Guidelines for identifying risk vulnerabilities associated with ICT sourcing

A.Cachia
Department of Informatics, University of Pretoria
Pretoria 0002, Republic of South Africa
yogiadelle@yahoo.com

C.J. Kruger*
Department of Informatics, University of Pretoria
Pretoria 0002, Republic of South Africa
Neels kruger@up.ac.za

Received October 2007

As organizations broaden their organizational boundaries with sourcing practices, it is imperative to identify risk vulnerabilities from a wider perspective than before. Specifically, organizations that make substantial use of ICT suppliers need to understand the risk vulnerabilities associated with ICT sourcing partnerships. Unfortunately, due to vulnerabilities being addressed from different levels of erudition, an inclusive list of risk vulnerabilities, associated with ICT suppliers, does not exist within the ICT industry. This article not only address ICT risk management discrepancies and the importance of ICT supplier management, but in drawing on the collective knowledge contained in diverse sources, two distinct lists containing risk vulnerabilities, from the customer organization's perspective, are generated, all, in order to accelerate the understanding of exposure when dealing with ICT suppliers.

*To whom all correspondence should be addressed.

Introduction

After the September 11th 2001 terrorist attack in the USA, risk management received renewed attention as a means of avoiding being placed in jeopardy by an event that might seem unlikely, impossible or even incomprehensible (Anderson, 2001). That tragic event sounded alarm bells for many organizations about the necessity not only to consciously manage risk, but also to be in a position to identify and understand vulnerabilities[1] with regard to risk.

According to the King Report (Institute of Directors, 2002), ICT has had a major impact on the way business is conducted, especially with traditional value chains disintegrating and organizational boundaries becoming blurred. Hunter and Bloch (2003) argues that due to the shift in the importance of ICT, stakeholders should not only understand what constitutes ICT risks, but also need reassurance that ICT risks are managed in an effective and efficient manner. As far back as 1998, Leenders and Blenkhorn argued that ensuring successful technological risk management necessitates a strong focus on supplier relationships. Porter (2001) concurs with this idea, maintaining that few (if any) organizations are totally self-sufficient, relying on suppliers to optimize their value chains. Du Rand (2003) agrees, adding that Information Technology Organizations (ITOs) depend on suppliers to provide technology services and assist in managing technology risks. ICT risks therefore need to be managed across the entire supply chain, from suppliers to customers, placing special emphasis on the transition from ICT suppliers and Outsource Partners to the Internal IT Organisation, Support Divisions and/or Line of Business.

In agreement with the King Report (Institute of Directors, 2002: 81) recommending[2] that organizations develop a 'demonstrable system of dynamic risk identification as part of their risk management strategy', Naidoo (2002) asserts that the days of intuitive risk management are over and suggests that in future any such endeavours will be considered poor corporate governance practice. Due to ICT risk management becoming a legal matter, rather than just a managerial necessity, Clemons (2003), at a conference on strategic sourcing, asked whether there are any support and monitoring systems available to manage risk and rewards with regard to strategic ICT sourcing.

Coles and Moulton (2003) points out that as a rule, traditional ICT risk assessment is approached from within a systems or a business process methodology. Most risk assessment models, for example those in use by KPMG,

[1] A *vulnerability* is a weakness that exposes an organization to hurt, harm or attack and enables the risk to have impact. (Oxford, Kliem 1999).

[2] This recommendation is for a system of risk management and internal control of which dynamic risk identification is one mechanism.

Cobit and others, therefore consider risk in its totality and do not provide specific guidelines for the identification of risk vulnerabilities associated with sourcing, supplier organizations or supplier relationships. Unfortunately this leaves the organization with a biased view of risk, especially with regard to sourcing and supplier vulnerabilities, complicating the formulation of a combined risk strategy.

Vulnerabilities associated with supplier relationships are not new and many clues, hints and points of advice are available from numerous disparate sources, for example project management practices, capability maturity models, software development, project sourcing, outsourcing, etc. However, these are typically employed in an *ad hoc manner* on an operational or tactical level, and not synergised to give a broader, comprehensive view of only those vulnerabilities associated with suppliers. In the quest to identify ICT sourcing and supplier vulnerabilities, Anderson (2001) argues that it might be possible to instinctively identify many of these vulnerabilities from within the perspective of ITOs, especially when supplier relationships are actively managed with open communications and information sharing.

The aim of the article is therefore to generate guidelines for the identification of risk vulnerabilities, from a customer organization's perspective, in order to accelerate understanding of possible exposure when dealing with ICT suppliers. This study includes an analysis of an ITO where ICT is considered to be an integral part of the business. The proposed guidelines are not necessarily exhaustive, but they do collate suggestions scattered across a number of disparate sources - suggestions which, when viewed in a holistic manner, render one capable of identifying the most important risk vulnerabilities associated with ICT sourcing.

In order to achieve the above-mentioned objective, the scope of the research covers the following topics:

- The importance of ICT supplier management
- ICT Risk Management discrepancies
- ICT risk vulnerabilities identified in literature
- ICT risk vulnerabilities identified in the case study.

The article ends with a short summary of the primary findings.

Methodology

The research scope was limited to two areas expounded upon in the ICT environment, namely *supplier management* and *risk management*. The substantial literature review drawn from accredited academic journals, accepted industry best practice, commercial research institutions and media articles introduces work already done on the above-mentioned topics, thus confirming the pertinence of the topic. Analysis of the literature (exploratory research) led to the identification of a generic list of ICT risk vulnerabilities. However, since organizations across the world do not as a rule publish or make available all vulnerabilities, the validity of using only a literature review to formulate an inclusive list of risk vulnerabilities was questioned[3]. Moreover, in order to adhere to the principle proposed by Anderson (2001) 'that it might be possible to instinctively identify many ICT vulnerabilities from within the perspective of ITOs', further insight was sought through harvesting vulnerabilities instinctively identified by an ITO. Unfortunately, information used to manage suppliers is for the most part considered confidential by companies, and therefore any elaboration on information contained in company-confidential documentation was minimised as far as possible to include only the gist of arguments proposed and/or lessons learned. Similarly, opinions expressed by interviewees were only included when they added new insight to the line of reasoning. At all times company sources were treated as extremely confidential. Although this placed a limitation on the value of the study, the authors are of the belief that when viewed holistically, the case study provided enough insight to enhance the literature findings.

The organization chosen for the case study forms part of the financial services industry (including banking) with well-established e-business channels. Technology plays a strategic role in the organization and is managed by a large and mature ITO that provides traditional and inventive ICT services to the organization. The ITO has been practising supplier management for over three years and has collected valuable and unique information during this time. Previously unknown data was therefore collected using its supplier relationship management tool developed in-house to form a supplier management model, as well as minutes of meetings and periodic supplier evaluations. ICT supplier risk vulnerabilities were deduced from these sources and organized in the same categories as the list developed from ICT industry sources (i.e. the literature review). Via structured in-depth personal interviews with senior ITO participants[4] involved in managing key ICT supplier relationships, risk vulnerabilities were further scrutinized to try and identify the most applicable ones. In matching and comparing the vulnerabilities identified in literature with the vulnerabilities identified in the case study[5], valuable insight was gained into the management of ICT supplier risk vulnerabilities. The research method followed thus formed the basis for a grounded theory approach, consisting of three phases namely (1) identifying research areas of focus, (2) deciding on the most appropriate research design and (3) elaborating on research results (refer to Figure 1: Research Methodology).

[3] According to Yin (2003), given the complex nature of supplier relationships and the unique management thereof, the sources and nature of many ICT supplier vulnerabilities are only identifiable through confidential sharing of strategic information.

[4] In total 8 structured interviews were conducted.

[5] Confidential source list consists of 146 documents.

