, one risk per one PostIT note • Risks categorised under risk categories, strategy and operational	• 156 individual risks • 16 risk categories • Risk dimensions:

	dimensions	strategy or operations
	• Discussion of connections (weak-medium-strong) between the categories	• Risk category relations
		• Transcript of the workshop discussion

Table 2 Workshop activities and outcomes

As the focus of this paper is the multiple dimensions and perspectives of IT outsourcing risks, the data presented in this paper is sourced from the workshop discussions. The workshops were recorded (audio only) and later transcribed. The transcripts captures the discussion of what kind of uses there would be for a risk ontology, what kind of categorisation there is for the risks and what are the connections between these risk categories. The strategic and operational dimensions of the risks were also discussed. In order to better understand the multiplicity of the risks, we analysed the transcripts and found point where participant were either agreeing or disagreeing on the categorisation or description of the suggested risks. From this data we could distil the differences of risks in different stages of the outsourcing and along different organisational roles.

4   Multidimensionality of risks

There are numerous ways to categorise risks. Our workshops identified 16 different subcategories of risks, with some complex, if not convoluted relationships between them. Perhaps to highlight the difficulties of this topic, the very definition of the basic concepts was not that clear and took considerable time to discuss and move towards a consensus. As the following dialogue between two workshop participants who are discussing a classification of a risk illustrates, the risks could be categorised in multiple ways depending on the perspectives of the organisation, the role the person analysing the risk in the organisation has and on the technologies that are involved:

Participant 1*: "So, 'contracts management', is that part of 'vendor management'? Are we happy with that?"*

Participant 2*: "It's a bit more than that."*

Participant 1*: "Well, it could also be customer management."*

Participant 2*: "Yes."*

Participant 1*: "It's interesting because we're looking at this all in terms of controlling vendors..."*

Participant 2*: "It's the other way –you can apply to everyone."*

Participant 1*: "Do you want to add a separate category of customer management?"*

Participant 2*: "Vendor management is really about managing..."*

Participant 1*: "It's about relationship management."*

Participant 2*: "...the contract isn't it?"*

Participant 1*: "Either way."*

Participant 2*: "There are incentives that are built into a contract to either promote or discourage certain behaviours, and the effectiveness of those penalties in reality might shape people's views about whether or not they want to take on that risk."*

Participant 1*: "I think you're actually onto something there in terms of when board or executive first considers the possibility of outsourcing, that they want to understand the broad reputational and, potentially IP risks..."*

Participant 2*: "...other such risks that any organisation would consider as part of any commercial engagement...It could be that this contractual thing or legal and regulatory framework contract design is more than just a point in time thing, it's a pre-strategy."*

Participant 1*: "Absolutely."*

Participant 2*: "If we see there's no real difference, we can add it to strategy or do something else with it."*

Participant 1*: "That gets really quite applicable to things like cloud, for example."*

In the other parts of the workshop, the participants discussed risks across the different phases of the project. We could identify statements from all four phases as described in literature (Gewald and Hinz 2004): pre-deal phase, the contractual phase, the transition phase and the delivery phase. In*Table 3*

we present excerpts from different discussions that were around classification and categorizations of risks and how the risks fit into the different stages of outsourcing.

