Secrets of a successful outsourcing contract: a risk analysis

Ojelanki Ngwenyama
Ryerson Polytechnic University, ojelanki@ryerson.ca

W. Sullivan
wesullivan@yahoo.com

Follow this and additional works at: http://aisel.aisnet.org/ecis2006

Recommended Citation
http://aisel.aisnet.org/ecis2006/64
Secrets of a Successful Outsourcing Contract: A Risk Analysis

Ojelanki K. Ngwenyama, School of Information Technology Management, Ryerson University, Toronto, Ontario, Canada, M5B 2K3, Phone: (416) 979-5000 Ext. 4203, e-mail: Ojelanki@ryerson.ca
William E. Sullivan, IT University of Gothenburg, Forskningsgången 6, Building Patricia, Lindholmen, 417 56 Göteborg, Phone: + 46 31 772-6037, e-mail: wesullivan@yahoo.com

Abstract

Outsourcing information systems on a large scale is a difficult challenge. The public sector has seen some spectacular information systems (IS) outsourcing failures. Public officials have come under fire for sloppy management of IS outsourcing engagements and legislators are demanding higher standards of outsourcing practice and more accountability from public sector managers. This paper analyzes a large outsourcing contract for software maintenance services in Alberta, Canada from a risk perspective. This contract offers insights into how one public organization approaches the risks inherent in the practice of IS outsourcing. We use a risk framework and content analysis to identify which risk management strategies are included in the contract and how they are implemented. Although IS outsourcing risk factors are widely acknowledged in the literature, they may not be fully specified in the outsourcing contracts implemented in some public organizations. Our findings highlight some of the differences in the suggestions made in the academic literature on IS outsourcing and the techniques implemented in an actual outsourcing contract to manage the risks inherent in this growing sector of the international economy. We also find that not all risks need to be addressed in the contract to have a successful outsourcing relationship.

Keywords: Outsourcing, Public Sector IT Management, Information Systems Management, Risk Management, Contracts.
1 INTRODUCTION

Recent failures of information systems (IS) outsourcing contracts in the public sector have brought the risks associated with outsourcing into focus. Service problems and cost over-runs have plagued jurisdictions such as the State of Connecticut (LeSueur 1999), the County of San Diego, California (Field 2002), and the British Ministry of Defense (Arnott 2003). These and other well-publicized failures have fueled the public perception of sloppy management practices in public organizations. Political fallout is influencing public officials to take corrective action. However, Gartner Group predicts that 75 percent of enterprises will fail to recognize and mitigate the risks associated with outsourcing (Murphy 2003). While there is a growing body of research on IS outsourcing risks (Lacity and Hirschheim 1993a; Lacity, Hirschheim et al. 1995; Lacity, Willcocks et al. 1995; Earl 1996; Aubert, Patry et al. 1998; Aubert, Dussault et al. 1999; Bryson and Ngwenyama 2000; Gay and Essinger 2000; Sullivan and Ngwenyama 2005), there is relatively little empirical research into how these risks are addressed in contracts.

In this paper we take a successful outsourcing contract and examine the risk factors identified and the mitigation strategies that are implemented. We define a successful outsourcing contract as one that has been in place for at most 2 years and is expected to be renewed at the end of its current term. Our reason for investigating IS outsourcing contracts is that they play a central role in the structure and management of any outsourcing arrangement. Lacity and Hirschheim (1993a) note that every manager they interviewed stated that the contract was the most important element of a successful outsourcing relationship because it is “the only mechanism to establish the balance of power between the parties” (Lacity and Hirschheim 1993b) p. 200). While the contract plays a central role in defining the outsourcing relationship, there are limitations to a contract as a mechanism for managing the outsourcing engagement. In order to help advance the discourse on risk management strategies in IS outsourcing, we conduct an empirical analysis of a large outsourcing contract from Alberta, Canada.

This paper examines the role contracts play in addressing risks and specifying risk management strategies. In Section 2 of the paper we present our framework of outsourcing risk factors and mitigation strategies. In Section 3 we outline our research method (content analysis) and justify its use. In Section 4 we present our findings and Section 5 provides a conclusion outlining the contributions of this paper and offers suggestions for further research.