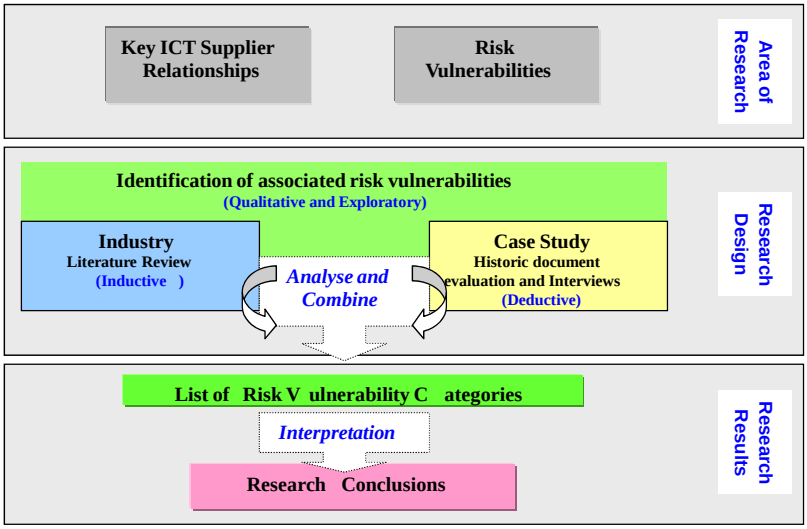

Figure 1: Research methodology

ICT Risk Management discrepancies

Deloach (2001) is of the opinion that current assumptions about and approaches to assessing risks may no longer be appropriate. This is primarily due to risks previously thought of as impossible, now becoming a reality. Deloach therefore advises organizations to refine their risk management approach to cost-effective and strategic risk management activities by developing capabilities to aggregate risk information to evaluate the risk in the organisation more broadly, i.e. also to identify vulnerabilities. The King Report (Institute of Directors, 2002:97) describes Risk Management as being '…the identification and evaluation of actual and potential risk areas (therefore also vulnerabilities) as they pertain to the company as a total entity, followed by a process of either termination, transfer, acceptance (tolerance) or mitigation of each risk'. In a similar manner, Suh and Han (2002) describe the purpose of risk management as an effort to minimise expected loss, and risk analysis as the basis on which (these) risk decisions should be made.

Recently, although not specifically focusing on ICT, the Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2003) provided practical guidance to assist an organisation in building effective programmes to identify, measure, prioritize and respond to risks. Of interest is the fact that the framework, like the King Report (Institute of Directors, 2002), includes the identification of vulnerabilities and suggests that risks need to be identified in internal and external factors. Internal factors proposed are infrastructure, personnel, process and technology, while external factors are believed to comprise economic, business, natural environment, political, social and technological matters. In order to control and manage risk, the COSO framework encourages the identification of what they consider to be 'risk events'. In essence, according to the COSA framework, a risk event (RE) occurs when a threat (T) exploits a risk vulnerability (V).

A risk event (RE) occurs when a threat (T) exploits a risk vulnerability (V),

thus

T + V = RE

With regards to ICT Risk management, the high rate of development and obsolescence in ICT makes decisions on ICT expenditure particularly difficult. Traditionally, management was not able to apply cost/value principles to ICT as easily as in other areas of business. This led to the perception that ICT expenditure is motivated by strategic instinct rather than sound commercial principles. According to Coles and Moulton (2003), traditional ICT risk analysis methodologies therefore wrongly focus on addressing only the possible impact on operations and systems. Risk management models, for example the KPMG IT risk management assessment model, are therefore not holistic in nature, only assessing risk from an internal point of view, and/or assuming that supplier risks are addressed when various risk categories, e.g. reliability, business focus, IT skills and resources, etc., are evaluated. In a similar manner, risk assessment and managerial tools, as listed by the Institute of Internal Auditors (1998), do not specifically supply detail with regard to identifying vulnerabilities associated with ICT suppliers.

The importance of ICT supplier management

According to Ford (1998), changes in the ICT industry, global economic slowdown, as well as local and international regulatory requirements, are all altering the ICT supplier management landscape. Ford is of the opinion

that these changes are raising the risk stakes, pushing supplier management to a strategic level. Fernandez (1995) earlier described the characteristics of a strategic supplier relationship as commitment to partnership, early involvement in decision making, mutual trust and crisis management. In agreement with Fernandez, Ford (1998) describes strategic relationships as substantial and maintains that it is not easy to change them quickly without incurring significant costs both in terms of disruptions and developing new relationships. Ford therefore asserts that strategic relationships are important assets and without them organisations cannot operate or even exist. He adds that an organization's performance does not only depend on its own actions and wishes, especially when interdependencies are present. Hutt, Stafford, Walker and Reingen (2000) supports this thinking, stating that both communication and the pro-active exchange of information strengthen relationships. In similar vein, Leonard (2000) argues that building and maintaining a sound relationship creates alignment between parties. Lacity (2002) adds yet another dimension to the line of reasoning by arguing that collaborative interactions occur when both sides share similar goals and comments. However, Lacity stresses the fact that the best relationships embrace mutual dynamics, with each party aiming for fairness, not domination or exploitation. Cooray and Ratnatunga (2002) also believes that through relationship management, successful long-term relationships can be developed despite substantial differences between firms. Melymuka (2003) concurs, and argues that even though not all suppliers have the same importance to an organization, supplier management (and the risks associated with it) is now becoming a core competency.

ICT risk vulnerabilities identified in literature

The quest to identify a holistic list of risk vulnerabilities associated with ICT sourcing, led to the identification of a number of holistic categories[6] in literature (refer to Table 1 and Appendix A: ICT supplier vulnerabilities identified in literature). The section that follows is a summary of vulnerability categories, as presented in appendix A.

The Cobit guidelines, Cosgroe (2003), Lehman (2003), Berinato (2004), Kliem (1999), Kern, Willcocks and Lacity (2002) and KPMG (2000 and 2003) all agree that in an attempt to minimize risks, formal supplier contracts need to be entered into. All these sources warn of typical flaws when contracts are poorly formulated and/or badly understood and managed. Some vulnerabilities were identified that specifically relate to service contracts and the management thereof, for example Service Level Agreements (SLAs) not in place or not agreed upon, only technical metrics, undefined procedures, etc. Lacity (2002) describes numerous vulnerabilities in her discussion of ICT outsourcers, putting forward the theory that the very nature of outsourcing agreements and their formalization in legal contracts creates risk. Lacity also maintains that poor understanding of the organization's ICT portfolio propagates poor vendor practices, thereby increasing risk. Watkins and Bazerman (2003) asserts that suppliers should be chosen and managed objectively and not on the basis of personal relationships. Watkins also believes that good communications counter vulnerability between the contracting parties and soften internal organizational obstacles, e.g. silos create risk vulnerabilities.

Lehmann (2003 (Part 1)) expresses concern about defective monitoring of actual service delivery, while Kliem (1999) highlights the notion that risk vulnerability might also be seated in the inappropriate reporting of delivered services. Cobit (IT Governance Institute 2002) agrees that both these service delivery issues need to be controlled. In addition, Lacity (2002) mentions poor availability and reliability of systems and the Internet from service providers, which might hurt business performance. Cosgroe (2003) and Desmond (2003) state that purchasing inappropriate or poor quality software makes the organization vulnerable to further ICT expenses. Coles and Moulton (2003) confirms that some of these vulnerabilities might be the result of an inherent flaw in the software product, e.g. poor security.

Lehmann (2003 (Part 1)), supported by Mphasis (2002), is concerned about the factors that influence a supplier, for example merger and acquisitions, and lawsuits that spill over to affect the organization. According to Mphasis (2002), suppliers' ability to survive is influenced by a number of market factors, forces that can expose an organization's supply chain. Steenstrup et al (2003) and Lehmann (2003a and b) agree, adding that financial health factors might also pose a threat to the supplier's ability to survive. Cobit in IT Governance Institute (2002) and the King Report (Institute of Directors, 2002) are more specific about suppliers' non-compliance with legal and regulatory requirements, which might expose the organization, for example insider trading. Naidoo (2002) adds that suppliers can possibly use confidential organizational or client information illicitly.

The King Report, together with others (Lehmann, 2003; Siegil, 1996; Cosgroe, 2003; Mphasis, 2002; Goodwin, 2003; and Kern *et al*., 2002), all stress that when suppliers do not disclose or share important internal information with the organization, this leaves the organization vulnerable to poor service, for example poorly selected sub-contractors, high percentage of inexperienced personnel, etc. Varon (2003) also points out that vendors cannot respond well to risks if they under-price. Throughout the literature on the subject it is therefore evident that poor relationships form a breeding ground for vulnerabilities. Kern *et al.* (2002) and Ford (1998), supported by the Software Engineering Institute (SEI). 2003 and Cobit (IT Governance Institute, 2002), therefore contend that relationships need to be nurtured and not only managed.

[6]It became apparent that in general a vast number of vulnerability dimensions tend to complement one another. Dimensions were therefore placed in logical groupings (categories) to provide the structure for further comparison and analysis.

Table 1: Risk vulnerabilities categories as identified from the literature review.

