# A Framework for Information Security Risk Management in IT Outsourcing

Baber Majid Bhatti
*University of South Australia*, baber.bhatti@unisa.edu.au

Sameera Mubarak
*University of South Australia*, sameera.mubarak@unisa.edu.au

Sev Nagalingam
*University of South Australia*, sev.nagalingam@unisa.edu.au

# A Framework for Information Security Risk Management in IT Outsourcing

**Baber Majid Bhatti**
School of Information Technology and Mathematical Sciences
University of South Australia
Adelaide, Australia
Email: baber.bhatti@mymail.unisa.edu.au

**Sameera Mubarak**
School of Information Technology and Mathematical Sciences
University of South Australia
Adelaide, Australia
Email: sameera.mubarak@unisa.edu.au

**Sev Nagalingam**
School of Management
University of South Australia
Adelaide, Australia
Email: sev.nagalingam@unisa.edu.au

## Abstract

Information Technology Outsourcing (ITO) is a common business practice to outsource delivery of Information Technology (IT) services to external suppliers. During past two decades, ITO has grown significantly and has also become an established field of research. With rapid innovations in IT, information security is an increasing concern as new risks emerge in ITO that have not been explored by earlier studies. This paper highlights the insufficiency of the knowledge in ITO and investigates the need for information security risk management (ISRM) in ITO. It aims at creating an ISRM framework for ITO, which will contribute to knowledge and will help businesses improve their ITO strategy and better manage information security risks in their ITO arrangements.

**Keywords** Information Security, Information Security Risk Management, Information Technology Outsourcing

# 1 INTRODUCTION

Businesses often outsource their Information Technology (IT) scopes to external service providers for effectively delivering IT-enabled business processes, application services or infrastructure (Gartner 2017). Common objectives of IT Outsourcing (ITO) are improved quality of service, higher efficiencies, more cost savings, reduction in the number of in-house IT resources, strategic alliances, or delegation of operational risks and responsibilities to a third party to focus on core business activities instead of efforts on technical service delivery (Patil and Wongsurawat 2015). During the recent years, there has been a tremendous increase in the volume of ITO businesses globally (Gunasekaran et al. 2015). In the last two decades, the overall outsourcing business activities have grown at a rate of over thirty percent annually (Kabiraj and Sinha 2016). Gartner appraised the combined worth of global IT and business process outsourcing market at USD 424 billion in 2014 (Lacity et al. 2016). According to Gartner, ITO is currently the largest category of spending on information security and is expected to remain among the top three growing areas until the end of 2020 (Moore 2016). Despite its huge popularity, the failure rate of ITO is high and much attention is required to understand the reasons behind such failures (Dhillon et al. 2017). As an example, Australian Bureau of Statistics (ABS) chose to outsource their IT application for Australian population census to IBM Australia (Kalisch 2016). The scope of load testing to determine system resiliency was outsourced to another firm, Revolution IT (Barlow 2016). In the night of August 2016 when Australian citizens had to complete the online census forms, the ABS website failed (Merkel 2016). Even after taking reasonable information security risk measures, thorough testing by technical experts and following the prevailing information security best-practices, the incident could not be avoided, and a clear responsibility of this incident could not be attributed to either ABS (the ITO client) or IBM (the ITO supplier) (Kalisch 2016). This suggests that there is a need for improved Information Security Risk Management (ISRM) in ITO setups (Barlow 2016; Kalisch 2016; Merkel 2016).

ITO has also become an established field of research (Liang et al. 2016). The earliest research outputs on ITO started getting published in 1991 (Lacity et al. 2009) and the later studies examined a range of topics including ITO motivations, long-term consequences of ITO (Delen et al. 2016; Lacity et al. 2009), ITO decisions, outcomes of those decisions and the measurements of ITO successes or failures (Lacity et al. 2009; Lacity et al. 2017). However, existing knowledge is not enough to explain the high failure rate in ITO and the unprecedented risks that are increasingly being encountered by organisations, like those coming from the use of rapidly evolving technologies (cloud computing, internet of things, disruptive technologies etc.). There is a wide consensus among researchers and professionals that although information security is important, it is a less studied research area that contributes to ITO risks (González et al. 2016; Lacity et al. 2016; Liang et al. 2016). This paper is part of a bigger research project which aims to explore how the advancement in Information and Communication Technologies (ICT) impacts the ISRM in ITO businesses and will propose a framework for managing information security risks over the lifecycle of ITO. Besides adding to the existing knowledge, which is presently insufficient in the domain of ISRM in ITO, this research will help organisations better manage their information security risks emerging from their ITO partners and improve their strategic ITO decisions.

