A study on the lock-in risk in IT outsourcing projects: the mechanism and the control system

Cong Guodong*

School of Business Administration, Zhejiang Gongshang University, Xuezheng Str.18, Hangzhou, P.R.China

Received 1 March 2014, www.tsi.lv

Abstract

This paper, proposes an insight into the mechanism of lock-in risk, which is the primary risk and the greatest concern in managing IT outsourcing projects. Based on Transaction Cost Theory (TCT), it develops an integrated three-layer model to instruct the mechanism of lock-in risk, namely, what will lead to lock-in risk (risk drivers), and what lock-in risk will result in (risk consequences). Four risk drivers such as asset specificity and three risk consequences such as cost escalation are identified and discussed in detail. Meanwhile, it instructs why four kinds of control could mitigate lock-in risk both from the sources and the consequences. Therefore, the effectiveness and reliability is enhanced throughout the risk management process of IT outsourcing projects, particularly for dynamic risk identification, controlling and monitoring.

Keywords: (project management, lock-in risk, IT outsourcing, risk management)

1 Introduction

With the rapid development of IT outsourcing projects, the accompanied high-risk is also highlighted. Since there exist broadly the information asymmetry throughout the outsourcing process, clients are inevitably faced with lock-in risk, even large companies have to suffer excessive dependence on vendors while outsourcing information system projects [1]. Lock-in is such a state that, without bearing the loss or sacrificing some or sometime even all of the assets to the vendor, the client can not get out of the relationship [2]. Lock-in state will result in such hazard as the technical capacity declining, or losing bargaining power, and cost escalation [3]. Therefore, lots of academic research has paid attention to lock-in risk with different perspective, such as Transaction Cost Theory (TCT) [4] and relationship governance, either focuses on service provider behaviour [5] or from the perspective of service buyer in large multinational companies [6]. The research either provides a framework or approach to assess lock-in risk.

However, little in-depth and specific analysis is proposed on the mechanism of lock-in risk, which leads to negative impact the effect of mitigation system. Especially in IT outsourcing projects, just some of the risk factors related to IT outsourcing projects are identified, let alone the factors are attained in certain countries within limited cultural contest [7]. This paper, addressing the issue, illustrates the mechanism of lock-in risk based on TCT. Namely, it constructs an integrated three layer model to demonstrate the transmission mechanism from four risk drivers (the set of risk factors) to the risk, and then from the risk to the three risk consequences. Meanwhile, it proposes a clear instruction on why and how four kinds of control will carry out on the four risk drivers and three risk consequences, which improves the applicability and reliability of the analysis on the lock-in risk.

2 The mechanism of the lock-in risk

Hereinafter the mechanism of the lock-in risk will be demonstrated as a three-layer model, which is consisted of the transmission mechanism from four risk drivers (the set of risk factors) to the risk, and then from the risk to the three risk consequences.

2.1 THE MECHANISM BETWEEN RISK DRIVERS AND LOCK-IN RISK

The risk drivers are the reasons leading to lock-in risk. The definition, characteristics and function on lock-in risk are illustrated as below.

2.1.1 Small number of vendors

As IT outsourcing projects are closely integrated with organization management at all management levels, it is easier to form path dependence within IT outsourcing process. If clients choose only a small number of or even a single outsourcing service provider, they will trap themselves in lock-in risk.

The obvious situation is if their choice is limited, they will be under disadvantage in contract negotiation and

* Corresponding author - Tel: +86-15934214332; fax: +86-0571-28004233;
E-mail: cgd@zjgsu.edu.cn

changing vendors [8]. Worse still, vendors are likely to adopt more opportunistic behaviour, e.g. to take the opportunity to bargain during the entire contract period or at updating occasion, as vendors are more aware of the true cost than other tenders.

Without exploiting multiple vendors to promote competition among vendors, there will be no convenience to evaluate a single vendor [2]. The other hazard is, without common vision and values, which will encourage both sides more commitment to partnership development, vendors will prohibit themselves to perform their duties with correct attitude throughout the outsourcing process.