Poor service agreements and management thereof	Insight into supplier's future survivability
Poor contracts and management thereof	Undisclosed information of supplier internal operations
Inappropriate and poor service delivery monitoring	Supplier's inappropriate solution/product or service offering
Inappropriate and poor service delivery reporting	Supplier's lack of enterprise risk assessment
High level of dependency on technology	Supplier's non-compliance with legal and regulatory requirements
Poor supplier management practices	Supplier breaches confidentiality
Implementing new or complex technology	Supplier's lack of service availability & reliability
Poor quality control in implementing and managing technology	Supplier's poor responsiveness to risk
Not nurturing the quality of the relationship	Supplier's external organisational accountability
Relationship yields low economic value	Supplier's product flaws
Flawed outsourcing partnership/s	Large financial exposure on the part of supplier
Poor communication between the parties	Supplier's incompetent service delivery
Awareness of supplier's financial stability/health	Supplier compromises its integrity

According to Ford, the implementation of new or complex technology also raises the risk stakes, for example if the supplier manipulates uncertainties. According to the Software Engineering Institute (SEI). 2003 and Cosgroe (2003), a high level of dependency on technology creates vulnerabilities relating to the dependency on a supplier.

ICT risk vulnerabilities identified in the case study

In order to adhere to the proposition put forward by Anderson (2001) that it might be possible to instinctively identify many ICT vulnerabilities from within the perspective of ITOs, and Yin's (2003) argument that the sources and nature of many ICT supplier vulnerabilities are only identifiable through confidential sharing of strategic information, further insight was sought through examining vulnerabilities instinctively identified by the ITO[7]. Numerous risk vulnerabilities were identified in the case study documents (refer Appendix B: Case Study ICT Supplier Key Relationship Vulnerabilities). In matching the industry and case study lists of vulnerability dimensions, it was found that only 14% of vulnerability dimensions were exact matches (see Figure 2). This was primarily due to sources addressing vulnerabilities from either a strategic or a detailed (operational) perspective, especially with regard to the level of erudition.

Careful scrutiny of vulnerability dimensions from a holistic perspective, however, again confirmed the notion that vulnerability dimensions are in fact related. Viewing vulnerability dimensions as interdependent entities, i.e. vulnerability categories, therefore not only proved to be extremely valuable when it came to drawing comparisons between case study documents and literature findings, but also in guiding the structured interview process that followed (see Table 2).

Of interest is that although case study documents, like literature findings, place strong emphasis on vulnerabilities associated with flawed relationships, vulnerabilities caused by financial exposure, incompetence and integrity are also emphasized. In grouping vulnerability dimensions into vulnerability categories, three new categories could therefore be identified namely: (1) Large financial exposure on the part of the supplier, (2) Supplier incompetent service delivery and (3) Supplier compromises its integrity. The eight senior managers interviewed (participating in strategic ICT supplier management), not only confirmed that the vulnerability categories (as identified in the literature, and case study documents) are applicable and can definitely help organizations to successfully identify risk vulnerabilities associated with strategic ICT sourcing, but also provide practical insight into the successful management of ICT risk vulnerabilities. According to managers interviewed:

- 'Most vulnerabilities are within the organization's control and a small percentage are within the supplier's control'.
- 'Poor project management and internal control are the root causes of supplier vulnerabilities'.
- 'Be careful of "not authenticating vendor's *sales hype*" vs. the "*true ability*" to deliver'.
- 'Supplier management process must be end-to-end and not built around individuals (personalities)'.

[7] Company A: 1999 – 2004. Various confidential documents relating to risk management and strategic supplier management were analysed. Confidential source list consisted of 146 documents. For legal and competitive reasons these documents are not publicly available and Company A confidential.

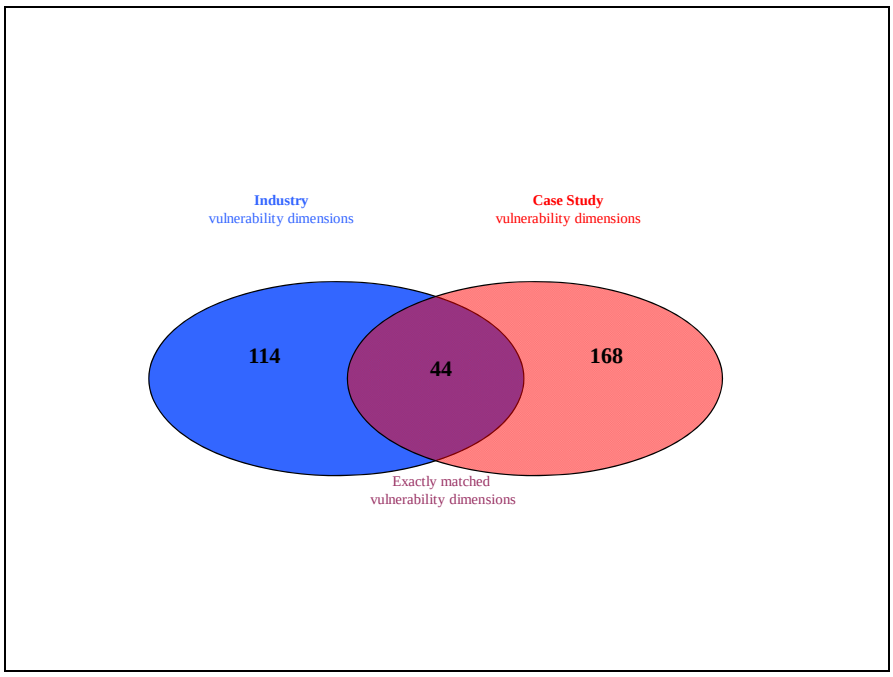

Fig 2: Exact matches of vulnerability dimensions

Table 2: Comparison between case study documents and literature findings

Vulnerability category	Literature (# found)	Case Study (# found)	Frequency
Poor service agreements and management thereof (7)	9	14	23
Poor contracts and management thereof (1)	15	24	39
Inappropriate and poor service delivery monitoring	2	10	12
Inappropriate and poor service delivery reporting	3	1	4
High level of dependency on a technology	2	8	10
Poor supplier management practices	4	8	12
Implementing new or complex technology	2	5	7
Poor quality control in implementing and managing technology	2	8	10
Not nurturing the quality of the relationship (3)	9	21	30
Relationship yields low economic value (4)	10	19	29
Flawed outsourcing partnership/s (2)	25	7	32
Poor communication between the parties	2	1	3
Awareness of supplier's financial stability/health (8)	16	5	21
Insight into supplier's ability to survive in the future	13	2	15
Undisclosed information about supplier’s internal operations (6)	13	13	26
Supplier’s inappropriate solution/product or service offering	2	5	7
Supplier's lack of enterprise risk assessment (5)	9	18	27
Supplier’s non-compliance with legal and regulatory requirements	1	7	8
Supplier breaches confidentiality	1	1	2
Supplier’s lack of service availability and reliability	1	2	3
Supplier's poor responsiveness to risk	2	5	7
Supplier's external organisational accountability	5	3	8
Supplier’s product flaws	1	5	6
Large financial exposure on the part of the supplier	0	6	6
Supplier’s incompetent service delivery	0	8	8
Supplier compromises its integrity	0	2	2

- 'Be careful of *manage-by-contract* syndrome'. In predictable demand, exact contracting is possible, but with unpredictable demand, non-exact contracting must be done. Not all eventualities can be contracted for as contracts become difficult to manage or change'.

- 'Strategic relationships can create reciprocity that does not make business sense'.

- 'An organization's image/reputation might be compromised when using a supplier that is not trusted in the market.'

- 'Appropriate criteria need to be considered in identifying strategic ICT relationships'.

With reference to Table 2, in analysing the frequency of occurrence[8], it became apparent that; (1) Poor contracts and the management thereof, (2) Flawed outsourcing partnerships, (3) Not nurturing the quality of the relationship, (4) Relationships yielding low economic value (5) Supplier's lack of enterprise risk assessment and (6) Undisclosed information about the supplier's internal operations can be considered the 'more important' risk vulnerability categories identified. However, even though senior managers interviewed all agreed that the different categories and vulnerability dimensions are all applicable, all rated the list of categories very differently and it seems that differences could be the result of the individual's experience, ability, skills and knowledge.