2 FRAMEWORK FOR ANALYZING RISK FACTORS

Several researchers have offered risk analyses of IS outsourcing (Lacity, Hirschheim et al. 1995; Earl 1996; Aubert, Patry et al. 1998; Aubert, Dussault et al. 1999; Bhattacharya, Behara et al. 2003) others have examined the process or results of outsourcing in different environments (Aubert, Patry et al. 2000; Rohde 2004). Sullivan and Ngwenyama (2005) developed a risk framework from a thorough review of previous research on IS Outsourcing. They applied this framework to three sets of outsourcing guidelines from different jurisdictions around the world. We apply the same framework to a successful outsourcing contract to investigate the differences between a free-form policy document and a formal contract that guides and limits the behavior of multiple parties. The framework specifies seven IS outsourcing risk categories and related risk factors, which if not appropriately addressed, may lead to negative outcomes. The framework provides an integrated set of categories for classifying risks and suggested management strategies for managing risks related to IS outsourcing engagements. We present the seven risk categories and their related risk factors in Table 1. These risk factors were developed from a thorough review of previous research on IS outsourcing (Lacity and Hirschheim 1993b; Willcocks and Fitzgerald 1994; Lacity, Willcocks et al. 1995; Earl 1996; Rao, Nam et al. 1996; Aubert, Patry et al. 1998; Aubert, Dussault et al. 1999; Ngwenyama and Bryson 1999; Willcocks, Lacity et al. 1999; Bryson and Ngwenyama 2000; Gay and Essinger 2000; Lacity and Willcocks 2001; Bhattacharya, Behara et al. 2003).

The management strategies suggested to address each of these risk areas are presented in a separate table to emphasize our changed focus from abstract policy guidelines to actual contracts. While this framework is not exhaustive, it is the only one we have found that integrates the main risks of IS outsourcing along with the suggested mitigation techniques. Since the framework is documented
in detail in Sullivan and Ngwenyama (2005) we limit our discussion of specific risks to those required to analyze this contract.

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Risks Associated with Each Risk Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) The outsourcer’s lack of experience</td>
<td>1. Lack of experience with the function or process to be outsourced. 2. Lack of experience with the technology to be outsourced. 3. Lack of experience with IS Outsourcing.</td>
</tr>
<tr>
<td>2) Vendor’s lack of experience</td>
<td>1. Lack of experience with the function or process to be outsourced. This applies to the vendor organization itself as well as the personnel assigned to the project. 2. Lack of experience with the technology to be outsourced. This applies to the vendor organization itself as well as the personnel assigned to the project. 3. Lack of experience with IS Outsourcing.</td>
</tr>
<tr>
<td>3) Opportunistic behavior by the vendor</td>
<td>1. Vendor’s use of guile, deceit, or other unethical behavior. 2. High switching costs may shield the vendor from being replaced due to poor performance. 3. Few viable vendors in the market, effectively lock the outsourcer into a single vendor. This weakens the bargaining position of the outsourcer. 4. Asset specificity refers to systems that are built that have no other productive use within the outsourcing firm. This makes it difficult for the outsourcing organization to dismiss the vendor and walk away from the engagement.</td>
</tr>
<tr>
<td>4) Vendor financial instability</td>
<td>1. Vendor willingness to shirk under the terms of the contract. A vendor with nothing to lose is more willing to walk away from the contract and declare bankruptcy. 2. Vendor pursuing other, more profitable clients. 3. Outsourcer may become dependent upon an organization that ceases operation. 4. The number of qualified personnel employed by the vendor. If some personnel leave the vendor’s employment, there should be other capable personnel who can support the contract.</td>
</tr>
<tr>
<td>5) Vendor performance monitoring</td>
<td>1. Inability to completely specify the scope of work to be performed – service levels, transaction volume and frequency. 2. Problems measuring vendor performance may lead to declining service levels and rising costs. 3. Problems measuring system performance may lead to declining service levels and rising costs. 4. Application of incentive and penalty clauses in the contract that depend upon performance measurement.</td>
</tr>
<tr>
<td>6) Contract horizon and technological discontinuity</td>
<td>Contract Duration impacts all aspects of risk relating to changes over time: 1. Loss of skilled personnel due to turnover. 2. Technological discontinuity – Technology that was part of the contract becomes obsolete requiring a shift to new technologies. 3. Business or operating environment of the outsourcing firm changes requiring a different relationship with the vendor. 4. Viability of the Vendor Firm is compromised from other events.</td>
</tr>
<tr>
<td>7) Loss of core competencies and proprietary information</td>
<td>1. Loss of core competence due to contracting out or outsourcing key process areas. 2. Loss of key personnel due to perceive fear of career curtailment due to outsourcing of organizational function. 3. If the vendor begins to perform core functions and processes, two problems may arise: a) the vendor replaces the outsourcing firm in its domain  b) the vendor moves in a direction different from one that the outsourcing firm would have chosen.</td>
</tr>
</tbody>
</table>