Section 2 discusses relevant literature along with gaps in knowledge. Section 3 proposes and discusses a framework for ISRM in ITO. Conclusion and future works are discussed in Section 4.

# 2 LITERATURE REVIEW

## 2.1 The ITO Perspective

Outsourcing is an arrangement where an organisation delegates the delivery of some of its business functions to another organisation and purchases it back as a service (Kabiraj and Sinha 2016). It is a widespread phenomenon adopted by businesses and is adopted by almost every business today (Kabiraj and Sinha 2016). The current maturity of global outsourcing has been possible due to the proliferation of technology (Sirkin et al. 2008). The global outsourcing market is increasingly becoming more viable and competitive (Pedersen et al. 2013). Outsourcing of information technology comprises delivery of IT-enabled business processes, application services or IT infrastructure (Gartner 2017). The global ITO market has been consistently growing during the past few decades and was estimated at USD 424 billion in 2014 (Gunasekaran et al. 2015; Lacity et al. 2016). Although cost savings is a major reason for a business to opt for ITO, it is not the only one. The most common reasons for businesses to outsource their IT are: cost savings, technical reasons, improved quality, increased flexibility, strategizing focus on core capabilities, access to global markets (Lacity et al. 2017; Martinez-Noya et al. 2012; Premuroso et al. 2012). Despite the fact that ITO is flourishing, the failure rate of ITO projects is also quite high in outsourcing setups (Dhillon et al. 2017). The most important factors leading to failures by negatively affecting the ITO decisions are: fear of losing control, security and intellectual property, political agendas, transaction costs, high business risks, high service complexity and high service interdependence (Bhagwatwar et al. 2011; Lacity et al. 2017; Poppo and Zenger 2002).

## 2.2 Lifecycle of Outsourcing

Comprehensive studies of risk analysis in ITO usually start with understanding the lifecycle of outsourcing (Chou, DC & Chou 2009). Several ITO lifecycle models have been proposed, many of which are proprietary. Recently the standardisation bodies have also started introducing their versions to bring standardisation to the global ITO market. An example of such a standard is ISO 37500 whose compliance can be expected as a requirement in future Requests for Proposals (RFPs) for the government or large-scale projects (ISO 2014). A brief overview of the popular outsourcing lifecycle models is presented here:

i. **ISO 37500:** The standard covers main phases, processes and governance of outsourcing irrespective of the organisation or industry (ISO 2014). It can be extended to any particular industry, location or organisation (Ritchie 2015). It provides a balanced view for both, the ITO client and the supplier organisations, and guides both of them on developing mutually beneficial collaboration for minimising the risks (ISO 2014). There are pressing concerns of the modern ITO industry which are not yet addressed by ISO 37500. These concerns include information security & privacy, cloud sourcing and social responsibility, which are expected to be addressed in the future version of the standard (Babin and Quayle 2016).

ii. **Managing outsourcing - The life cycle imperative:** The model was proposed for client organisations for improving their probability of success while minimising their risk exposure (Cullen et al. 2005). It does not require the business or sourcing strategy as a pre-requisite to the lifecycle (Cullen et al. 2006). It defines 54 activities encapsulated in nine building blocks and four phases: (1) Architect, (2) Engage, (3) Operate and (4) Regenerate.

iii. **Outsourcing Professional Body of Knowledge by IAOP:** There are five stages in this process model, each of which has a finish-to-start dependency (Professionals 2014). The completion of every stage is assessed through a gate, i.e., formally defined completion criterion. As compared to ISO and LSE lifecycle models, the IAOP model is quite abstract (Babin and Quayle 2016).

iv. **Outsourcing life cycle – Global Sourcing Association UK (GSA-UK):** It is a non-prescriptive model which applies to both, the client as well as the supplier organisations (UK 2016). The model emphasises governance as a critical mechanism for maintaining alignment and enabling relationships between the client and the supplier organisations (Babin and Quayle 2016). The model does not provide much details about the end of term activities like terminating or continuing the outsourcing relationship (Babin and Quayle 2016; UK 2016).

IT security is among the five major adaptive challenges of ITO client organisations and concerns related to it have increased during the recent years (Willcocks et al. 2011).