Most interviewees indicated that in viewing vulnerabilities from a holistic perspective, i.e. as interdependent vulnerability categories, the focus is primarily relegated to the managerial and tactical level. Although most interviewees indicated that this might be good practice, a number of interviewees argued that on a strategic level, (due to the economic impact on the organization, either in the long term or due to large financial investment), vulnerabilities categories need to be unbundled to expose concealed dimensions and risks. As an example, one participant pointed out that the vulnerability category 'Poor service level agreements and the management thereof' should typically be controlled on an operational level for a specific service that the supplier has agreed to provide. Project or functional control should thus be allocated to the manager who is accountable for the management of the SLA, problem solving and reporting. In a large ITO with many projects, functions and supplier SLAs, 'poor service level agreements and the management thereof' escalates to a strategic level when the service levels of a particular supplier are consistently inadequate and/or unreliable. The collective economic impact on the organization is therefore much larger than normally anticipated, and requires a higher or strategic-level focus and intervention. In other words the problem becomes a strategic relationship issue, where specifics, especially with regard to dimensional flaws, become paramount.

[8]Literature and case study company confidential documentation.

Most interviewees were also of the opinion that the organizations own information, practices, processes and procedures can control most vulnerabilities encountered. However, some interviewees stressed that it is those dimensions that are under the control of the supplier, or mutually controllable by both parties, that are the most tedious to manage. Interviewees therefore emphasised that vulnerabilities cannot be mitigated through influence, staying abreast and informed of the supplier's state of affairs and through collaboration alone. A robust relationship with suppliers is seen as a key success factor in identifying and influencing risk vulnerabilities. As one interviewee states 'organisations need to ensure that ICT supplier relationships are of a sound nature, and managed at a strategic level in order to lessen risk vulnerabilities escalating beyond the operational level, thus becoming a strategic concern'.

Conclusion

In this article it is argued that identifying risk vulnerabilities associated with ICT suppliers is becoming a legal necessity. Unfortunately, due to vulnerabilities being addressed from different levels of erudition, an inclusive list of risk vulnerabilities associated with ICT suppliers does not exist within the ICT industry. Drawing on the collective knowledge contained in diverse sources, the main thrust of the article is the formulation of two distinct lists of risk vulnerabilities, grouped into risk categories (appendixes A and B) associated with ICT suppliers. However, even though the knowledge contribution is specific in that it not only offers guidelines for identifying risk vulnerabilities associated with ICT sourcing, but also provides insight into risk identification, measures to combat risk vulnerabilities still need to be adapted to suit the specific needs of the individual organizations, and also the specific circumstances surrounding each and every risk vulnerability.

References

Anderson, M.F. 2001. 'Key risk considerations. Risk management'.[online] URL: http://www riskmanagement.com.au. Accessed 7/11/2003.

Berinato, S. 2004. 'You sue, you lose: The high cost of litigation'. [online] URL: http://www.cio.com/archive/020104/supplier.html. Accessed 20/2/2004.

BITS Advisory Council. 2004. 'BITS framework, financial services roundtable'. [online] URL: http://www.bitsinfo.org. Accessed 20/2/2004.

Blundell, D. 2003. 'Equip yourself to meet ECT legislation'. [online]URL: http://www.enews.co.za/sections/QuickPrint/Print.asp?StoryID=136342. Accessed 10/5/2004.

Clemons, E.K. 2003. 'Understanding sourcing as a strategic business: The risks and rewards of strategic sourcing and inter-firm alliances'. Paper presented at The Wharton School, Strategic Sourcing Conference, Bangalore, 10 March 2003.

Coles, S. & Moulton, R. 2003. 'Operationalizing IT risk management'. *Computers & Security* **22**(6): 487–493.

Company A. 1999 – 2004. Various confidential documents relating to risk management and strategic supplier management. Results from 8 personal interviews with strategic Company A management. Confidential source list consists of 146 documents.[9]

Cooray, S. & Ratnatunga, J. 2002. 'Buyer-supplier relationships: A case study of a Japanese and Western alliance', *Long Range Planning* **34**(6): 727-740.

Cosgroe, L. 2003. 'Maximising value from IT vendors. Ware'. CIO research reports. [online] URL: http://www2.cio.com/research/surveyreport.cfm?id=65. Accessed 12/11/2003.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2003. 'Enterprise risk management framework—draft'. [online] URL: http://www.coso.org. Accessed 10/11/2003

Deloach, J. 2001. 'Enterprise risk management. Key risk considerations post September 11'. Reprinted as '2002-01-10 key risk considerations', with permission from KnowledgeSpace Internal Audit and Risk Community – a subscription-based website sponsored by Anderson. [online] URL: http://www riskmanagement.com.au. Accessed 10/5/2004.

Deloitte. 2004. 'Global Banking Industry Outlook, 2004. Top ten issues, financial service industry'. [online] URL: www.deloitte.com. Accessed 11/7/2007.

Desmond, P. 2003. 'A better way to deal with vulnerabilities'. [online] URL: http://itmanagement.earthweb.com**.** Accessed 11/7/2003.

Du Rand, L. 2003. 'Mastering the IT shuffle'. *Computerweek Strategis,* April: 37.

South Africa. 2002. 'Electronic Communications and Transactions (ECT) Act 25 of 2002', assented to 31 July 2002, commencement date 30 August 2002, p. 10.

Fernandez, R. R. 1995. *Total quality in purchasing and supplier management.* Delray Beach. Lucie Press.

Ford, D. 1998. *Managing business relationships.* England: John Wily & Sons, Ltd.

Gordon, M. 2002, 'Everything's coming up suppliers!' *ABA Bank Compliance*, **23**(7): 4 – 130.

Goodwin, B. 2003. 'September attacks key driver for IT security investment, survey finds'. *ComputerWeekly*.com [online] URL: http://www.computerweekly.com articles. Accessed 7/11/2003.

Hunter, R. & Blosch, M. 2003. 'Managing the new IT risks', Gartner EXP CIO Signature [online] URL**:** http://www.commonperu.com/html/eventos/2006/cio/ppt/gartner/GARTNER_Applying_Enterprise_Architecture.pdf. Accessed 15/10/2006.

Hutt, M. D., Stafford, E. R., Walker, B. A. & Reingen, P. H. 2000. 'Case study. Defining the social network of a strategic alliance', *Sloan Management Review*, **41**(2): 51-62.

Institute of Directors. 2002. *King Report on corporate governance of South Africa 2002.* Johannesburg. Centre of Directorship and Corporate Governance.

Institute of Internal Auditors. 1998. [online] URL: http://www.theiia.org. Accessed 10/11/2003.

IT Governance Institute. 2002. *The COBIT framework DS1 delivery and support. Define and manage service levels and maturity models,* 3rd Edition. [online] URL: http://www.isaca.org. Accessed 17/11/2007.

IT Governance Institute. 2002. *Management guidelines DS2 delivery and support. Managing third-party services*, 3rd Edition. [online] URL: http://www.isaca.org. Accessed 17/11/2007.

Kern, T., Willcocks, L. P. & Lacity, M.C. 2002. 'Application service provision: Risk assessment and mitigation', *MIS Quarterly Executive* **1**(2):113 - 126.

Kliem, R. 1999, 'Managing the risks of outsourcing agreements', *Information System Management,* **15**(3):91 - 93.

KPMG. 2000. IT risk management benchmarking V4 questionnaire. Management of information. *Information Risk Management.* [online] URL: http//www.isaca.org Accessed 10/11/2007.

KPMG. 2003. 'IT risk management benchmarking V2 self-assessment'. [online] URL: http//www.isaca.org Accessed 10/11/2004.

Lacity, M. 2002. 'Lessons in global information technology sourcing', *IEEE*, **35**(8):26 – 33.

Leenders, M. R. & Blenkhorn, D. L. 1988. *Reverse marketing. The new buyer-supplier relationship.* New York: The Free Press, Macmillan.

Lehmann, C. 2003a, 'Assessing supplier risk: Part 1'. MetaGroup Research [online] URL: http://www metagroup.com. Accessed 11/11/2007.

Lehmann, C. 2003b. 'Assessing supplier risk: Part 2'. MetaGroup Research [online] URL: http://www metagroup.com. Accessed 11/11/2007.

Leonard, A.C. 2000. 'A conceptual framework for managing relationship between all participants during IT service and

[9]For legal and competitive reasons these documents are not publicly available and Company A confidential.

support activities', *South African Journal of Industrial Engineering*, **13**(2):81-96.

Hornby, A.S. 1995. *Oxford advanced learner's dictionary of current English*. Oxford: Oxford University Press.

