Law and Technology 2009/2010

Master Thesis

Topic: Continuity in Information Technology Outsourcing

Desislava Valentinova Stankova-Bogoeva

ANR: 434659

E-mail: d.v.stankova-bogoeva@uvt.nl

Thesis supervisor: prof.mr.drs. C. (Kees) Stuurman

TABLE OF CONTENTS

ABSTRACT

Lately, IT Outsourcing (ITO) has become a key business strategy and market trends such as multisourcing and globalization have made the outsourcing relationship even more complex. Considering the growing strategic value of the ITO projects for customer organization, the need to identify and manage all risks endangering the outsourcing relationship and to take the necessary measures for ensuring business continuity, becomes indisputable.

The intent of the present study was to research contractual instruments to ensuring service and business continuity of the customer in an ITO project, as the general legal framework currently does not provide specific ITO continuity related solutions. This thesis endeavors to show that tools such as Back-up and Disaster Recovery provisions, Software Escrow Agreements, Step-in Rights and Exit Provisions, complemented by an evolutionary IT project management, are among the key efficient measures applicable when continuity is targeted.

It was concluded however, that, due to numerous legal or practical limitations, none of the abovementioned instruments is able to fully guarantee continuity. This gives reasons to recommend that in certain circumstances, when continuity is of top priority for organizations, the decision to outsource should be carefully evaluated against all possible risks, and subsequently keeping IT services in house should be considered.

LIST OF ABBREVIATIONS

ARD = Acquired Rights Directive

BPO = Business Process Outsourcing

BC = Business Continuity

BCP = Business Continuity Planning

CAPEX = Capital Expenditure

COBIT = Control Objectives for Information and Related Technologies

CPU = Central Processing Unit

DoS attack = Denial of Service attack

DR = Disaster Recovery

DRP = Disaster Recovery Plan

DRT = Data Retention Time

EU = European Union

EUR = Euros

FM = Force Majeure

IP = Intellectual Property

IPR = Intellectual Property Right

ISO = International Organization for Standardization

IT = Information Technology

ITO = Information Technology Outsourcing

LoL = Limitation of Liability

MTDL = Maximum Tolerable Data Loss

MTPD = Maximum Tolerable Period of Disruption

OPEX = Operational Expenditure

RFP = Request for Proposal

RPO = Recovery Point Objective

RTO = Recovery Time Objective

SaaS = Software as a Service

SC = Service Continuity

SLA = Service Level Agreement

SoW = Statement of Work

SP = Service Provider

SPoC = Single Point of Contact

TUPE = Transfer of Undertakings (Protection of Employment)

USA = United States of America

Introduction

Outsourcing is not a new practice, yet many different understandings exist about what outsourcing exactly is. It is often compared to a marriage relationship and just as approximately half of all marriages fail, outsourcing failure rate tends to be considerably high too. Since it is the focus of other scientific and practical fields to explain the reasons and mechanism of outsourcing relationship failure, this study is aiming at bringing into light the available tools and instruments for dealing with failure in such a way that business and service continuity is achieved.

In order to overcome existing inconsistent understandings about the essence of outsourcing, a clear definition and diversification of the most common types should be considered. Outsourcing is generally a transfer of certain activities that a company has been providing internally to a third party provider who assumes responsibility for their performance, according to agreed service levels and against agreed price. Along with the transfer of activities, transfer of people, assets and contracts is often involved. Outsourcing is usually provided onshore (customer and provider are located in the same country), nearshore (in a nearby country) or offshore (in a far away country, typically India, Philippines, etc.). The most common forms of outsourcing are Information Technology Outsourcing (ITO) and Business Process Outsourcing (BPO), which despite the multiple common features, show many differences as well.

ITO is historically the earlier form of outsourcing and officially dates back to the 1960-s service bureau arrangements. It generally includes outsourcing activities such as: data center and systems infrastructure, voice and data networks, telecommunications, applications development, applications support and maintenance, server and desktop environments, IT project management, contract and vendor management, support, help desk and call center, IT training, disaster recovery and business continuity, as well as IT procurement.[1] Lately the scope of ITO goes even broader by including new services such as Software as a Service (SaaS) delivered through Cloud Computing infrastructure, website/e-commerce systems, etc.

[1]Mark Lewis, Computer Law: The Law and Regulation of Information Technology. Information Technology Outsourcing and services arrangements (6th edn, OUP, 2007) pp.139-182.

BPO is defined by Gartner as "the delegation of one or more IT intensive business processes to an external provider that, in turn, owns, administers and manages the selected processes, based on defined and measurable performance metrics". [2] BPO is sometimes considered to be the outsourcing form that is more tailored to customer`s needs, compared to ITO, which can be comoditisized to a certain extent for a broader range of customers.[3] Although BPO is showing significant growth in terms of numbers and significance, the present study will focus only on ITO within the scope described above, because only typical IT aspects related to continuity are targeted due to the length limitation of the study.

Typically, notwithstanding specific companies` needs and strategies, customers choose to outsource for a certain set of reasons. The most commonly mentioned are CAPEX[4] and OPEX[5] costs savings, access to supplier`s specific expertise, skills and infrastructure, opportunity to focus on "core" activities, access to new technologies and innovations, IT process and infrastructure improvement and standardization, risk mitigation by signing a legally binding contract for provision of certain service levels, etc.

According to Computer Economics "2009/2010 IT Outsourcing Statistics" currently between 19% and 33%[6] of all organizations in North America practice some kind of IT outsourcing. Furthermore, the typical organization spends about 5-6% of their IT budget on outsourcing services.[7] According to AMR Research Inc. report approximately 80% of companies plan to increase their amount of IT outsourcing or keep it the same level[8]. The above numbers clearly show the size of the outsourcing activities and the exponential growth of the outsourcing market that has only shown certain temporary slowdown during the economic crisis of 2008 – 2009.

[2] Gartner on outsourcing.

[3] Bharat Vagadia, Outsourcing to India – a legal handbook (Springer-Verlag, Berlin Heidelberg, 2007), pp. 1-9.

[4] Capital Expenditure – the expenditures used by organizations to buy fixed assets (such as IT hardware, office furniture, etc) or to add value to fixed assets.

[5] Operational Expenditure – the expenditures used by organizations to run and maintain their business (such as office expenses and utilities, maintenance fees, IT hardware supplies, transportation, etc.)

[6] Depending on the type of IT function outsourced.

[7] AMR Research 2009 Outsourcing statistics, <http://www.rttsweb.com/outsourcing/statistics/>

[8] SearchCIO.com, Feb 2010.

However, despite the optimistic hopes, the majority of outsourcing projects do not fulfill the initial expectations conferred on them. The two main indications of failure include premature termination of outsourcing contracts and dissatisfaction with outsourcing results, even when contracts are not terminated.[9] According to statistics over 50% of outsourcing contracts are prematurely terminated[10] and approximately the same percentage is applicable to the number of customers dissatisfied with the project results.

With the development of the outsourcing market, ITO has evolved to a second and third generation of outsourcing.[11] Nowadays, outsourcing has become a key business strategy and market trends such as multisourcing[12] and globalization, have made the outsourcing relationship even more complex to manage and maintain. Considering the growing strategic value of the outsourcing projects for the customer organization, the need to identify and manage all foreseeable risks endangering the outsourcing relationship and to take the necessary measures for ensuring business continuity, becomes indisputable.

Generally, the outsourcing projects encounter the following type of practical problems such as loss of everyday management control over IT processes and infrastructure, high costs for managing the outsourcing relationship, security vulnerability (especially in terms of confidential information), transfer and subsequent loss of key expert employees, customer dependency on crucial business service performance, quality problems, cultural differences and incompatibility between customer and provider, insourcing[13] complications, etc. Furthermore, incidents such as loss of important data, natural disasters or unresolved communication problems between the parties, even though not always followed by premature contract termination, can introduce significant risks for the service continuity of the customer.

---

[9] Achim Hecker, Hendrik Kohleick, 'Explaining Outsourcing Failure' (October 27, 2006). <http://ssrn.com/abstract=939411>

[10] DiamondCluster International, '2005 Global IT Outsourcing Study', (2005) <http://www.diamondconsultants.com/PublicSite/ideas/perspectives/downloads/Diamond2005OutsourcingStudy.pdf> , accessed 22.04.2010.

[11] Compared to the first generation, which characterized with cost reduction being the main reason to outsource and the services to be outsourced were only non-core day to day IT functions, assigned to a single provider

[12] Multisourcing defined as breaking the outsourced functions into multiple providers, as well as keeping some of them in-house as a strategic decision. Companies like General Motors and ABN Amro have currently switched to multisourcing model.

[13] Assuming back in house responsibility for the outsourced activities

Along with the practical problems, a number of legal problems regarding continuity in IT outsourcing are observed, such as IPR ownership and protection, insolvency complications, etc. The outsourcing activities are not statutory regulated as such by legislative acts that reflect the specifics of the process, and normative regulations are rather spread across multiple generic acts covering different aspects of outsourcing relationship. There is further lack of court practice about outsourcing disputes, since parties are relating the dispute to the court when the relationship is fully derailed. Additionally, courts are hesitant in deciding about the complexity of the case and even more specifically, they are cautious in issuing injunctions ordering the parties to perform what is due according to the contract (unlike ordering them not to do something)[14]. Many legal problems, such as the execution of foreign judgments occur with offshoring, where both parties are located in distant parts of the world and their legislation and case law applicable to outsourcing activities differ significantly.

It must be noted that statutory framework as such does not offer adequate legal solutions to the specific outsourcing problems, thus additional tools and instruments, ensuring business and service continuity in ITO, should be used. Such tools are incorporated in the outsourcing contract, seen as the instrument for day-to-day managements of the relationship and the most efficient tool for protection of the interests of both parties. The term "outsourcing contract" used in the present study includes not only the master contract, concluded by the parties, but also all the schedules, attachments and agreement that cover different aspects of the outsourcing relationship.

The IT outsourcing continuity topic is current due to the fact that outsourcing projects are growing in number and complexity by involving more than one service providers, as well as acquiring strategic value for the organization. It is relevant because outsourcing is facing a lot of risks and challenges and a high failure rate, as demonstrated above, therefore the need to ensure service and business continuity is significant. At the same time only a limited number of in-depth researches on this topic have been conducted, leaving a vast number of practical and legal issues that are not exhaustively studied. It is perspective because, as outsourcing projects are expected to further diversify and develop and the high complexity

[14] Richard Hawtin, 'No-one ever sues on an outsourcing contract' (2007) C.T.L.R., 13(3), 88-90.

and failure rate to continue growing, a detailed review of the contractual relations covering continuity would be undoubtedly necessary.

Subject of the present research are the contractual means of ensuring continuity in IT outsourcing projects. The goal of the study is to analyze the existing tools and instruments able to provide continuity in case of incidents and disruptions of the IT outsourcing relationship and to offer the most effective continuity solutions. Conformity with statutory provisions, high level of protection of the parties and reflection of the current state of art by the outsourcing contract are considered when analyzing the contractual outsourcing relationship. The study is conducted generally from customer perspective, yet keeping in mind possible implications for the continuity of the suppler as well.

The research methodology strategy is based on the goal of the study, i.e. to analyze the existing tools and instruments able to provide continuity in ITO and to recommend most effective solutions, and it mainly includes use of qualitative data, as analysis and efficiency of continuity solutions in respect to outsourcing projects could not be successfully measured in numbers. The main research technique used is documentary research (including legal research documents, operational and technical studies, as well as real life outsourcing contracts), combined with discussing relevant aspects of the topic with professionals in the field. While semi-structured discussions with outsourcing professionals have been used mainly to validate the reliability of the collected data, the documentary research has been the primary source of collecting information.

Chapter 1 deals with the background of ICT outsourcing continuity topic and focuses on general types of risks and the most common reasons for failure of the ITO projects. It further explains the process of business continuity planning, including risk assessment practices, business impact review, contingency considerations and recovery strategies. It also outlines the characteristics of the outsourcing contract generally applicable for ITO. Chapter 2 offers a general review of the non-IT specific legal measures for risk allocation incorporated in the outsourcing agreement, including limitation of liability and indemnification clauses, force majeure, insurance requirements, insolvency provisions and others. Chapter 3 focuses on generic measures for ITO project control, available to the parties before the incident occurrence, such as detailed scope of work of the project, service level agreement, clear and

comprehensive project management plan, etc. Chapter 4 provides an in-depth analysis of contractual tools that deal with specific ITO continuity problems, such as back up and disaster recovery agreements, escrow agreements, step-in rights and exit provisions.

1. Background and theoretical framework

As outlined in the Introduction, although progressively growing in scope and business significance, outsourcing bears a number of risks, both operational and legal, which create the need of adoption of effective risk management strategies in order to provide business and service continuity for the customer. The most common risks for an outsourcing project, general and IT specific, will be presented in this chapter, together with an overview of a risk management approach. The characteristics of the outsourcing contract, as the most practical legal solution to avoid and mitigate the risks, will be outlined briefly, together with an overview of the applicable legislation and the literature on the subject.

1.1. Business continuity and IT service continuity

In order to determine legal measures and instruments applicable to ensuring continuity, a clear cut definition and understanding of the terms Business Continuity (BC), IT Service Continuity (SC) and Business Continuity Planning (BCP) must be established.

Business continuity is often defined as the process of ensuring that organization`s business critical functions and activities will be available to their customers, partners, vendors and all other stakeholders. It is a methodology used throughout the entire organization and is based on development and use of a set of standards, policies and procedures, needed to ensure the service, consistency and recoverability. [15] Although often mistaken with disaster recovery, BC is the broader notion that includes disaster recovery. IT service continuity is a part of business continuity that refers to ensuring availability of IT functions and IT departments in an organization.[16] It can be reactive, in case of an incident, but also proactive, i.e. preventing risks from occurring. Business continuity planning is drafting of a plan of recovery and restoration of an organization`s business critical functions in case of an interruption within a certain time limit after an incident or disaster.[17]

The first step in BCP is Business Impact Analysis. It consists of identifying all business functions of the organization and assigning a certain level of importance to each one, by defining them as business critical and non-critical functions. A function can be determined as

[15] Business Continuity, <http://en.wikipedia.org/wiki/Business_continuity> accessed 11.04.2010

[16] ITIL Service continuity.