Table 1 – Risk Categories and Associated Risk Factors - Adapted from (Sullivan and Ngwenyama 2005)

2.1 Categories of Risk

This risk framework was initially applied to an analysis of IS outsourcing guidelines written by large public jurisdictions (Sullivan and Ngwenyama 2005). The intention of these guidelines was to promote sound policies related to the outsourcing of technology-dependent functions and processes. The guidelines were written to support serious reflection by public sector managers considering outsourcing. While these guidelines were written from the perspective of a single party, contracts regulate behavior between two or more parties.

Contracts represent an actual transaction in a concrete instance rather than reflection on an abstract idea or possible course of action. All parties to the contract must agree to its terms and conditions as well as the rights it affords and the obligations it imposes. This is very different from the unilateral perspective of guidelines. The contract allocates and balances the actual costs of the transaction between the parties.
Research on transaction costs (Coase 1937; Williamson 1975; Williamson 1979) specifies cost drivers such as search costs, monitoring costs, and management costs. While guidelines address these costs in abstract terms, contracts must specify them concretely. Further, contracts often do not address the issues related to search costs; they can address monitoring and management costs.

We now apply the risk framework to an actual contract to determine its strengths and weaknesses. What aspects of the outsourcing engagement might become risks if they are not addressed in the contract? What risks and management strategies cannot be addressed in the contract? Finally, we were interested in learning whether all risks must be addressed in a contract in order to have a successful engagement. After a thorough analysis of the contract, we found that most risks in our framework were not specifically mentioned. Further examination revealed that the nature of contracts make them unsuitable to address abstract risks. They are relatively better suited to specifying concrete risk management strategies and actions. Therefore, we modified our analysis to focus on risk management strategies suggested in the research literature (Klein and Myers 1999). We present the risk management strategies for each category as well as our research findings in Table 2.

3 EMPIRICAL MATERIALS AND RESEARCH METHOD

The empirical materials of this research consist of an outsourcing contract of 76 pages. The primary objective of our analysis was to use content analysis to surface any information about risk factors and risk management strategies embedded in the contract. The contract contains many of the clauses and terms suggested in the academic literature on IS outsourcing.

3.1 The Research Method

Content analysis is a method of manual or automated analysis of the semantic content of documents (e.g., newspapers, contracts, and transcripts of audio or video media), to make inferences, derive in-depth understanding, or to draw conclusions about the text (Weber 1990; Neuendorf 2002). Computer supported content analysis is a particularly powerful technique because of its potential to systematically analyze extremely large volumes of data that would overwhelm a human analyst. Another important advantage of using content analysis software tools is the consistency and reliability of the coding (Rosenburg, Schnurr et al. 1990; Roberts and Popping 1993). There are a variety of software packages to facilitate content analyses; in this study we use HyperRESEARCH 2.0. The use of an automated tool greatly assisted in organization of the data and its coding back to the analytical framework (26 risks and 29 management strategies). The following discussion shows how risk management strategies are implemented in the Alberta contract and the ramifications for practice.

3.2 Analysis Procedure

The contract from came in the form of a Microsoft Word document. We saved it as an ASCII text file and loaded it into HyperResearch 2.0 without modification. The content analysis of the documents followed a three stage procedure:

1) Definition of search terms for identifying themes within the documents;
2) Exhaustive searching of the documents for specific observations of themes; related to IS outsourcing risks and their effective mitigation; and
3) Analysis and interpretation of the empirical findings.

The starting point for constructing the search terms for our content analysis was our framework of the seven risk categories (cf. Table 1). From these we developed an initial set of search terms from which to begin our analysis. However, the identification of appropriate search terms required several iterations of searching, reading, and interpreting text segments.

4.0 CONTRACT ANALYSIS

A contract is a legal instrument for defining and managing a formal relationship between two parties. Although a contract cannot address all possible risks in the relationship, it can specify those which the parties are able to identify in advance. In our analysis of this contract we found most, but not all, risk mitigation strategies specified in the academic literature. Contracts are relatively better
suited to addressing concrete management strategies where one party to the contract can be required by the other to perform a certain action or refrain from a specific act. Secondly, the contract concentrated on specific mitigation strategies that the parties identified as important to the scope of the engagement. We present the risks and their suggested management strategies separately to emphasize the differences in the domains to which we are applying the framework. Our analysis of the Alberta contract focused on the presence or absence of risk mitigation strategies. The Risk management strategies presented in Table 2 are the result of a thorough review of previous literature on outsourcing described above.

