Information Security Requirement: The Relationship between Information Asset Integrity and Availability for ICT Outsourcing

Nik Zulkarnaen Khidzir

Infrastructure University Kuala Lumpur, Faculty of Information Technology Infrastructure, Kuala Lumpur, Malaysia
Email: nikz@iukl.edu.my

Azlinah Mohamed and Noor Habibah Arshad

Universiti Teknologi MARA, Faculty of Computer and Mathematical Sciences, Shah Alam, Malaysia
Email: azlinah@tmsk.uitm.edu.my, habibah@tmsk.uitm.edu.my

Abstract—**Information Communication Technology (ICT) Outsourcing provides effective ways to cut cost and improve efficiency in ICT services. Unfortunately, the outsourcing strategy still invites some critical risks especially information security risks. Fundamental concepts of information security requirements such as confidentiality, integrity and availability of information assets involved in the ICT outsourcing cycle need to be identified extensively to ensure these information assets are secure from information security risks. Therefore, the aim of this study is to determine the relationship between key information assets integrity and availability in the ICT outsourcing cycle. Questionnaires were distributed to 300 private companies from various industry and government agencies in Malaysia for the study. Results of the correlation coefficient (r) values > 0.7 verifies that a strong positive relationship exists between two information security requirements; integrity and availability of key information assets in every phase of ICT outsourcing. Findings reveal that the higher the integrity level, the higher the availability level of the key information assets, providing significant empirical evidence on the relationship between key information assets integrity and availability in the ICT outsourcing cycle. Subsequently, the integrity and availability of these key information assets could be better managed and controlled. Organizations can re-evaluate and improve their practices in managing information assets and urgently address information security risks to gain optimum benefits from their ICT outsourcing ventures.**

Index Terms—**Information Availability, Information Assets, Security Requirement, ICT Outsourcing, Information Integrity, Information Security**

I. INTRODUCTION

The ICT outsourcing strategy is widely associated with cutting costs, launching of new business ventures and improving efficiency.

However, the literature has emphasized the risks associated with ICT outsourcing project implementation, identifying information security risks as one of the critical risks in the process [1], [2]. Additionally, information as key assets has grown in importance, at par with its accelerating production, complexity, volume and demand, fulfilling the real information needs of the organization that has been restricted due to some obstacles [3] including information security risks. Thus, it is crucial to manage the confidentiality and availability of these information assets efficiently for failure to do so will cause much damage. To this end, the relationship among information assets security requirements were measured and analyzed. The empirical findings point to the significant relationship between information asset integrity and availability in ICT outsourcing projects amongst Malaysian private and government agencies. This suggests that organizations should carefully determine and evaluate their information asset security management practices in ICT outsourcing projects.

II. LITERATURE REVIEW

A. Literature Overview

This research article reviews several literatures and fundamental concepts of basic theories, earlier research findings in ICT outsourcing, information security risks, key information assets, and information security requirement principles.

B. ICT Outsourcing Implementation and Significant Risks

ICT outsourcing strategy involves transferring some or all of the ICT related decision making rights, business processes, internal activities and services to external providers who develop and administer these activities in accordance with the deliverables, performance standard and outputs, as agreed in a contractual agreement [4]. The literature has highlighted various ICT related projects commonly outsourced to external providers. Many organizations outsource their ISP services, web hosting, e-business solutions, ICT application maintenance and

support, software application services provision, application analysis, ICT infrastructure development, programming, support end-user, staff/user training courses, ICT security audit and security policy consulting or standards development [5], [6]. Despite the varying categories, the outsourcing processes or cycle remain almost similar. The generic conceptual phases of ICT outsourcing cycle as illustrated in fig. 1 are; the analysis of decision to outsource; selection of Service Providers; contract management and project on-going monitoring [7]. Organizations adopt the outsourcing strategy in their ICT projects as it plays a significant role in reducing ICT operational costs [8] and improving the efficiency of their ICT services whilst enabling them to focus on the core businesses. Unfortunately, outsourcing suffers from many potential risks [9] that must be recognized and managed [10] effectively. Recent studies reveal that information security risks are amongst the highest risks in ICT outsourcing [1], [2] that need to be addressed to ensure maximum benefit.
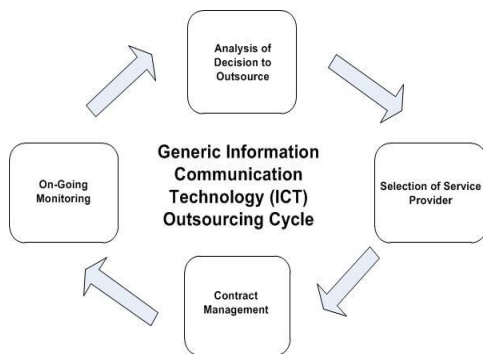