[17] Business Continuity Planning, <http://en.wikipedia.org/wiki/Business_continuity_planning> accessed 11.04.2010

critical if its loss or temporary disruption or delay is unacceptable for the relevant stakeholders. Criteria for acceptability could be the cost of recovery solutions, legal requirements, business reputation, etc. Recovery point objective (RPO) and Recovery time objective (RTO), meaning respectively the acceptable latency of data to be recovered and the acceptable time needed to recover the function, are usually defined and Maximum tolerable data loss (MTDL) and Maximum tolerable period of disruption (MTPD) are assigned. This BCP finishes with an analysis of the recovery requirements for each business critical function.[18]

Further step in business continuity planning is risk identification and assessment. Risk assessment is part of risk management and consists of determining risk probability and the magnitude of the adverse effects. In terms of business continuity it means identifying all possible incidents that could result in loss or delay of a business critical function and activity.[19] A company can use different casual or formal risk assessment methods, including specialized software. Results of risk assessment must be documented and need to receive the support of company management and all relevant organization levels, in order to create an adequate business continuity plan.

Contingency considerations should also be evaluated. A contingency is a planned substitute for a resource that incidentally becomes unavailable, such as data loss for example. In case of an incident or a disaster, contingencies should be available for the business critical functions of the organization, as defined in the business impact analysis. A contingency should be carefully identified, easily available and suitable to replace the unavailable resource.

Identification of recovery strategies is another crucial step in BCP. This phase is based on the information gathered and analyzed in the business impact analysis and the contingency considerations. The recovery strategies should offer a temporary complete or almost complete solution to the problem and the choice of the most suitable strategies is a

[18] Ibid: Business Continuity Planning (n 17)

[19] PACE, 'Business Continuity Planning Guide', <http://www.ogc.gov.uk/documents/PACE_-_BCPG.pdf> accessed 12.04.2010.

consideration of cost, speed and level of recovery[20] - the faster the recovery, the more expensive the solution.

The process ends up with drafting the BC plan, testing, reviewing and revising it on a regular basis.

1.2. Outsourcing risks

Outsourcing risk management strategies have been extensively studied and different approaches have been offered in the literature. However, in order to successfully ensure business continuity by mitigating the risks with a number of contractual provisions and plans, risks should be clearly identified first. Irrespective of the specific outsourcing project or technology, the risks occurrence and failure rate is usually higher in the following situations: in larger organizations with strong dependence on IT functions and business processes; when offshoring, due to the additional cross-border projects` complications, compared to nearshoring; when multiple service provider strategy is selected, due to the growing complexity in managing and coordinating all providers, compared to a single prime contractor.[21] A successful approach to risk categories` identification will be by following the outsourcing lifecycle[22], as well as seeing them from a perspective whether the reason for failure is based on a disaster event or it is just an inherent IT projects problem. A third category of risks typical for cross-border projects is also examined in order to outline the additional complexity immanent to those projects, and more specifically offshoring.

1.2.1. Risk differentiation based on ITO project lifecycle

1.2.1.1. Outsource decision risks

In the phase of deciding whether an activity should at all be outsourced, the customer should consider their business needs and strategies, as well as some objective conditions such as the outsourcing market and offerings and the specific legal requirements relevant for this market. The impact of outsourcing internal activity should be assessed, as well as the extent to which that activity is business critical for the customer. The consequences of

[20] Ibid: Business continuity planning guide (n 17)

[21] Ibid: Explaining outsourcing failure (n 9)

[22] Hunton & Williams, Marsh, 'Risk Management in Next Generation Outsourcing' (2008), <http://www.hunton.com/files/tbl_s47Details%5CFileUpload265%5C2125%5COutsourcing_white_paper_2.22.08.pdf> accessesd 11.04.2010.

possible service disruption should be further evaluated. It is also of a great importance to assess customer`s own experience with outsourcing – the function to be outsourced, the technology or the process. Lack of customer experience with outsourcing bears risks for the continuity of both the customer and the provider. Further problems at the stage of the lifecycle include the overall availability of a service provider on the respective market that could successfully perform the outsourced activities, thus a selection strategy needs to be adopted. Additionally, legal compliance issues should be evaluated - therefore the failure probability, if not involving a legal counsel at that initial stage of the outsourcing process, is much higher. Finally, a strategic decision should be taken as to the risks of not outsourcing the activity, especially concerning customer`s qualification and expertise to perform the service in house if it is business critical, against the possible drawbacks of the positive decision.

1.2.1.2. Service provider selection risks

The most significant risk for the outsourcing project at this stage is related to the clear definition and validation of the customer requirements and expectations. Premature termination of the outsourcing agreement and project failure are considerably higher in case of ill defined requirements and unclear expectations. Clear and detailed description of the scope of the work to be outsourced, the service levels expected and the draft duties and obligations of the parties, as a fundament for the outsourcing contract, should be included in the Request for Proposal (RFP). Continuity planning should be started at this stage by including continuity planning and recovery planning requirements in the RFP. Service provider`s lack of experience with the function, technology or the outsourcing process as such, as well as financial instability, may also jeopardize the success of the project, thus a due diligence needs to be performed including research, site visits and clear communication at all organizational levels. Since the outsourcing agreement is drawn up and concluded at this stage, it should be well structured and negotiated in order to avoid being stuck in an unnecessary limiting and inflexible contract that does not serve its purpose for years.

1.2.1.3. Operational risks

The operational phase includes a wide set of outsourcing risks that can negatively affect business continuity for the customer, starting with the failure of the provider to provide the services agreed upon. It can be due to financial or other problems leading to bankruptcy and

insolvency, total lack of experience, dependency on failing or badly managed subcontractors, etc. In cases of software development outsourcing for example, insolvency of the provider and subsequent failure to provide, may result in significant business and support problems for the customer, if they are left without a service and without the software source code needed to either continue performing the service itself or transfer it to another provider. Contingency plans, escrow agreements and relevant contractual insolvency provisions are proper instruments to address the abovementioned risks.

Furthermore, even in case of the contractor providing the service, quality issues, as well as inability to determine and monitor the quality of the activities performed need to be properly addressed, thus strict SLA and performance metrics should be elaborated. Over-dependency of the customer and loss of control over business critical functions are also among the operational risks. Lack of working change management procedure is another problem factor.

Additionally, security risks such as unauthorized access to or loss of confidential or business critical information, especially in IT services such as web hosting and application service outsourcing, could lead to a massive service disruption. IPR issues such as cases of infringement or licenses needed from third parties, as well as clear allocation of IPRs created during the outsourcing relationship, should also be taken into account when ensuring continuity. Natural disasters, although out of the control of any of the parties, may also cause service discontinuity, therefore risk transfer and mitigation measures, such as back up and disaster recovery strategies, should be incorporated in the outsourcing contract.

Furthermore, certain types of ITO, such as cloud computing for example, bear their very specific risks[23] like strict dependency on high speed internet connection, single points of failure for data transmission, processing and storage, interruptions in data transmission and uncontrolled environments leading to delays in data restoration, as well as the common risk of guessing passwords based on social networking, thus they require further security and redundancy measures.

[23] Bierce & Kenerson 'Case Study for Legal Risk Management for "CloudComputing": Data Loss for T-Mobile Sidekick Customers', Published: 29.10.2009, <http://www.outsourcing-law.com/2009/10/case-study-for-legal-risk-management-for-cloud-computing-data-loss-for-t-mobile-sidekick-customers/> accessed 18.04.2010.

1.2.1.4. Termination and exit risks

The lack of well defined and clear exit strategy may unnecessarily complicate the intrinsically complex exit process and put business continuity upon great risk. It is thus crucial for the parties to elaborate on a detailed Exit Plan and procedure even before the incident has occurred. Temporary or final step-in rights in case of inability of the provider to perform should be included in the outsourcing contract to ensure maintenance of service provision either by the customer or by an alternative provider.

1.2.2. Risk differentiation based on the nature of the risk event

1.2.2.1. Traditional IT projects risks

Failure to deliver the agreed services which threatens service continuity is often due to certain IT projects problems which usually fall in three categories – people related risks, project management process related risks and technical risks concerning the IT products used, with the first two categories covering the majority of failure reasons. People related risks usually include lack of needed expertise or IT resources, weak project manager, lack of top management support and general lack of stakeholder involvement. Process related risks on the other hand are associated with unclear requirements and scope definition, lack of in-depth project planning and even when project management plans are in place, lack of regular review and update, lack of clear mechanisms for change control, unclear communication, etc.[24]

Traditional IT projects risks can be addresses with series of measures, such as development of detailed Scope of Work and Service Level Agreement, drafting of comprehensive Project Management Plan and other measures that will be outlined in the next chapters. However, the focus of the present study will be more concentrated around continuity specific ITO problems and the contractual instruments to prevent or solve them.

1.2.2.2. Disaster related ITO risks

Disaster related risks are usually associated with unexpected and unavoidable events of natural, social, technical or even financial character. The time and nature of their incidence can be hardly predicted, yet the parties should try to identify them at the project offset and

[24] L. Kappelman, 'Early warning of IT Project Failure: The dominant dozen' (2006), Information Systems Management 2006/23, p.31-36.

take the necessary contractual and operational measures to mitigate their occurrence and consequences when service continuity is a priority.

Such risk events usually include natural disasters like flooding, fires, earthquakes, etc., financial disaster of the provider leading to insolvency, social risks such as loosing key IT staff and any other complications connected with technology, such as computer viruses for example. They can be addressed by a number of specific IT continuity measures such as back-up and disaster recovery provisions, source code escrow agreement, temporary step-in rights or the right to acquire certain assets. Detailed analysis of those measures will be provided in the next chapters

1.2.3. Cross-border project risks

A third main category of risks that needs to be mentioned in relation to ITO is connected with the problems typical for cross-border outsourcing, especially offshoring to destinations such as India for example. Although cross-border outsourcing projects share generally the same or similar risks with the other types of outsourcing, not only certain problematic aspects are more serious when two different legislations meet, but also additional problems may arise.

From a legal perspective offshore projects might face some challenges in respect of execution of foreign judgments or foreign arbitral awards, IP rights protection, selection of governing law, non-compete contractual clauses, liability of the parties, staffing issues, data protection, etc., which most probably will be regulated in a different way in the national legislations of the customer and provider, or even not regulated at all in one of them.

In terms of protecting the continuity of customer`s organization, the problem of enforcement, timely and properly, of foreign judicial acts or arbitral awards should be carefully considered. Although countries like India might allow the enforcement of foreign judgments, it is often a slow and complicated process, and the execution is subject to many conditions.[25] Furthermore, arbitration clauses, seen as a faster and more efficient alternative for judicial solutions, can be incorporated in the contract, yet their enforcement might again

[25] Indian Civil Procedure Code 1908 for example limits the enforcement options to reciprocal territories, which are a very limited number and exclude countries like the USA or the Netherlands. In non-reciprocal territories cases, the foreign judgment must fulfill the requirements of section 13 of the Civil Procedure Code 1908, which can be quite restrictive.

not be a simple and speedy process in typical offshoring countries[26], which undeniably affects customer`s options of maintaining service provision or replacing the provider.

Special attention should be also paid to the IP rights allocation, as sharing and creating IP during the term of the project is very probable. It is of fundamental importance to identify all IP rights and to set clearly in the outsourcing agreement the rules regarding IP ownership between the parties, taking into account the different national legal regimes protecting IP.[27] Although India for example has better IP protection than other offshoring territories such as China and Mexico, it is member of international IP conventions such as the Berne Convention, and has a Copyright Act, its IP legal protection is still considered relatively low compared to the EU or the USA.

1.3. The IT outsourcing contract

The outsourcing project usually lasts for a long period of time, somewhere between 5 and 10 years[28], and includes a complex set of legal and operational issues that need to be addressed by the outsourcing contract. In contrast with the popular understanding that outsourcing is a partnership, it should be taken into account that profit motives for customer and service provider are often not identical, thus the significance of a comprehensive contract, as a legal instrument to ensure both parties` interests are protected, is vital. The contract should address all previously identified risks for business critical functions of the organization. Among its main goals, together with covering topics such as parties` rights and obligations, business, operational, technical and financial issues, is to include a mechanism for change management. Given the vast complexity and long duration of the ITO projects, the successful contract should be complete, clear, flexible and containing options for re-negotiation in case of changes.

[26] Taking again India as an example, it should be noted that the Indian Civil Procedure Code 1908 allows foreign arbitration awards enforcement, but subject to satisfying certain criteria, such as the "public policy criterion", which is very wide in interpretation, thus very restrictive.

[27] Shalini Agarwal, Sakate Khaitan, Satyendra Shrivastava, Matthew Banks `Destination India: offshore outsourcing and its implications` (2005) C.T.L.R. 2005, 11(8), 246-262.

[28] The average contract duration for ITO contracts was 4.7 years in 1995 and increased to 6.2 years in 2003, HI Europe, The UK IT and Business Process Outsourcing Report, <http://exactsearch.com/ipi/IPI.nsf/LookupPDF/trui/$file/trui.pdf>, accessed 11.05.2010.

The standard ITO contract consists of a master contract and a set of agreements. The contract composing strategy could be of a decentralized contract, where the parent company of the customer concludes the master agreement (which includes mostly principles) with the parent company of the provider and the local agreements are subsequently negotiated and drafted by the local offices, covering specific topics such as scope and pricing; or a centralized contract, in which case the master agreement includes all principle and specific topics and the local offices are only allowed to adjust the local contracts to particular local legal requirements, such as for example labor regulations.[29]

A number of key points to be addressed in an outsourcing contract include clear scope of work, definition of services and service levels; measurement criteria and performance metrics; service credits and debits; benchmarking and technology refresh; parties` rights and obligations; acceptance testing; identification of assets to be transferred; employees transfer clauses; contract change management procedure; pricing and payment, duration, liability, insurances; warranties and indemnities; security and data protection; IPR provisions; termination and dispute resolution; competition issues and exit issues, covering service continuity.

Although clear and comprehensive outsourcing contract in its entirety is a key to ensuring the success of the ITO project, when it comes to continuity, specific contractual provisions or agreements play the major role. Different legal remedies to target potential problems with outsourcing may be used by both parties[30], including claims for damages, liquidated damages, relationship termination rights in case of partial or total failure to perform, insurances, insolvency clauses, etc. None of them however, would be able to successfully prevent service continuity disruption, but merely provide a certain kind of compensation for the service loss or delay and serve as a basis for ending the relationship between the parties.

For the purpose of the topic of this study, i.e. effectively ensuring continuity in IT outsourcing projects, the following contractual instruments will be examined in detail: back-up and disaster recovery agreements, software escrow agreement, step-in rights, exit plans.

[29] Ibid: Vagadia (n 3), pp. 15-22

[30] Pinsent Masons, 'User`s Guide to Outsourcing' (2008), pp. 3-8, <http://www.out-law.com/page-364> accessed 11.04.2010.