Moreover, it is more difficult to execute control without adequate competition during the outsourcing process, especially because of the enhancement of vendors' advantageous position. Finally, clients have to be more aware of the importance to summarize experience and lessons, which will improve the capability to discover and correct potential opportunistic behaviour.

2.1.2 Asset specificity

Asset specificity, which concerns investments made specifically on physical or human resource because of a given contract. The asset is utilized in particular relationship, and need transfer cost if the utilization is changed. Additionally, the value of the relationship-specific investments would fall if the relationship dissolves [9]. The asset specificity IT outsourcing project vendor invest includes information system team members training and equipment, reallocation of human resources and improvement of information system development environment. Among the specific assets, vendor investment and human resource attribute more to the outsourcing risk than other asset [10].

To some extent, asset specificity enhances clients' concern on the loss or the sacrifice the asset invested in the relationship, accordingly results in lock-in risks. Especially, switching vendor costs have a greater impact on the lock-in problem. Having invested a great deal of time and effort in getting the initial vendor fully operational, the client itself may be reluctant to do so with a new vendor. Since some clients do not retain in-house competencies with the outsourced activity, they may even be unable to do so [8].

For experienced vendors, they are good at turning the specific investment asset into bargaining weapon with clients while updating contract. The reason is that, the specific investment asset becomes the entry barriers for other vendors, which means the other side in the outsourcing relationship has to invest at least the same amount to get the opportunity.

On the other hand, without any objective compatibility on the organization layer, both vendors and clients would not put more effort into long-term relationship. More importantly, they will not make use of the specific asset and reduce opportunistic behaviour. In other words, they will not enhance the bilateral condition in the relationship and improve asset value, which will keep both sides in win-win situation. It is not the perspective that both clients and vendors are willing to see, even for the "worst" vendor that is fond of opportunistic behaviour, so both sides in the outsourcing relationship should strive for it.

2.1.3 Relatedness

Relatedness, also known as mutual dependence or connectivity, refers to mutual connection between tasks, business and functions [10]. The relatedness in IT outsourcing projects can be classified into two categories [11]: the relatedness between the business outsourced and stayed in-house, and that between the different kinds of business outsourced. In practice, two layers of relatedness should be distinguished, namely, the technical layer, which mainly focuses on the close connection among many kinds of technology adopted; the other is the management layer, which means the connection with internal management directly or indirectly, including the relatedness among the teamwork.

As proposed, risk factor 'Relatedness' has the lowest priority [7], it is effective "in Iranian organizations" though. The relatedness with the operation and the business enhances the reliance of clients on vendors. After an operation or a business is outsourced, if another operation and business closely related to the outsourced one, the original vendor owns a clear advantage over competitors, because it understands better than clients about the client's business, processes, style and even culture. Vendors may also take advantage of information asymmetry, or exaggerate the impact of the relatedness, so that clients have to rely on vendors' support not only in dealing with normal business, but also in the decision-making and management transformation.

Unless contract provides a benchmark for the boundary and responsibility of business units, the content for defining responsibility and compensation while service failure or loss occurs, therefore, the potential hazard of the relatedness will be out of control and the benefit of both sides will not be protected.

The most complicated problem of the relatedness is the controversial part of so-called 'extra work' or 'fuzzy work'. Unless there is a system to facilitate the climate of responsibility for vendors, so that they are willing to meet the requirement from client even if the requirement is beyond the contract strictly scope. Only in a high degree of trust, they would prefer resolving problems within reasonable scope to bargaining, since they are confident of better return in the long-term cooperation.