## 2.3 Theories of Outsourcing

An overview of outsourcing theories is pertinent for the theoretical underpinning of the practices (Chou and Chou 2009). The four popular outsourcing theories are discussed below.

i. **Theory of core competencies:** The organisations have a choice of performing activities either in-house or out-source. Core competency theory states that only the activities which are not considered as core competencies should be considered for outsourcing (Quinn 1992).

ii. **Transaction cost theory (TCT):** According to this theory, organisations choose to outsource on the basis of cost, which has two components: production costs and coordination (or transaction) costs (Hancox and Hackney 2000). If the transaction costs exceed the production cost advantages of the external supplier, the client organisation may rescind ITO (Gottschalk and Solli-Sæther 2005). As ITO practices are evolving fast and increasingly becoming complicated, the applicability of TCT is being questioned (Lacity et al. 2011; McIvor 2009).

iii. **Resource-based theory (RBT):** Initially proposed by Barney (1991), this theory considers outsourcing as a strategic decision that can be used to fill gaps in an organisation's capabilities and resources (Willcocks and Lacity 1998). This theory has two key points: (1) the resources are determinants of organisations' performance, (2) the resources must be rare, valuable and nonsubstitutable by others. To adapt to the changing environments, organisations develop dynamic capabilities through specific resources (Gottschalk and Solli-Sæther 2005).

iv. **Agency theory:** Agency theory is concerned with resolving two problems in the outsourcing relationships (Eisenhardt 1985): (1) when the goals or desires of the outsourcing client and supplier are in conflict, and it is difficult for the client to verify the activities performed by the supplier, (2) risk sharing when the risk preferences of both the parties are different. This often results in scope change requests through which the suppliers charge the clients for any extra scopes not covered in their ITO contracts (Gottschalk and Solli-Sæther 2005; Hancox and Hackney 2000).

It may be noted that none of the popular outsourcing theories deal with ISRM. The reason may be attributed to a delayed realisation of the significance of ISRM as an important factor affecting ITO decisions and their outcomes. This indicates the need for further work toward development of ISRM based theories of ITO, which will also help to improve the ISRM framework presented in this paper.

## 2.4 Information Security Risk Management (ISRM) in ITO

After discussing outsourcing lifecycles and theories, an understanding of ITO risks will establish the context of risk which is the focus of this paper. "Risk" is a function of the likelihood of occurrence of an event and the potential damage it can cause to the business (Blakley et al. 2001; Technology 2012). Information security refers to protecting information and information systems from unauthorised access, use, disclosure, disruption, modification in order to provide integrity, confidentiality and availability (Government 2017). In the context of ITO, information security involves confidentiality, integrity and availability of information or intellectual property pertaining to client and supplier organisations engaged in ITO (Dhillon et al. 2017). ISRM is the process of assessing, mitigating and maintaining information security risks to an acceptable level (Stoneburner et al. 2012). Typically, main steps of the ISRM process are: (1) risk identification, (2) risk assessment and (3) risk control (Whitman and Mattord 2016).

| Perspective | Top-3 Information Security Risks in ITO |
|---|---|
| ITO client | (1) Trust that ITO supplier applies proper security controls (Arjun and Subhajit 2007; Dhillon et al. 2017).<br>(2) Ability or willingness of ITO supplier to comply with client's security policies, standards and processes (Dhillon et al. 2017).<br>(3) Trust that ITO supplier will not abuse client's proprietary information or knowledge (Dhillon et al. 2017; Handley 2012). |
| ITO supplier | (1) Information security competency of the supplier's team (Dhillon 2008; Dhillon et al. 2017).<br>(2) Lack of comprehensiveness of ITO decisions of the client, which are important for the relationship (Dhillon et al. 2017; Goo et al. 2007).<br>(3) Dissipation of ITO supplier's knowledge due to staff turnover (Dhillon et al. 2017; Inkpen and Crossan 1995). |

*Table 1. Top-3 Information Security Risks in ITO*

González et al. (2016) conducted a rare, longitudinal study on ITO risks over a 12 years period from 2001 to 2013 and enlisted 87 risks with details. Among those, they found following risks as most important: (1) Qualification and capability of the staff of ITO suppliers, (2) Excessive dependence of ITO client organisations on the suppliers with the passage of time after outsourcing, (3) Lack of ITO suppliers' compliance with the expectations of their clients, (4) Hidden costs not explicitly covered in the ITO contract or budget, (5) Information Security risks as the ITO supplier has access to client's sensitive systems and data of the client; critical when a supplier is providing ITO services to multiple clients, (6) Employees' opposition to ITO is a risk at the client side. Earlier researchers (González et al. 2016; Lacity et al. 2016) mostly assume information security as a distinct ITO risk. However, other risks may sometimes lead eventually to information security risks. For example, a compromise on qualification and capability of a supplier's employees may render ITO more vulnerable to information security breaches, or employees opposing ITO may themselves become a source of information security risks. Information security is now consistently rated among the top ITO risks, and further research on it is required (Dhillon et al. 2017; González et al. 2016; Jimmy Gandhi et al. 2012; Lacity et al. 2016; Nassimbeni et al. 2012).