1.4. Relevant legislation and literature

Defining the applicable legislation varies significantly depending on specific national legal regimes of the parties, a situation that becomes even more complex when they are located in different countries. A basic differentiation can be made between the countries within the Common law system and the Civil law system.[31] This difference should be specifically taken into account when the ITO project involves an organization from a European civil law country and a provider from a typical offshoring destination country, such as India for example, whose legal system is based on the UK common law. However European companies, according to the Rome convention (1980), are free to choose the national state law they wish to govern their contractual relationship. Generally, relevant legislation in reference to outsourcing projects in the EU includes EU transnational legal sources such as Directives and the national legislation of the states concerned. Civil and civil procedure codes, Privacy and data protection acts, IPR acts, Commercial codes and some specific IT laws such as E-commerce acts, E-signature acts are typically the regulatory framework for ITO projects.

Relevant literature is fragmented and limited number of research and practical studies focus on ensuring continuity with legal measures. The available literature is mostly in the form of short articles explaining ITO process, risks and failure or providing practical tips on drafting ITO contracts in general. Most of the literature focuses on offshore projects, assuming they bear the most risks, especially considering the cultural and legal differences between the parties. More in depth studies on legal aspects of outsourcing materialized in books are scarce. Comprehensive and reliable researches focusing on practical legal aspects of ensuring ITO service continuity hardly exist.

[31] Jurisprudence being the main source of legal norms in Common law, while codification and statutes - the main source of legal norms in Civil law.

2. Non-IT specific tools of risk allocation and sharing in the ITO contract

As outlined in the previous chapter, a significant step towards ensuring service and business continuity includes risks identification and assessment. After the risks have been defined and analyzed, proper risk management strategies should be incorporated in the contract. The following are the most typical and effective measures applied to ITO contracts, regardless the technology or services outsourced.[32]

2.1. Nature of the obligations

One of the first things that parties need to consider when drafting the contract is to set the nature of the obligations as such, which would subsequently provide a basis for assessment whether a non-performance has occurred, as well as the respective consequences and liability issues. Parties can choose between two types of approach in this respect – "best effort" obligations or those that require specific results. Setting obligations, which have fixed terms and require particular result, is the preferable option from customer `s perspective, as when the specific term has expired with no performance from the provider, this automatically will put the supplier in default. In comparison, with the best or reasonable effort types of obligations, the customer would have to spend much more effort and time to provide evidence for the non-performance and, yet the result might not always be in their favor.

2.2. Limitation of Liability

Almost all outsourcing contracts include limitation of liability (LoL) clauses, which aim at limiting liability for any indirect, consequential, incident or special damages, even for loss of profits. Financial liability can be limited on a per-event basis, or a total cap of liability (i.e. 1 million EUR) can be fixed for both customer and provider. LoL clauses however mostly favor the supplier in an ITO project, thus, they represent a proper tool for sharing and minimizing risks mostly from provider`s perspective. It is important to consider that according to the Principles of European Contract Law, parties are allowed to exclude their liability for non-performance, except when it is intentional or the limitation is unreasonable.

[32] Ibid: Vagadia (n 3), pp.55-67.

Nevertheless, as outsourcing projects tend to be complex in nature, the provider usually subcontracts part of the services they are not specialized in to third party contractors, such as hardware or software maintenance and support, software development, web-hosting, etc. In such cases, the contract should include a clause that provides liability for the supplier for the acts or omissions of their subcontractors.

2.3. Liquidated Damages

In addition, liquidated damages[33] can be agreed upon in the contract as a compensation tool in case of non performance. They can be set as a fixed amount or a percentage of the sums due for the project. A limit is usually fixed on the total amount to be paid as liquidated damages for both parties, as they traditionally represent the expected loss by the respective party in case of non performance of the other. In order to be enforceable, they should not be punitive and should be a fair calculation of the actual harm suffered by the claiming party.

2.4. Indemnification clauses

Another useful instrument for risk shifting in ITO contracts is an indemnification clause (i.e. "hold harmless" clause). Indemnities represent possible financial compensation or legal protection against any claims arising in connection with the performance of the contract. With outsourcing contracts, a typical indemnity clause can be related to any claims by the supplier employees against the customer, third party claims for IPR infringement, etc. Generally, indemnification clause is triggered when third party rights are negatively affected.

2.5. Disclaimers

Furthermore, disclaimers are usually used in ITO contracts, especially for protection of the provider. Providers usually tend to disclaim the accuracy of advices, reports and data, provided by them, or a failure of business results. However, it is recommended for the customer to resist such clauses, in view of ensuring business continuity. Additionally, a provider may try to avoid providing warranties for the uninterrupted performance of a system or a network, as well as that software is free of bugs or viruses for example, but it is

[33] Liquidated damages represent a contractually fixed amount to be paid by the party in breach of the contract as a compensation for the damages suffered by the other party. This amount is the entire final amount to be paid regarding the damages incurred as a result of the breach.

strongly recommended that customer denies such clauses and rather negotiates strict service levels in a detailed Service Level Agreement.

2.6. Insurance

Additional instrument for risk management in ITO projects is the inclusion of insurance provisions in the contract as a classic risk transfer tool. Standard types of insurances required for the supplier include property insurance for any equipment to be delivered, professional indemnity, errors and omissions insurance, public liability insurance, employer`s liability insurance, etc. and insurance covers amounts can be fixed in the contract.

2.7. Force Majeure

Force Majeure clauses are another way to manage risks with contractual means. They limit either party`s liability for events that are beyond their control and could not have been foreseen and prevented by the non performing party. However, for business critical functions and services, the customer might not want to experience failure or interruption, regardless of the cause of the event, therefore different disaster recovery requirements to be implemented by the provider could be included, as well as a requirement for certain actions to be taken by the provider in case of a force majeure event, in order to ensure service continuity. In any case the customer should seek to reduce provider`s option to use FM provisions as an excuse to cease performing.

2.8. Insolvency provisions

In a situation where the service provider is facing an insolvency event, customer continuity is a significant challenge, as well as the need to either carry on receiving the service from the respective provider or to terminate the contract and replace the provider with a viable one.[34] Although insolvency of one of the parties is usually contractually defined as a termination event, often the trustee of the insolvent supplier might attempt to oppose the termination, intending to maintain the operational activity of the provider in order to maximize their estate. The customer organization will then be facing the options of waiting for the provider to be in default, which is not the best solution from a continuity perspective or to activate their termination for convenience clause, if present, which however, might be

[34] Norton Rose Group, `Satyam: what are the consequences for offshore outsourcing?` Published 16.01.2009, <http://www.nortonrose.com/knowledge/publications/2009/pub19079.aspx?lang=en-gb&page=all>, accessed 12.05.2010.

a considerably expensive solution, because of the high termination fees usually associated with its activation.

A more reasonable solution to the insolvency problem in ITO projects would be the inclusion of "early warning termination triggers" [35] in the outsourcing agreement that can allow the customer to terminate and replace at an earlier stage, when certain signs indicate the insolvency probability, before even the provider has already disrupted the provision of the services. Such indications may include certain low credit ratings of the provider, or any other event that gives rise to a reasonable doubt that the provider will be able to maintain their financial stability or continue performing under the agreed contract requirements. Although very promising, a specific weakness of this approach is that many IT service providers do not have official credit ratings, while further subjective criteria might be strongly opposed by the supplier. Still, if early warning insolvency criteria can be negotiated between the parties, such a termination option will enable the customer with a valuable tool.

Another concern with insolvent providers is related to the provision of transition services and assistance. As much as most customers will be tempted to require such assistance free of charge, it could be again opposed by the trustee, who can attempt to decline the services at all due to the lack of any compensatory return. In order for the customer to receive such a crucial assistance without any disturbances, it might be wiser to provide payment for it.

Moreover, several other key concerns regarding continuity should be considered and reflected in the agreement in case of a provider going insolvent, such as how to protect the customer from a trustee trying to prevent it from using intellectual property products licensed by the supplier, any problems with enforcing a source code escrow agreement, or the existence of certain legal obstacles for purchasing back any assets needed from the supplier. Going into the details of insolvency provisions however, would mean exploring a way too broad topic, which is not the focus of the current thesis, especially considering that resolution options are significantly dependent on the specific national insolvency legislation governing the contract, and therefore, the main insolvency issues are only sketched.

[35] John Beardwood, 'Bankruptcy & Insolvency Risks in Outsourcing Transactions: A Wake-Up Call' (2008), <http://www.fasken.com/files/Publication/e9cc8578-6707-4514-a86c-59b4b806b358/Presentation/PublicationAttachment/2d93dd77-ea7f-4bc9-a8aa-0e6078f63b8a/Bankruptcy_and_Insolvency_Risks_in_Outsourcing_Transactions.pdf> accessed 24.05.2010.

Those and other contractual clauses - if enforced - provide effective means for risk management in the ITO relationship in terms of rights and obligations allocation, as well as financial compensations. For the customer being financially compensated for service loss or delay is better than suffering all the consequences of such failure, however, it doesn`t provide continuity as understood within the BC definition provided in the previous chapter. More specific strategies and tools, aiming at ensuring service continuity for all business critical functions, should be contractually agreed. Next chapters are dealing with specific ITO risks able to undermine continuity and the respective contractual instruments for risk management.

3. Generic measures for ITO project control

As already outlined in the previous chapter, a number of general tools for risk allocation are available to the parties, when they enter into an agreement. The discussed instruments however, are applicable to most commercial projects and do not reflect the specifics of the IT field. In this chapter further measures to control the quality and reliability of the IT-project will be dealt with, which although not always directly related to continuity, create the basis for a successful project and thus contribute to it.

3.1. Services definition and Service Level Agreement (SLA)

3.1.1. Services definition

Defining the scope of the outsourcing project is a key fundament for the parties in their way of preventing service disruption. A significant part of practical problems with ITO projects originate from unclear scope definitions and scope misunderstandings, clearly justifying the need of both parties` extensive involvement in defining and documenting the scope. For the customer a clear services definition and Statement of Work (SoW) means well defined and documented requirements and expectations, while for the service provider it is a good way of organizing their own understanding of what is expected to deliver and what is out of scope, thus defining both parties` responsibility boundaries. SoW could be a separate document attached to the contract or a part of the SLA.

The SoW may include detailed description of the outsourcing activities, as well as the main deliverables, together with a description of the project sites, equipment or software to be delivered, and an outline of activities that both parties agree to be out of scope. In case of interrelated activities, trigger activities[36] and milestones should be also defined. Clear demarcation line should be put between the rights and obligations of both customer and provider by stating what activity is expected by each one of them in order to fulfill project goals.

[36] Such a trigger activity for the provider to perform an IT service might be the preceding transfer of network equipment or software licenses by the customer. In this case, customer`s delay in performing the trigger activity, will, under certain circumstances, waive provider`s liability for the delay of the respective inter-related activity.

Nevertheless, even with the most clearly defined scope, life is dynamic as is business, and in the 5 to 10-year duration of the standard ITO project, changes will inevitably occur. Including a simple yet unambiguous change management procedure, provides means for dealing with change and adds the needed flexibility that eventually reduces to a great extent the chances for project failure.

3.1.2. SLA

SLA is usually a schedule to the ITO contract, which defines minimum levels of services performance and realistic performance metrics. It should be in line with the business objectives and priorities of the organization, instead of only focusing on technical details. It is important to remember that if a service is not included in the SLA, it practically does not exist in the project.

Performance metrics can be specified based on either subjective or objective criteria. Typical subjective criteria for performance include "reasonable efforts", "best efforts", "professional manner" etc. that are preferred by providers, but are not able to provide customers with the high level of comfort needed, especially regarding business critical services. Objective criteria, however, are based on specifications, baseline performance metrics, service levels the customer has already achieved and benchmarked service levels.[37]

The specific form of minimum service levels depends largely on the type of function outsourced. In IT support projects for example, service levels can be measured with parameters such as reaction time, resolution time, hardware replacement time, etc. Fault prioritization is often made in the SLA, where different priority types of faults are assigned different reaction and/or resolution time. In web-hosting services and electronic commerce, the service levels can be measured as a percentage of website availability for a period of time, as a 100% uptime might not be achievable.[38]

3.1.2.1. Effective approach in defining service levels and metrics

An effective approach to defining service levels that will be realistic, yet ensuring customer satisfaction and a spirit of understanding in the project, includes selecting a limited number of service levels to be binding to avoid too much and too complicated data; choosing

[37] Ibid: Vagadia (n 3), pp. 93-103.

[38] Jagvinder Kang, 'Service Level Basics', Technology Law Alliance.

objective criteria for measurement; ensuring that the customer is able to measure and verify the service levels independently from the provider.[39] Additionally, the selected levels should be reasonable and achievable and metrics should be easily collected.[40] Moreover, the SLA should define precisely the service levels, so that it is clear for both parties what exactly is to be measured, i.e. in case of computer system availability for example, would the service level be attained if the operating system is working, but the application program failed.

A SLA for application services, such as SharePoint services for example, should set the service levels of data availability during normal operations, as well as in case of failure (software/hardware).[41] The agreement should further include provisions regarding all types of faults and restore options, such as entire "server farm" breakdown, single server failure, lost document or emergency access to documents. Historical data availability should also be included as a service requirement, if needed.

Additionally, in IT application services outsourcing, the SLA should contain provisions regarding application brownouts[42], as they can affect significantly service performance and undermine the overall business continuity of the customer.[43]

Another example of typical SLA refers to IT hardware maintenance and support projects. The agreement should differentiate between warranty maintenance and extended support services. Furthermore, clear contact points should be established, preferably a single point of contact (SPoC), such as help desk contact. To be clearly defined, SLA parameters shall include the reaction, resolution and hardware replacement time frames, management escalation procedure, optional support services, such as on site-services, network audits, software upgrade, and development of network design documents.

[39] Ibid: Kang (n 38)

[40] Ibid: Vagadia (n 3), pp.93-103.

[41] 'What's the Service Level Agreement?', Published 17.09.2007, <http://blog.sharepoint-recovery.com/2007/09/17/whats-the-service-level-agreement/> accessed 23.02.2010

[42] Application Brownout refers to a stage of application performance where the application is still working, but poorly performing.

[43] Andrew Hiles, E-business Service Level Agreements, Strategies for service providers, e-commerce and outsourcing (The Rothstein catalog on service level books, 2002), pp.1-28.

3.1.2.2. Service credits regime

Service credits regime refers to the consequences in case of service levels not met by the provider, mostly in terms of service credits payable to the customer, as a percentage of the fees due for the respective period. However, they are usually capped at a certain percentage (i.e. 10% of the total charges for the project), thus leaving the customer with the risks of service failure, therefore, their more important function in terms of continuity is to prevent the provider from failing, rather than resolving the problem when a failure occurs.

The amount of the service credits can be set as a fixed sum or a mathematical formula to be applied that is defined in advance, with the mathematical formula being the more precise approach. It should be taken into account, however, that service credits are pre-estimates of the actual losses as a result of the service failure, and thus, they cannot be unreasonably high because of the risk of not being enforceable.

