UNIVERSITY OF LJUBLJANA

FACULTY OF ECONOMICS

MASTER'S THESIS

INFORMATION SYSTEMS AND INFORMATION TECHNOLOGY SECURITY OUTSOURCING IN SLOVENIA

Ljubljana, August 2016 SAŠKO MUKAETOV

AUTHORSHIP STATEMENT

DECLARE

1. this written final work of studies to be based on the results of my own research;

2. the printed form of this written final work of studies to be identical to its electronic form;

3. the text of this written final work of studies to be language-edited and technically in adherence with the FELU's Technical Guidelines for Written Works, which means that I cited and / or quoted works and opinions of other authors in this written final work of studies in accordance with the FELU's Technical Guidelines for Written Works;

4. to be aware of the fact that plagiarism (in written or graphical form) is a criminal offence and can be prosecuted in accordance with the Criminal Code of the Republic of Slovenia;

5. to be aware of the consequences a proven plagiarism charge based on the this written final work could have for my status at the FELU in accordance with the relevant FELU Rules;

6. to have obtained all the necessary permits to use the data and works of other authors which are (in written or graphical form) referred to in this written final work of studies and to have clearly marked them;

7. to have acted in accordance with ethical principles during the preparation of this written final work of studies and to have, where necessary, obtained permission of the Ethics Committee;

8. my consent to use the electronic form of this written final work of studies for the detection of content similarity with other written works, using similarity detection software that is connected with the FELU Study Information System;

9. to transfer to the University of Ljubljana free of charge, non-exclusively, geographically and time-wise unlimited the right of saving this written final work of studies in the electronic form, the right of its reproduction, as well as the right of making this written final work of studies available to the public on the World Wide Web via the Repository of the University of Ljubljana;

10. my consent to publication of my personal data that are included in this written final work of studies and in this declaration, when this written final work of studies is published.

The undersigned Saško Mukaetov, a student at the University of Ljubljana, Faculty of Economics, (hereafter: FELU), author of this written final work of studies with the title INFORMATION SYSTEMS AND INFORMATION TECHNOLOGY SECURITY OUTSOURCING IN SLOVENIA, prepared under supervision of Prof. Dr. Aleš Groznik, Full time professor

Ljubljana, 30 August 2016 Author's signature:

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

Conventionally, software applications that companies are operating are installed on personal computers or servers, which are located on the organizations properties. When companies agree to deploy new software solutions for their business, they buy a software license from a software vendor and internal Information Technology (hereinafter: IT) people or a third-party firm installs the software on the in-house computer systems. The complete process of buying and implementing a software solution, entails capital investments for licenses, hardware and software implementation. After implementation, the software maintenance is carrying processes like backups, bug fixes, upgrades and updates, which are necessary and further expenses will incur. The utilization of extensive enterprise applications such as Enterprise Resource Planning (hereinafter: ERP) or Customer Relationship Management (hereinafter: CRM) can add up additional costs that can be very high for many small or medium companies. With the aim to diminish the primary expense that come along with the whole process of buying a software license and then later the maintenance of it, a software distribution method can be used that was introduced in the late 1990s. Application Service Providers (hereinafter: ASPs) offer individuals or companies' access to software applications and related services over a network, instead of installing them on the companies' in-house IT and information systems (hereinafter: IS). Rouse (2010) says, occasionally, this process also referred to "apps-on-tap', can become an important alternative, not only for small companies with low budgets for investing in information technology, but also for bigger enterprises as a form of outsourcing.

The ASP hosts and manages the application from a central location rather than on each client's site. Several users may rent access to the same software via the network, such as the Internet, and in return, the ASP charges a fee for the services, which depends on the number of users, applications, transactions, or other measures. The ASP either owns the software or has an agreement with the vendor that enables him to license out the access of the software. All ASP services are designed to be a one-to-many offering, which means that many companies can subscribe to the service over a specific contact period. The Internet mainly supports the expansion of the ASP business model. The high software requirement and the increasing need of companies to focus only on the core competencies, due to the increasing competitions among industries and businesses, foster the use of ASPs. Michael Corbett, as outsourcing expert says, "The single most visible result of this hyper-competitive environment is rapid commoditization". This overactive competitive environment forces organization to become superior dedicated and more specialized, to evaluate each activity to determine if and how it provides a unique competitive advantage. According to Corbet (2004), as a result, companies and businesses are investing in those areas that provide bigger advantage and exclude or outsource the activities that are not fundamental to the centre business model.