Mphasis, 2002. 'Management discussion of risks and concerns'. [online] URL: http://www.mphasis.com/pdfs/MphasiS_Q4_FY03_MD&A%20_of_Risks_Concerns.pdf. Accessed 7/11/2003.

Melymuka, K. 2003. 'How will you manage your suppliers?', *Computer world* **37**(1): 32-33.

MetaGroup. 2002. 'MetaFACts: IT Spending Quarterly Review and Outlook'. First Albany – Meta Technology Research. [online] URL: http://www metagroup.com**.** Accessed 20/2/2004.

MetaGroup. 2003. 'Refining information value from supply chains', MetaGroup IT Leadership & Value Management Newsletter, December 2003. [online] URL: http://www.metagroup.com. (Accessed 20/2/2004).

Murray, S. 1998. 'How much, how good,' *The Banker*, **149**(874): 40 – 42.

Naidoo, R. 2002. *Corporate governance*. Cape Town: Double Storey Books, Juta.

Porter, M.E. 2001. 'Strategy and the Internet,' *Harvard Business Review*, **79**(3): 63-78.

Proszesky-Kuschke, B. 2003. 'Despositum and escrow: Their current application in computer source code in South African law', *De Jure*: 278 – 288.

Segil, L. 1996. *Intelligent business alliances. How to profit using today's most important strategic tool*. New York: Random House Inc.

Software Engineering Institute (SEI). 2003. 'Risk management paradigm. Risk management overview. Carnegie Mellon University, Pittsburgh'. [online] URL: http://www.sei.cmu.edu/programs/sepm/risk/risk.mgmt.overview.html. Accessed 12/11/2003.

Steenstrup, K., Kolsky, E., Thompson, E., White, A., Purchase, E. & Topolinski, T. 2003. 'How to assess an application supplier's financial stability'. Tactical guidelines TG-19-7111, Gartner [online] URL: http;//www.gartner.com. Accessed 10/11/2007.

Suh, B. & Han I. 2002. 'The IS risk analysis based on a business model', *Information and Management* **41**(2):149 – 158.

The Committee of Sponsoring Organisations of the Treadway Commission (COSO). 2003. 'Enterprise risk management framework. Exposure draft for public comment'. [online] URL: http://www.erm.coso.org. Accessed July 2003.

The Institute of Internal Auditors. 1998. *List of risk analysis, assessment and management tools*, Vol. 1. [online] URL:http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=207. Accessed 20/2/2004.

Tittle, J. G., Dupont, C. P., Fleming, R. G. & Hoefer III, A. 2002. 'Measuring value in client-vendor relationships'. [online] URL: http://www.csc.com/solutions/applicationoutsourcing/knowledgelibrary/914.shtml. Accessed 12/11/2003.

Varon, E. 2003. 'Getting the best from your vendors (What really works)'. [online] URL: http://www.cio.com/archive/110103/vendor.html**.** Accessed 12/11/2003.

Vecchiatto, P. 2003. 'Software vendors disappearing, says Gartner'. [online] URL: http://196.30.226.221/sections/quickprint/print.asp?SotryID=134286. Accessed 12/11/2003.

Ward, J. & Griffiths, P. 1996. *Strategic planning for information systems.* 2nd Edition. England: John Wiley & Sons, reprinted June 1998.

Watkins, M. D. & Bazerman, M. H. 2003. 'Predictable surprises: The disasters you should have seen coming', *Harvard Business Review*, **March**: 72 – 80.

Yin, R. K. 2003. *Case study research: Design and methods.* 3rd Edition. USA: Sage Publications.

Appendix A

ICT Supplier Vulnerabilities identified in literature

Vulnerability Category	Vulnerability	Reference
Poor service agreements and management thereof	Services Agreements are not properly defined	IT Governance Institute, 2002, Management Guidelines DS2 Delivery and Support. Managing Third-party Services, 3rd ed., p. 64, 65
	Technical and organisational interfaces are not documented	
	Measurement is based on technical metrics only - not business objectives	Cosgroe, Lorraine, 2003, 'Maximising Value from IT Vendors. Ware.' 4 Nov 2003, CIO Research Reports
	Low service cost vs service capability - you get what you pay for	Cosgroe, Lorraine, 2003, 'Maximising Value from IT Vendors. Ware.' 4 Nov 2003, CIO Research Reports
	Service measurement is not agreed	Fernandez, Ricardo R, 1995, *Total Quality in Purchasing and supplier management.* St. Lucie Press
	No formal SLA/s in place	KPMG 2000, 'IT Risk Management Benchmarking V4 Questionnaire. Management of Information', *Information Risk Management*, Aug. 2000
	No regular review of Service Agreement against original objectives	
	No completion, review or termination date of Service Agreement	
	Problem resolution procedures are not documented	Conversation with IBM Consultant
Poor contracts and management thereof	No Formal agreements in place before work starts	IT Governance Institute, 2002, Management Guidelines DS2 Delivery and Support. Managing Third-party Services, 3rd ed., p. 64, 65
	No formal process to ensure formal agreements & legal advice	IT Governance Institute, 2002, Management Guidelines DS2 Delivery and Support. Managing Third-party Services, 3rd ed., p. 64, 65
		Berinato, Scott, 1 February 2004, 'You Sue, You Lose: The high cost of Litigation'. CIO.com
	Contract does not reflect the work or is not □ppropriately defined	IT Governance Institute, 2002, Management Guidelines DS2 Delivery and Support. Managing Third-party Services, 3rd ed., p. 64, 65
	Exit, penalties and rewards not contractually agreed	IT Governance Institute, 2002, Management Guidelines DS2 Delivery and Support. Managing Third-party Services, 3rd ed., p. 64, 65
		Berinato, Scott, 1 February 2004, 'You Sue, You Lose: The high cost of Litigation'. CIO.com
	No Non-disclosure agreement between the parties	IT Governance Institute, 2002, Management Guidelines DS2 Delivery and Support. Managing Third-party Services, 3rd ed., p. 64, 65
	Not utilising Escrow contracts in legal uncertainties (Depostitum and escrow: their current application in computer source code in South African Law)	
	Intellectual property rights and liabilities are not agreed between the parties	
	Unclear or vague Issue resolution, Mediation and Arbitration procedures in contract	Berinato, Scott, 1 February 2004, 'You Sue, You Lose: The high cost of Litigation'. CIO.com
	The easily foreseeable problems e.g. project failure are not dealt with in formal agreements	
	Supplier has invariable pricing model	Cosgroe, Lorraine, 2003, 'Maximising Value from IT Vendors. Ware.' 4 Nov 2003, CIO Research Reports
	Contract period is too long or too short	
	Not all elements of scope of work contractually agreed between the parties	KPMG 2000, 'IT Risk Management Benchmarking V4 Questionnaire. Management of Information', *Information Risk Management*, Aug. 2000
	Not updating contracts periodically	Lehmann, Carl, 24 Oct. 2003, 'Assessing Supplier Risk: Part 2', MetaGroup Research Delta 2575