In order to stimulate the service provider to perform to their best, service debits can be agreed upon for provider`s performance in excess to the service levels. In case of service credits already accumulated, after exceeding service levels, the amount of the debits can be respectively deducted from the credit due amount.

However, in order to provide service continuity, a clause stating that parties should continue performing their obligations (payment, services) while any disputes over service level performance are pending, should be included.

3.2. Other measures

Further measures that parties can take to provide avoid typical IT projects failure triggers and to preserve quality, focus on establishing and maintaining consistent project management and clear communication. Following a recognized project management methodology such as the one offered by the Project Management Institute (PMI) or Prince2 would greatly contribute to the stability of the project. The parties should not underestimate the importance of drafting and, even more important, implementing a comprehensive Project Management Plan, which would consist of a set of specific management plans such as Communication Management Plan, Risk Management Plan, Change Management Plan, etc. and making it a part of the outsourcing agreement. Special attention must be given to communication at all levels between customer and provider and the significance of

establishing good customer-supplier relationship. The communication rules and the general importance of good communication grow exponentially with increasing the number of providers in the multisourcing approach. Applying evolutionary projects management by drafting and following Project Management Plan as part of the entire agreement, especially the Communication Management Plan, would decrease the likelihood of incidents, will increase the overall project quality, will further establish the basis for clear communication and good coordination of provider/s and will ultimately diminish the probability of continuity disrupting events.

Additionally, attention should be given to security[44] as an important project and organization need and the measures taken to maintain. Such measures mostly concentrate on drafting relevant security requirements that coincide with the real customer`s security needs and making them part of the outsourcing agreement, as well as referring to security standards such as ISO 27001, ISO 27002, Control Objectives for Information and related Technology (COBIT), etc. Furthermore, providers should be obliged to perform incident management and keep confidentiality.[45] On the other hand, the customer should have the contractually agreed right to perform security audits – by itself or via another specialized company, and respectively to be entitled to terminate the agreement in case certain security issues occur. Managing security risks increases its importance even more, when multisourcing or when shared environments are used.

In addition to the abovementioned tools, further less continuity specific instruments could be mentioned such as drafting confidentiality agreements or requiring a bank guarantee for performance to be provided by the supplier. Although confidentiality requirements can be a priority issue for specific organizations such as banks, drafting and implementing a thorough confidentiality agreements related to the ITO project is an efficient way to mitigate confidentiality risks, and as such to contribute to continuity. Furthermore, although performance guarantees are usually perceived as mainly focusing on financial problems, their connection to continuity can still be traced, particularly in the perspective of maintaining financial resources to “buy” replacement services when service provision by current supplier is discontinued.

[44] The notion of security understood as physical, technological and procedural security.

[45] Sam De Silva, ‘A contractual approach to manage security risks when outsourcing’ (2009) C.T.L.R. 2009, 15(3), 51-57.

In conclusion, it must be considered that drafting an optimal SLA, Project Management Plan or any of the other outlined instruments, is a smart way to set up a working ITO relationship and to provide a certain level of comfort of both parties that project quality will be kept and expectations are matching. All of the tools discussed above are greatly reducing the risk of dissatisfaction of the results and a subsequent premature termination of the relationship - the two main criteria of ITO projects failure, as outlined in the introduction. However, SLAs and the other measures as such are not directly targeted at ensuring service continuity, rather than defining performance expectations and establishing good project management, therefore more continuity specific contractual instruments, will be presented in the following chapter.

4. Specific ITO continuity measures

Establishing a working relationship between customer and provider in an outsourcing project, based on clear communication, methodological project management and unification of expectations, is crucial for the project sustainability and success, as argued in the previous chapter. In this chapter, however, the focus will be narrowed down to very specific continuity instruments applicable to ITO projects from a legal perspective.

4.1. Back up and disaster recovery provisions

4.1.1. Disasters Overview

Latest generation ITO relates to IT processes that are more than just supporting functions, but rather strategic services that affect the entire company and consequently their availability reflects on organization`s market positioning, financial results and overall business continuity. The following table shows the business consequences (expressed financially) of several companies` ITO services outages that lasted for hours only.

Company	Date	Duration of outage	Losses, costs
AT&T	February 1998	6 – 26 hours	Rebates of $40 M
Charles Schwab	February – April 1999	6 – 26 hours	Losses over $20 M, Over $70 M invested in infrastructure
e-Bay	June 1999	22 hours	Revenues $3-$5 M, Shares: down 26%
E*Trade	February – March 1999	Over 5 hours	Revenues: $3 M, Shares: down 22%

Table 1, Source Comdisco[46]

Further to just temporary financial losses, a disaster event reflecting on the IT infrastructure and services of an organization, can significantly affect their market share, their competitive advantage, not to mention the perception of their reliability by the public, in case of wider disaster publicity.

[46] Ibid: Hiles (n 43), pp. 1-29

Disaster is any event than can cause disruption or negatively affect the normal operations of the organization.[47] Typical disasters as to the IT infrastructure and services can be divided into three main categories: natural disasters (earthquakes, floods, etc.), technical disasters (e.g. computer viruses, DoS attack, hacking) and human activities (e.g. incidental or intentional disruption caused by current or past employees, etc.).[48] For business critical infrastructure, technology and processes, a plan should be implemented to recover from a disaster (Disaster Recovery Plan), which should focus on both prevention of a disaster and operations continuity.

In terms of IT functions and services, the following continuity objects could be distinguished:

Continuity object	Measures to be taken
Platform continuity	Rapid replacement of system components.
Data continuity	Frequent backup and restoration programs and fault tolerant storage systems.
Application continuity	Fail-over clustering, snapshot copying, storage area networks, redundant communication services.
Site continuity (buildings and equipment)	Equipment duplicates at a remote safe location, data center, application hosting.

Table 2, Objects of continuity[49]

Types of negative consequences on data, applications, systems and networks include freezes, corruptions and losses.

4.1.2. Disaster protection measures

The following disaster protection measures can be taken as to IT incidents: fault tolerance, duplication & mirroring and archived backups.[50] The fault tolerance measure aims at providing a quick recovery for interrupted service and continuous operations by means such

[47] Michael Wallace, Lawrence Webber, The disaster recovery handbook. A step-by-step plan to ensure Business Continuity and protect vital operations, facilities, and assets (AMACOM, New York, 2004), pp.1-29.

[48] B. Rike, 'Prepared or Not…That is the Vital Question' (2003) Information Management Journal, Lemexa: Vol. 37, Iss. 3; p.25.

[49] Dorian J. Coigias, E.L. Heibelger, Karsten Koop, The backup book. Disaster recovery from desktop to data centers (3rd edn, Schaser-Vartan Books, Lecanto, 2003), pp.1-34.

[50] Ibid: Coigias (n49), pp.7-34

as spear parts, cluster server-duplicates, etc. It is most often combined with duplication (data) and mirroring (hardware) which consists of creating and maintaining an exact copy (replica) of the initial object. It is also called replication and again serves as a quick fix in case of a disaster. The archived backups represent snapshots of data kept in safe locations and provide historical information and record of the data to be protected.

4.1.3. Disaster recovery plan/Disaster recovery agreement

From customer perspective, backup and disaster recovery consideration can be an additional requirement to the outsourcing service provider - therefore a requirement as to the drafting and implementation of a disaster recovery plan should be incorporated in the outsourcing contract. The plan would need to be additionally tested and validated, and in case of changing continuity requirements, amended. However, backup and disaster recovery can be in itself the core service offered by providers and in this case, the scope of the outsourcing contract will focus on them, i.e. a separate backup and disaster recovery agreement will be elaborated. In any case the DRP should be at least a schedule to the contract and should be made legally binding for both parties.

Key considerations in order to successfully implement a DRP include maintaining uninterrupted data records, backup and storage; capabilities for rapid transfer of voice and data communication packets to alternative locations[51]; having a contingency organization.

The disaster recovery plan, reflected in the contract, should provide for three types of measures in connection to the IT infrastructure and services – preventive, detective and corrective. Typical obligations of the service provider to be set in the agreement include:

- To take the necessary steps towards service restoration according to the plan
- To successfully restore all services within the service levels agreed
- To ensure the operational continuity of the services during the disaster situation and invocation of the DRP
- To ensure that services that are indirectly affected by the disaster, continue performance after the core services restoration
- To ensure all services that are in any way affected by the disaster are fully available

[51] Disaster Recovery Plan, 02.02.2009, <https://online.penson.com/PensonBusinessContinuityPlan.pdf> accessed 11.04.2010

The DRP should include provisions related to the following issues:[52]

- Objectives
- General principles and requirements – how the invocation of the DRP will affect normal operations of the services, the SP to ensure their disaster recovery services liaison to the customer or to other providers in terms of DR.
- Key personnel information – the personnel to be in charge for general disaster recovery activities and specifically if an incident occurs.
- Third party contact details – subcontractors and other providers
- Key IT processes and backup strategy
- Risk management plan – identification of risks related to business critical IT functions such as failure and disruption scenarios, single point of failure, identification of risks linked to the interaction with the services provided by other service providers, business impact analysis
- Service levels – including RPO, RTO, Data Retention Time (DRT), etc.
- Service levels exemptions – events such as scheduled maintenance, as result of the acts of the customer, failure of the customer to grant access to facilities and equipment.
- Emergency response provisions – including trigger events, invoking the plan and activating the emergency response, emergency alert and escalation, etc.
- Recovery provisions – processes and sequence of events
- Insurances – to be made as part of the organization`s continuity strategy
- Consequences if SP fails to meet service levels and objectives – service credits, other remedies
- Specific disaster recovery plans as to the different types of technologies to be recovered

Once drafted and accepted, the DRP has to be continuously reviewed and updated as business needs and requirements will most likely change in the 5 to 10-year course of the outsourcing project. Additionally, the plan may contain a requirement for the provider to

[52] IT disaster recovery (DR) plan template: A free download and sample plan, Published: 13.10.2009, <http://searchdisasterrecovery.techtarget.com/generic/0,295582,sid190_gci1370683,00.html> accessed 13.04.2010

possess and follow certain security standards, such as the ISO/IEC17799:2000[53]. Furthermore, the service provider should be required to carry out disaster recovery testing according to DRP. The requirements regarding the testing methods and results should be part of the DRP.

4.1.4. Limitations

When reflecting on service continuity in ITO projects, a special attention should be paid to the interconnection between DR and Force Majeure (FM) clauses of the contract. In some cases, disaster recovery provisions may be combined with the FM clauses and a key objective of the customer should be to prevent the provider from invoking the FM provision as an excuse for not fulfilling their disaster recovery obligations. It is very important to draft the FM clause in a way that it does not prevent the disaster recovery provisions from activating, since an FM clause may generally excuse the provider from performing all obligations under a contract, including the DR ones.[54] In the best case scenario, when disaster recovery is concerned, a customer might want the FM clause to state that in case of a disaster, the provider will still have to perform and will not be able to invoke the FM option, however, many suppliers will seriously try to resist this attempt.

A proper drafting of the FM clauses will focus on excusing provider`s inability to perform only for acts that are unforeseeable and genuinely outside of their control. The definition, however, should not be too broad, especially if the provider is based in typical outsourcing destinations, where interruptions of power supply, of infrastructural outages are common. The customer should make sure such events are not included in the FM provisions, which should only cover incidents and acts that are indeed out of the control of the provider.

In connection with the FM clauses, the provider`s obligations as to disaster recovery should be clearly described in the DRP, as outlined above. There should be no uncertainty about the specific business critical services to be protected and the specific types of incidents covered, in order to make sure all such events fall outside the FM scope.

In addition, several practical limitations regarding the efficiency of this instrument in terms of continuity must be mentioned, such as provider`s technical inability to restore all lost or

[53] Standards for information security management.

[54] Matt Karlyn, 'The Essential Lawyer: Force Majeure Meets Disaster Recovery', CIO Decisions Magazine Archives, <http://searchcio-midmarket.techtarget.com/magItem/0,291266,sid19_gci1213262,00.html> accessed 20.04.2010.

corrupted data or provider`s own continuity disruption. Naturally, back-up and disaster recovery planning will not be able to reach its all goals, if important relevant risks are not taken into account and respectively, the applicable response strategies are not drafted. Last but not least, back-up and disaster recovery services are usually connected with high direct and indirect costs for the customer organization, and therefore, financial and strategic prioritization might often exclude them as unviable options.

4.2. Source Code Escrow agreements

Instead of developing software in house or purchasing off-the-shelf software, many companies would prefer to outsource the software development to an external company that provides specific software. However, as specific software many times becomes critical for the organization, companies would need to ensure their continuous availability as well as operations and maintenance. The reality is that a considerable number of the software companies that provide custom made software are typically start-ups who, although being brilliant in software development, are not always that skilled in managing and maintaining a company. For that, and many other reasons that can cause a provider to go out of business, to go bankrupt, to be in a material breach or to just fail to provide proper software maintenance services, companies can benefit from another continuity instrument, namely the software source code escrow. Being able to access the source code of the business critical software, should a trigger event occur, is an efficient step for ensuring continuity.

4.2.1. Source code

A clear distinction should be made in respect of the software code. There are generally two types of software code - object code and source code. The object code is a binary machine readable code which contains instructions for the host machine, i.e. the computer CPU, to perform some tasks and run the programs, but it is hard or even impossible for a human to read or understand. The source code however is written by the programmers in a text editor or visual programming tool and can be understood by other programmers, familiar with the programming language.[55] As the custom developed source code is an important asset for proprietary software providers and considering potential confidentiality or competition issues, they will not be willing to disclose it to customers, no matter the importance of the

[55] Jonathan L Mezrich, 'Source code escrow: an exercise in futility' (2001), <https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=5+Marq.+Intell.+Prop.+L.+Rev.+117&srctype=smi&srcid=3B15&key=5627984601f8c2492c7dfe99ec454a06> accessed 15.05.2010.

said software for the customer. Thus, a source code escrow is an attractive continuity option for the customer, while at the same time minimizing confidentiality or competition risks for the provider.

4.2.2. Source code escrow agreement

Source code escrow is generally when the developer company deposits the software source code[56], together with supporting documents, updates and enhancements, with an escrow agent, who undertakes to release it to the customer in case a trigger event occurs, such as bankruptcy, insolvency, material breach of the contract or any failure to deliver agreed maintenance services related to the software. In the best case scenario this situation is beneficial for both parties – it provides certain continuity guarantees for the customer that the source code is accessible if the provider fails to perform their operational and maintenance obligations, and from the proprietor`s perspective it protects the software from unauthorized disclosure, modification and confidentiality issues.[57] However, in a non perfect world, in order for the best case scenario to become reality, the role of the best fitted escrow agreement that is able to shape both parties` obligations in the most efficient way, should be carefully considered.