2.1.4 Client's expertise in IT operations

The term expertise is defined as special skill and knowledge from training, learning and practice [10], including abstract information, knowledge accumulation and skill in people's memory. In the IT outsourcing

project context, the definition is adopted that, expertise is the capability to combine external information and internal process to create particular ability. Risk factor "vendor's lack of expertise with an IT operation" has been identified as the best risk factor [7], just as the author mentioned, that is "experts' opinions in Iranian organizations". From the perspective of clients, no other expertise is more important than that of their own, since that is the best equipment to protect their own benefit in the long process of IT outsourcing project.

Lack of expertise will lead to two kinds of hazard. The first one is that organization learning affects greatly on lock-in risk. The reason is, vendors occupy a comparative advantage about information, knowledge and skills in relative area, which forces clients to accumulate adequate technical expertise and knowledge. Otherwise, path dependence will push clients on the downstream of declining ability on information acquisition, data processing, independently identifying and solving problems, and even no intellectual property to govern vendors' modifications in event of termination.

The other hazard is, even if vendors decline the service satisfaction for clients, clients will find it difficult to find out the truth for their unawareness of the expectation and need of users. Therefore, they lock themselves in the relationship without any opportunity to terminate the contract while vendors are under performance requirement, which demonstrates their vivid example of lock-in.

Without firm assurance between both sides, such as relational governance, it will be difficult to promote a beneficial atmosphere for strengthening organizational learning and cross- organizational knowledge transferring. Both client and vendors could not benefit from the trust between them: for clients, the efficiency of mastering the latest technology will not be improved, and the way to collaborate technology and business will not be found, which means the capacity of managing IT assets will not be enhanced; for vendors, better understanding on client industry and businesses will not be attained, and the vision of business will not be expanded. In other words, they are far from win-win. Undoubtedly, both sides are reluctant to lock themselves in such situation.

2.2 THE MECHANISM BETWEEN LOCK-IN RISK AND RISK CONSEQUENCES

Clients are aware of their dilemma of lock-in, and they are trying to alleviate the "painfulness", such as form a well working relation with its ITO vendor for handling emergent issues, daily operation and events that have not been foreseen [6]. However, clients have to deal with three risk consequences as shown below:

2.2.1 Cost escalation

The first and the greatest, in most occasions, is the cost escalation. As long as clients are locked in, they will be incapable of monitoring the scope and content of the service provided by vendors. Additionally, since they know less and less about the latest development of technologies related to the outsourced business, they will also lose the right to speak on what kind of technology could match and implement the business outsourced.

Therefore, vendors might attain great advantage of opportunistic behaviour. E.g. they may persuade clients into adopting extraordinary hardware, upgrading or developing more software. Even if the worst situation is not happening, namely, clients are confused and manipulated to pay for 'useless' service, the service cost will increase significantly.

2.2.2. The debasement of service quality

The second obvious risk consequence is the debasement of service quality. The reason is also mainly that, service providers' behaviour is often on the edge of "opportunistic" [5]. Specifically, it is the vendors, rather than clients, that establish the evaluation criteria about service quality. Even clients are aware of problems or speak out of complaints, vendors are good at finding sufficient excuses to prove that they meet or even exceed the quality requirements of the contract, and then blame clients' complaints to additional requirements, then seek to increase service charges for amending the contract.

2.2.3 The descending of client's value

Another risk consequence need to be treated seriously is the descending of client's enterprise value, including internal and external value. The internal value descending refers to the deterioration of competitiveness and the staff identification to the enterprise; the external value descending refers to the value impact outside of the enterprise, such as market value. If the enterprise is a listed company, the value will be directly reflected by stock price and market capitalization.

An open market is agile to the announcement of IT outsourcing projects. As proposed, the offshore outsourcing has a positive impact on the enterprise value, namely, capital market approves the value of outsourcing deals that contain high asset specificity, because the market believes that the research and development to match customer characteristics and other targeted contracts will help the company gain a strategic advantage or innovation assets [12].

The reaction of open market, as mentioned above, is definitely the "positive" part of the story. However, the clients in lock-in risk will be reluctant to find themselves blocked in the opposite situation, or even tragedy. As long as the investors sense their "painfulness", what kind of choice they will make is not hard to imagine.