The outsource process is ~~a~~ very much a risk process that involves a set of different risk factors. Businesses and organisations strive to achieve a balance between the expected benefit and the relative risks stemming from outsourcing, by choosing the most appropriate answers to the following questions: what to outsource, to whom, when or for how long and finally how to manage the outsource arrangement. Concerning the first question, both researches and practitioners agree that activities related to the core business of the organization should be kept in-house, while those that are peripheral to the business are more suitable for outsourcing.

In circumstance of information technologies and information systems (hereinafter: IT/IS) security outsource, the supreme meaningful motive for which businesses and companies decide to outsource information technologies and information systems security is that, a single organisation, particularly the one that is of medium or small size, is questionable, does it possess all the abilities, skills and knowledge obligatory for effective security management. Mainly, since security threats and incidents are increasing together in number and in diversity (DTI, 2004). According to Karyda, Mitrou and Quirchmayr (2006), another fact that drives organisations towards information technologies and information systems security outsourcing is the difficulty of attracting and retaining qualified and experienced employees in the area of security, as well as the high costs of employing them.

Description and purpose of the research. Information technologies and information systems outsourcing covers a wide range of information technologies and information systems related functions, including software development, hardware maintenance and web hosting, and constitutes well-established and fast growing industry. In the market, there is an increased demand for web hosting, e-commerce hosting, remote data storage services and security services. As the main objective of this paper is to look for market demand of information systems and information technologies security outsourcing, it is most important to understand if IS/IT security outsourcing should be examined under different perspective from traditional information systems and information technologies outsourcing.

Considering the fact that primary reason for which companies turn to information systems and information technologies outsourcing are financial, they include some expectations of improved rate of returns on investments (hereinafter: ROI), reduced cost and economies of scale that otherwise could not be realized internally. By outsourcing, the~~re~~ information systems and information technologies functions organizations also aim to: have improved access to specialized knowledge and best practices, receive better quality services, have increased business continuity capability in case of internal incidents and achieve flexibility with regard to technology.

According to Gottschalk and Solli-Saether (2006), companies expect to gain improved competitiveness and a chance to focus their efforts and use their resources on their core competence as a collective learning in the business, especially how to coordinate diverse

production skills and integrate multiple streams of technology.

Operating and management information systems and information technologies (hereinafter: IS/IT) security services is a prospering business area, but there are not many information systems and information technologies security outsourcing investigations and researches done. There are many reasons for that. Theoretical instruments and methods to information systems and information technologies outsourcing research, for example, Resource-Based Theory (hereinafter: RBT), Transaction Cost Theory (hereinafter: TCT), Resource Dependence Theory (hereinafter: RDT) and Agency Cost Theory (hereinafter: ACT) cannot be affected in the information systems and information technologies security outsourcing examination. Comparing the usual information systems and information technologies outsourcing, in the case of security outsourcing decision-making is much more problematic by cause of many reasons. It is not well defined which security functions are appropriate for outsourcing and which should be kept in-house. No set of standards and principles, describing security services whose outsourcing would expressively benefit companies exists. Information systems and information technologies security could be of strategic significance for many organizations. However, it is usually considered as a simple commodity asset. Approximating the cost of security is challenging.

Most usual information systems and information technologies outsourcing resolutions are based on cost approximation and the ROI assessment. Moreover, estimating the cost of security is not direct. Regardless of whether security is chased in-house or outsourced, risk remains with the organization, which has to stand the impact in case of demonstrated risks. Conclusively, as many studies and specialists suggest like Dhillon and Backhouse (2000), Goodwin (2004), Nosworthy (2000) and Siponen (2000) there is the subject of raising or increasing security awareness between end-users and generating the security sophistication within the organization,.

The information systems and information technologies, IS/IT security services that the organizations and businesses are more likely to outsource include intrusion monitoring, e-mail virus and spam filtering, penetration testing, information technologies IT auditing, firewall configuration and management, virus protection, network monitoring, security upgrades, security education and training, virtual private network (hereinafter: VPN) management, user access management, data classification and more. According to a study by the The Corporate IT Forum, just 5% of the respondents had outsourced security and 48% said that they would not outsource their information technology IT security teams (Ashford, 2012).