The Alberta contract defines an outsourcing relationship between the Ministry of Human Resources and Employment (HR&E) of Alberta, Canada and CGI, Inc. of North America. In July 2002, HR&E entered into a four year $12 million contract with CGI1, Inc. to secure application maintenance services for their existing application portfolio. The contract specifies that the vendor will provide application maintenance services for the entire portfolio of software applications of HR&E. The HR&E has over 75 different applications in areas including: finance, program design, regional delivery, strategic services, and human resources. The application maintenance services specified in the contract include upgrades and development of additional applications to support the current portfolio as long as it will not require more than 300 hours of programmer time. Additional services such as strategic planning, application enhancements, and general consulting are also included in the scope of work.

As a result of the page limitations for this paper, we present only a subset of the risk categories and related risk factors that we found in the contract. Further, since the findings are summarized in Table 3 we do not discuss all the risk management strategies that were included within the contract. However, this limited presentation should serve to illustrate the process that we followed and how it can be applied to other outsourcing contracts.

**Detailed Findings**

**Risk Category 1. Outsourcer’s Lack of Experience**

Alberta HR&E is aware of their lack of experience relative to outsourcing there is functions. While some management strategies can not be addressed in the contract, those that could be appropriately addressed were included in this contract. The contract is not an appropriate mechanism to specify management strategies 2, 4, or 6. However, the following management strategies can be incorporated into a contract: 3) have a third-party firm perform an independent verification and validation (IV&V) function, 5) sign detailed, fully-specified contracts, and 7) require the vendor firm to specify all costs associated with transitioning services from the outsourcing firm to the vendor organization. While the contract does not directly specify an experienced IT project manager for the engagement (Management Strategy 1), the contract does specify a comprehensive management structure that we discuss in the following section of the paper.

The Alberta contract specifies audit functions that will be performed by separate government entities or by the project management teams. The contract is detailed and very complete. The contract specifies the applications to be supported and the tools to be used. If additional services are required, there is a detailed procedure for specifying the new service and determining its cost. Finally, the contract specifies transition activities in detail. The Alberta contract requires the vendor firm to assume all costs and services related to the transition.

11.6.2 PHASE-IN TRANSITION PRICING

The Proposal must include a Fixed Price to provide the transition services specified in section 9.5 and Appendix D of this RFP including all components of the Vendor’s proposed Phase-In Transition plan. (Alberta Ministry of Human Resources and Employment 2002) {Section 11.6 Pricing Information}

This clause effectively eliminates this risk from the outsourcer’s perspective.