The software escrow agreement is concluded between three parties – the software provider, the customer and the escrow agent. Its scope and subject commonly includes an obligation for the vendor to deposit the software source code within the agent, together with any subsequent updates, enhancements and modifications. However, since the probability of the customer not having the necessary knowledge and skills to confirm the deposited code corresponds to the object code provided is considerably high, the agent could also provide verification services in respect of the software. Additionally, the agreements can also allow the customer to perform regular audits with validation purposes. Moreover, it is essential to provide a clear definition in the agreement of what constitutes “source code” in order to

[56] In specific services like SaaS, the continuity needs of the customer will also include object code escrow, because, unlike the typical ITO where the object code is also run on the customer`s machines, with SaaS the object code is stored with the provider only.

[57] Periklis A Pappous, ‘The software escrow: the court favorite and bankruptcy law’, (1985), Santa Clara Computer&High Tech L.J. 309.

cover all possible documents and modifications vital for the customer.[58] Besides, the term of the contract should be set up for the same period as the software license.

The agreement further obliges the escrow agent to keep the code deposited safe and confidential and to make it available to the customer in case a release event occurs, according to the list of trigger events negotiated. The release events agreed in the contract are usually subject to extensive negotiations and it has to be noted that customers should insist on including not only events of financial disaster of the provider such as bankruptcy, which under certain circumstances are hard to enforce, but also provider`s failure to provide software support or other related services. In any case careful consideration of the trigger events will protect the software proprietor as well against a premature or abusive release of their source code. When any of the trigger events occurs, the agreement can provide for the customer the duty to send proper notification to the agent explaining the reasons for requesting the release of the code.

When bankruptcy, insolvency or the provider going out of business are among the reasons for the customer to request the release of the code, the agent usually is able to easily verify it, thus is not expected to object to the release. In cases however, when the customer claims provider`s failure to provide proper software maintenance as a release event, the escrow agent might need to wait for a court decision to validate this fact. In order to make the procedure faster and the agreement more efficient as a continuity provision tool, the parties can agree to an arbitration procedure for resolving the problem out of court.[59]

In relation to the release grounds and the release procedure strategies considered in the escrow agreement, parties can adopt a first-call approach, where the provider will immediately allow the source code release upon the inquiry of the customer. However, most suppliers will be highly reluctant to agree on such a release procedure and they would rather negotiate the trigger event to be an extreme circumstance, communicated by a notice, followed by a certain period for consideration and in case of lack of mutual consent as to the release event, the dispute would have to be taken to court or arbitration. In this situation

[58] 'Source Code Escrow - A "Win Win" Solution', Published: 18.12.2006 - Manitoba, Canada, <http://www.hg.org/articles/article_1652.html> accessed 17.05.2010.

[59] Eric S Freibrun, 'Source Code Escrow Agreements - Balancing the Interests of Users and Vendors' (1995), <www.innovasafe.com/doc/freibrun.doc>, accessed 15.05.2010.

the whole procedure can take up months, which might turn to be unacceptable from a continuity perspective.

Furthermore, the agreements should include a provision obliging the software proprietor to submit any updates or modifications to the escrow agent that clearly correspond to the software versions provided to the customer. Fulfilling this task is crucial, as the customer will be practically unable to use the source code of version e.g. 1.1 in a meaningful way, if the current software version they use is 5.1., and in reality as many as 80-90% of software providers fail to submit the latest source code versions to the escrow agent.[60] Moreover, accessing the source code and all accompanying documentation including the latest updates, does not necessarily provide the customer with the full opportunity to ensure software continuity as they might not be able to operate or modify the software without certain assistance from the provider, thus it is advisable to include an agreement provision in this respect, obliging the software vendor to provide additional consultancy services to the customer after the release.

Another clause typically contained in the escrow agreement relates to paying the fees to the agent. The final decision about who pays the fees is left to the discretion of the parties – the costs can be borne by the customer, the provider, or split between them. However, the agreement may entitle the agent to destroy or release the code to the customer, should the fees are not paid on time, when it is agreed that the provider is responsible for paying them, thus providing a strong incentive for payment.

Furthermore, the parties should include extra care when drafting the limitation of liability and indemnities provisions of the agreement. Many times limitations of liability clauses will exclude agent`s liability for their negligent actions, as well as for any special or consequential damages.[61] Considering the idea of the escrow aiming to provide the customer with the necessary safeguards against losing the latest versions of the software, it is advisable for the customer, as well as the provider, to insist that the agent assumes broad liability for their own negligent actions. The agent should be obliged to indemnify the other parties for any damages resulting from their acts of negligence, misconduct or material breach of the

[60] Iron Mountain study, <http://www.ironmountain.com/ipm/>, accessed 24.05.2010.

[61] Ibid: Mezrich (n 55)

agreement, as well as for breach of any warranties they have provided. The idea of broader agent liability, is further supported by the fact that software escrow agents are usually not part of a regulated profession, as for example are other types of escrow providers such as lawyers and banks, and no specific regulations, codes of conducts or requirements (e.g. holding an insurance) are applicable to them.

The software escrow agreement might further contain provisions regarding the use of the source code after release. It should provide the customer with the license to use the software for purposes of modification, corrections and other needed activities, because of otherwise running into the danger of acquiring access to the code, but not being legally entitled to use it for the continuity enhancing purposes. However, the contract should state that the use of the code after the release will be still in accordance with the license provided and any requirements should be fulfilled by the customer, including strict confidentiality.

As to the termination of the software escrow agreement, both parties should have the right to terminate it in case the original software license has expired. If it is still valid however, the agreement must stay in force, should the customer objects to its termination.

4.2.3. Limitations

Even though the software source code escrow is in general a good strategy when service continuity related to the use of software is targeted, several factors can negatively influence the efficiency and execution of the contract.

Bankruptcy of the software developer is seen as one of the main reasons for complications for enforcement of the agreement, as bankruptcy law often regulates such contracts in a way that puts the agreement execution at risk. Commonly the trustee for a bankrupt company will have the authority to protect the estate of the bankrupt provider that can reach to include the software licenses and escrow agreements. Specific insolvency and bankruptcy rules are regulated in a different manner depending on the national legislations. However, when comparing the bankruptcy legislation of the USA, the UK and Germany for example, a certain tendency is observed towards trying to hold property in place, including software, in order to maximize the proprietor`s estate. US bankruptcy law for example provides three means of limiting access to source code: first, in case the escrow agreement is confirmed as an “executory contract” by the court, which practically means the trustee

can decide on whether to accept or reject the contract; second, it is the situation in which the source code submitted to the escrow agent is considered part of the developer`s estate and as such cannot be transferred; and third – the automatic stay provision of the code, which may not allow the access by the user[62]. The analysis of the UK Bankruptcy Act and Companies Act, as well as German`s Bankruptcy Act shows that similar provisions are contained there putting at risk the execution of the contract. Those problems might be partially alleviated by structuring the escrow agreement in a way that aims at differentiating it from any continuous software maintenance agreements, as well as not setting up the position of the escrow agent as a custodian or agent of the software provider.

Further risk factors for the escrow agreement enforcement and its efficiency as a continuity tool include escrow agent`s long term viability, the short life of software and the transition to open source software, the customer`s lack of technical knowledge that can actually position him in a situation of having the source code, yet not knowing how to use it for continuity purposes, the loss or accidental destruction of the deposited source code by the agent, the lack of any industry and professional standards applicable to software escrow agents and the risk of not being able to actually activate the release of the code due to unclear trigger events definition and procedures. It should be additionally noted that the actual percentage of source code escrow releases actually occurring is very low, usually less than 0.5% of all escrow agreements[63], which clearly indicates that at this stage of development of software escrow services, this specific tool might not be unproblematic, yet with a diligently selected escrow agent and properly drafted agreement, it can provide at least some level of continuity guarantee.

4.3. Step-In Rights

When entering into an outsourcing project, customers usually do not focus on the possible project failure options, or the situation in which they will be faced with the complication of a non-performing provider. However, in order to prevent any disasters from disrupting service provision, it is important for parties, in the very beginning of the IT outsourcing, to contractually set the rules for temporarily stepping-into the provider`s service provision role

[62] John M Conley, Robert M Bryan, 'Software escrow in bankruptcy: an international perspective' (1985), 10 N.C. J. INT'L & CoM. REc,. 579.

[63] Ibid: Mezrich (n 55)

or painlessly walking out of the project. Step-in rights for the customer are seen as an instrument for ensuring continuity, focused on the situation when the provider is unable to perform the services. The 2009 scandal with one of the largest Indian software companies Satyam for example, have practically demonstrated the strong need of contractual step-in rights and exit clauses as strategic tools targeting continuity.

It should be noted however that very little literature exists on step-in rights in outsourcing projects, and even when present, it does not provide an in-depth legal analysis of this instrument. Thus, the analysis given in this study is generally a personal interpretation, based on experience and the scarce literature that is available.

4.3.1. Step-In Rights definition

Step-in rights are rights agreed in a contract that allow the customer or third party representatives to step into the "shoes" of the provider and assume responsibility for delivering all or part of the outsourced services, according to a previously defined set of circumstances. As they represent a considerable intervention with provider`s affairs when invoked, most providers are reluctant to accept them, while for the customer they are a must-have risk mitigation strategy concerning ITO projects. The reason to include them in the outsourcing agreement, is to provide the customer with the opportunity to have uninterrupted services, even when the provider unexpectedly ceases to carry them on.

The standard trigger events for execution of the step-in rights include insolvency of the provider, breach of the service levels, material breach of the contract, force majeure events, but they can also reach to include any other emergency situations or complaints from end users, for example call center users.

4.3.2. Scope of Step-in Rights

The scope of the step-in rights might include the option of taking over certain services, but it can also go further to stepping into the contracts of the provider with key subcontractors, including the right to be assigned or novated certain software licenses or the right to continue using premises, as well as the right to buy provider`s assets. The abovementioned rights will be either for the customer or in many cases for appointed representatives that possess the necessary skills and expertise to undertake the provision of services. Furthermore, the stepping-in can be temporary – for a certain period of time needed by the provider to assume back the provision of the services and in this case stepping out should be

carried according to agreed rules; or final, a right to buy, which must not be mistaken with the transfer rights agreed in the exit provisions.

For the successful drafting of step-in provisions of the agreement, several key aspects should be considered so that the clauses are tailored as to the specific needs of the projects.[64] Among the most important issues to be taken into account by the customer are: the definition of the critical processes and services that will need to be prioritized when stepping-in, the exact scope of the outsourced services, as well as whether the IT systems are owned and hosted by the provider and the number of outsourcing providers engaged in the provision of services. Furthermore, the customer needs to consider if they possess the necessary expertise to successfully take over the services or a third party will need to be involved. Additional questions such as what intellectual property rights are involved in the project and who owns them should be answered. Finally, possible complications related to trans-border projects and specifically to offshore outsourcing need to be taken into account.

In most agreements, the providers will consent to facilitate the assignment or novation to the customer or third party representatives of software licenses, key-subcontracts or other relevant agreements. It should be considered, however, that such assignment or novation can be performed in accordance with the conditions of the relevant agreement and the consent of the respective subcontractor or licensor should be obtained, thus, the role of the provider often will be more of a facilitator of this transition.

The customer should be further entitled to step-in the rights of the provider in using specific premises for the provision of outsourcing services. This can take the form in stepping into a lease or rent agreement. The commercial and other specific terms, upon which such premises shall be made available, need to be outlined in agreement and further detailed, should a trigger event occur.

Moreover, the customer might have the right to acquire assets, such as software and hardware that the provider has been using in the service provision. In this respect two types of assets can be differentiated – sole use assets, being the assets that belong to the provider

[64] Jill Stabler, 'Step-in rights – It`s the plan, not the provision that really counts', 25.03.2009 <http://www.alsbridge.eu/knowledge/articles.html?id=161> accessed 23.05.2010.

and shared use assets that are rented or partly owned by the provider that are both used to support IT service continuity management, within the scope of the project. Regarding the sole use assets, the customer should negotiate the right to require the transfer of ownership to them following a notice submitted certain period in advance. The method of defining the price payable of the assets might be set in the agreements, for example their Net Book Value by the time of stepping in. In connection with the shared use assets, the customer should have the right to rent the shared use assets or to be licensed for their use or where the provider owns the intellectual property rights in any software, to be entitled to receive continued support or maintenance in order to be able to assume responsibility for carrying out the part or the whole project being currently affected by the disaster event.

4.3.3. The right to buy

Another further reaching step for the customer is the option to step-in permanently by exercising a specific right to buy option. An example of this is the Built Operate Transfer (BOT) model, according to which the supplier "builds" a company dedicated to providing the outsourced services to the customer and undertakes to "operate" it for a certain period of time. At certain point of the operation, the customer has the right to be "transferred" the entire facility according to specific rules, including pricing conditions, agreed in the initial agreement.

This option differs from traditional exit provisions, which allow the customer to acquire only certain provider`s assets such as IPR, by entitling the customer to buy the entire service provisions facility. A special risk with this option however is the transfer process, which is undeniably very complicated due to the transfer of multiple types of assets, therefore the transition rules and procedures must be thoroughly defined in the contract.

4.3.4. Other key aspect of step-in rights

Several additional key aspects in respect to step-in should be also taken into account when drafting the step-in provisions, such as notice periods, costs, as well as provider`s duty to assist and facilitate. The notice should be balanced in such a way that it can grant the provider enough time to prepare for the step-in, while at the same time not being too long so that customer`s service continuity is considerably damaged. Additionally, the notice should contain the reason, i.e. the trigger event, details of any third party representatives and description of the step-in. Concerning the costs of step-in, it would be advisable to the

customer to negotiate the waiving of provider`s fees during the step-in, as well as to recover their own and any third parties` costs incurred in connection with the step-in. Moreover, the provider would have to be obliged to assist for the smooth step-in by submitting information about the services performed, the assets used and in general to provide access to their documentation and resources, as well as to assist in case the assets need to be relocated.

4.3.5. Limitations

It must be noted, however, that step-in rights are not very often exercised for a number of practical and legal reasons.[65]

First, in case the customer outsources their entire service provision, e.g. in full call center outsourcing, there will usually be no available staff with respective expertise to assume the provision of the service, thus, no practical applicability in terms of continuity is feasible.

Second, when no skilled staff and knowledge are available to the customer, they might want a specialized third party representative to step-in and undertake the services. In this case, the agreement should have been drafted in such a way as to allow third parties to step-in and no additional limitations on this particular party entering the project should be present. This is explicitly sensitive topic in highly specialized IT fields, where the companies with the necessary know-how might be direct competitors to the service provider, therefore making their involvement into provider`s work and information highly undesirable.

Third, in shared infrastructure and environment, used by the provider to carry on services for multiple customers, confidentiality requirements might prevent the customer from obtaining access to the infrastructure.