The ultimate goal of the company is to achieve the balance between in-house and outsourced security services that will lead to better information system IS security management at reasonable costs for the organizations. One of the objective of this research paper is to find out what are the expectations of the companies with the regard to the enterprise applications

offered via the IS/IT outsourcing business model, with the emphasis on the information systems and information technologies IS/IT security outsourcing services. Second objective is to investigate what are the main concerns and doubts of the companies, in order, to make the decision on implementing information systems and information technologies IS/IT security outsource model. The last objective is to analyze the most important and challenging factors about service level agreement (hereinafter: SLA) and contractual agreement for information systems and information technologies IS/IT security services outsourcing.

Below are some of the research questions addressed:

- Is a specific, accurate and reliable contracting agreement SLA, defined for the outsourced services? – By your opinion, what are the factors and parameters you consider most important/challenging for the SLA for information systems and information technologies security outsourcing and why? (Prices, verification of services, track of services etc.)

- How the outsourced information systems and information technologies IS/IT security services are measured, controlled and verified by both parties in the agreement?

- What are the reasons/expectations for which your business or organization turn to information systems and information technologies IS/IT security outsourcing?

- Which information technologies, IT security functions are suitable for outsourcing and which should be kept internally?

Research methodology. The thesis will first contain theoretical part, explaining more about the Information Systems and Information Technologies and then continuing with the theoretical clarification of the information systems and information technologies outsourcing and specifically security outsourcing with the use of books, scientific articles and researches. I will conduct structured interviews with several organizations and businesses where I will collect data from questionnaires using descriptive methodological approach.

The survey questionnaire will help in getting data and overview about security awareness level of the Slovenian market itself, so the main questions will be about different perceptions for information systems and information technologies IS/IT security that currently are using in the outsource market. Also, the structured interviews with the organizations will deliver information about which security functions are suitable for outsourcing and which should be kept internally. This will give my thesis also additional research point; explore important area like decision-making factors for risk and the legal part of the information systems and information technologies IS/IT security outsourcing. The structured survey interviews allow flexibility that is necessary since most of the organizations interviewed are big enterprises.

INORMATION SYSTEMS AND INFORMATION TECNOLOGIES (IS/IT) OVERVIEW

1.1 Introduction

Information systems are formed to accomplish specific objectives and are systems that in general, are processing some data into information and knowledge. Data or raw data, refers to a description of activates, transactions, or customers and products that are recorded, stored or classified. Data is_the raw material that the information is producing. In order for that information to be useful, data must be with good quality, integrity and reliability. To do that, the data must be maintained.

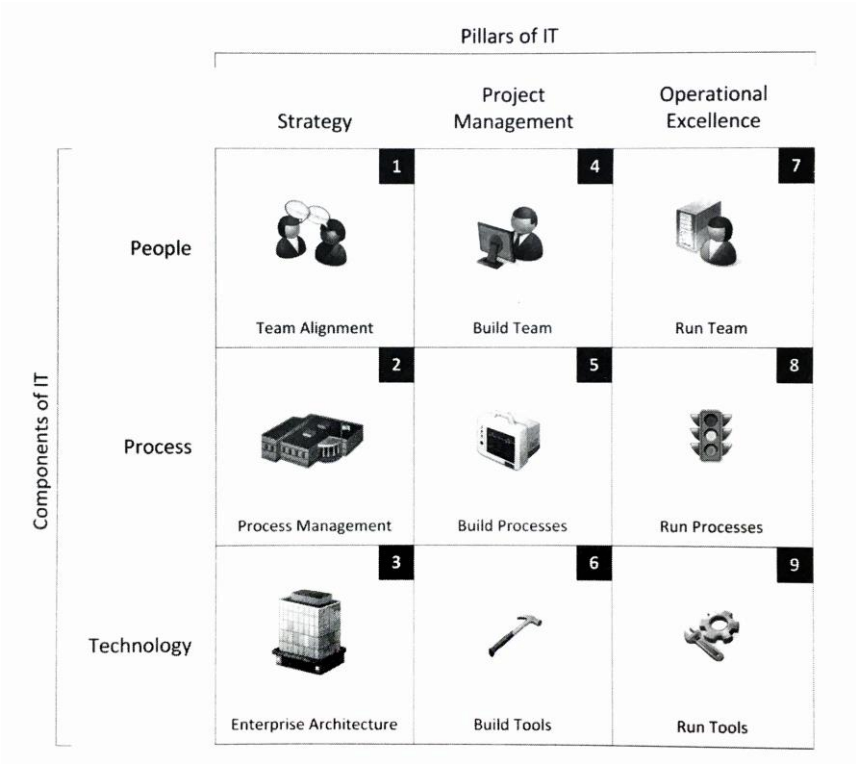
Stored, organized and searchable data is a database. Processed and organized data, putted into context in order that it has meaning and present evident value to a process is information. Altogether, data and information is the knowledge, which should be meaningful, understandable and applied to a current problem or activity that will result in learning and accumulated experience. Businesses and organizations are using varieties of computing systems, which generated the term Information Technology. According to Turban, Volonino and Wood (2013), the information technology IT is organization's set of information systems IS, the users that they acquired and the management system that supervises them.