	Non-compete clauses omitted from contracts	Kern, Thomas, Willcocks, Leslie P. and Lacity, Mary C., 2002, 'Application Service Provision: Risk assessment and mitigation', *MIS Quarterly Executive* Vol. 1, No. 2., June 2002, University of Minnesota
	Omitting sub-contractor management in contract	Kliem, Ralph, 1999, 'Managing the risks of outsourcing agreements', *Information System Management,* Summer 1999
Inappropriate and poor service delivery monitoring	Process for monitoring economic value, service delivery and relationship quality	IT Governance Institute, 2002, Management Guidelines DS2 Delivery and Support. Managing Third-party Services, 3rd ed., p. 64, 65
	No Supplier management system for continuous performance rating, also against purchase order & contract compliance	Lehmann, Carl, 24 Oct. 2003, 'Assessing Supplier Risk: Part 2', MetaGroup Research Delta 2575
Inappropriate and poor Service delivery reporting	Irregular service delivery reporting	Kliem, Ralph, 1999, 'Managing the risks of outsourcing agreements', Information System Management, Summer 1999
	Poor performance not linked to contractual rewards & penalties	Kliem, Ralph, 1999, 'Managing the risks of outsourcing agreements', *Information System Management,* Summer 1999
	No formal process to report economic value, service delivery and relationship quality	IT Governance Institute, 2002, Management Guidelines DS2 Delivery and Support. Managing Third-party Services, 3rd ed., p. 64, 65
High level of dependency on technology	High degree of product customisation	Cosgroe, Lorraine, 2003, 'Maximising Value from IT Vendors. Ware.' 4 Nov 2003, CIO Research Reports
	High level of integrated management between supplier and ITO	Software Engineering Institute (SEI) 2003, 'Risk Management Paradigm. Risk Management Overview', Carnegie Mellon University, Pittsburgh
Poor supplier management practices	Supplier relationship is build only on personal levels	Watkins, Michael D. and Bazerman, Max H., 2003, 'Predictable Surprises: The Disasters you should have seen coming', *Harvard Business Review*, March 2003 (72 – 80).
	Subjective views on suppliers	
	Too much influence from special interests	
	Poor assessment of own IT portfolio	Lacity, Mary, 2002, 'Lessons in Global Information Technology Sourcing', University of Missouri, St.Louis, *IEEE,* Aug. 2002 (26 – 33)
Implementing New or Complex Technology	Supplier manipulates uncertainties	Ford, David, et al., 1998, *Managing Business Relationships,* John Wily & Sons, Ltd., England, p18 - 25
	Not implement and Use technology according to its purpose	
Poor quality control in implementing and managing technology	Not exchange appropriate information to improve quality control	Fernandez, Ricardo R, 1995, *Total Quality in Purchasing and supplier management.* St. Lucie Press
	Flawed risk management process	Lehmann, Carl, 24 Oct. 2003, 'Assessing Supplier Risk: Part 1', MetaGroup Research Delta 2574
Not nurturing the quality of the Relationship	Not analysing cost and service level variances	IT Governance Institute, 2002, Management Guidelines DS2 Delivery and Support. Managing Third-party Services, 3rd ed., p. 64, 65
	No relationship owner assigned to ensure quality of relationship	
	No supplier performance rewards and penalties	
	Inability to manage supplier relationships	Kern, Thomas, Willcocks, Leslie P. and Lacity, Mary C., 2002, 'Application Service Provision: Risk assessment and mitigation', *MIS Quarterly Executive* Vol. 1, No. 2., June 2002, University of Minnesota
	Assess & Understand what has happened in the relationship previously when contracting new work	Ford, David, et al., 1998, *Managing Business Relationships,* John Wily & Sons, Ltd., England, p6-7
	Not understanding the positioning of the relationship in the relationship life-cycle (pre-relationship, Exploratory, Developing, Stable stage)	
	Not adjusting management level when change in relationship status	
	Contrained communications between parties	Software Engineering Institute (SEI) 2003, 'Risk Management Paradigm. Risk Management Overview', Carnegie Mellon University, Pittsburgh
	No team work between the parties when delivery to the business	

Relationship yields low economic value	No formal process for due diligence before partner selection	IT Governance Institute, 2002, Management Guidelines DS2 Delivery and Support. Managing Third-party Services, 3rd ed., p. 64, 65
	Unclear relationship purpose and economic value thereof	
	Thorough understanding of quality, quantity, price and service of purchase	Leenders, Michiel R., and Blenkhorn, David L., 1988, *Reverse Marketing. The new Buyer-Supplier Relationship,* The Free Press, Macmillan, New York, USA
	Rigid product offerings – all or nothing	Cosgroe, Lorraine, 2003, 'Maximising Value from IT Vendors. Ware.' 4 Nov 2003, CIO Research Reports
	Quality of free consulting	
	References and capacity to deliver not validated	Berinato, Scott, 1 February 2004, 'You Sue, You Lose: The high cost of Litigation'. CIO.com
	Supplier's expectations needs to be managed/realistic	Ford, David, et al., 1998, *Managing Business Relationships,* John Wily & Sons, Ltd., England, p116
	Not understanding supplier's previous Project delivery failures	
	Not recognising costs other than "price" of purchasing (production, goods handling, storage, capital, relationship handling, admin & dev costs)	
	No or ad hoc process of relationship value assessment	
Flawed outsourcing partnership/s	Undefined processing levels	IT Governance Institute, 2002, Management Guidelines DS2 Delivery and Support. Managing Third-party Services, 3rd ed., p. 64, 65
	Poor security audit results	
	Not addressing monitoring and contingency requirements	
	Contract not cover conclusion/exit and handover	
	No tendering process followed	KPMG 2000, 'IT Risk Management Benchmarking V4 Questionnaire. Management of Information', *Information Risk Management*, Aug. 2000
	No management framework	
	No board level accountability defined	
	Low level of control in outsourcing management	
	Re-negotiating contracts based on previous contract instead on market prices	Lacity, Mary, 2002, 'Lessons in Global Information Technology Sourcing', University of Missouri, St.Louis, *IEEE,* Aug. 2002 (26 – 33)
	Excess fees for services assumed were under the baseline umbrella agreement	
	Not understanding the market options when selecting the best supplier	
	Not understanding the various Outsourcing types/options	
	Inflexible to changing business needs	
	Continious service level failure	
	Joint venture is not attracting/keeping external customers	
	Not managing the user-supplier interface	
	Outsourcing noncore activities that might be future competitive advantage	
	Loose or standard agreements	
	No change mechanisms in contracts (realignment points, fluctuating volume of demand, etc)	
	Contracts term too long term	
	Not keep critical core competencies in-house (IT Governance; Business requirements; ensuring tech ability and architecture & managing external suppliers)	
	Assesing Application Service provision outsourcing with unique assessment criteria	Kern, Thomas, Willcocks, Leslie P. and Lacity, Mary C., 2002, 'Application Service Provision: Risk assessment and mitigation', *MIS Quarterly Executive* Vol. 1, No. 2., June 2002, University of Minnesota
	Lack of maturity and experience to manage outsourcing	

	Poor transition planning & management	
	Suppliers lack of maturity and experience in Outsourcing	
Poor communication between the parties	Barriers in organisation that impede communications	Watkins, Michael D. and Bazerman, Max H., 2003, 'Predictable Surprises: The Disasters you should have seen coming', *Harvard Business Review*, March 2003 (72 – 80).
	Organisational silos that disperse information and responsibility	
Awareness of supplier's financial stability/health	Supplier has inappropriate/unstable Sources of funding	Lehmann, Carl, 24 Oct. 2003, 'Assessing Supplier Risk: Part 1', MetaGroup Research Delta 2574
	Supplier has insufficient capital available	
	Supplier's Capital "burn rate" too high	
	Supplier's projected breakeven points are very high	
	Supplier's unviable pricing models	Cosgroe, Lorraine, 2003, 'Maximising Value from IT Vendors. Ware.' 4 Nov 2003, CIO Research Reports
	Suppliers has poor track record with other customers	Steenstrup, K., Kolsky, E., Thompson, E., White, A., Purchase, E. and Topolinski, T., 4 June 2003, 'How to Assess an Application Supplier's Financial Stability', Tactical Guidelines TG-19-7111, Gartner
	Supplier has a negative Income Statement	
	Supplier's Financial results compare poorly with competitors in industry	
	Supplier share price is volatile	
	Supplier has low number of new deals (per quarter)	
	Spplier's 2 largest shareholders has low profit	
	Supplier's Revenue per employee is inappropriate	
	Supplier's service offerings □onsist of too many low margin services	
	Supplier is exposed to many Foreign exchange transactions /accounting	Mphasis, 2002,'Management discussion of risks and concerns'
	Supplier Liquidity is low	
	Supplier is using expensive funding for large capital expenditure	
Insight into supplier's future survivability	Supplier does not have a clear Product vision	Steenstrup, K., Kolsky, E., Thompson, E., White, A., Purchase, E. and Topolinski, T., 4 June 2003, 'How to Assess an Application Supplier's Financial Stability', Tactical Guidelines TG-19-7111, Gartner
	Supplier has poor investment decision making ability	
	Predicted life expectancy of supplier is short	Kliem, Ralph, 1999, 'Managing the risks of outsourcing agreements', *Information System Management,* Summer 1999
	Supplier is dependent on large % of income from few large customers	Mphasis, 2002,'Management discussion of risks and concerns'
	Supplier only play in one vertical market	
	Supplier support is geographical concentrated	
	Supplier has poor international operations	
	Supplier has outstanding delivery disputes with customers	
	Supplier has too many fixed price contracts	
	Supplier is offering massive discounting	
	Supplier has high Merger & Acquisition activity	
	Supplier is unable to attract and retain professional talent	
	Supplier only offer low margin products	
Supplier's inappropriate solution/product or service offering	Niche technology/solution with no alternative suppliers	Cosgroe, Lorraine, 2003, 'Maximising Value from IT Vendors. Ware.' 4 Nov 2003, CIO Research Reports
	Poor software quality that requires many patches	Desmond, Paul, 2003, A better way to deal with vulnerabilities. Earthweb. 10 July 2003. Jupitermedia Corporation