3 The control system on lock-in risk: why and how

The control system is to incentive individuals to work for fulfilling the organization's target [13]. It is suggested that, two formal control, behaviour control and output control, and two informal control, self-control and clan control [14] are available for a client. Therefore, clients are capable of making use of various control measures as a control portfolio accordingly, with the success of outsourcing project in mind.

3.1 THE CONTROL SYSTEM ON RISK DRIVERS

Hereinafter it will be demonstrated in detail why and how the control system affects on the risk drivers to alleviate the lock-in risk.

3.1.1. Small number of vendors

It is more difficult to implement control without adequate competition during the outsourcing process, especially because of the enhancement of vendors' advantageous position. Under such circumstance, informal control is preferred since it is easier to promote full participation of both sides.

Informal control will never be treated as a complementary system in the IT outsourcing projects. E.g., clan control is helpful to establish common vision and values, which will encourage both sides more commitment to partnership development. Particularly, trust between two sides will facilitate vendors to perform their duties with correct attitude throughout the outsourcing process.

Formal control is the assurance of informal control. E.g., contract could also become a useful control tool. In a detailed contract, e.g. SLA (Service Level Agreement), contingency plan, clause changing management, coordinating system and so on should be taken into consideration; flexible payment, terms of stage performance evaluation should also be integrated into contract, which ensures the incentive function of contract, both positively and negatively. Particularly, SLA can improve mutual trust. The advice is both sides should pay attention to change management, since changes pose negative impact on the output of mutual trust and commitment.

Additionally, clients should be more aware of the importance to summarize experience and lessons, which will improve the capability to discover and correct potential opportunistic behaviour.

3.1.2 Asset specificity

Control system can constrain vendor behaviour from both team and individual level. Particularly, output control, can be combined with the input-output ratio of assets to incentive vendors; clan system, with its cultural advantage, will aid vendors maintain the devotion and even passion on client service and satisfaction.

Moreover, cost monitoring could be utilized as the way to control exclusive use of assets and resolve problems in the process, which is the best way to protect the asset. The first step of cost monitoring is to preset the milestone, and the second one is to measure mathematically the important and the relative business cost, and then defines a reasonable fluctuation range of cost [15].

3.1.3 Relatedness

The purpose of control system is to identify problems and reduce negative effects derived from the relatedness. With the complexity of the relatedness taken into account, it is reasonable to make use of multiple means of control. E.g. the implementation of output control will improve vendors' performance in the outsourcing business and related business, in other word, to ensure them to "do the right thing"; behaviour control, on the other hand, is to promote vendors to comply with the contract honestly and strictly, namely, ensure them to " do the thing right"; moreover, informal control, is to encourage vendors to provide satisfactory service, which can also be labelled as "do the thing with right attitude."

As a complementary control tool, contract provides a benchmark not only for the boundary and responsibility of business units, but also the content for defining responsibility and compensation while bifurcation or loss occurs, therefore, the potential hazard of the relatedness is under control and the benefit of both sides is protected.

Moreover, cost control will regulate a reasonable fluctuation range of cost, detect and properly handle unexpected cost caused by the relatedness to keep the total cost under control. Another option is the application of management mode different with in-sourced business, that is, to allow vendors to be more proactive and creative to solve problems rather than entangle in unnecessary details.

3.1.4 Client's expertise in IT operations

The most important role of control system to contribute for the client's expertise in IT operations is the potential to encourage organizational learning and cross-organizational knowledge transferring. Both client and vendors benefit from the beneficial atmosphere between them: for clients, the willingness and the efficiency of following the latest technology is improved, and the way to collaborate technology and business is found, which means the capacity of managing IT assets is enhanced; for vendors, better understanding on client industry and businesses is attained, and the vision of business is expanded.