Another term that is significant to be stated is "CBIS". Computer-based information system (hereinafter: CBIS) is an information system that procedures computer technology to accomplish all the propositioned assignments and requests through various applications. Although, not entirely all information systems IS, are computerized. In this modern digital living, most are. So, the term information system – IS is used synonymously with the term – CBIS.

According to Rainer, Prince and Cegielski (2013), the components of a computer-based information systems CBIS are the information technology IT components (hardware, software, databases and networks) and information technology IT pillars graphically presented on Figure 1., the procedures that are combination of the information technology IT components in route to develop and process information and produce a required output, and the people that use, interface and utilize the hardware and software.

Companies, organisations and businesses rely on many businesses utilities from their information technology, IT department and the work there. The information technology department is to guard the constancy of the business's information technology infrastructure. Main apparatuses of an organization's information technology, IT infrastructure are the hardware, software, networks and communication capacities together with the Internet and Intranets, databases and data employees and the information management employees.

Figure 1. Components and Pillars of IT



Source: K. S. Proctor, Optimizing & Assessing Information Technology – Improving Business Project Execution, 2011.

The whole strategy and maintenance of company's information technology infrastructure can determine the capacity to efficiently store, protect and manage data (Turban et al., 2013).

The term infrastructure is changed and modified in the information technology and information system IT/IS field. When the term was initiated, had narrow and only technological reference and more traditional view, centralizing all technological means as computers, data communications and operating systems and also the labourers (information systems operators and information system designers) and all organizational procedures in the information systems department of a company to be part of the infrastructure. More recently, this term has heavier feel, progressively denoted to as IT – based infrastructure with developed point of national and international information technology polices making the information technology investments to provide also the telecommunication part, allowing individuals and organizations with interconnection on a grand scale. According to Renkema (2000), this perception of information technology – based infrastructure also expanded importance as key element on the strategic management of information technology, allowing improved interaction and cooperation between separate employees, functional employees, business units and the associates in the business chain.

Before, information technology managers had the option to either build in-house or complete purchase of the technology or services. Nowadays, IT people have the option for outsource, in which the technology or service is rented or leased on a regular or as-needed basis (Turban et al., 2013).

1.2 Information Security and Information Security Market

1.2.1 Information Security

The level of guard against damage, loss, threat or some criminal undertakings is a general description of security. Information security indicates entirely of the processes and polices aimed to defend an organization's information and information systems IS from unapproved access, usage, disclosure, distraction, modification or damage. Any action that can harm the correct performance of organization's information system or information itself can be seen as deliberate criminal action. Significant notions of information security are the terminologies threat, exposure and vulnerability. A threat to an information system IS is any threat to which a system may be exposed. The exposure of an information resource is the harm, loss or damage that can result if a threat compromises that resource. An information resource's vulnerability is the likelihood that the system will be damaged by a threat. According to Rainer and Cegielski (2012), the influences that are growing the vulnerability of organizational information resource are:

- the interconnected, interdependent, wirelessly networked business environment
- speedier, smaller and inexpensive computers and storage devices
- declining skills needed to be a computer hacker
- international organized crime fascinating over cybercrime
- absence of IT management maintenance

1.2.2 Information Security Market

Living in a world where protection of companies' information is important aspect of their security, we can expect that software solutions for this problem are rising. The market for information security and network cyber security software, services and equipment are aggressively trying to persist and survive. Just the greatest companies, which are in the right market segment, are profitable and smashing up their smaller competitors. On company's perspective, where they are operating in difficult economic times and having low budgets for security services are facing the need for more secured environment due to powerful increase of shared information on the Internet and on the digital social media presence. According to Axelrod (2004), company's management departments are willing to see the risk preference as