Furthermore, in shared infrastructure model, the provider might be highly reluctant to agree on the customer having the right to acquire assets, would affect or even prevent him from the opportunity to further provide their services to other customers. Moreover, in multisouring projects, when services are outsourced to different providers, exercising step-in rights in respect to some or all of them would undoubtedly require excessive efforts and costs, or it can even turn out to be inapplicable for lack of know-how and resources.

[65] Jagvinder Kang, 'Outsourcing contracts: step-in rights', <http://www.tlawa.co.uk/docs/tla-outsourcing-2.pdf> accessed 23.05.2010.

Another motivation for the provider to make their best to resist invocation of step-in rights, are the cost implications. The situation of discontinued payment of service fees, while customer is using their premises and assets, together with the obligation of paying any additional costs of the step-in, would undoubtedly create a strong incentive for the provider to dismiss certain step-in rights.

Furthermore, a difficulty with enforcing step-in rights comes from the duration of the step-in, as most customers would want to continue exercising step-in rights for a long period of time until the situation is resolved. From a provider`s perspective this situation would be hardly acceptable, especially having in mind the abovementioned cost implications during the step-in period.

Moreover, it is not only difficult to negotiate step-in rights and later invoke them due to the expected resistance by the provider, but in reality there is a high probability that the customer is not completely prepared how to deal with the step-in situation. In this respect, it is not only the inclusion of the step-in provision that is important, but also the plan that the customer has created for dealing with the crisis period.

Finally, when assessing step-in rights` efficiency and its enforcement potential, the emotional resistance factor should be also considered. Since stepping into another companies` doings is rather an aggressive tactics, a significant level of reluctance to assist and facilitate this process by the provider and their employees can be expected.

Based on the abovementioned shortcomings of the step-in rights concept in ITO projects, several alternatives can be mentioned[66], such as addressing the disaster by escalation meetings between the parties that aim at elaborating a less intrusive plan for remedying the situation, using service credits, exercising the right to terminate the contract and claim damages or temporarily suspend the provision of the services. Although they have some level of remedial effect and provide a certain form of compensation, those measures are not completely efficient in outsourcing business critical IT processes and services, when speedy restoration of the services is crucial for the business continuity of the organization.

[66] Ibid: Kang (n 65)

4.4. Exit Provisions

Just as step-in rights, exit provisions need to be negotiated at the offset of the outsourcing project, when customer`s bargaining power is stronger. In order to preserve the service continuity, customers needs to have negotiated provider`s assistance with assuming back in-house of the services or transferring them to an alternative provider.

The outsourcing agreement will usually contain the following type of exit provisions: an obligation for both parties to develop and agree upon an Exit Plan, an obligation for the provider to submit information in the exit transition period and assist, an obligation to transfer ownership of the IPRs and assets used for the provision of services and contracts, arrangements covering transfer of personnel, as well as an option to extend the exit period to face any unexpected delays.[67]

4.4.1. Exit Plan

Regarding the development of an exit plan, in practice the parties often only include an outline of it in the agreement and declare their intention to develop a detailed exit plan at a later stage, which many times does not materialize in a comprehensive plan until the last possible moment. It is much more convenient if the plan is drafted in the beginning of the project since it can derive certain rules, based on the transition in – lessons learned that are likely to be lost in the long term project. The issues that need to be covered in a exhaustive exit plan, include the conditions for initiation, the customer rights to require transfer of assets or to continue using shared use assets or premises, as described above, the assignment or novation of agreements and IPRs, the scope of the exit plan, including responsibilities of both parties, key activities to be performed, timetable and documentation to be provided. The plan will need to be reviewed regularly and updated, should the specifics of the project change.

4.4.2. Continuous service provision

As ITO projects are usually complex, it is expected that assuming the services back in-house and especially selecting an alternative provider is a timely process, thus customer should insist on having the right to buy additional periods of ongoing services from the provider during the transition. An indefinite term will likely be resisted by the supplier therefore a maximum time limit should be fixed. The services rendered during the exit might be

[67] Ibid: Pinsent Masons (n 30), pp. 54-61.

provided under the same charging conditions, as well as the service levels should be met, although the provider might not accept fulfilling certain requirements, such as providing improvements and enhancements.[68]

4.4.3. IPR

Both parties must agree on who will own the IPRs at the exit of the contract. Regarding the foreground[69] IPRs, it is best for the costumer to negotiate that they own all IPRs created during the term of the contract (e.g. bespoke software). In any case, they would need to have the right to manufacture the product created and to outsource it to alternative providers. Additionally, the right to use certain third party background[70] rights on which the foreground IPRs owned by the customer depend, should be negotiated.

Furthermore, the project might involve IPRs owned by the service provider or by third parties and used by him in the provision of services. If continuity depends on such IPRs, it is advisable that the outsourcing agreement contains clauses providing the customer with the right to use those products. It is important in the first place to be able to identify those IPRs and to prioritize them from the continuity perspective. Should the provider be reluctant to grant broad license for certain proprietary products, the customer might consider limiting the scope of the access and use of such products to the really continuity critical ones, or for a limited period of time. Regarding third party IPRs, the customer will be in best position to negotiate continuity of licenses before even the project starts to avoid unnecessary obstacles during exit or unreasonably high charges for them.

On exit customers should also decide whether to grant licenses in their foreground IPRs to the provider or restrict them. When providing the licenses, it is desirable to include certain conditions such as limiting provider`s right to sub-license to direct competitors, if of course, direct competitors can be clearly defined.[71]

[68] C. Reed, J. Angel, Computer Law: The law and regulation of information technology, (OUP 2007), pp.139-193.

[69] Foreground IPR – IP created during the term of the project.

[70] Background IPR – IP created before the start of the project.

[71] 'Protecting IP rights throughout an outsourcing project', <http://www.brownjacobson,.co.uk/press_office/articles/protecting_ip_rights_through_o.aspx> accessed 23.05.2010.

4.4.4. Transfer of assets

The provider should be obliged to return all assets previously owned by the customer, as well as to provide the customer with the option to acquire from him other necessary assets in order to ensure smooth transition and avoidance of service disruption.

The contract must include provisions defining a procedure for identifying the assets and establishing their purchase price. For assets identification purposes, it is the optimal solution if the provider is obliged to keep an asset register during the term of the agreement. The register will typically contain information on all assets used in the service provision, such as software, hardware, premises, licenses, data, etc. and should be regularly updated by the provider to include the most current releases and versions. A copy of the register must be handed to the customer on exit to enable him to choose from the list. In relations to the asset transfer, it should be mentioned that, when the provider is using the same platform or environment to render services to multiple customers, they will not be able to transfer most of the assets to the customer without a disruption to their own service provision, thus they will most probably try to resist such obligations.

In outsourcing commoditized IT services, obtaining necessary assets will not be an insuperable obstacle as they will be widely available. In more cutting edge or specialized services however and if service continuity is of high priority, the customer needs to consider engaging with a provider who will be able to transfer the necessary assets, or if not possible, keeping the services in-house in order to have full control on them.

4.4.5. Transfer of contracts

In ITO providers most probably have a number of contracts with third parties such as software licenses, IT maintenance or disaster recovery contracts. A provider should be obliged to transfer some or all of them or to offer third party replacement services at no additional cost. The agreement should provide for a clear way to identify them, at its best the maintenance of the abovementioned assets register, as well as a mechanism for their transfer. The clauses concerning the transfer of contracts, should contain details as to the balancing of upfront payments or liability for actions performed before the transfer.[72]

[72] Ibid: Pinsent Masons (n 30), pp.54-61.

Since such transfer is dependent on the third parties` position however, it is possible that the supplier will not be able to successfully transfer them. Again, it is a matter of customer`s strategic decision whether to outsource those IT services, if their continuous performance is business critical for the organization.

4.4.6. Transfer of personnel

The customer or the alternative provider in many cases will not possess all the necessary knowledge and expertise to assume the services. In this respect the agreement should provide for the transfer of personnel on exit to the customer or to an appointed provider in order to ensure specific knowledge for the service provision is maintained. This transfer should be dealt with in accordance with the relevant statutory provisions regarding personnel protection and special attention should be paid to the compliance with all relevant acts, such as TUPE[73] and other legislation based on Acquired Rights Directive (ARD)[74]. As there are many uncertainties in relation to the application of ARD and TUPE, it is advisable to have all personnel transfer details arranged by contract.

The idea of the ARD is that in case of transfer of undertakings the employees` rights will be safeguarded with the new employer and they will be given the same or similar employment terms as with the previous employer. The TUPE regulations apply when there is a "relevant transfer" and the new 2006 TUPE extend the transfer definition[75] compared to the initial 1981 Regulations to be applicable to "service provision change" in the circumstances set in the act[76]. Those circumstances, applied to the scope of the current study, cover initial ITO, subsequent ITO to another provider and insourcing. In addition, according to TUPE 3(3)(a)(i) prior to the service provisions change there must have been "an organized grouping of

[73] Transfer of Undertakings (Protection of Employment) Regulations 2006

[74] Council Directive 2001/23/EC on the approximation of the laws of the Member States relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses.

[75] John Mcmullen, 'An Analysis of the Transfer of Undertakings (Protection of Employment) Regulations 2006' (2006) Industrial Law Journal, Vol. 35, No. 2

[76] Art. 3(1)(b) TUPE :
(i) activities cease to be carried out by a person ("a client") on his own behalf and are carried out instead by another person on the client's behalf ("a contractor");
(ii) activities cease to be carried out by a contractor on a client's behalf (whether or not those activities had previously been carried out by the client on his own behalf) and are carried out instead by another person ("a subsequent contractor") on the client's behalf; or
(iii) activities cease to be carried out by a contractor or a subsequent contractor on a client's behalf (whether or not those activities had previously been carried out by the client on his own behalf) and are carried out instead by the client on his own behalf. "

employees with principal purpose the carrying out of the activities on behalf of the client". In this situation, except for some specific cases[77], the transfer of personnel is mandatory and the employer cannot opt out of it. The personnel would have to be transferred together with all rights and obligations under the employment contract (except for pensions) and they cannot be dismissed only based on the transfer itself. Such a dismissal, or change of the employment terms, will be automatically unfair, unless it is based on ETO (economic, technical or organizational) reasons.

Since the employees would be transferred together with all liabilities, it is crucial for the transferee to request that the transferor provides all the information in connection with them. In this respect the contract should include warranties by the transferor that all the information is provided and is correct and no other employees, other than those listed, will be transferred.[78] The Regulations provide for a complaint procedure, should a transferor fail to provide the necessary information. Furthermore, it is also mandatory to inform and consult employees` representatives about the transfer, for the failure of which, TUPE provides joint and several liability for both employers.[79]

Although the customer might not want to accept the transfer of personnel they deem unnecessary for the project, it would be mandatory to accept all the staff assigned to the transferred service, as outlined above, thus, the main remedy applicable would be a contractually agreed right to claim compensation from the provider for the personnel transferred. Additionally, the customer might seek indemnities for claims brought by employees in connection with the transfer or based on employment terms prior to the transfer, such as unpaid salary.

Another staff related risk is the difficulty in keeping all key people, as many of them might become de-motivated by the transition and might not agree to be transferred to the customer[80], all that leading to loss of important expertise.

[77] TUPE 3(3)(a) (ii)"the client intends that the activities will, following the service provision change, be carried out by the transferee other than in connection with a single specific event or task of short-term duration; and
(b) the activities concerned do not consist wholly or mainly of the supply of goods for the client's use."
[78] Ibid: Vagadia (n 3), pp. 147-151
[79] C. Reed, J. Angel, Computer Law: The law and regulation of information technology, (OUP 2007), pp.188-189.
[80] TUPE and ARD allow the employees to opt out of the transfer.

4.4.7. Exit assistance and consulting

The truth is that smooth transition can hardly be achieved without the assistance of the service provider. A well arranged contract will include provisions ensuring that customer receives assistance, which consists of: exit planning, provisions of information about the assets, processes used, details of key personnel, logistics assistance in transportation of the transferred assets, trainings of customer`s staff or new provider`s experts, provision of documentation, and any other assistance reasonably required as to ensure the successful transition. The customer might also want to have the option of receiving provider`s consultancy in selecting an alternative service supplier.

4.4.8. Exit costs

In respect to the cost involved in the exit period, there are generally two kinds of costs associated – cost for planning and performing the exit and costs for terminating the services.

Regarding the first type, the customer will usually prefer to receive provider`s assistance at no additional cost. However, requiring the provider to dedicate time and resources to the smooth exit for free might not always be the most efficient approach to obtaining the needed assistance, as they will try to not focus on that, since no payment is received. Thus, for continuity reasons, more viable tactics could be for the customer to invest some money in the exit, ensuring the proper performance of the exit obligations by the provider. In order to further motivate the provider to really do their best, an exit assistance fee might be only payable upon a successful transition.

As to the second type of costs, the provider might want to be compensated for the terminations of the services, but as this is mostly applicable when the agreement is terminated by the customer for convenience and not in disaster or provider failure cases, its practical significance for continuity is not of great importance.

4.4.9. Limitations

Carefully drafted exit provisions are essential from a customer continuity perspective. However, several typical problems regarding their applicability and enforceability must be outlined.

Detailed Exit Plan is often not drafted until a very late stage of the project, many times until a certain incident happens. As already mentioned above, it not only puts the customer in

considerably weaker bargaining position compared to the initial phase of the project, but the late incident based composition of the Exit Plan also implies the risk of missing out important details. Another common problem with the timing is the case of drafting detailed provision way too early and failing to update them with the progress of the project, so that finally they reflect only the initial state of affairs between the parties, which might have changed significantly during the long outsourcing duration.

Furthermore, the invocation of exit provisions is closely related to the termination of the contract. In this respect, clear termination rights for the customer should be negotiated, in such a way that non-performance of the provider unlocks those rights, which subsequently provides a reason to use the exit conditions.

In addition, since the assistance of the provider during exit is crucial as already mentioned above, the customer should try to avoid any lack of motivation of the supplier during the exit period, thus trying to stimulate it by both positive measures, such as payment for those services, or negative ones, including claiming damages for example.

In conclusion, a key concern regarding unproblematic exit is related to not only having the drafted exit provisions, but also a further idea and a plan as to the specific steps to be taken after exit. In this respect, it is in best customer`s interest to take all efforts to be practically prepared for exit, and especially for the post-exit period.

5. Conclusion

This thesis has outlined the main contractual instruments applicable for maintaining business and service continuity of the customer in traditional, as well as in several types of novel ITO projects, in the light of the growing significance of ITO for organizations in terms of number and scale of outsourcing activities, and moreover considering its strategic impact on organizations as part of their key business strategy. Considering the central goal of the study, i.e. to analyze available legal tools and to offer effective solutions, a selection and analysis of general means for ITO project control and specific ITO continuity instruments has been provided. It has been observed however that statutory legal framework relevant to ITO projects offers generic regulation of mostly non-ITO specific matters like IPR, data protection, insolvency, contracting in general, etc., and is fragmented in multiple acts, hence, specific contractual tools for ensuring continuity have been offered.