There are only a few studies which explicitly analyse information security risks in ITO. One such recent study by Dhillon et al. (2017) identified 26 information security risks in ITO from the perspectives of both, clients and suppliers. In order to exhibit how the organisational perspective can change risk perception, their top three information security risks from the perspective of clients as well as suppliers are presented in Table 1. A difference in perspectives of ITO clients and suppliers about information security risks in ITO does not imply that they always think different. According to Dhillon et al. (2017), there are common information security concerns too, which include: (1) legal and regulatory compliance, (2) technological maturity of ITO supplier's environment, (3) ability of ITO supplier to comply with client's security policies, standards, and processes, (4) dissipation of ITO supplier's knowledge, and (5) information security competency of ITO supplier.

After a detailed literature review of ITO and related information security risks, gaps in knowledge are identified and provided in the next section.

## 2.5 Current Gaps in Knowledge

With rapidly increasing automation in the recent years (Brynjolfsson and McAfee 2014), regulatory and contractual requirements are ever-changing, and new ITO types are emerging (Bachlechner et al. 2014; Kulkarni and Dwivedi 2008; Larsen et al. 2013; Liang et al. 2016). Examples of the traditional ITO types include offshore outsourcing, nearshore outsourcing, transitional outsourcing and business process outsourcing (BPO), while examples of the new types include crowdsourcing, cloud computing, multi-sourcing and open-sourcing. With new types, new practices in ITO emerge and give rise to unprecedented risks, which must be addressed (Doomun 2008; Liang et al. 2016). This raises research questions: whether the ISRM knowledge from previous types is equally applicable to these new types, how do the new information security risks affect the ITO outcomes or what could be the effective measure to mitigate those risks (González et al. 2016; Larsen et al. 2013; Liang et al. 2016)? The research literature, however, has still not sufficiently resolved the gaps created due to recent changes in the fast-moving IT industry and is insufficient in addressing the emergent issues this area (June et al. 2010; Lacity et al. 2016; Liang et al. 2016). Hence, there is a need for of new research to address the emergent information security issues in ITO (Dhillon et al. 2017; Liang et al. 2016).

| Authors | ITO Framework | Limitations |
|---|---|---|
| Dhillon et al. (2017) | Information security Framework in ITO | (1) Based on inputs from 11 participants, only comprising US clients and Indian suppliers. Hence, representativeness of the experts can be questioned. (2) High level and lacks details for application in real life. (3) Developed on the viewpoints of participants but was not empirically tested in real life. |
| Nassimbeni et al. (2012) | FMEA (Failure Mode and Effect Analysis) assessment framework | The framework does not cover information security risks. |
| Doomun (2008) | Multiple layer security framework for IT | The framework can be useful to identify, monitor and evaluate information security risks in ITO, but it lacks empirical validation. Also, the framework is process-centric and lacks specific details. |

*Table 2. ITO Risk Management Frameworks*

Although conceptual frameworks have previously been proposed for ITO, their focus is not on the ISRM. Only a limited number of studies present frameworks for information security risks in ITO, and each one has its own shortcomings, as mentioned in Table 2. As, for example, Lee's framework (Lee et al. 2012) is about outsourcing risk management in supply chain, while Chou's framework (Chou et al. 2015) presents a knowledge-process-governance management framework. It is concluded that a detailed and empirically tested ISRM framework for ITO is very much required because only a limited number of ITO frameworks address ISRM but those are either not sufficiently detailed or tested in real-life scenarios.