Informal control will contribute for the degree of expertise in IT operations, that is, establish the consistency of the interests for both sides, which reduces

the barrier of knowledge transferring. Under the framework of informal control, both sides are willing to employ flexible approaches such as cross-organization teams, virtual organizations to enhance the intellectual capital investment, and organizational learning, which eventually promote the orderly transformation from individual knowledge into organizational capacity.

Formal control could also utilize the standardization, namely, both sides adopt the same standard technical and professional language, which strengthens the understanding and communication, and continuously improves learning efficiency and knowledge quality. In this way, the degree of expertise in IT operations will be upgraded constantly for both client and vendors.

3.2 THE CONTROL SYSTEM ON RISK CONSEQUENCES

Hereinafter it will be demonstrated in detail why and how the control system affects on the risk consequences to prevent the lock-in risk.

If the risk is characterized by "potential" and "possible" hazards, risk consequence will be the "fact" of damage that has really happened and demonstrated. Hence, after the risk consequences occurred, if the source of the consequences could be traced and control measures could be carried out, the problems and the risks will be solved fundamentally. However, the other way should never be ignored, that is the direct control executed on the consequences themselves. The reason is, doing so is "the pill right to cure symptom" to the case, which is easy for both sides to understand and support.

3.2.1 The principle to control risk consequences

As for lock-in risk , the principle to control is: once one of the three risk consequences appeared, the first thing to do is to track the four risk drivers based on risk mechanism discussed above, then analyse the role of each risk drivers, and take the appropriate measures; secondly, apply control system on risk the consequences. Only in a parallel way, the objectives of lock-in risk management could be achieved effectively.

There exist lots of risks that lead to three risk consequences, and then will it be "unfair" to just blame lock-in risk? The answer is: as the biggest risk, it is always "safe" to probe into the issue from lock-in risk, and fortunately great harvest will seldom disappoint those staring at it.

In addition, the risk consequences caused by the lock-in risk also possesses distinctive features: the speed of problem deterioration is "stunning", while clients are able to do nothing, or are left no other choice but allow vendors creating various excuses. These features are all due to the special status of lock-in risk itself, without any exception. E. g., cost escalation becomes a black hole, users keep complaining about service quality to nowhere, employee loyalty has fallen sharply, and many negative comments spread on the internet, and so on.

Throughout the management process of lock-in risk, Iceberg Theory must be kept in mind: Behind every big problem, there will be at least thirty small hidden problems. Therefore, the control of lock-in risk should be executed from both the sources and the consequences, so that the best control results could be satisfied.

3.2.2 The measures to control risk consequences

Once any of the indications mentioned above emerges, the signal of risk consequences is alerting that control measures must be taken. Above all, clients will learn to take advantage of utilizing the control portfolio, namely, adopt one or some of the four controls according to the situation.

The implementation of output control will improve vendors' performance in monitoring cost; behaviour control, on the other hand, is to promote them to keep an eye on the cost honestly and strictly; informal control, is to encourage them to provide extra effort to work out more effective ways to help clients prevent the cost out of control.

Take the control of cost escalation as an example. Clients could make out the benchmark of the service output and behaviour, namely, establish the regulation for a reasonable fluctuation range of cost, and then monitor the abnormal change in order not to fall into the trap of unexpected cost.

It is more challenging and promising to utilize informal control, yet there are several options by the best exercises and samples from the leading companies. E.g., one option is to apply a different management style in the outsourced business in order to allow vendors to be more proactive and creative to solve problems rather than entangle in unnecessary details. Another option is for CIO, namely, play a new role as "CIO leader" that emphasizes on strategic business issues of both sides and coordinate IT with business. In this way, IT outsourcing projects will be more powerful support for the emprise strategy, and will create more value for both sides than before.

In order to disclose the mechanism and the control system of the lock-in risk in IT outsourcing, this paper proposes an integrated three-layer model as shown in Figure 1.