Phase	*Workshop quotes*
Decision to outsource e.g. the pre-deal phase	*The regulatory and legal framework, I think is actually quite important and is something you need to address right at the very, very beginning before you get down to anything else, after you've done the strategy. – a workshop participant*
	...There is also the perspective that the way you construct your outsourcing agreement, the strategy around that, if you're not allowed for the ability to change technology based on what's happening in the market and the environment in which you operate your business, then you risk the potential of either being left behind or incurring a very high cost to actually move once the contract is in place.
Selection of vendor e.g. the contractual phase	*...if you think about the life cycle, you spend a small amount of time and a small amount of dollars in the front. Most of the dollars are actually spent on the 90% back end. The evaluation is just something that happens at a point in time...The focus should always be on the back end because that's where the dollars are.*
	No, I was just talking about the nature of strategic alliances simply because it seem to me even if people go into these negotiations roughly thinking in those terms, but when you start talking about...But there is a trend about strategic alliancing where a different commercial model of operation and engagement. So, I think that is right and that's more under vendor engagement, vendor management.
Transition e.g. the transition phase	*...Outsourcing will help to get to that new service delivery model so all the risks that identified with the delivery model. But there's a general risk or an overriding risk of the organisation not being able to drive to the new service delivery model and there's so many organisations are okay at the strategy but kind of fail [at the transition].*
	But do be aware that the industry trend is that – and it has been decreasing over the last decade or 12 years, the average duration of contracts – average duration – has fallen by probably about 18 months. So, where the average duration might have been six and a half to seven years, it's now probably under five years.
Operation e.g. the delivery phase	*.... but you can have the same contract, it's what people do with it that makes the difference, the execution. So, you've got an advantage through the strong relationship with IP in the contract. The advantage is temporary; it has a life span of some duration, right. And, I think the idea of what is contemporary versus what is sustainable might be an interesting dynamic to apply to the risk management stuff as well.*
	The moment you start talking about governance and control in the same category, it no longer remains governance it just becomes assurance and it goes down to all the people and beat the hell out of them sort of stuff.

Table 3 Risks in different phases of outsourcing

The other theme that emerged from the data was the difference in the perspectives of risk when different organisational roles where considered. The workshop participants had experience of dealing with IT outsourcing risks in their own roles and they had to interact with other departments in their organisations. The main stakeholders that were mentioned in the discussion were the regulators, the relationship between the vendors and clients and the legal department. The following *Table 4* presents some of the discussion that the workshop participants had around different organisational roles and the risks from their perspective.

Role	Workshop quotes
Regulators	*Now, a regulator might use a {risk and controls} framework like this to say: "actually I'm looking at an industry, I'm looking at the kinds of controls you've got in place, I've got all this research here that says those controls are next to useless– I'm going to intercede. Conversely… if a regulator looks at an industry and says actually those controls are extremely effective, I'm going to become less intrusive in the industry because I can see actually they're regulating themselves quite effectively.*
Vendors vs. clients	*… Going back to the interoperability, to me that's like a Nirvana that will never actually happen. I think the practical point is that every client environment has a level of legacy about it, some are worse than others, and any service provider comes along, they will just be concerned about their patch because they have to have a commercial model..*
	Clients are actually quite risk averse so I think that's the – the other risk in strategy is that the strategy has a certain commercial model risk outcome to it, and what actually happens in reality is clients really are always quite, "Yes, yes. We want a risk/reward relationship," but when that reward goes to the service provider if they over perform they're not that keen. So, they'd rather have the money themselves.
Legal department	*A lot of times, legal is like, "Oh my God, what can I do to kind of fit with this strategy?" It's only at some points where you go, "Actually guys, you really cannot do this," but all the time they will push the boundaries.*
	… Contract complexity, not in terms of how complex the contract is but the fact that you might be juggling multiple contracts with different suppliers, with different lock in times, with different…

Table 4 Risk from organisational role perspective

5 Discussion and conclusion

The workshops confirmed to us that there are multiple dimensions in risks in IT outsourcing that should be incorporated into discussion when IT outsourcing risks are discussed. Our findings highlight that under-researched areas, such as stakeholders or phases of the outsourcing, are seen as important dimensions for the practitioners.

The main insight from the workshop discussion was the linkage between the strategy, the phase the outsourcing is in and the perceived risk. Different things are risks for different phases and what is considered a risk depends on what the outsourcing strategy is. How the risk is managed and controlled is related to both the phase and the organizational role of the person(s) / group responsible for controlling the risk, where that responsibility is either formal (i.e. the person(s) / group are the formal risk owners as per the organizational governance structure) or informally (i.e they just happen to be managing the risk because it falls within the gamut of things they typically manage). For example, the vendors pose different risks if the relationship between the vendor and the client is based on a strategic alliance or if the outsourcer is only seeking cost cutting opportunities.

These differences in the perception of the risk are, however, not as clear as the example above. Another insight from the workshop discussion was that differences in the role can lead to subtle differences in both the perception of what the risks are and how they should be controlled. These differences could well account for some of the variation in the literature in and around the identification and categorisation of risks, with different roles seeing the risks as slightly different from how they are seen by other roles, with implications for the treatment and control of those risks.