Figure 1. Generic ICT outsourcing phases implementation

C. Information Security Risk in ICT Outsourcing

TABLE I.   ICT OUTSOURCING PHASES AND INFORMATION SECURITY RISKS

ICT Outsourcing Lifecycle	Information Security Risks (ISRs)	Reference Literatures
Analysis of Decisions to Outsource	Information Leakage, Poor Information Security Study	[2],[11],[12]
Selection of Service Provider	Unauthorized Exploitation of Intellectual Property Right (IPR)	[2],[13],[14],[15]
Contract Management	Information Leakage	[2],[12]
On-Going Monitoring	Environmental Disaster, Information Leakage	[2],[16],[17],[18]

Failure of ICT outsourcing projects is commonly attributed to information security risks. In order to allow a detailed analysis of the problem, identification of the information security risk in every phase of the ICT outsourcing project is mandatory. Generic phases of ICT outsourcing include analysis decision to outsource, selection of service providers, contract management and on-going monitoring [7]. Prior literature has highlighted and analyzed some of the information security risks in ICT outsourcing phases. Table I show several literatures

on the information security risks related to the ICT outsourcing cycle.

D. Key Information Assets in ICT Outsourcing Cycle

Information asset is one of the asset groups in ICT projects associated with all information security domains [19]. It refers to a collection of facts in the form of paper or electronic messages, content, subject matter and substance form from which conclusions may be drawn for executing the missions and objectives of the organizations [19], [20]. The following fourteen information asset categories involved in the ICT outsourcing cycle were highlighted in a recent study: Business and Financial Records, Clients' Profiles, Business Continuity Plan, Archived Data/ Information, Policy & Procedure Documents, Financial Proposal Document, Technical Proposal Documents, Solution Requirement Specification, Business Requirement Architecture, Systems Documentation, Electronic Files and records, Training Material, Legal & Contract Documents and Databases & Data Files [21]. Table II illustrates the relevant key information assets for each phase of ICT outsourcing.

TABLE II.   KEY INFORMATION ASSETS AND ICT OUTSOURCING PHASES

Key Information Assets	Appearance			
	Analysis of Decisions to Outsource	Selection of Service Provider	Contract Management	On-Going Monitoring
Business & Financial Records	√	√		√
Client's Profiles	√	√		√
Business Continuity Plan	√	√	√	√
Archived Data/ Information	√			√
Policy & Procedures	√		√	√
Financial Proposal Doc.		√		
Technical Proposal Doc.		√		
Solution Requirement Specification		√		
Business Requirement Architecture		√		
System Documentation			√	√
Electronic Files & Records			√	
Training Material			√	√
Legal & Contract Documents			√	√
Databases & Data Files				√

E. Information Security Requirement Principles

Information security involves the activities, processes, controls and efforts that aim to protect information and data, and their underlying infrastructures. Confidentiality, integrity and availability are the core principles of information security [22], [23], [24] and broadly used in most study fields [21]. Confidentiality refers to the

limitations on the use and retention of different kinds of information [22], [23], [25], [26]. Integrity is the guarantee that information has not been manipulated [22], [23], [25], [26] while availability is ensuring that authorized users have access to information and associated assets when required [22], [23], [25], [26]. Information assets might be improperly disclosed due to its confidentiality being exposed, modified in an inappropriate way, if its integrity is jeopardized, and destroyed or lost because its availability is threatened [27]. However, the study emphasizes two information security requirement principles; integrity and availability of related key information assets in ICT outsourcing cycle. The results were measured and statistically analyzed to investigate the relationship between them.