# 3 THE PROPOSED FRAMEWORK & DISCUSSION

In order to address the gaps highlighted in Section 2.5 above, the outcome of this research has been divided into two parts. Firstly, new information security risks emerging due to latest ITO practices and technologies will be identified. This will be done through a combination of literature review and interviews with professionals in the industry. Secondly, a lifecycle-based framework will be developed for managing information security risks in ITO. An initial version of this model is shown in Figure 1 below. It can be considered as an extension of the models by ISO (2014) and Cullen et al. (2005). These two models were selected because the latter is rigorously detailed and process-oriented but addresses only clients' perspective, while the former addresses both clients' and suppliers' perspective but misses out the latest pressing concerns of ITO industry including ISRM. Although neither addresses ISRM, they acknowledge this need. Hence, ISO (2014) and Cullen et al. (2005) together establish the context based on which a model is being proposed here. The main concept of the proposed framework is a continual presence of information security risk management as part of governance function throughout the lifecycle of ITO. The ITO lifecycle has been encapsulated into four phases: outsourcing strategy formulation or review, initiation of ITO engagement between client and supplier organisations, transitioning the outsourced scope to the supplier and ITO service delivery, which then loops back into the lifecycle. The ISRM activities in each of these phases play critical roles in assuring that the information security risks are monitored, controlled and managed with the acceptable limits of the organisation.

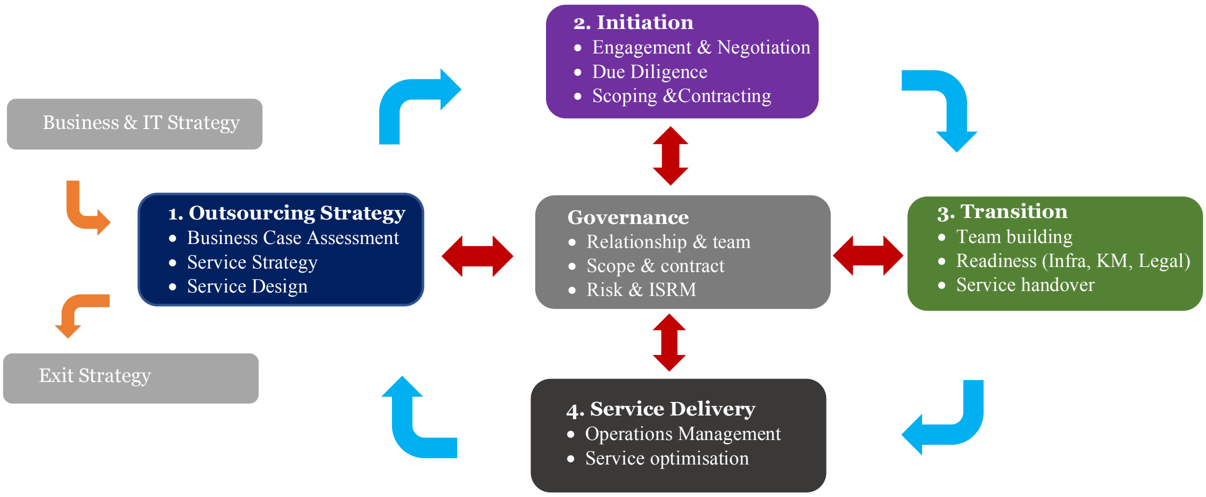

*Figure 1 Proposed ISRM framework for ITO*

In each of the phases, the ISRM activities are defined on the three dimensions: confidentiality, integrity and availability (CIA) of information and services. During the first phase (Outsourcing Strategy), the ISRM activities ensure a secure design of services and information, as derived from the business and IT strategies and the business requirements. It also includes identification of the required service, performance and confidentiality levels of the IT services which are being considered for outsourcing. During the second phase (Initiation), the ISRM activities validate that the offered ITO scopes through due diligence, ensure the scopes are feasible on the scale of CIA and checks the inclusion of these concerns in the contract. During the third phase (Transition), the ISRM is responsible for ensuring the readiness of infrastructure, knowledge management (KM), business processes, team capabilities and legal formalities from the viewpoint of CIA. Another important consideration of ISRM is to ensure that the services are handed over by the IT team of a client to the IT teams of the suppliers in a robust and secure fashion. After completion of the scope handover, main the service delivery becomes the accountability of the ITO supplier. In the fourth phase (Service Delivery), the ISRM keeps a close watch on the operations management of the outsourced scope. The supplier is required to keep a close watch on the services through continual surveillance. The incident management function is active, and the ISRM activities work proactively to foresee the probable risks and define their mitigation in advance. Any security breaches, risks or data leakages are instantly noticed and reported, and remedial actions are taken in accordance with the service agreement levels (SLAs). Another set of ISRM activities in this phase facilitate transformation, which is an initiative to improve the service to the contracted levels. The transformation may include deployment of new systems, migration to new systems, enhanced service monitoring and controlling capability, and ensures that CIA is built into the entire process. Optimisation of the information security controls is also part of this phase.