---

1 In May 2004 CGI merged with American Management Systems and is now one of the largest integrated IT services firms in North America.
<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Management Strategies Suggested to Address Risks</th>
<th>HRE Contract</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) The outsourcer’s lack of experience</td>
<td>1. hire a professional information systems project manager who is familiar with the technology to manage the contract.</td>
<td>Addressed</td>
</tr>
<tr>
<td></td>
<td>2. hire an experienced outsourcing consultant to assist in the creation and management of the contract.</td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td>3. hire an experienced consultant to perform an independent verification and validation (IV&amp;V) function on the contract.</td>
<td>Addressed</td>
</tr>
<tr>
<td></td>
<td>4. outsource incrementally with small projects and gain experience over time.</td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td>5. sign detailed contracts not sketchy, open-ended contracts.</td>
<td>Addressed</td>
</tr>
<tr>
<td></td>
<td>6. prepare detailed estimates of the cost to manage the contract once it is implemented.</td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td>7. require vendor firms to specify all costs associated with transitioning services from the outsourcing firm to the vendor organization.</td>
<td>Addressed</td>
</tr>
<tr>
<td>2) Vendor’s lack of experience</td>
<td>1. hire a professional project manager to manage both the contract and the vendor from the outsourcing organization’s side of the relationship and act as an advocate for the organization’s goals.</td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td>2. perform a comprehensive background review of all potential vendors and check their references.</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>3) Opportunistic behavior by the vendor</td>
<td>1. include penalty and incentive clauses in the contract to manage the vendor’s behavior.</td>
<td>Penalties not incentives</td>
</tr>
<tr>
<td></td>
<td>2. hire an outside consultant to perform an independent verification and validation (IV&amp;V) function.</td>
<td>Addressed</td>
</tr>
<tr>
<td></td>
<td>3. hire a professional IT project manager for the engagement.</td>
<td>Addressed</td>
</tr>
<tr>
<td></td>
<td>4. Check professional references thoroughly</td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td>5. avoid proprietary technologies and employ mainstream technologies as much as possible. If a specific technology is required, ensure that adequate capability is maintained within the organization to support the technology.</td>
<td>Addressed</td>
</tr>
<tr>
<td></td>
<td>6. negotiate flexible contracts that can be renegotiated at specified intervals.</td>
<td>Addressed</td>
</tr>
<tr>
<td>4) Vendor financial instability</td>
<td>1. carefully consider a potential vendor’s size and financial stability before entering into a large, long-term contract.</td>
<td>Addressed</td>
</tr>
<tr>
<td></td>
<td>2. ensure that the vendor achieves an acceptable profit on the engagement</td>
<td>Not Addressed</td>
</tr>
<tr>
<td></td>
<td>3. place vendor source code in escrow in case of bankruptcy or cessation of operations.</td>
<td>Not Necessary</td>
</tr>
<tr>
<td>5) Vendor performance monitoring</td>
<td>1. avoid signing incomplete contracts. Organizations should make sure that they specify all relevant service levels and how they will be measured.</td>
<td>Addressed</td>
</tr>
<tr>
<td></td>
<td>2. include incentive and penalty clauses in the contract.</td>
<td>Penalties not Incentives</td>
</tr>
<tr>
<td></td>
<td>3. specify outcome-based performance metrics rather than work-based performance metrics</td>
<td>Addressed</td>
</tr>
<tr>
<td></td>
<td>4. retain key personnel and their specific knowledge on performance monitoring teams.</td>
<td>Not Addressed</td>
</tr>
<tr>
<td>6) Contract horizon and technological discontinuity</td>
<td>1. negotiate flexible contracts that can be renegotiated a specified intervals.</td>
<td>Addressed</td>
</tr>
<tr>
<td></td>
<td>2. Develop thorough technology transition plans with the vendor. Ensure that vendor specifies replacement technology.</td>
<td>Addressed</td>
</tr>
<tr>
<td></td>
<td>3. place vendor source code in escrow account in the event of vendor bankruptcy</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>7) Loss of core competencies and proprietary information</td>
<td>1. take appropriate steps to retain key personnel and specific knowledge within the organization.</td>
<td>Not Addressed</td>
</tr>
<tr>
<td></td>
<td>2. make clear and distinct separations of IS activities and functions and require binding non-disclosure and non-compete clauses within the contract.</td>
<td>Addressed</td>
</tr>
<tr>
<td></td>
<td>3. work with the vendor to develop comprehensive plan for knowledge transfer.</td>
<td>Not Addressed</td>
</tr>
<tr>
<td></td>
<td>4. Develop detailed disaster recovery plans.</td>
<td>Addressed</td>
</tr>
</tbody>
</table>

Table 2: Risk Management Strategies suggested in the academic literature (Adapted from Sullivan and Ngwenyama 2005) as well as summary of research findings for the Alberta HRE Contract
Risk Category 3. Opportunistic Behavior by the Vendor

Opportunism on the part of the vendor is a significant risk in any outsourcing contract and it can occur at any time during the outsourcing process. Opportunism includes making unrealistic or untrue representations about vendor capabilities in the proposal phases of the process and shirking under the terms of the contract once the contract has been executed. Other more subtle forms of opportunism include locking the outsourcing organization into proprietary technology that few other vendors are qualified to support and/or building systems that are narrowly focused and have no other useful purpose (asset specificity).

The Alberta contract does not mention any of the risks related to vendor opportunism as they are presented in the literature. However, the Alberta contract includes most of the management strategies that we have listed in our framework to address this risk. In addition, they have one of the most extensive management control systems of any outsourcing contract we have seen.

The management and control systems for the Alberta contract are implemented through two committees that oversee the contract. This contract specifies both an IT Contract Committee and a Contract Management Committee to oversee the contract. An equal number of AHRE employees and CGI (vendor) employees sit on each of the committees. The Contract Management Committee deals with the operational issues relating to the day-to-day management of the contract. This includes monitoring the vendor’s performance under the contract in accordance with the performance metrics that have been established for the contract. In addition, the Contract Management Committee conducts regular progress reviews and evaluates the responsibilities of both AHRE and the vendor to ensure that the responsibilities are clearly defined and properly executed.