Although measures for maintaining project quality and control are considered crucial for the success of the ITO endeavor, and as such are inevitably related to continuity, an even more comprehensive analysis of specific IT continuity tools, including back-up and disaster recovery plans and provisions, source code escrow agreements, step-in rights for the customer, as well as exit provisions, has been presented. The analysis comprises of main reasons to use each of the instruments, essence, practical recommendations for drafting, and an outline of the main limitations or drawbacks regarding efficiency and enforcement.

Back-up and disaster recovery provisions and planning, being the first presented instrument, have been considered as key tools for prevention and correction of negative consequences of natural, technical, social or even financial disasters. As the timing and scale of disasters are by definition unexpected, it is highly recommended for an organization which relies on IT as strategic function, to include back-up and recovery measures in the hotlist of contractual topics when outsourcing. Furthermore, up-to-date storage and data replication technology allows continuous data protection, which can back-up all the data almost immediately, thus providing a high level of safety for customer`s data. However, this instrument might not be fully efficient if, for technical reasons, data cannot be restored or is restored with errors, or the service provider itself has suffered service disruption. Additionally, contract drafting deficiencies such as Force Majeure clauses, which allow service provider to deny

performance on force majeure grounds, can make the disaster recovery tool useless in certain situations.

Regarding business critical software, a Source Code Escrow solution has been analyzed. From continuity point of view, having an access to key custom software source code, stored with a third party agent, if the provider is no longer able or wishing to render their services, is practically the best next thing to developing the software in-house. Nevertheless, risks such as the escrow agent own viability problems, loss or destruction of the deposited source code or the lack of deposited latest versions and updates are seen as considerable obstacles for the efficiency of the tool. Furthermore, even if successfully released, the source code might be unable to serve the customer in maintaining their operation and services, if specific technical knowledge as to what to do with the source code is missing. A significant problem with enforceability from a legal perspective is connected with supplier`s insolvency, when trustees might logically try to dismiss the escrow agreement in their endeavors to maximize provider`s estate.

Another useful tool, relevant when the provider has ceased to perform, is the provision of step-in rights for the customer in the outsourcing contract. It indeed could be a very effective instrument, if the customer has the resources and know-how needed to perform the services or a well prepared third party is allowed to step-in. Moreover, this approach can be applicable if the outsourcing model is based on single prime provider, who is not using the same platform to provide services to other customers. In shared environments however, the supplier will be unwilling to allow stepping-in or buying as this could compromise the confidentiality in respect to other customers and might further damage their entire service provision capability.

Furthermore, the significance of clear and comprehensive exit provisions has been analyzed as a key step towards providing continuity. Such provisions would usually include the rules for transferring from provider to customer of assets (e.g. hardware used for the IT services), contracts (e.g. software licenses) and people, as well as it might additionally require the supplier to continue performing the services for a certain period of time and/or to render exit assistance. In order for exit provisions to serve as an effective continuity tool, they should be exhaustively drafted at an initial project stage, when the customer still has a

stronger bargaining power and should subsequently be regularly updated. Again, if the suppler is using certain assets or employees to provide services to multiple customers, provisions ensuring their transfer to customer might be resisted. From a practical perspective, in some cases like offshoring, such transfer will not be even possible, for example the transfer of all service-dedicated employees from India to the country of the customer.

It has been also outlined that in addition to the general outsourcing and IT risks, further ITO complications can be expected in offshoring, stemming from the cultural, organizational and legislative differences between the parties. Difficulties with enforcing foreign judicial or arbitral decisions, together with the decreased operational control and management of the projects, as well as the lower infrastructure and power reliability of typical offshore destinations, turn offshoring into a riskier endeavor in cases when continuity is essential.

Moreover, multisourcing can be a successful outsourcing model when continuity is targeted, as the spread of the work between different service providers is able to ensure higher level of un-interruption of services. However, companies willing to follow this model should consider the higher failure rate connected with multisourcing due to the communication and coordination complexity.

It can be concluded that, in order to ensure continuity, organizations should start negotiating and drafting the presented instruments in the early stages of the ITO project and should tailor them to fit their specific needs. The contractual provisions should be drafted in such a way to avoid or reduce tools` limitations. However, as discussed, it is hardly possible to avoid or prevent all risks related to the applicability of those continuity means, which always keeps the option for disruption of customer`s IT functions and services. Therefore, when IT service continuity is strategically perceived as a key priority for the organization, the safest solution might be to keep IT services in house and not outsource them, which could reach as far as, for example, developing own bespoke software or having own data center. A balanced solution between third party outsourcing and not outsourcing at all could be to establish a captive facility, which as part of the organization of the customer, provides services from an abroad location, or to follow the BOT model, which allows customer to acquire the facility upon occurrence of contractually agreed events.

As mentioned in the Introduction, the literature providing a comprehensive legal analysis of ITO continuity instruments is very limited or even missing. Available articles usually introduce one or just some of the tools, sometimes ignoring important legal aspect, while focusing on the technical side, and not providing a complete overview of the continuity topic in its integrity. In this respect, the academic and practical contribution of the present study is seen as providing specific legal analysis of a complete set of the most typical ITO continuity instruments, combined with practical drafting recommendations.

Nevertheless, as available literature on most of the instruments is scarce, developing a further legal analysis of some of them, such as the step-in rights or the disaster recovery provisions, as part of a separate study would be a significant prospect for future research. Additionally, a special area of future consideration must focus on the need of introducing certain regulatory changes in order to reflect the specifics of ITO, and especially to protect continuity of customer organization. As seen from the analysis provided, even when parties take continuity protection measures by means of contracting, those measures might still be unenforceable due to existing insolvency regulations, cross-border legislation disparities and other statutory limitations.

Finally, based on the above conclusions, successfully ensuring continuity in ITO could be seen as a combination of evolutionary IT project management and coordination to provide the overall project quality, together with comprehensive legal and practical consideration of risks, reflected in an exhaustive outsourcing agreement, supported by an updated legal framework, which addresses specific outsourcing continuity problems.

APPENDIX 1

ITO Risk Matrix

№	ITO Risk Matrix					
	Risk Description	**Risk Category** *(legal/practical)*	**Continuity specific risk** *(yes/no)*	**IT Specific tool** *(yes/no)*	**Preventive tools**	**Risk Response measures**
1	Lack of IPR protection	Legal	No	No	Initial contractual definition of background and foreground IPR	Clear identification of all IP and respective ownership
2	Unclear IPR ownership	Legal	No	No	Initial contractual definition of background and foreground IPR ownership	Clear identification of all IP and respective ownership
3	Insolvency of provider – inability to terminate before provider`s default	Legal	Yes	No	Early warning contractual termination triggers	Termination based on trigger events
4	Unclear obligations and performance metrics	Legal	No	No/yes	Definition of specific result obligations and service levels (instead of “best efforts”)	Periodical measurement and assessment
5	Unrealistic long term contract – lock-in	Legal	No	No	Termination rights, termination for convenience	Termination
6	Lack of specific statutory regulation	Legal	No	Yes	Drafting of specific contractual instruments	(Statutory changes)
7	Difficulties in timely and properly enforcing foreign judicial or	Legal	No	No	Carefully selecting contract governing law	(Accepting the risk)

	arbitral acts				Carefully selecting outsourcing locations	
8	Exit chaos	Legal/practical	Yes	No	Clear Exit provisions Detailed Exit Plan	Activation of exit provisions
9	Unavailability of specific software licenses after contract termination	Legal/practical	Yes	Yes	Exit provisions providing for assignment or novation of software licenses	Assignment or novation of software licenses
10	Lack of contract flexibility	Legal/practical	No	No	Change management	Contract updates based on change management procedures
11	Lack of access to key data (loss or corruption of key data)	Practical	Yes	Yes	Back-up arrangements for data storage and replication.	Data restoration according to the agreed service levels
12	Unexpected change of Project scope	Practical	No	No	Statement of Work (SoW) Change Management Plan	Contract changes. Update of the Project Plan.
13	Unclear expectations and requirements	Practical	No	No	SoW as part of the master outsourcing agreement Clear communication	SoW to be made available to the respective stakeholders Clear communication at all levels Periodic project reports
14	Natural, technical or social disasters	Practical	Yes	Yes	Back-up and Disaster Recovery provisions	Activation of disaster recovery provisions. Restoration of data, platforms, applications or facilities.
15	Communication problems between parties	Practical	No	No	Clear and mutually agreed communication plan Regular and clear project	Re-consideration of project communication plan.

					progress reports.	
16	Coordination problems with multiple providers	Practical	No	No	Clear Project Management Plan.	Update of Project Plan Reduction of number of providers
17	Loss of key expert staff	Practical	Yes	No	Periodical coordination between team members; keeping them informed about project progress. Incentive and motivation measures	Assignment of new team members Involvement of external experts
18	Software provider discontinue supplying software or software maintenance	Practical	Yes	Yes	Source Code Escrow	Source Code release
19	Extortion or commercial espionage	Practical	No	No	Confidentiality Agreement	Damages, injunction
20	Shared environments confidentiality risks	Practical	No	No	Security audit rights	Damages, injunction
21	Unavailability of specific physical assets after contract termination	Practical	Yes	No	Exit provisions providing for transfer of assets	Transfer of assets Purchasing of new replacement assets
22	Security vulnerability	Practical	No	No/yes	NDA, security audit rights, security standards	Damages, injunction
23	Insolvency of provider – discontinue service provision and assistance	Practical	Yes	No	Termination and exit assistance clauses. Financial incentives for exit and termination assistance	Activation of exit assistance clauses
24	Service provision disruption in case of disputes	Practical	Yes	No	Continuous service provision obligations for the provider	Service provisions continuance based on the

					until dispute resolution	contractual obligations
25	Customer over-dependency on crucial business service performance	Practical	No	Yes	Multisourcing	Insourcing
26	Financial losses, financial instability of the customer as a result of project failure	Practical	No	No	Provider insurance Bank guarantee	Compensation
27	Inability to determine the quality of service delivered	Practical	No	Yes	Clear SLA	Periodic measurements based on objective measurable criteria

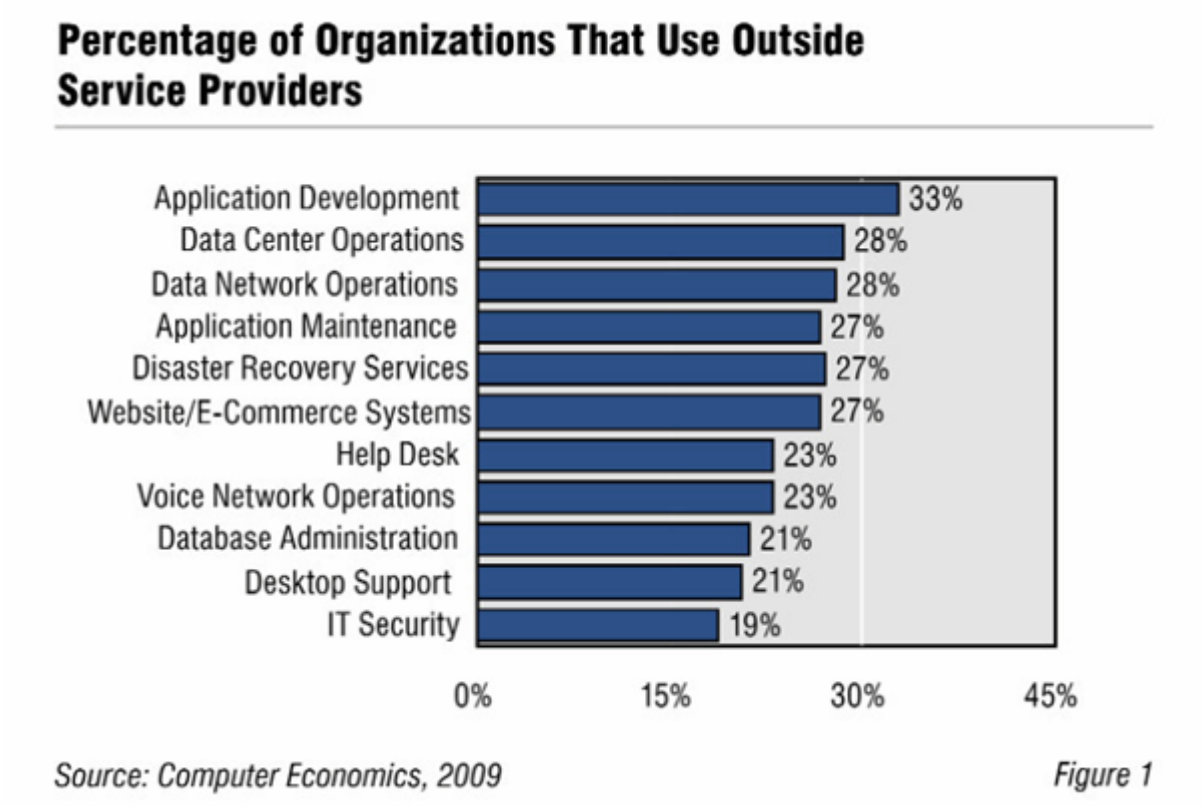
Appendix 2 Figures from the literature review

2.1. Potential Types of Exposure

Potential Types of Exposure		
Natural threats or hazards	Technical and Mechanical hazards	Human Activities and Threats
Fire	Power outage/failure	Computer error
Flood	Gas leak	Loss or misfiled documents/records
Hurricane	Software failure/malfunction	Vandalism
Eartquake	Sewage failure/backup	Theft
Lightning strike	Builduing structural failure	Bomb threat
Tornado, wind storm	Electrical shortage/faulty wiring	Civil disorder
Snow and ice storms	Toxic spill	Strikes
Wind	Radiation contamination	Kidnapping
Tidal Wave	Loss of physical access or resources	Terrorism
Typhoon	Bilogical contamination	Sabotage
Moid and mildew	Train derailment/airplane crash	Loss of key personnel
Insects and rodents		Epidemic

Source Rike, B. “Prepared or Not…That is the Vital Question”, Information Management Journal. Lemexa: Vol. 37, Iss. 3; pg.25.

2.2. Percentage of organizations that use outside service providers



Computer Economics, IT Outsourcing Statistics: 2009/2010, http://www.computereconomics.com/page.cfm?name=Outsourcing

References

Books:

1. Andrew Hiles, *Business Continuity: Best Practice*, (2nd edn, Rothstein Associates, 2004).

2. Andrew Hiles, *E-business Service Level Agreements, Strategies for service providers, e-commerce and outsourcing* (The Rothstein catalog on service level books, 2002), pp.1-28.