Undisclosed information of suppliers internal operations	Inability to work with other suppliers during project implementation	Cosgroe, Lorraine, 2003, 'Maximising Value from IT Vendors. Ware.' 4 Nov 2003, CIO Research Reports
	Supplier is overselling its capabilities for software development	Kern, Thomas, Willcocks, Leslie P. and Lacity, Mary C., 2002, 'Application Service Provision: Risk assessment and mitigation', *MIS Quarterly Executive* Vol. 1, No. 2., June 2002, University of Minnesota
	Poorly selected Sub-contractors/3rd party	
	Supplier has insufficient Security Policy	Goodwin, Bill, 7 Nov. 2003, 11 'September attacks key driver for IT security investment, survey finds', *ComputerWeekly*.com
	Unstable Executive Management	Lehmann, Carl, 24 Oct. 2003, 'Assessing Supplier Risk: Part 1', MetaGroup Research Delta 2574
	Supplier's policies and procedures are not clearly counicated	Institute of Directors, 2002, 'King Report on Corporate Governance of South Africa 2002', Centre of Directorship and Corporate Governance
	Operating environment – customer base & potential	
	Supplier has high % of new personnel	
	New or revamped technology	
	Supplier has volatile products acquisitions and disposals including distributorship	
	Bureaucracy affect performance and response times	Segil, Larraine, 1996, Intelligent Business Alliances. How to Profit Using Today's Most Important Strategic Tool, Times Business. Random House. New York
	Supplier's disaster recovery is insufficient	Mphasis, 2002,'Management discussion of risks and concerns'
	Not understanding business impact of delivery failure	IT Governance Institute, 2002, Management Guidelines DS2 Delivery and Support. Managing Third-party Services, 3rd ed., p. 64, 65
	Parties do not have a shared product vision	Software Engineering Institute (SEI) 2003, 'Risk Management Paradigm. Risk Management Overview', Carnegie Mellon University, Pittsburgh
	Supplier does not have a forward looking view on its service/product offerings	
Supplier's lack of Enterprise risk assessment	Not clearly understand role of suppliers in the IT value chain	MetaGroup, 2003, 'Refining Information Value from Supply Chains', MetaGroup IT Leadership & Value Management Newsletter, Dec. 2003
	Not continuously monitoring supplier exposure over time	Lehmann, Carl, 24 Oct. 2003, 'Assessing Supplier Risk: Part 2', MetaGroup Research Delta 2575
	Failure to update business continuity plans to adjust from supplier's service delivery failures	Lehmann, Carl, 24 Oct. 2003, 'Assessing Supplier Risk: Part 1', MetaGroup Research Delta 2574
	Not using suppliers that provide New or fresh insights	Cosgroe, Lorraine, 2003, 'Maximising Value from IT Vendors. Ware.' 4 Nov 2003, CIO Research Reports
	Fixed pricing models based only on technical implementation and not value delivery or business gainshare	Cosgroe, Lorraine, 2003, 'Maximising Value from IT Vendors. Ware.' 4 Nov 2003, CIO Research Reports
Supplier's non-compliance to Legal and Regulatory requirements	Poor Corporate Governance and business risk management	IT Governance Institute, 2002, Management Guidelines DS2 Delivery and Support. Managing Third-party Services, 3rd ed., p. 64, 65
		Institute of Directors, 2002, 'King Report on Corporate Governance of South Africa 2002', Centre of Directorship and Corporate Governance
Supplier breach confidentiality	Insider trading due to access to confidential partner information	Naidoo, Ramani, 2002, *Corporate Governance*. Double Storey Books, Juta, Cape Town, South Africa
Supplier's lack of service Availability & Reliability	Poor Systems & Internet availability from ASP supplier	Kern, Thomas, Willcocks, Leslie P. and Lacity, Mary C., 2002, 'Application Service Provision: Risk assessment and mitigation', *MIS Quarterly Executive* Vol. 1, No. 2., June 2002, University of Minnesota
Supplier's poor responsiveness to risk	Under or over pricing	Varon, Elana, 2003, Getting the best from your vendors (What really works). CIO, 1 Nov 2003
	Supplier's resource availability	Conversation with IBM Consultant
Supplier's external organisational	Supplier Merger and Acquisition activity	Lehmann, Carl, 24 Oct. 2003, 'Assessing Supplier Risk: Part 1', MetaGroup Research Delta 2574
	Exposure to the effects of Lawsuits against supplier	

accountability	Supplier's status regarding Regulatory bodies it reports or needs to comply to	
	Supplier is not managing its supplier Partnerships or Strategic Alliances	
	Supplier is not complying to Regulatory requirements	Mphasis, 2002,'Management discussion of risks and concerns'
Supplier's product flaws	System security flaws	Coles, Robert S. and Moulton, Rolf, 2003, *Operationalizing IT Risk management,* 0167-4048/03, Elsevier

Appendix B - Case Study ICT Supplier Key Relationship Vulnerabilities

(Due to confidentiality of information, reference details only available on special request)

Vulnerability Category	Vulnerability	Reference
Poor service agreements and management thereof	Only short term view of SLA performance and not trend	Dashboards
	Ineffective SLA level problem solving	
	No specific focus on mission critical SLA's	
	Reliability of service not improving	T2
	Volatile/non-stable service delivery	
	Inability to do analysis of performance	D10
	Weakness in the SLA's	T15
	No Penalties in SLA's	G5
	Persons that set-up SLA also measure it	Int. 6
	Inappropriate SLA measures	
	No SLA's when handed over to production	D20
	SLA's not derived from contract	Int. 5
	All SLA's are at technical levels	G5
	Processes and procedures lacking	T10
Poor contracts and management thereof	Unmanaged Strategic Alliance expectations	Strategic Alliance MOU's
	Weak or inappropriate Initiatives/project agreements	
	Poor Initiatives/Project delivery agreement	
	No Confidentiality agreement relating to 3rd party use of information	
	Not explicit on which country's Governing laws is the contracting basis	
	No Confidential Information usage clause/agreement	
	No view of Initiatives/Project performance	Dashboards
	Re-active contract renewal	
	Contract content agreed, but not actually signed	T9
	No consideration for exit clauses or terminations	T12
	Non-performance is not considered and formalised	
	Too many contracts - ineffective management	T14
	Unmanaged "usage" contract that effects budget	T17
	No Master agreement to cover essential static basics	G5
	Contracts with flexible currency	Int. 5
	Re-active/late contract assessment when up for renewal	
	Not managing contract lifecycles	
	Inappropriate licensing agreement	M3
	Contract and details not communicated to Project Manager	Int. 4
	Inappropriate contract that does not reflect actual costs	Int. 6
	No penalties or rewards in contracts	
	Rigid contracts that cannot be adjusted to reflect what we want/use	
	Not have a contract portfolio view	Int.3
	Contract period too long	Int. 2
	Contract agreed, but not signed	I16
Inappropriate and poor service delivery monitoring	Not reviewing projects and assignments	Strategic Alliance MOU's
	Project/Initiative status overview	Dashboards
	Inconsistent strategic/overall monitoring	
	Non SLA services MTTR high	T2
	Non SLA services high failures	
	3rd Party services influence are unclear	T10
	Not all projects is based on direct financial benefits	T14
	Poor project controls	G5
	ineffective contract management	Int. 5
	Deficient technology update reports	D20