The IT Contract Committee is a higher level of management representing both the AHRE and CGI management teams. This committee is designed to oversee the Contract Management Committee and resolve any disputes that may arise in the lower committee. The IT Contract Committee plays a strategic role in determining the technological direction for the engagement and ensuring that the resources expended under the contract meet the strategic needs of AHRE. While having two management committees drives up the transaction costs associated with the contract, there is much less risk of Alberta losing control of this engagement.

There is no mention of hiring a professional project manager for the engagement other than a clause that gives AHRE the right to refuse any vendor personnel assigned to the engagement. This clause does not address the need for a strong project manager who represents the outsourcing organization and their interests. However, the two contract management committees, discussed above, provide this function in a somewhat different form than is suggested in the academic literature.

There is no mention of a need to avoid proprietary technology or adhere to open standards. However, since the focus of this contract is on the maintenance of existing systems, this is not a major weakness in the contract.

Controlling the risks related to vendor opportunism requires careful management strategies. The first management strategy presented in our framework is the suggestion to include penalty and incentive clauses in the contract to manage the vendor’s behavior. While the contract does include penalties for failure to meet service levels, there are no incentives to improve service over the course of the contract. This could be a potential weakness in the contract. However, there are no indications from the people that we spoke with at AHRE that there are any adverse effects arising from a lack of incentives.

Independent verification and validation (IV&V) ensures that all representations made by the vendor during the course of the engagement are accurate and complete. Alberta addresses the independent verification and validation (IV&V) function through several clauses that relate to both security audits and financial audits. These audits may be performed by AHRE or others retained for the purpose of ensuring accuracy and completeness in the vendor’s charges and the work performed. The audit clause from the Alberta contract is presented in its entirety in the appendix. Another clause in the contract expands upon this access requirement stating that the auditors and AHRE personnel must be allowed access to operational, administrative and methodology documentation related to the engagement as well as be allowed to attend the meetings of all system development and maintenance projects. In addition, the vendor is required to assume “the costs related to reasonable internal and
external audit activity” (Alberta Ministry of Human Resources and Employment 2002) related to this contract.

Risk Category 4. Vendor Financial Instability

The risks associated with the financial stability of the vendor can become significant drivers of overall project success or failure. Any state jurisdiction has an interest in treating all vendors equally while also ensuring that the public interest is protected. Alberta takes a flexible approach to addressing a vendor’s financial position and stability. The risks relating to a vendor’s financial instability are generally addressed before a contract is signed. However, a vendor’s financial position may change over time.

Alberta recognizes the risk relating to a vendor’s financial position and addresses it in an innovative manner. The Alberta contract requires the selected vendor to post an irrevocable, unconditional letter of credit on a Canadian financial institution that is acceptable to the Alberta Human Resources and Employment Ministry in the amount of CA$1,000,000. The letter of credit is payable to the Minister of Finance of Alberta. In the event that AHRE determines that CGI is in default on the contract, AHRE will notify CGI of their intent to call upon the letter of credit. The parties will have 21 days to resolve any disagreements relating to the contract. If resolution cannot be reached in 21 days, then AHRE will ask the Alberta Minister of Finance to call upon the letter of credit up to the entire amount. Any final settlement will be determined by arbitration or by the Canadian Courts. This letter of credit amounts to about 8% of the overall contract value over four years. However, if there are problems with the engagement or the vendor they are likely to develop well before the four year term of the contract. Therefore, the letter of credit represents a significant proportion of the total value of the contract. This is an innovative contract requirement that serves to cover the outsourcing organization’s exposure to a vendor’s financial weakness while providing the vendor with a concrete incentive to ensure quality service. While this contract provision does not relieve an outsourcing organization from performing due diligence on a prospective vendor, it does help to ensure that a financial remedy is readily available in the event of poor performance. If the vendor is found to be in default or breach of the contract, then damages are readily available in 21 days.