III. RESEARCH METHODOLOGY

An empirical study was conducted to determine the confidentiality and availability of information assets among private and public agencies in Malaysia. Primary data was collected using questionnaires as the data collection tool for the study. The validity of the research data collection tool was established through feedback from ICT outsourcing project practitioners and information security professionals. The information assets in each phase of ICT outsourcing were determined from literatures. These were used to measure integrity and availability of key information assets mean scores among private and government agencies in Malaysia. In a previous study [21] reliability tests were conducted on (i) a set of 5 key information assets integrity and availability items involved during the analysis of decision to outsource phase, (ii) a set of 7 key information assets integrity and availability items during the selection of Service Providers phase, (iii) a set of 6 key information asset integrity and availability items during contract management and (iv) a set of 9 key information assets integrity and availability items during on-going monitoring. The results showed high alpha readings ($\alpha >$ 0.8) [21] for all item sets, indicating that the entire sets of measured items were excellent. Purposive sampling technique [28] was applied to collect primary data through electronic and postal mail to 300 potential respondents. About 110 respondents provided feedback for this survey. The 36% response rate was considered to be relatively normal [29] and acceptable to represent a sample population of the study. Analysis of primary data was supported by the application of appropriate statistical techniques.
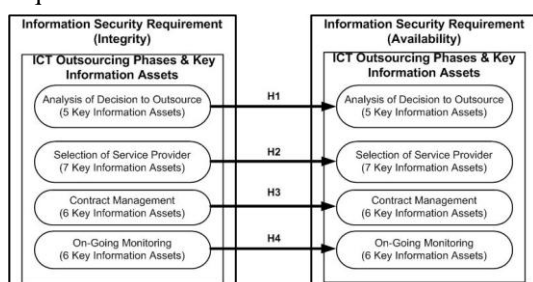

Figure 2.   Research Model for Relationship between Key Information Asset Integrity and Availability in each Phases of ICT Outsourcing

A research model (Fig. 2) was developed focusing on the integrity and availability of the related key information assets during phases of the ICT outsourcing cycle.

Based from research model in Fig. 2, four hypotheses have been developed to test the relationship between each set of key information asset security requirements, integrity and availability levels. The hypotheses are:

H1:   There is a positive relationship between information assets integrity and availability during the analysis of decision to outsource phase

H2:   There is a positive relationship between information assets integrity and availability during the selection of service provider phase

H3:   There is a positive relationship between information assets integrity and availability during the contract management phase

H4:   There is a positive relationship between information assets integrity and availability during the on-going monitoring phase

IV. RESULTS DISCUSSIONS AND FINDINGS

The results of the study captured the respondents' demographic profile and their opinions on the integrity and availability of key information asset in each phase of ICT outsourcing. The analyses lead to several significant discoveries and expansion of existing knowledge. This section discusses the findings of the study in detail.

A. Demographic Profile and ICT Outsourcing Project Characteristics

ICT project managers and senior information system officers from various industries and government agencies participated in this study. Only 18.2% respondents had working experience of less than 5 years. The other 81.8% respondents had more than 5 years' experience in ICT project. 15.5% of those had 11 to 15 years as well as 15 to 20 years' experience. The majority, 40.9%, had been working for 6 to 10 years. The majority of respondents are from government agencies (79.1%), 11.7% from government-linked companies (GLCs) and 9.1% from private companies. Nevertheless, the 79.1% government agencies respondents represented numerous businesses and industrial sectors. The ICT outsourcing projects' characteristic analysis revealed that 57.3% of the projects concerned Application System Development, ICT Infrastructure Maintenance (26.4.3%), IT/IS Strategic Planning Results (6.4%), ICT Security Maintenance (5.5%), ICT Knowledge Transfer & Training (2.7%) and ICT Application Maintenance at 1.8%. Results of the study revealed that Joint-Venture-Outsourcing (43.6%) was the most popular outsourcing strategy practiced in ICT project implementation among Malaysia organizations. Selective outsourcing approach accounted for 30.9% and Total outsourcing approach, 25.5%. For the majority (16.7%), the main reason for outsourcing ICT projects is the lack of internal resources and human expertise to implement the project. The study also found out that most of the organizations outsource their ICT projects to only one service provider (58.2%). Most of the

project durations were medium-term being between 1 to 3 years (62.7%), while short-term (less than 1 year) and long-term (more than 3 years) represented 18.2% and 19.1% respectively. Responses received from organizations were overwhelming with ICT outsourcing projects costing between RM 1 Million to RM 5 Million (23.6%).