Each phase in this proposed framework is governed by a distinct set of processes, which cover overall risk governance, ISRM, ITO scope and contract governance, partner relationship and team governance. Hence, there will be four sets of governance processes, each for a phase. Those four sets of governance processes have been encapsulated in a central governance function as shown in Figure 1. The gaps mentioned in Section 2.5 will be addressed in those sets of processes, which will be detailed as this research progresses. The emergent issues created due to recent changes in the fast-moving IT industry will be addressed by specialised processes in this governance function. Workflows of those processes will be developed in the future part of this research.

# 4 CONCLUSION & FUTURE WORKS

This research emphasises the need for a detailed and empirically tested framework for managing information security risks in ITO. An ISRM framework for ITO has been developed, which proposes a continual governance of information security risks throughout the lifecycle of outsourcing. The application of this framework will help in controlling the information security risks and keeping them within acceptable limits of the organisations. This study will contribute to knowledge and will help to improve the ITO experience of the businesses.

During later stages of this research, the proposed framework for ISRM in ITO will be refined through detailed interviews with industry professionals using the qualitative approach and will be empirically validated by applying it to a real-life business for a period of at least three months. If all of the key recommendations from this research cannot be applied in a single organisation, the recommendations will be split into subsets, and each subset will be applied in at least one distinct organisation. The effectiveness of the proposed framework will be quantified on the dimensions of usefulness and applicability. The feedback from industry will also help in making the framework more useful and realistic to the needs of the IT industry.

# 5 REFERENCES

Arjun, K. P., and Subhajit, B. 2007. "Offshore Technology Outsourcing: Overview of Management and Legal Issues," *Business Process Management Journal* (13:1), pp. 21-46.

Babin, R., and Quayle, A. 2016. "Iso 37500 – Comparing Outsourcing Life-Cycle Models," *Strategic Outsourcing: An International Journal* (9:3), pp. 271-286.

Bachlechner, D., Thalmann, S., and Maier, R. 2014. "Security and Compliance Challenges in Complex It Outsourcing Arrangements: A Multi-Stakeholder Perspective," *Computers & Security* (40), pp. 38-59.

Barlow, K. 2016. "Census Failure 'Not a Hack, Not an Attack'. So What Was It?" Retrieved 12 June 2017, 2017, from http://www.huffingtonpost.com.au/2016/08/09/census-failure-not-a-hack-not-an-attack-so-what-was-it_a_21448470/

Barney, J. 1991. "Firm Resources and Sustained Competitive Advantage," *Journal of Management* (17:1), pp. 99-120.

Bhagwatwar, A., Hackney, R., and Desouza, K. C. 2011. "Considerations for Information Systems "Backsourcing": A Framework for Knowledge Re-Integration," *Information Systems Management* (28:2), pp. 165-173.

Blakley, B., Mcdermott, E., and Geer, D. 2001. "Information Security Is Information Risk Management," in: *Proceedings of the 2001 workshop on wew security paradigms,* V. Raskin (ed.). Cloudcroft, New Mexico: pp. 97-104.

Brynjolfsson, E., and McAfee, A. 2014. *The Second Machine Age : Work, Progress, and Prosperity in a Time of Brilliant Technologies*, (0th ed.). New York: W.W. Norton &amp; Company.

Chou, D. C., and Chou, A. Y. 2009. "Information Systems Outsourcing Life Cycle and Risks Analysis," *Computer Standards & Interfaces* (31:5), pp. 1036-1043.

Chou, S. W., Techatassanasoontorn, A. A., and Hung, I. H. 2015. "Understanding Commitment in Business Process Outsourcing Relationships," *Information & Management* (52:1), pp. 30-43.

Cullen, S., Seddon, P. B., and Willcocks, L. 2005. "Managing Outsourcing: The Life Cycle Imperative," *MIS Quarterly Executive* (Vol. 4 No. 1:March 2005).

Cullen, S., Seddon, P. B., and Willcocks, L. 2006. *Managing Outsourcing: The Lifecycle Imperative.* London School of Economics and Political Science London.

Delen, G. P. A. J., Peters, R. J., Verhoef, C., and van Vlijmen, S. F. M. 2016. "Lessons from Dutch It-Outsourcing Success and Failure," *Science of Computer Programming* (130), pp. 37-68.

Dhillon, G. 2008. "Organizational Competence for Harnessing It: A Case Study," *Information & Management* (45:5), pp. 297-303.