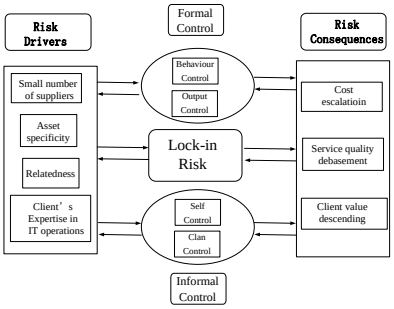

FIGURE 1 The three-layer model of lock-in risk

4 Summarization

This paper, intends to provide an insight into the mechanism of lock-in risk, which is the primary risk and the greatest concern in managing IT outsourcing project risk. Based on Transaction Cost Theory, it instructs s the mechanism of lock-in risk with a three-layer model. Moreover, it proposes a clear instruction on why and how four kinds of control will carry out on the four risk drivers and three risk consequences, which improves the applicability and reliability of the analysis on the lock-in risk.

With the effort, the lock-in risk could be diagnosed and controlled systematically. In other words, the risk could be prevented beforehand, and also be tracked as long as risk consequences emerge. The paper contributes for both academic and practice as a helpful tool throughout the whole risk management process, especially for risk identification, evaluation and monitoring.

Future research will focus on the empirical method in order to further illustrate the contribution of each factor within the three-layer model of the lock-in risk, and further analyses the mutual relationship between certain factors. In addition, it will also study the effectiveness of mitigation system, namely, how the mitigation system work on the risk drivers rather than lock-in risk itself. Therefore, a complete management framework will be established both for academic and for practice.

Acknowledgments

This research is supported by Humanity and Sociology Foundation of Ministry of Education of China (Grant No. 10YJC630034), Zhejiang Provincial Natural Science Foundation of China (No. Y6110539).

References

[1] Gonzalez R, Gasco J, Lopis J 2005 *Industrial Management and Data Systems* **105**(1) 45-62
[2] Aubert B A, Rivard S, Patry M 2004 *Information and Management* **41** 921-32.
[3] Bahli B, Rivard S 2013 *Decision Support Systems* **56** 37-47
[4] Alaghehband F K, Rivard S, Wu S, Goyette S 2011 *The Journal of Strategic Information Systems* **20**(2) 125-38
[5] Mathew S K 2011 *Strategic Outsourcing: An International Journal* **4**(2) 179-200.
[6] Hodosi G, Rusu L, Choo S 2012 *International Journal of Social and Organizational Dynamics in IT* **2**(3) 29-47
[7] Keramati A, Samadi H, Nazari-Shirkouhi S 2013 *International Journal of Business Information Systems* **12**(2) 210-42
[8] Aubert B A, Patry M, Rivard S. *Wirtschafts informatik* 2003 **45**(2) 181-90
[9] Williamson O E 1985 *The Economic Institutions of Capitalism* The Free Press: New York chapter1
[10] Bahli B, Rivard S 2005 *Omega* **33** 175-87
[11] Earl M J 1996 *Sloan management review* **3** 26-32
[12] Florin J, Bradford M, Pagach D 2005 *The Journal of High Technology Management Research* **16**(2) 241-53
[13] Kirsch L J, Sambamurthy V, Dong-Gil K, Russell L P 2002 *Management Science* **48**(4) 484-98
[14] Ouchi W G 1980 *Administrative Science Quarterly* **25**(1) 129-41
[15] Osei-Bryson K M, Ngwenyama O K 2006 *European Journal of Operational Research* **174** 245-64

Authors

Guodong Cong, born in August, 22, 1972, Weihai, P.R.China

Current position, grades: lecturer and researcher
University studies: Zhejiang Gongshang University
Scientific interest: project management, IT outsourcing risk management
Publications: 9
Experience: Dr. Guodong Cong got his Ph.D. degree in Management from Huazhong University of Science and Technology, P.R. China. Before his Ph.D., he worked in a foreign trading company as a project manager, served for over ten IT projects as team leader and project manager. He also provided consulting and training service for over twenty famous companies on IT outsourcing projects. His email is cgd@zjgsu.edu.cn.