Figure 3 highlights the dimensions of outsourcing risks that are supported by our workshop data: the different phases of the project and the stakeholders. The additions sourced from our data are accentuated with red in the figure below.
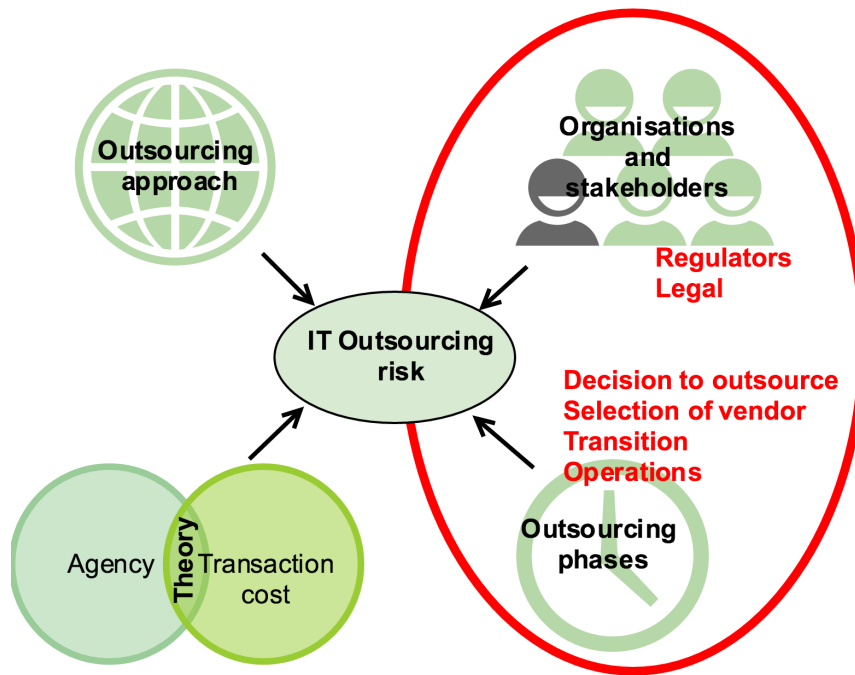
Figure 3 Dimensions discussed in the workshops

Our findings suggest that IT outsourcing risks are contextual and the perceived risks are dependent on the stage of outsourcing. Different members of the organisation see different risks and have different insights that reflect both their experiences and their position in the outsourcing endeavour further complicate this contextuality. The risks are different also for customers and vendors.

This research has confirmed a number of dimensions in IT outsourcing risk and provides some additional depth to the understanding of those dimensions. It has uncovered a more complex picture than first expected, which suggest that in order to be able to properly capture this multidimensionality, traditional, flat, two-dimensional taxonomies are simply not enough. We see that the results of the investigation of the multidimensionality of risks as a confirmation of the need for further investigation and the development of an ontological representation tool that underpins the desired risk and controls framework. Our next steps are then to further investigate the identified dimensions, and any other dimension that arise during that investigation and with a view to develop both ontology and framework. Given the success of the workshop method used to date, we anticipate further practitioner for as the primary means of date collection.

6   References

Akao, Y., Mazur, G. H., and King, B. 1990. *Quality Function Deployment: Integrating Customer Requirements into Product Design*. MA: Productivity Press Cambridge.

Aubert, B.A., Rivard, S. and Patry, M., 2004. "A transaction cost model of IT outsourcing," *Information & Management*, (41:7), pp.921-932.

Baskerville, R., and Woodharper, A.T. 1998. "Diversity in Information Systems Action Research Methods," *European Journal of Information Systems* (7: 2), June, pp 90-107.

Boyd, B.Y. 2014 "Cloud control: managing the risks of engaging and terminating cloud services." *Information Management Journal* Nov.-Dec. 2014: 20

Bunker, D., Hardy, C., Babar, A. and Stevens, K., 2016. "Exploring Practitioner Perspectives of Sourcing Risks: Towards the Development of an Integrated Risk and Control Framework," *Australasian Conference on Information Systems*, Adelaide, South Australia

Crow, K. 1994. "Customer-focused Development with QFD," *Annual Quality Congress Proceedings American Society For Quality Control*, pp 839-839.