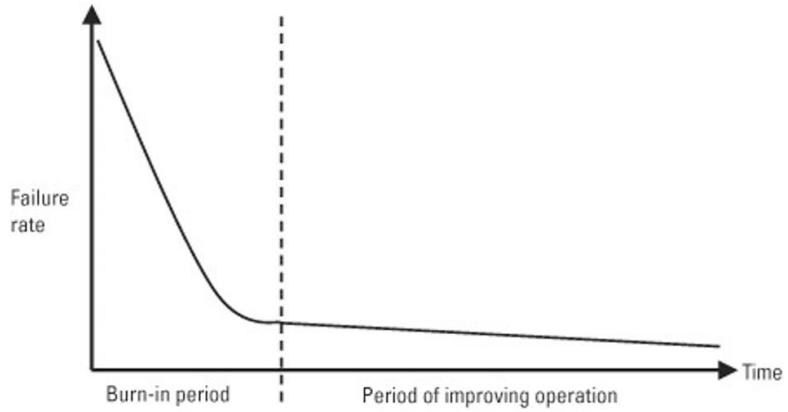
the cost of additional protection versus the possible damage if something bad occurs, and they consent on luck.

1.3 Information Security Risks

More common IT-related security risks that can affect outsourcing or how outsourcing affects or indicates them are the threats and vulnerabilities as two sides of IT security risks. Threats can be observed as they are occurring from internal sources or threats from external sources. Threats that can appear from internal source can attack the integrity, confidentiality and the availability of a company's computer networks and systems. Example for an internal threat can be an employee that might be fired or still on staff from the IT department that possess sensitive information and knowledge of the company's systems, procedures, applications, access to applications and other systems and have the aspiration to make a damage. That employee, supplier or consultant can procedure the knowledge for own advantage. Other internal threat that can happen is the person in the IT department who can leave an error or hole in the system application and not report it. Threats from external source also can happen. The hacker is the person who attacks the company's system and is a greatest kind of threat. Damaging the web site, steal credit card money and valuable assets or leave "smart-aleck" notes to a core system are the possible actions that can happen from a hacker attack. The well-known terms computer viruses and spams that are all over the Internet are in this group also. Worm, Trojan horse or just a computer virus can be made by someone who is not certain who can infect and how the virus will be referred to others. Companies and organizations, especially bank institutions or telecommunication operators, are always having some policy regarding employees Internet activates and they provide strict access and e-mail allowing's. Interesting example in this regard of external source of IT security threat is the industrial or national spy, which can be dangerous to a company or organization. Group of persons or just a single individual spy can steal networks, operations, data secrets that can indicate to a straight selling of the information to an outside party. Vulnerabilities can range from technical to human form. In all today's modern computer systems and networks there are lot of characteristics for vulnerability. In general, they are easily accessible although they are complex and written for more features rather than with better security. According to Axelrod (2004), the technology that control, monitor and manage the computer systems or the software solutions in general is not built to be highly secured.

Many risks can happen from software applications. They are system risks, operational risks, and operator and administrator risks. In figure 2, there is the pattern in which more obvious errors in the software are seen and secured earlier and over time different errors can occur creating the on-going drop in failure rate without wear-out period. According to Axelrod (2004), the vendor or the maintenance support centre of the bought software sometimes can be without support policy, so new software replacement must be achieved.

Figure 2. Pattern of Software failure



Source: C. W. Axelrod, Outsourcing Information Security: Computer Security Series, 2004.

IS/IT OUTSOURCING

2.1 IS/IT Outsourcing introduction

All organizations and companies are building and creating the IT strategy and the decisions on the IT investments based by the core IS and its processes for developing, acquiring and implementing. These processes and decisions for investing can be made by choosing in-house development or outsourcing. In-house development process is mainly done in the company's IT department and this decision is often taken when the company possess sensitive, proprietary or confidential data information with the help of consulting vendors or companies. Choosing the development process of the IT by third party or vendor is outsourcing. The outsource vendor or the third party company for doing the IT development or IT processes in the same country is called onshore sourcing. Choosing to outsource the processes by company in other country non-domestic is called offshore sourcing. Other options for outsourcing can be the rent or purchase of some IT services via the cloud computing or the (hereinafter: SaaS) - software as a service solution (Turban et al., 2013).