Dhillon, G., Syed, R., and Sá-Soares, F. d. 2017. "Information Security Concerns in It Outsourcing: Identifying (in) Congruence between Clients and Vendors," *Information & Management* (54:4), pp. 452-464.

Doomun, M. R. 2008. "Multi-Level Information System Security in Outsourcing Domain," *Business Process Management Journal* (14:6), pp. 849-857.

Eisenhardt, K. M. 1985. "Control: Organizational and Economic Approaches," *Management Science* (31:2), pp. 134-149.

Gartner. 2017. "It Outsourcing." Retrieved 2 June 2017, 2017, from http://www.gartner.com/it-glossary/it-outsourcing

González, R., Gascó, J., and Llopis, J. 2016. "Information Systems Outsourcing Reasons and Risks: Review and Evolution," *Journal of Global Information Technology Management* (19:4), pp. 223-249.

Goo, J., Kishore, R., Nam, K., Rao, H. R., and Song, Y. 2007. "An Investigation of Factors That Influence the Duration of It Outsourcing Relationships," *Decision Support Systems* (42:4), pp. 2107-2125.

Gottschalk, P., and Solli-Sæther, H. 2005. "Critical Success Factors from It Outsourcing Theories: An Empirical Study," *Industrial Management & Data Systems* (105:6), pp. 685-702.

Government, U. S. 2017. "U.S. Code, Title 44, Chapter 35, Subchapter Iii, § 3542," L.I. Institute (ed.). Legal Information Institute: Cornell University Law School.

Gunasekaran, A., Irani, Z., Choy, K.-L., Filippi, L., and Papadopoulos, T. 2015. "Performance Measures and Metrics in Outsourcing Decisions: A Review for Research and Applications," *International Journal of Production Economics* (161), pp. 153-166.

Hancox, M., and Hackney, R. 2000. "It Outsourcing: Frameworks for Conceptualizing Practice and Perception," *Information Systems Journal* (10:3), pp. 217-237.

Handley, S. M. 2012. "The Perilous Effects of Capability Loss on Outsourcing Management and Performance," *Journal of Operations Management* (30:1), pp. 152-165.

Inkpen, A. C., and Crossan, M. M. 1995. "Believing Is Seeing: Joint Ventures and Organization Learning*," *Journal of Management Studies* (32:5), pp. 595-618.

ISO. 2014. "Iso 37500:2014 Guidance on Outsourcing," in: *Guidance on outsourcing*. Geneva, www.iso.org: International Organization for Standardization (ISO), p. 72.

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

June, W., Jason, O. C., and Meiga, L.-N. 2010. "Information Technology Offshore Outsourcing Security Risks and Safeguards," *Journal of Information Privacy and Security* (6:3), pp. 29-46.

Kabiraj, T., and Sinha, U. B. 2016. "Strategic Outsourcing with Technology Transfer under Price Competition," *International Review of Economics & Finance* (44), pp. 281-290.

Kalisch, D. W. 2016. "Census 2016: Lessons Learned – Improving Cyber Security Culture and Practice," I.o.P.A. (ACT) (ed.). Australian Bureau of Statistics official website: Australian Bureau of Statistics.

Kulkarni, N., and Dwivedi, V. 2008. "The Role of Service Granularity in a Successful Soa Realization a Case Study," in: *2008 IEEE Congress on Services - Part I,* L.-J. Zhang and P. Hofmann (eds.). Honolulu, HI, USA: Institute of Electrical and Electronics Engineers (IEEE), pp. 423-430.

Lacity, M., Khan, S., and Willcocks, L. 2009. "A Review of the It Outsourcing Literature: Insights for Practice," *The Journal of Strategic Information Systems* (18:3), pp. 130-146.

Lacity, M., Khan, S., and Yan, A. 2016. "Review of the Empirical Business Services Sourcing Literature: An Update and Future Directions," *Journal of Information Technology* (31:3), pp. 269-328.

Lacity, M., Willcocks, L., and Khan, S. 2011. "Beyond Transaction Cost Economics: Towards an Endogenous Theory of Information Technology Outsourcing," *The Journal of Strategic Information Systems* (20:2), pp. 139-157.

Lacity, M., Yan, A., and Khan, S. 2017. "Review of 23 Years of Empirical Research on Information Technology Outsourcing Decisions and Outcomes," in: *Proceedings of the 50th Hawaii International Conference on System Sciences,* W.V. Grembergen (ed.). Hilton Waikoloa Village, 69-425 Waikoloa Beach Drive, Waikoloa, HI 96738: p. 11.