B. Information Security Requirement Mean Score: Integrity and Availability of Information Assets

Information security requirement mean score for sets of key information assets in each ICT outsourcing phases were measured to determine its integrity and availability level.

As summarized in Table III, the information assets integrity (4.0691) level mean score was the highest during the analysis of decision to outsource phase. The high mean score of integrity signifies the respondents' extreme care about the integrity of the organization's key information assets at the early phase of ICT outsourcing cycle. The results proved that integrity of information asset during the analysis of decision to outsource phase is given greater priority compared to other phases in ICT outsourcing cycle. Therefore, organizations should strengthen their information security efforts to ensure integrity of the information assets when analyzing outsourcing decisions. Meanwhile, information asset availability (3.9212) level mean score was the highest during the contract management phase. The high mean score of availability explained the respondent required appropriate access to key information assets when required as input to manage ICT outsourcing contract wisely. This result establishes that the availability of the information assets during the contract management phase became top priority in the ICT outsourcing cycle.

TABLE III. MEAN SCORE KEY INFORMATION ASSET INTEGRITY AND AVAILABILITY IN ICT OUTSOURCING PHASES

Information Communication Technology Outsourcing Phases	N	Key Information Security Assets Security Requirement			
		Integrity		Availability	
		Mean	Std. Dev.	Mean	Std. Dev.
Analysis of Decisions to Outsource	110	4.0691	0.66495	3.9055	0.77895
Selection of Service Provider	110	3.9571	0.68622	3.8610	0.74557
Contract Management	110	3.9833	0.68251	3.9212	0.70484
On-Going Monitoring	110	3.9556	0.62424	3.8990	0.70394

N = No. of Respondents

Table III also depicted the lowest, integrity (3.9556) level during the project on-going monitoring phase. The evidence shows that information asset integrity levels decrease towards the end of the ICT outsourcing cycle. Meanwhile, the information asset availability (3.8610) level was the lowest during Selection of Service Provider compared to other phases. However, the organization should still maintain the availability of the information assets during this phase. The availability mean score also described the implication of information assets

availability to support decision making when selecting capable service providers for ICT outsourcing ventures. Without sufficient information, organizations are unable to make wise decisions and will probably expose the project to greater information security risks. Therefore, better decisions could be achieved with sufficient, relevant and accurate information assets in place during the selection of service providers.

C. Analysis of the Relationship between Integrity and Availability of Information Assets

The Bivariate Pearson Correlation test was then conducted on the formulated research hypotheses to determine the significant relationship, strength and direction of the integrity and availability of information asset for each ICT Outsourcing phase. The correlation coefficient values, (r) was derived to explain the relationship strength between them. A result of p-value < 0.01 is considered significant. A weak relationship is indicated by a (r) value of less than 0.4, values between 0.4 and 0.7 indicate moderate relationship and a strong relationship has a value higher than 0.7.

TABLE IV. HYPOTHESES TEST RESULTS FOR THE SIGNIFICANT RELATIONSHIPS BETWEEN INTEGRITY AND AVAILABILITY OF KEY INFORMATION ASSETS

Hyp.	Correlation Coefficient (r)	Sig. (*p-value*)	Decision	Results
H1	0.796	0.000*	Significant	Strong +ve Relationships
H2	0.813	0.000*	Significant	Strong +ve Relationships
H3	0.812	0.000*	Significant	Strong +ve Relationships
H4	0.802	0.000*	Significant	Strong +ve Relationships

*Correlation is Significant at the 0.01 levels (2-tailed)

As revealed in Table IV, the results of the hypotheses tests indicate positive correlations for the four hypotheses. H1, H2, H3 and H4 were accepted and the null was rejected based on significant *p-value* < 0.01. The correlation coefficient (r) values were 0.796 for H1, 0.813 for H2, 0.812 for H3 and 0.802 for H4. All the significant hypotheses described strong relationship strength between information assets integrity and availability in all ICT outsourcing phases. The strongest relationship level was during Selection of Service Providers. Thus, there is a high probability that increased information assets availability will also increases its integrity level for the Selection of Service Provider phase. Meanwhile, the weakest relationship between integrity and availability was during the analysis of decision to outsource phase.