Choosing to use some external resources to operate, manage or even build an information system, companies can choose different forms, like using cloud computing, software as a service (SaaS) provider or ASP. The outsourcing vendor or external provider can be domestic or from foreign country. Choosing domestic outsource company can be done when skills, assets or resources are needed for some function that the actual stuff do not posses. For example, installing new chain management system can require new 20 to 30 people with skills, knowledge and experience in supply management software. Instead to hire new stuff and provide additional training as a plus cost, the company can outsource this process. Choosing an offshore outsourcing carries more cost-driven analysis, considering, for example, a skilled person in the United States will earn much more than the same skilled

individual in Russia. The Internet and the new trends in communication via Internet bargain the barriers and significantly reduced the costs of it. Any outsourced service also carries a lot of responsibilities. According to Laudon and Laudon (2015), any company that outsource a service, has obligation to completely understand the project scenario, its necessities, developing and implementing process and the support of it, the benefits, cost analysis and monitoring process.

Outsourcing as a term, can be used significantly to define different kinds of services delivered by third parties. According to Axelrod (2004), concentrating on outsourcing IT services, it has developed a production that companies are operating and accomplish revenues in multi billions of dollars per year and reaching double digit growth.

The expression information technology IT outsourcing is the transmission of an organization's in-house IT infrastructure, employees, processes and developments or applications to an outside external resource provider. Outsourcing can contain everything from the simplest to the highest sophisticated IT infrastructure, process or application. Because the outsourcing of information is sensitive procedure, outsourcing contracts are created to manage non-core information technologies, information or processes. According to Palmatier (2001), the outsource market can be divided into three main groups:

- application outsourcing (hereinafter: AO)

- business process outsourcing (hereinafter: BPO) and information utilities

- platform IT outsourcing

Businesses are purchasing IT applications from outside service appliers or external organizations in many circumstances. Companies with outsourcing can test and try a new IT technology, minus gigantic up-front investments in procurement the technology. Companies can use outsourcing to guard their inner networks and make path to external experts. The outsource trend is rising and many companies reposition processes offshore for cost savings, although the risks may rise. According to Rainer and Cegielski (2013), the only component which defines the risk level is the decision where services are being offshored.

By Frost (2000), Business Process Outsourcing, BPO promises to be the future for running an IT successful business. BPO involves both the outsourcing and redesign of business processes. Large corporations need to innovate and stay ahead of the competition, and to act in that way they often need to place new services, products and solutions to the market. BPO enables companies to shatter the boundaries of their traditional businesses.

Companies are deciding to outsource an IT function like network or computer management, applications, development, testing, support or some of the information security functions. The reasons for going for outsourcing can be to cut on costs, but still have the productivity benefits, or company wants to concentrate on the core business objective. By Axelrod, 2004,

the decision process of choosing what function to outsource can be very difficult for companies. The decision can be occasionally very subjective and can require huge numerical investigation of determination of costs of choosing the ASP or the outsourcing vendor. Analysis of reasons and benefits that outsource can deliver versus in-house functioning must be done.

2.2 Drivers for IS/IT Outsourcing

2.2.1 Decisions and motives for IS/IT Outsourcing

Many examples and case studies are showing that outsourcing can be choice for companies to solve industrial conflicts. According to Pratap, (2014), outsourcing can be additionally controversial and can be seen as political or an act to make labour problems. There is an example of the US bicycle industry leader Schwinn, when shifting the production to Taiwan, followed mayor labour problems in its factories in the early 1980s in the states.

Beyond the stories that are saying that outsourcing is complex process, mixed up with many external factors and people, companies can have strong motives for choosing the outsource option for their development or implementation of the IT services. In the book "Outsource or Else!" according to Mezak and Hilliard, 2016 owners of a company, the outsource decision is detailed presented and particular in a case when the outsource decision saved the company. They sum up the process and clarify the benefits of software outsourcing as perfect IT solution. The key benefits of software outsourcing are:

- fast improvement and new technology knowledge in company's IT staff and the programming team
- more flexible IT team
- more quality IT talented outsourced team, resulting in better and higher access and speed
- technical expertise that can be demanding for employing locally
- up-to-date IT innovation by giving company's IT team to work and meet clients and teams with better experience
- learning of the latest software development technologies by practises and participations

Key finding about the decision for IT outsourcing, when companies are questionable about the performance of hiring outsourced developers, is showing that high quality developers can be met everywhere. Managers and business people, who do not posses' knowledge for software outsourcing process, can act by default that the excellence of performance is superior of onshore developers. However, great offshore companies hire also great and

educated developers. They can be highly trained and experienced people with advanced knowledge of the latest IT trends, so companies just need to know how to search for them.