Dibbern, J., Winkler, J., and Heinzl, A., 2008. "Explaining variations in client extra costs between software projects offshored to India," *MIS Quarterly* (32:2), pp 333-366.

Duncan, N. B. 1998. "Beyond opportunism: a resource-based view of outsourcing risk," System Sciences, 1998., *Proceedings of the Thirty-First Hawaii International Conference on, IEEE 1998*, pp 675-684.

Earl, M.J., 1996. "The risks of outsourcing IT," *MIT Sloan Management Review*,(37:3), pp 26.

Eisenhardt, K. M. 1989. "Agency theory: An assessment and review," *Academy of management review* (14:1), pp 57-74.

Elango, B., and Chen, S. 2012. "Learning to manage risks in international R&D joint ventures through ownership decisions," *Management Decision* (50:8), pp 1425-1444.

Franceschini, F., Galetto, M., Pignatelli, A. and Varetto, M. 2003, "Outsourcing: guidelines for a structured approach", *Benchmarking: An International Journal*, (3:10), pp 246-60

Gandhi, S., Gorod, A., and Sauser, B. 2012. "Prioritization of Outsourcing Risks From a Systemic Perspective," *Strategic Outsourcing* (5:1), pp 39-71.

Gewald, H. and Hinz, D., 2004. "A Framework for Classifying the Operational Risks of Outsourcing-Integrating Risks from Systems, Processes, People and External Events within the Banking Industry," *Pacific Asia Conference on Information System (PACIS) proceedings* 2004

Gonzalez, R., Gasco, J., and Juan, L. 2006. "Information Systems Outsourcing: An Empirical Study Of Success Factors," 2006. Information systems outsourcing: A literature analysis. *Information & Management*, (43:7), pp.821-834.

Gonzalez, R., Gasco, J., and Llopis, J. 2010. "Information systems offshore outsourcing: an exploratory study of motivations and risks in large Spanish firms," *Information Systems Management* (27:4), pp 340-355.

Herath, T., and Kishore, R. 2009. "Offshore Outsourcing: Risks, Challenges, and Potential Solutions," *Information Systems Management* (26:4), October, pp 312-326.

ISACA. 2014. Vendor Management, Using COBIT® 5, Rolling Meadows, IL USA: ISACA.

Jain, A., and Thietart, R-A. 2013. "Knowledge Based Transactions and Decision Framing in Information Technology Outsourcing," *Journal of Strategic Information Systems* (22:4), December, pp 315-327.

Jurison, J. 1995. "The role of risk and return in information technology outsourcing decisions," *Journal of Information Technology* (10:4), pp 239-247.

Lacity, M. and Rottman, J., 2008. "*Offshore Outsourcing of IT Work*. Palgrave Macmillan UK.

Lacity, M.C., Khan, S., Yan, A., and Willcocks, L.P. 2010. "A Review of the IT Outsourcing Empirical Literature and Future Research Directions," *Journal of Information Technology* (25:4), October, pp 393-433.

Protiviti. 2015. "2014 Vendor Risk Management Benchmark Study", http://www.protiviti.com/en-US/Documents/Surveys/2015-Vendor-Risk-Management-Benchmark-Study.pdf- Retrieved 21st July 2016

Sharma, A. 1997. "Professional as agent: Knowledge asymmetry in agency exchange," *Academy of Management Review* (22:3), pp 758-798.

Willcocks, L.P., Lacity, M.C. and Kern, T. 1999. "Risk mitigation in IT outsourcing strategy revisited: longitudinal case research at LISA, " *The Journal of Strategic Information Systems* (8:3), pp 285-314.

Yim, A. 2014. "Failure risk and quality cost management in single versus multiple sourcing decision," *Decision Sciences* (45:2), pp 341-354.

Zaitsev A. and Bunker D., 2016. "Developing an Ontological View of Outsourcing Risk, Risk Categories and Their Relationships Using Protégé and OWL", *Pacific Asia Conference on Information System (PACIS) proceedings* 2016

Copyright