3. Angel Kalaydjiev, *Law on Obligations. General Part* (Sibi Publishing, Sofia, 2001).

4. Bharat Vagadia, *Outsourcing to India – a legal handbook* (Springer-Verlag, Berlin Heidelberg, 2007).

5. C. Reed, J. Angel, *Computer Law: The law and regulation of information technology*, (OUP 2007), pp.139-193.

6. C. Warren Axelrod, *Outsourcing Information Security* (Computer Security, Artech House, 2004), pp. 49-53.

7. Dorian J. Coigias, E.L. Heibelger, Karsten Koop, *The backup book. Disaster recovery from desktop to data centers* (3rd edn, Schaser-Vartan Books, Lecanto, 2003), pp.1-34.

8. Mark Lewis, *Computer Law: The Law and Regulation of Information Technology*. *Information Technology Outsourcing and services arrangements* (6th edn, OUP, 2007) pp.139-182.

9. Michael Wallace, Lawrence Webber, *The disaster recovery handbook. A step-by-step plan to ensure Business Continuity and protect vital operations, facilities, and assets* (AMACOM, New York, 2004), pp.1-29.

Articles:

10. Achim Hecker, Hendrik Kohleick, 'Explaining Outsourcing Failure' (October 27, 2006). <http://ssrn.com/abstract=939411>

11. Ann H. Spiotto, James E. Spiotto, 'The Ultimate Downside of Outsourcing: Bankruptcy of the Service Provider'(2003) 11 Am. Bankr. Inst. L. Rev. 47 at 62.

12. B. Rike, 'Prepared or Not…That is the Vital Question' (2003) Information Management Journal, Lemexa: Vol. 37, Iss. 3; p.25.

13. Bierce & Kenerson 'Case Study for Legal Risk Management for "CloudComputing": Data Loss for T-Mobile Sidekick Customers', Published: 29.10.2009, <http://www.outsourcing-law.com/2009/10/case-study-for-legal-risk-management-for-cloud-computing-data-loss-for-t-mobile-sidekick-customers/> accessed 18.04.2010.

14. Brad L. Peterson, 'Seven Key Questions for Drafting Effective Exit Provisions', <http://www.outsourcing-legal.com/exit.html> accesses 15.04.2010.

15. Craig Rattray, 'Offshore outsourcing - an investor's perspective', Financier Worldwide, August 2004, <http://www.dlapiper.com/files/Publication/783830a0-1ed4-4970-9768-4719622a5ca2/Presentation/PublicationAttachment/153c38b5-5c1d-474f-b2c8-4bab744f891c/Offshore_outsourcing.pdf> accessed 25.02.2010.

16. David Fitoussi, Vijay Gurbaxani, 'IT Outsourcing Contracts and Performance Measurement' (2010). <http://www.crito.uci.edu/projectsMIS04papers.asp> accessed 19.04.2010.

17. Dean Davison, 'Top 10 risks of offshore outsourcing', Published 16.02.2004, <http://searchcio.techtarget.com/news/article/0,289142,sid182_gci950602,00.html> accessed 20.02.2010.

18. Eric S. Freibrun, 'Source Code Escrow Agreements - Balancing the Interests of Users and Vendors' (1995), <www.innovasafe.com/doc/freibrun.doc>, accessed 15.05.2010.

19. H. Ward Classen, 'Fundamentals of software licensing' (1996), IDEA – The journal of Law and Technology. <http://euro.ecom.cmu.edu/program/law/08-732/Transactions/Fundamentals.pdf>, accessed 3.05.2010.

20. Hunton & Williams, Marsh, `Risk Management in Next Generation Outsourcing` (2008),

<http://www.hunton.com/files/tbl_s47Details%5CFileUpload265%5C2125%5COutsourcing_white_paper_2.22.08.pdf> accesses 11.04.2010.

21. Jagvinder Kang, 'Outsourcing contracts: step-in rights', <http://www.tlawa.co.uk/docs/tla-outsourcing-2.pdf> accessed 23.05.2010.

22. Jagvinder Kang, 'Service Level Basics', Technology Law Alliance.

23. Jahyun Goo, 'Structure of service level agreements (SLA) in IT outsourcing: The construct and its measurement', Published: 13 February 2008, <http://sce.uhcl.edu/cs/pub/Kim_C35.pdf> accessed 17.03.2010.

24. Jill Stabler, 'Step-in rights – It`s the plan, not the provision that really counts', 25.03.2009 <http://www.alsbridge.eu/knowledge/articles.html?id=161> accessed 23.05.2010.

25. John Beardwood, 'Bankruptcy & Insolvency Risks in Outsourcing Transactions: A Wake-Up Call' (2008), <http://www.fasken.com/files/Publication/e9cc8578-6707-4514-a86c-59b4b806b358/Presentation/PublicationAttachment/2d93dd77-ea7f-4bc9-a8aa-0e6078f63b8a/Bankruptcy_and_Insolvency_Risks_in_Outsourcing_Transactions.pdf> accessed 24.05.2010.

26. John K. Halvey, 'Information technology outsourcing transactions: process, strategies and contracts' (1997) C.T.L.R., 3(2), 87.

27. John Mcmullen, 'An Analysis of the Transfer of Undertakings (Protection of Employment) Regulations 2006' (2006) Industrial Law Journal, Vol. 35, No. 2

28. John M Conley, Robert M Bryan, 'Software escrow in bankruptcy: an international perspective' (1985), 10 N.C. J. INT'L & CoM. REc,. 579.

29. Jonathan L Mezrich, 'Source code escrow: an exercise in futility' (2001), <https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=5+Marq.+Intell.+Prop.+L.+Rev.+117&srctype=smi&srcid=3B15&key=5627984601f8c2492c7dfe99ec454a06> accessed 15.05.2010.

30. Kate Phizackerley, 'Outsourcing Exit Strategy - Planning Ahead For the Full Contract Life Cycle', <http://ezinearticles.com/?Outsourcing-Exit-Strategy---Planning-Ahead-For-the-Full-Contract-Life-Cycle&id=2726556> accessed 15.04.2010.
31. L. Kappelman, 'Early warning of IT Project Failure: The dominant dozen' (2006), Information Systems Management 2006/23, p.31-36.
32. Li-jie Jin, Vijay Machiraju, Akhil Sahai, 'Analysis on Service Level Agreement of Web Services', Software Technology Laboratory, HP Laboratories Palo Alto, HPL-2002-180, Published: June 21st , 2002, <http://www.hpl.hp.com/techreports/2002/HPL-2002-180.pdf> accessed 12.04.2010.
33. Linda Markus Daniels, 'Does Your Source Code Escrow Agreement Achieve Its Objectives?' (2007), <http://www.innovasafe.com/pdf/Does%20Your%20Source%20Code%20Escrow%20Agreement%20Achieve%20Its%20Objectives_Linda%20Markus%20Daniels.pdf>, accessed 20.05.2010.
34. 'Managing the risk of IT Outsourcing agreements', <http://e-articles.info/e/a/title/Managing-the-Risk-of-IT-Outsourcing-Agreements/> accessed 15.03.2010
35. Matt Karlyn, 'The Essential Lawyer: Force Majeure Meets Disaster Recovery', CIO Decisions Magazine Archives, <http://searchcio-midmarket.techtarget.com/magItem/0,291266,sid19_gci1213262,00.html> accessed 20.04.2010.
36. Matthew K. O. Lee, 'IT Outsourcing Contracts: Practical Issues for Management' (1996), Industrial Management & Data Systems, Vol. 96, 1, pp.15-20.
37. Nabarro LLP, 'What are step-in rights?', RICS Construction Journal, February 2009, <http://www.nabarro.com/Downloads/what-are-step-in-rights.PDF> accessed 05.02.2010.
38. Norton Rose Group, `Satyam: what are the consequences for offshore outsourcing?` Published 16.01.2009,

<http://www.nortonrose.com/knowledge/publications/2009/pub19079.aspx?lang=en-gb&page=all>, accessed 12.05.2010.

39. Ojelanki K. Ngwenyama, William E. Sullivan, 'Secrets of a Successful Outsourcing Contract: A Risk Analysis', <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.105.2660> accessed 05.03.2010.

40. Paul Kirvan, 'IT Disaster Recovery Plan Template', <http://searchdisasterrecovery.techtarget.com/generic/0,295582,sid190_gci1370683,00.html> accesses 20.04.2010.

41. Periklis A Pappous, 'The software escrow: the court favorite and bankruptcy law', (1985), Santa Clara Computer&High Tech L.J. 309.
42. Pinsent Masons, 'User`s Guide to Outsourcing' (2008), <http://www.out-law.com/page-364> accessed 11.04.2010.

43. 'Protecting IP rights throughout an outsourcing project', <http://www.brownjacobson,.co.uk/press_office/articles/protecting_ip_rights_through_o.aspx> accessed 23.05.2010.

44. Protiviti. APICS. 'Managing the risks of outsourcing: a survey of current practices and their effectiveness', <http://www.protiviti.com/en-US/Insights/Surveys/Pages/Managing-Outsourcing-Risks-Survey.aspx> accessed 22.03.2010.

45. Pushkar Sinha, 'Data recovery techniques and limitations', <http://ezinearticles.com/?Data-Recovery-Techniques-and-Limitations&id=264278> accessed 17.04.2010
46. Richard Hawtin, 'No-one ever sues on an outsourcing contract' (2007) C.T.L.R., 13(3), 88-90.

47. 'Risks of Offshore Outsourcing', Published: 11.11.2008, <http://outsourceportfolio.com/risks-of-offshore-outsourcing/> accessed 15.03.2010.

48. Sam De Silva, 'A contractual approach to manage security risks when outsourcing' (2009) C.T.L.R. 2009, 15(3), 51-57.

49. Sam De Silva, 'Best Practice for Contract Management', Published: 30.10.2008, <http://www.it-director.com/business/content.php?cid=10828>, accessed 15.03.2010.

50. Sam De Silva, 'Lessons Learned - Contract Renewals and Exit Management', Published: 07.04. 2009, <http://www.it-director.com/business/content.php?cid=11186>, accessed 15.03.2010.

51. Sam De Silva, 'Avoiding Service Level Howlers', Published: 12.12.2008, <http://www.it-director.com/business/content.php?cid=10955> accessed 15.03.2010.

52. Sam De Silva, 'Smart Outsourcing: Avoiding the Pitfalls', Published: 19.01.2010, <http://www.it-director.com/business/content.php?cid=11830> accessed 15.03.2010.

53. Samitha De Silva, 'FSA operational risk systems and control: guidelines for outsourcing' (2003) C.T.L.R., 9(8), 217-225.

54. Shalini Agarwal, Sakate Khaitan, Satyendra Shrivastava, Matthew Banks `Destination India: offshore outsourcing and its implications` (2005) C.T.L.R. 2005, 11(8), 246-262.

55. Shalley Dash, 'The Economic Implications of Outsourcing', Institute of Integrated Learning and Management.

56. Simon Colvin, Garfield Smith, 'An introduction to IT outsourcing', last updated February 2008, <http://www.out-law.com/page-501> accessed 21.02.2010.

57. 'Source Code Escrow - A "Win Win" Solution', Published: 18.12.2006 - Manitoba, Canada, <http://www.hg.org/articles/article_1652.html> accessed 17.05.2010.

58. Treasury inspector general for tax administration, 'Better Emergency Preparedness Planning Could Improve Business Continuity Efforts', 13.02. 2009, Reference Number: 2009-20-038, <http://www.tigta.gov> accessed 15.03.2010.

Other sources:

1. AMR Research 2009 Outsourcing statistics, <http://www.rttsweb.com/outsourcing/statistics/>, accessed 29.03.2010.
2. Basic guide to TUPE, <http://www.out-law.com/page-448> accessed 14.06.2010.
3. Business Continuity Planning, <http://en.wikipedia.org/wiki/Business_continuity_planning> accessed 11.04.2010
4. Business Continuity, <http://en.wikipedia.org/wiki/Business_continuity> accessed 11.04.2010
5. Center for Research on Information Technology and Organizations at the Paul Merage School of Business, University of California, Irvine, 'Writing the Optimal Outsourcing Agreement. An ACS: Expertise In Action White Paper' (2009). Paper based on research conducted by Professors Vijay Gurbaxani and David Fitoussi.
6. Computer Economics, IT Outsourcing Statistics: 2009/2010, <http://www.computereconomics.com/page.cfm?name=Outsourcing> accessed 26.05.2010.
7. Council Directive 2001/23/EC on the approximation of the laws of the Member States relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses.
8. DiamondCluster International, '2005 Global IT Outsourcing Study', (2005) <http://www.diamondconsultants.com/PublicSite/ideas/perspectives/downloads/Diamond2005OutsourcingStudy.pdf>, accessed 22.04.2010.
9. Disaster Recovery Plan, 02.02.2009, <https://online.penson.com/PensonBusinessContinuityPlan.pdf> accessed 11.04.2010
10. EKAM Solutions Ltd, Disaster Recovery, <http://www.ekam.ie/data_recovery.pdf>, accessed 20.04.2010.
11. HI Europe, The UK IT and Business Process Outsourcing Report, <http://exactsearch.com/ipi/IPI.nsf/LookupPDF/trui/$file/trui.pdf>, accessed 11.05.2010.

12. Iron Mountain study, <http://www.ironmountain.com/ipm/>, accessed 24.05.2010.

13. IT disaster recovery (DR) plan template: A free download and sample plan, Published: 13.10.2009, <http://searchdisasterrecovery.techtarget.com/generic/0,295582,sid190_gci1370683,00.html> accessed 13.04.2010

14. ITIL Service Continuity Management, <http://www.itlibrary.org/index.php?page=IT_Service_Continuity_Management> accessed 15.04.2010

15. PACE, 'Business Continuity Planning Guide', <http://www.ogc.gov.uk/documents/PACE_-_BCPG.pdf> accessed 12.04.2010.

16. Sample software escrow agreement, <www.jian.com>, accessed 20.05.2010.

17. Short Survey of the Principles of European Contract Law: Introduction to the Principles of European Contract Law Prepared by The Commission on European Contract Law, <http://frontpage.cbs.dk/law/commission_on_european_contract_law/survey_pecl.htm> accessed 23.04.2010.

18. Technology Law Assistance, Buyer's guide technology contracts.

19. Transfer of Undertakings (Protection of Employment) Regulations 2006

20. 'What is an Indemnification Clause?', Published: 21.05.2009, <http://www.associatedcontent.com/article/1747916/what_is_an_indemnification_clause.html>, accessed 27.05.2010.

21. 'What's the Service Level Agreement?', Published 17.09.2007, <http://blog.sharepoint-recovery.com/2007/09/17/whats-the-service-level-agreement/> accessed 23.02.2010

22. <www.SearchCIO.com>, February 2010