Other finding is suggesting that companies should follow and focus on the core vision of the business. Considering everything the software development process can be complex and can require many tasks and requests, a team of talented people must be working together as a team, not just the greatest developer to gain all the attention. This finding is recommending that the business leader should focus on how the software solution would be delivered to the market and what will be the strategic plan of delivering it, so the software developers team would follow this vision, just to inspire your business idea and achieve the highest achievement.

Further finding is about how to find the right outsource company for your IT services. Companies should first have a strong knowledge of all the technical requirements that the outsource company must posses. Furthermore, could check the company portfolio to see recent projects done and could ask for references from other companies or clients that worked with the one to proceed opinions. In the end, a proposal can be sent with the project demand, time and cost analysis for hiring the development team. This process can be done to multiple outsourcing companies and candidates. Visiting the companies and scheduling a meeting can then follow, to comforting that company culture can fit the outsource organization and vice versa and a strong working relationship could happen. This investigation can be crucial for the project development. After finding several possible outsourcing companies or organizations as candidates for developing your IT project senior meetings and visits can be done. Practical motives for this kind of visits can make sure that the outsource company had done similar projects, as the earliest investigation recommend, with the one that the company needs.

The other motive is to make sure that great, capable, experienced leaders will work with the company. Furthermore, the technologies, testing processes, communication channels and methodologies of the IT process can be seen and talked in person. Further finding, that can help the IT outsourcing process decision, is that quality matters as much as the price. Business leaders should know that quality is not defined only on the technical abilities and knowledge, but also by team's eager to learn, cooperate, communicate and of course by the general fit with the company's culture and core values. Even taking in account that an offshore outsource applier can cost between 25 to 65 percent lower than an onshore developer, additional risks can rise if the offshore outsource appliers include poor infrastructure or working circumstances. Indeed effective and strong balance is needed among capacity and price. According to Mezak and Hilliard (2016), cultural differences and relationships are other aspects that must be taken in consideration same as drivers for the outsource decision process.

In the following, these are the strongest company's drivers and motives for selecting outsourcing as method for the IT services.

2.2.2 Cost-Beneficial Motive

In general, all evaluated literature about what drives companies to select outsource as solution for the development or implementation of their IT services, the first and the strongest motive is the cost saving reason. Started in the 1980s and 1990s, when competition and recession encouraged the organizations towards excluding the luxury of possessing all parts of a company value chain. In that time organizations started to re-engineering and de-layering the business processes and outsourcing option started to be part of corporate organizing. Diversification and the run of conglomerates, after raised acquisitions into unrelated areas created the corporate headquarters to be very unfamiliar of the initial business. In this stage of organizations, the outsource option as an option for cutting costs and make better savings increased popularity. According to Rattrap (2014), this plan for selecting third party and narrower manufacturing base continued to increase also in behalf of increased economies of scale and scope in the favour of the contractors.

Outsourcing can lower the fixed IT costs by allowing them to move from mayor capital expenses to operational expenses, or from fixed to variable costs. IT capital expenses can contain enterprise software licenses, networking equipment or servers. Outsourcing can exclude the need to purchase hardware, installing and building software or paying software-licensing fees. This outsourcing technique can deliver superior flexibility and can exclude the necessity for major capital investments. For example, the State Street Bank in Boston possess its own extremely personalized software to manage its properties and assets and around 25 percent of the bank IT budget is for software development. The bank outsourced the data centre to a private cloud to achieve cost savings and their software to be more efficient. By the end of 2014, the bank expected and realized $600 million in savings (Rainer et al., 2014).

To make efficient cost saving strategy, organizations and companies are using combined IT strategies for the IT processes like outsourcing (domestic sourcing (onshore) and offshoring), SaaS or cloud computing methods (Turban et al., 2013).