Inappropriate and poor Service delivery reporting	Focus on activities/initiatives/projects in isolation and not across the enterprise	Dashboards
High level of dependency on technology	Supplier technology has a high level of embedded ness in the technology architecture	T1
	No internal awareness of the supplier relationship	T7
	Niche solutions provider	
	Informal communications	T10
	High level of interdependency of technologies	Absa Strategic Alliance measurement. 3 Nov 2003
	High level of Authentication and Authorisation of supplier into your systems	Absa Group IT Road show
	Reciprocity	Int. 3 Int. 1
	Interdependency of supplier's technologies with other technologies	I20,D2
Poor supplier management practices	Joint marketing disagreements	T5
	Not empowering customer staff to understand technical problems	T13
	Supplier is not reporting of all sales & marketing efforts across enterprise	D17
	Not reporting of all formal engagements	
	Supplier relationship is build only on personal levels	Int. 4
	Not keeping abreast of global economic & ICT supplier trends	Int.1
	Ad hoc or once of due diligence of supplier	Int.6
	Country risks	Int. 2
	Disconnect between SBU/GSF requirements/projects	I16
Implementing New or Complex Technology	Leading edge technology	T1
	Disregard/ignorance of Architectural direction & standards	I16
	Poor co-ordination between systems interfaces	
	Too much hands off on project	I17
	Experimental ventures might not have value	Strategic Alliance MOU's
Poor quality control in implementing and managing technology	Poor project management and/or planning	T2, Int. 6
	Multiple software from different vendors in technology domain	I17
	Weak risk management on security issues	T12
	Project too large and unmanageable	T13
	No external evaluation of critical work	I17
	No audits on deliverables	D19
	No Post -implementation reviews	D20
	No communications process of confidential info to lower levels	T9
Not nurturing the quality of the Relationship	Dependency on monopoly supplier	T1
	No Good will between parties	Strategic Alliance MOU's
	Deteriorating Co-operation keenness	
	Sharing of information	
	Poor or no Relationship Governance	
	Poor or no Relationship trust	
	Relationship conflict	
	Sharing of Strategic information	T3
	Scrambled Communications	Dashboards
	No relationships owner for accountable relationship quality	
	Supplier has no opportunity to solicit further business	
	Interaction inefficiency	T4
	Diminishing interest of Senior involvement in relationship over time	T8
	Poor accounting (invoice & payment) practices between the parties	T10
	Too few formal discussion	G5
	Relationship interaction with Business at an inappropriate level	I16
	Poor reputation for partnering	Int. 6

	Not managing relationship benefit expectations	
	Not having a shared view of relationship risks	Int. 3
	Not exploit existing technology	Absa Strategic Alliance measurement. 3 Nov 2003
	Not sharing required strategic information	Int. 5
Relationship yields low economic value	Large ICT expenditure with monopoly supplier	T1
	Strategic direction of relationship becomes misaligned	Strategic Alliance MOU's
	Not tracking the benefits of the relationship	
	Not achieving stated benefits from relationship	G1
	Unknown, untapped opportunities from supplier	Dashboards
	Long lead times of initiatives/projects	
	Pipeline of supplier proposals few	T2
	Many small projects with high management costs	T2, G5
	Small benefits from costly efforts	T3
	Inability to stop projects when necessary	T5
	Not levering opportunities from companies in Holdings group	T14
	Not levering opportunities from suppliers relationship network	Int. 4
	Supplier do 1st to market initiatives with competitors	T17
	Supplier not advising on technology trends of the area they play in	D13
	Business case not developed for project	I2
	Project in Progress without Cost Agreement	C1
	Relationship purpose is unclear	Int. 6
	Business benefits of projects not clear	D16
	Only reporting Financial benefits of the relationship and ignoring the non-financial benefits	T14
Flawed outsourcing partnership/s	Supplier has inadequate DRP policy and procedures	G5
	No thorough supplier due diligence before enter into Outsourcing agreement	Int. 6
	Supplier has low maturity to manage outsourcing	Int. 5
	ITO has low maturity to manage outsourcing	
	Outsourcing for wrong reasons	
	Outsourcing core capability	
	Supplier has inadequate security policies and procedures	G5
Poor communication between the parties	Organisational silos disperse information and responsibility	D12
Awareness supplier's financial stability/health	Supplier Poor financial results	D2
	Supplier Poor product development and weak R & D	D7
	Supplier is a private company not obligated disclose financials	Int. 5
	High level of M & A	Int. 2
	Financial instability of supplier's subsidiaries/business in other countries/regions	D13
Insight into supplier's future survivability	Not obtaining expert analysis or advice if supplier survivability is sound	Int. 2
	Supplier Continuous poor financial results	D2
Undisclosed information of Supplier's Internal Operations	Supplier is unaware or not using the appropriate processes & procedures	T12
	Supplier has weak ops problem escalation processes/procedures	
	Supplier's Business Model with 3rd Party is flawed	
	Supplier has to develop it own new policies or policy changes during project implementation	
	Supplier's operational control lies outside country borders	T13
	Supplier's Financial Accounting practices and reporting differ substantially	T14
	Supplier has insufficient skills training and resource planning	D4
	Supplier's Service delivery operating model and org structure is flawed	I20

	Supplier's poor Corporate Governance and Accounting practices	Int. 6
	Suppliers undisclosed Merger & Acquisitions activity	
	Supplier keeps insufficient stock levels	I10
	Poor time to market - Project implementation - history	Absa PFS
	Supplier has unreliable Procurement process	I7
Supplier's inappropriate solution/product or service offering	ITO has little power to influence solution/product offering for needs	T1
	Supplier technology or implementation practice is causing new security issues	D5
	Product functionality not leveraged	D20
	Supplier gives poor advice and have low knowledge of needs	Int. 4
	Supplier Marketing/Selling inappropriate Technology	Dashboards
Supplier's lack of Enterprise risk assessment	Service failures have a high impact on the Enterprise	T2
	Indirect impact projects have on the larger enterprise	Strategic Alliance MOU's
	Relationship does not deliver promised value	
	Large financial exposure to the Supplier	Dashboards
	Poor implementation planning of Initiatives/Projects	
	Business Continuity is not part of project/service delivery	T9
	Only ICT participation in Strategic Supplier Meetings	T11
	Supplier does not recognise or understand Business priorities	G5
	Supplier used as Strategic Advisor	I17
	Business consequences of technology	I21
	Slipping on Critical timelines of projects	
	Not measuring business impact of project/service delivery	Absa PFS
	Suppliers implementation approach is inappropriate	
	Supplier develops the business case to solicit funding of project or solution	C4
	Insufficient knowledge transfer for assessing business impact on projects/technology implementation	Int. 5
	Not having a shared view of business risks	Int. 3
	Not categorising suppliers to manage relationships appropriately according to business impact	G6
	Not calculating business cost of project slippage	D18
Supplier's non-compliance to Legal and Regulatory requirements	Acting in manner that might legally be construed as being one entity	Strategic Alliance MOU's
	Breaching competition laws	
	Intellectual Property rights ownership not agreed	
	3rd party non-compliance to legal requirements	Int. 6
	No policy and regulatory risk assessment	T12
	Contract in exit clause if marginal non-compliance	Int. 4
	BEE fronting	G5
Supplier breach confidentiality	Supplier shares Enterprise Confidential Information inappropriately	Strategic Alliance MOU's
Supplier's lack of service Availability & Reliability	SLA not linked to seasonal ebbs and flow	Int. 4
	Not contractually agreed during pilot or while developing per phase	Int. 6
Supplier's poor responsiveness to risk	Not having priority customer status with the suppliers	T1
	Supplier is not escalating issues, risks to appropriate levels	Strategic Alliance MOU's
	Supplier not available during peak service requirements e.g. for additional capacity	I15
	Not making virus patches available fast enough	Absa Group IT Road show
	Supplier does not apply or share best practise	I19
Supplier's external organisational accountability	Supplier BEE non-compliance	T5
	Supplier is not taking part in industry forums	I15
	Supplier uses 3rd parties inappropriately	G5
Supplier's product flaws	Extensive customisation of technology products	I19

	Supplier avoids Open Standards	I21, Int. 2
	Hardware/component failure	Absa Group IT Roadshow
	Bug/s in software	
	Continuous re-active patching	I23
Large financial exposure to supplier	Financial exposure trend - long term or short term misaligned with strategic direction	Dashboards
	Financial exposure in relation to your other suppliers - Balance portfolio of supplier spent	
	large Budget vs Actual variances	
	Project funding not according to Operational blueprint	I18
	Strategic misalignment of projects	D18
	Not using a supplier portfolio to spread exposure	Int. 6
Supplier's incompetent service delivery	Supplier focus on one level (strategic, tactical or operational) only	Strategic Alliance MOU's
	Supplier does not do Strategic level problem solving	T4
	Supplier has unresolved disputes with 3rd parties	T17
	Supplier is unresponsiveness or incomplete RFP/RFI	I17
	Low service delivery capacity and sustainability	Absa PFS
	Supplier has deficient Skills & Knowledge	
	Supplier has poor capability to deliver service	Int. 3
	Supplier is developing poor IT solutions	I22
Supplier compromises its integrity	Supplier behave unethically	Int.2
	Solicitation of staff	Strategic Alliance MOU's