Risk Category 5. Vendor Performance Monitoring

The effort to measure vendor performance is rife with pitfalls. Performance measurement impacts all other aspects of the engagement and often determines the success of the outsourcing engagement. The Alberta contract devotes significant attention to this issue and began tracking performance metrics and applying penalties one month after the contract start date. There are an initial 19 service levels specified in the contract in several categories such as: Customer Satisfaction; Applications; Quality of Service Request Implementations; Quality of Application Documentation; Loss of Data, Backup/Recovery Failure, Retention Failure; Critical Output/Input; Security Violation; and Staff Availability. Each performance metric is described with an indicator, a standard and a target service level. If the service level is not met, the vendor’s invoice is reduced by a predefined formula in the following month. Our review of these performance metrics did not indicate that they would induce the vendor to do anything detrimental to AHRE in order to meet a particular service level. The service levels are reasonable and the combination of service levels appears to be balanced and thoughtful.

The management strategy that advises the specification of outcome-based performance metrics appears to be followed wherever possible. One example of this is the minimum requirement of a 3.5 out of 5 rating on all customer satisfaction surveys which are to be completed on a regular basis. Most of the other service metrics stipulated in the contract specify performance in terms of successful outcomes rather than number of hours worked or number of lines of code written. The performance metrics indicate that AHRE is very clear about what they are paying for in this contract. The Contract Management Committee is responsible for developing any additional performance metrics that may be necessary over the course of the contract.

Risk Category 6. Contract Time Horizon and Technological Discontinuity
Allowing for change is one of the most difficult areas of the contract to write and administer. This includes the loss of qualified personnel, the development of new personnel, and often radical changes in the technologies specified in the contract and deployed within the organization. These types of changes and future developments are inherently difficult to address in a contract written to cover the present as well as the future. The term of the outsourcing contract necessitates some flexibility. The longer the term of the contract, the more flexibility is required to adapt to the changing needs of the outsourcing organization and the changing technological landscape. However, the more flexible the contract becomes, the less completely it is specified. This creates a dynamic tension and a need for careful balance between creating a contract that is thoroughly specified and a document that will allow for growth and change to deal with future technological realities.

Alberta takes a novel approach to managing the risks associated with the contract time horizon. The Alberta contract has a separate section called the Annual Supplementary Operating Agreement (ASOA) that does an excellent job of addressing the inherent tension between the need for flexibility and the need for a fully specified contract. The ASOA has the:

- objective of defining annual Service Level expectations, business transaction volume projections, and to respond to the impact of changes in information technology, management techniques, and AHRE’s expense reduction, service and application needs. This is intended to enable the Vendor to meet the requirements for the performance, availability, security, integrity, flexibility and functions of Application Maintenance environment (Alberta Ministry of Human Resources and Employment 2002).

This clause gives the contract the necessary flexibility to improve service levels each year and also to adapt to technological changes that are sure to develop in the future.

**Risk Category 7. Loss of Core Competencies and Proprietary Information**

The potential loss of core competencies and proprietary or sensitive information is a significant risk in any outsourcing contract. As more IT functions are outsourced, organizations run the risk of losing the ability to effectively perform or even manage mission-critical operations for the firm. A related risk is the potential loss of sensitive and/or essential organizational data which could be disastrous for the organization. The Alberta contract devotes significant attention to data security and retention requirements. It does not mention the need for retention of key personnel nor does it specify any knowledge transfer procedures. However, the need for clear and distinct separations of IS activities and functions is addressed through the clearly defined scope relating to the maintenance of the existing application portfolio. While the maintenance of the entire application portfolio is likely to impact other IT functions within the organization, the issues related to these impacts are not addressed.

The Alberta contract devotes a great deal of attention to issues relating to data security, confidentiality, retention, and recovery. An entire section of the contract specifies how confidential data is to be treated, who can access such data and the security measures that must be in place to ensure the data is safeguarded from unauthorized access. Further, the contract specifies that no “client identifiable information” can be disclosed outside of AHRE without a legally binding order from a competent jurisdiction. In addition, the contract requires the vendor and their personnel to observe all of AHRE’s existing data security and access policies for the duration of the engagement. The contract also specifies that AHRE will perform regular security audits of the vendor’s data management practices respecting AHRE’s data. Finally, the contract has a performance metric relating to loss of data that requires immediate notification in the event that any data is lost, corrupted, or cannot be restored from a back-up within two days. Another performance metric relates to security breaches relating to unauthorized access to systems or data. The failure to meet either of these performance metrics 100% of the time can result in penalties to the vendor of up to 10% of their invoice and recurrences will result in the vendor being found in breach of the contract.