Larsen, M. M., Manning, S., and Pedersen, T. 2013. "Uncovering the Hidden Costs of Offshoring: The Interplay of Complexity, Organizational Design, and Experience," *Strategic Management Journal* (34:5), pp. 533-552.

Lee, C. K. M., Ching Yeung, Y., and Hong, Z. 2012. "An Integrated Framework for Outsourcing Risk Management," *Industrial Management & Data Systems* (112:4), pp. 541-558.

Liang, H., Wang, J.-J., Xue, Y., and Cui, X. 2016. "It Outsourcing Research from 1992 to 2013: A Literature Review Based on Main Path Analysis," *Information & Management* (53:2), pp. 227-251.

Martinez-Noya, A., Garcia-Canal, E., and Guillen, M. 2012. "International R&Amp;D Service Outsourcing by Technology-Intensive Firms: Whether and Where?," *Journal of international management* (18:1), pp. 18-37.

McIvor, R. 2009. "How the Transaction Cost and Resource-Based Theories of the Firm Inform Outsourcing Evaluation," *Journal of Operations Management* (27:1), pp. 45-63.

Merkel, R. 2016. "Census Website Fail: Abs Should Have Known Better," in: *ABC News Australia*. ABC News Australia website: ABC News Australia.

Moore, S. 2016. "Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016." Retrieved 11 June 2017, 2017, from http://www.gartner.com/newsroom/id/3404817

Nassimbeni, G., Sartor, M., and Dus, D. 2012. "Security Risks in Service Offshoring and Outsourcing," *Industrial Management & Data Systems* (112:3), pp. 405-440.

Patil, S., and Wongsurawat, W. 2015. "Information Technology (It) Outsourcing by Business Process Outsourcing/Information Technology Enabled Services (Bpo/Ites) Firms in India," *Journal of Enterprise Information Management* (28:1), pp. 60-76.

Pedersen, K. B., Svarre, K. R., Slepniov, D., and Lindgren, P. 2013. "Global Business Model–a Step into a Liquid Business Model," *Journal of Multi Business Model Innovation and Technology* (1:1), pp. 101-114.

Poppo, L., and Zenger, T. 2002. "Do Formal Contracts and Relational Governance Function as Substitutes or Complements?," *Strategic Management Journal* (23:8), pp. 707-725.

Premuroso, R. F., Skantz, T. R., and Bhattacharya, S. 2012. "Disclosure of Outsourcing in the Annual Report: Causes and Market Returns Effects," *International Journal of Accounting Information Systems* (13:4), pp. 382-402.

Professionals, I. A. o. O. 2014. "Outsourcing Professional Body of Knowledge – Opbok Version 10: The Standards," J. Chittenden (ed.). Zaltbommel, www.vanharen.net: Van Haren Publishing.

Quinn, J. B. 1992. *Intelligent Enterprise : A Knowledge and Service Based Paradigm for Industry*. New York : Toronto : New York: Free Press ; Maxwell Macmillan Canada ; Maxwell Macmillan International.

Ritchie, M. 2015. "Outsourcing's Booming Business." Retrieved 30 June 2017, 2017, from https://www.iso.org/news/2015/01/Ref1922.html

Sirkin, H., Hemerling, J., and Bhattacharya, A. 2008. *Globality: Competing with Everyone from Everywhere for Everything*. Business Plus.

Stoneburner, G., Goguen, A., and Feringa, A. 2012. *Risk Management Guide for Information Technology Systems*, (NIST Special Publication 800-30 ed.). NIST website: National Insitute of Standards and Technology (NIST).

Technology, N. I. o. S. a. 2012. "Guide for Conducting Risk Assessments." NIST website: National Institute of Standards and Technology (NIST), p. 05.

UK, G. S. A. 2016. "The Global Sourcing Standard." www.gsa-global.com: Global Sourcing Association UK (GSA-UK).

Whitman, M. E., and Mattord, H. J. 2016. *Principles of Information Security*, (5th ed.). Boston: Course Technology, Cengage Learning.

Willcocks, L., Cullen, S., and Craig, A. 2011. *The Outsourcing Enterprise from Cost Management to Collaborative Innovation*. London: Palgrave Macmillan UK : Imprint: Palgrave Macmillan.

Willcocks, L., and Lacity, M. 1998. *Strategic Sourcing of Information Systems : Perspectives and Practices*. Chichester, England ; New York: Wiley.

## COPYRIGHT