V. CONCLUSION

This study empirically establishes the significant relationship between integrity and availability of Information Assets during the ICT outsourcing cycle for private and public agencies in Malaysia. The study proposes that integrity of information assets during the Selection of Service Provider phase is given greater

priority above all other phases of ICT outsourcing. At the same time, information asset availability level was the highest during the contract management phase. The evidence highlights the top priority placed on the availability of information assets during the contract management phase in the ICT outsourcing cycle. It was also recognized that the integrity level could influence the availability level during the implementation of ICT outsourcing projects. Therefore, the higher the integrity level, the higher the availability level of the information assets. Integrity and availability were positively and strongly correlated in all phases of the generic ICT outsourcing cycle. Understanding the relationship pattern between these two information asset security requirements will enable ICT professionals, information security experts and outsourcing practitioners to prioritize information security issues effectively. Furthermore, ICT outsourcing involves careful planning and without a cogent strategy to deal with information security risks, ICT outsourcing projects may run the risk of failure.

REFERENCES

[1] D. Davison. (December 2003). Top 10 Risks of Offshore Outsourcing. [Online]. Available: http://techupdate.zdnet.com

[2] G. Hinson. (December 2007). Top Information Security Risk for 2008: Information Security Risk, CISSP Forum. [Online]. pp. 5. Available:http://www.naavi.org/cl_editorial_08/Top_information_ security_risks_for_2008.pdf

[3] J. Ward and J. Peppard, "Information as an Asset: The Senior Management Agenda," in *Strategic Planning for Information System*, 3rd ed., John Wiley & Sons, 2004, pp. 467

[4] S. Dhar and B. Balakrishnan, "Risk, benefits and challenges in global IT outsourcing perspective and practices," *Journal of Global Information Management*, vol. 14, no. 3, pp. 39-69, 2006.

[5] NISER, Information Security Management System (ISMS) Survey, 2003.

[6] N. H. Arshad, Y. May-Lin, A. Mohamed, and S. Affandi, "Inherent risks in ICT outsourcing project," in *Proc. 8th WSEAS Conference*, 2007, vol. 8, pp. 141 – 146.

[7] S. R. H. S. Aris, N. H. Arshad, and A. Mohamed. "Conceptual Framework of Risk Management in IT Outsourcing Project", *WSEAS Transactions on Information Science & Applications*, vol. 4, no. 5, pp. 816-831, 2008.

[8] Investopedia Dictionary. (January 2013). Definition of Outsourcing. [Online]. Available: http://www.investopedia.com

[9] N. Z. Khidzir, A. Mohamed, and N. H. Arshad, "Information security risk factors: Critical threats and vulnerabilities in ICT outsourcing," in *Proc. International Conference on Information Retrieval and Knowledge Management*, March 2010, pp. 193 – 198.

[10] P. O'Keeffe and S. Vanlandingham, "Managing the risks of outsourcing: A Survey of Current Practices and their Effectiveness," Protiviti Inc., 2004.

[11] M. Merkow and J. Breithaupt, "Securing Information Assets," in *Information Security Principles and Practices*, Prentice Hall, 2005, pp. 27.

[12] S. Garfinkel, "All your data belongs to Us: Data servicing in another problem for data privacy," *Technology Review*, 2007.

[13] M. Ju, S. Kim and T. H. Kim, "A study on digital media security by Hopfield neural network," *Lecture Note in Computer Science: Advances in Neural Networks*. 2007, vol. 4493, pp. 140-146.

[14] T. Sota, "Plagiarism in the age of electronic publishing," *Population Ecology*, vol. 46, no. 3, pp. 219, 2004

[15] B. Vassiliadis, V. Fotopoulos, A. Ilias, and A. N. Skedras, "Protecting intellectual property right and the JPEG2000 coding standards," *Advanced in Informatics*, 2005, vol. 3746, pp. 705-715.

[16] S. Halliday, S. Badenhorts, and V. Solms, "A business approach to effective information technology risk analysis and management," *Information Management and Computer Security*, vol. 4, no. 1, pp. 19-31, 1996.