The maintenance of the organization’s application portfolio requires people who are knowledgeable about the functions and processes of AHRE but, the contract does not provide any insight into how this knowledge will be retained by AHRE. It appears from the contract that the
network and infrastructure functions will be retained by AHRE. However, the contract does not specify who will administer development and production servers that support applications running on the network or maintenance and development activities by the vendor. Finally, there is no indication within the contract of any formal knowledge transfer processes that will be used to maintain existing organizational knowledge within AHRE.

5 CONCLUDING DISCUSSION – CONTRIBUTIONS TO IS OUTSOURCING RESEARCH AND PRACTICE

The framework applied in this paper attempts to unify the disparate research regarding the risks of IS outsourcing and the appropriate means of addressing these risks. Our focus in this paper has been on the outsourcing contract as an instrument to specify management strategies to address the risks inherent in the practice of IS outsourcing. By applying the risk framework developed by Sullivan and Ngwenyama (2005) to a specific contract we have been able to surface some of the limitations of the framework as a way to analyze contracts. However, through this research we have also highlighted some of the weaknesses of contracts as a mechanism to control risks related to IS outsourcing. We have also shown that not all the risks promoted in the research literature need to be included or addressed in the contract in order to have a successful outsourcing engagement. Further, we have revealed that some suggested risk factors and management strategies suggested in the literature inherently conflict and cannot be pursued simultaneously.

We have provided IT managers with guidance and suggestions for ways to implement management strategies to address the most significant risks associated with outsourcing IT functions. This research highlights some of the more innovative approaches to addressing risks. This paper also differentiates between risks that can be addressed and management strategies that can be implemented in a contract as well as those that cannot be effectively addressed in a contract. We find that the outsourcing contract is a relatively crude instrument for dealing with the subtleties and complexities of a large outsourcing arrangement. An outsourcing contract must be supported by other documents and close management of the engagement to be effective.

This research focused on the risks of outsourcing from the perspective of the outsourcing organization. However, the vendor organization also faces significant risks related to the contract. The risks on one side of the contract might impact the risks for the other party to the contract. For example, the outsourcer’s lack of experience with any aspect of the engagement or with outsourcing itself may present significant risks for the vendor firm.

In an effort to control or minimize shirking or underperformance on the contract by the vendor Lacity and Hirschheim advise outsourcing organizations to avoid signing incomplete contracts and to fully specify all aspects of the contract, particularly in the area of performance metrics (Lacity, Hirschheim et al. 1995). However, they also recommend signing flexible contracts that can be renegotiated at regular intervals (Lacity, Hirschheim et al. 1995). This leaves many organizations in a difficult position trying to balance these two conflicting objectives within the same outsourcing contract. The Alberta contract has a built-in mechanism for change in the Annual Supplementary Operating Agreement (ASOA) that allows them to review the status and volumes of the contract each year without penalty. The main provisions of the contract remain in force and provide structure but, the processing volumes and technical skills needed for each succeeding year can be adjusted to suit the needs of the HR&E.

Another tension arises in the academic literature from Lacity and Hirschheim’s suggestion to outsource incrementally using small projects to learn and then progressing to larger outsourcing initiatives (Lacity, Hirschheim et al. 1995). While Earl suggests that smaller contracts require too much management oversight and any cost advantages are lost (Earl 1996). These types of conflicts in the research literature are not easy to resolve and represent delicate balances that must be carefully managed in the context of the engagement.

The Alberta outsourcing contract represents a sizable commitment and significant risks for the outsourcing organization from both a financial and an operational perspective. However, they have executed a well-crafted and reasonably complete contract that addresses many of the risks identified in the research literature. It should be noted that while the Alberta contract was large and posed
potentially serious risks for the outsourcing organizations, the scope of work to be performed was clearly defined and specified. Our concern is that other scopes of work that are less well-defined may create significant challenges for both the outsourcing organization and the vendors trying to support them. This is an area for further research.

Another critical point surfaced in this research is the relative importance of the risks in this, or any other, framework. Depending upon the scope of the work to be performed, some risks identified in the research literature will play a more significant role than others; there is not a one-to-one relationship between risks and contracts. While we have shown that not all risks need to be addressed in a contract, we have not been able to determine the relative importance of the risks in a successful or unsuccessful outsourcing engagement. Clearly, some risks are more important than others to ensure that an outsourcing relationship achieves its stated goals. However, we leave this as a point for further research.

BIBLIOGRAPHY


Murphy, J. (2003). Ways to Evaluate and Address Your Outsourcing Risk, Gartner Research.