[17] J. Bitha and R. V. Solm, "A Cycle Approach to Business Continuity Planning," *Information Management and Computer Security*, vol. 4, no. 4, pp. 328, 2000.

[18] S. M. Hawkins, D. C. Yen and D. C. Chou, "Disaster Recovery Planning: A Strategy for Data Security," *Information Management and Computer Security*, vol. 8, no. 5, pp. 222, 2000.

[19] *The Malaysian Public Sector Information Security High-Level Risk Assessment (HiLRA) Guide*, MAMPU, Perpustakaan Negara Malaysia, 2005.

[20] *The Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM)*, MAMPU, Perpustakaan Negara Malaysia, 2005.

[21] N. Z. Khidzir, A. Mohamed, and N. H. Arshad, "Critical information asset security requirements in ICT outsourcing", in *Proc. International IT and Society Conference*, 2010, vol. 1, no. 1, pp. 88-95.

[22] A. Vorster and L. Labuschagne, "A framework comparing different information security risk analysis methodology," in *Proc. South African Institute of Computer Scientist and Information Technologist on IT Research in Developing Countries*, 2005, pp. 95–103.

[23] D. B. Parker, *Toward a New Framework for Information Security, Computer Security Handbook, 4th ed.,* edited by Seymour Bosworth and M. E. Kabey. New York: John Wiley & Sons, 2002.

[24] Wikipedia, The Free Encyclopedia. (January 2010). Information Security: Basic Principles, Key Concepts. [Online]. Available: www.wikipedia.org

[25] Code of Practice for Information Security Management, ISO17799:2005, ISO Standard – 2005

[26] V. A. Canal, "The global voice of information security: On information security paradigms," *The ISSA Journal*, September 2005.

[27] B. Blakley, E. McDermott, and D. Geer, *Information Security is Information Risk Management*, 2001.

[28] Uma S. Sekaran, *Research Method for Business – A Skill Building Approach*. John Wiley & Sons, 2000.

[29] R. L. Scheaffer, W. Mendenhall III, A. L. Ott and K. G. Gerow, *Elementary Survey Sampling. 7th Edition*. Brook/ Cole Publishing Company, 2011.

Nik Zulkarnaen Hj Khidzir, a PhD candidate at Universiti Teknologi MARA, has been involved in ICT industry for the past 12 years. He graduated in Computer Science from Universiti Putra Malaysia in 2001. He obtained his Master's degree (MSc. IT) from Universiti Teknologi MARA in 2006. His areas of interest are Software Engineering, Information Security Risk Management and Business Computing/IT. Within 3 years as an academic, he has written several articles for publication in indexed proceedings (e.g. IEEE, ISI, Scopus, etc) and journals, is a regular presenter at national and international conferences and seminars. He is a Member of the International Association of Computer Science and Information Technology (IACSIT) and Information Retrieval and Knowledge Management Society (PECAMP). He was also the former President of Universiti Teknologi MARA (UiTM) Postgraduate Society (2010 – 2011).Currently, Nik Zulkarnaen is a lecturer at Infrastructure University Kuala Lumpur.

Datin Dr. Noor Habibah Hj. Arshad, an Associate Professor at the Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA has been teaching for the past 26 years. Her areas of interest are IT project management, risk management and IT Governance. She has co-authored several books, written numerous academic articles, and is a regular presenter at national and international conferences. She is also a reviewer for WSEAS Conference Proceedings and Journal since 2007. In the international arena, she was a member of the Technical Committee of Asia-Pacific Committee on e-Customer Relationship Management (APSeC). She has received several academic awards and research recognition nationally and internationally. She is also active in consultancy work with the Ministry of National Resources and Environment and Hicom Communication Sdn Bhd.

Azlinah Hj. Mohamed, a Professor at the Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA has been teaching for the past 23 years. She is the current Dean of the Faculty of Computer and Mathematical Sciences. Her areas of interest are Artificial Intelligence (AI) and Knowledge Management (KM) and System Engineering. She has also co-authored several books, written numerous academic articles, and is a regular presenter at national and international conferences. Her research work has received recognition in local and international level competitions. She is a member of several national and international professional associations and authorities (e.g Malaysia Information Technology Society (MITS) and World Scientific and Engineering Academy and Society (WSEAS)).