2.2.3 Improved Innovation and Capabilities Access

Four influential factors are driving the innovation revolution in company's perspective. The demand, described through actual gross national product in the world's leading and most rising economies, is doubling each 14 to 16 years and that generates a host of innovative professional marketplaces, certainly huge to attract innovation. Second factor that drives the innovation revolution is ~~that~~ the supply of researchers or experts, knowledge and technologies, accelerated and the access to them, turn out to be easier than ever. Software analysis, telecommunications and market feedback technologies are processes that smaller companies can perform and can participate in emerging markets, in the interest of lower costs and risks. The grown of communication capabilities via the Internet and other IT abilities and the interactions among them, is the third factor for effective innovation revolution. Together with the lower taxes, privatization, the lower barriers to enter foreign, international markets

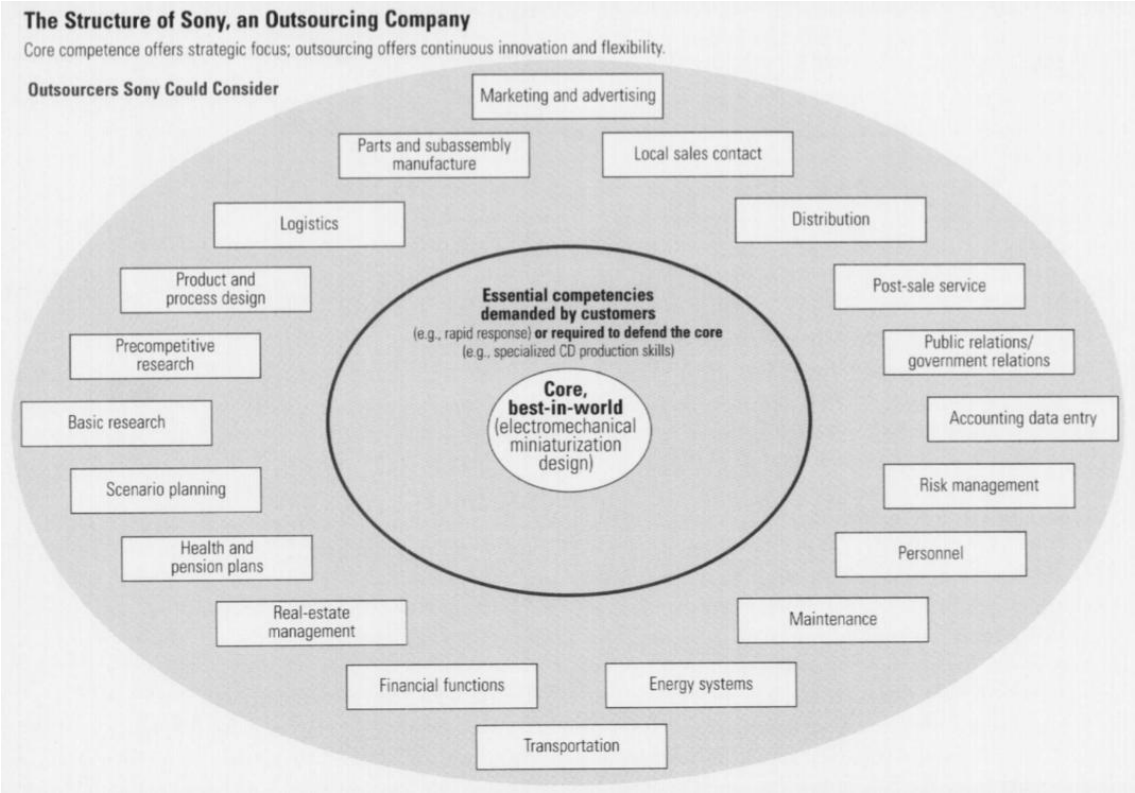
and the lower capital investments needed, companies and organizations worldwide have the power to develop and achieve expansion in knowledge more easily. According to Quint (2000), latest communication platforms and systems, management strategies and software solutions have allowed far improved coordination of innovation actions.

While the cost saving motive for companies and organizations is one of the primary reasons for outsourcing, and continued to be important, other noticeable inspiration for organizations and companies is the desire to gain knowledge of new technologies, practices and abilities. For example, study case in the Indian banking industry showed that banks and bank institutions value factors like access to innovative skills or services or development in customer services way further then clean cost savings. This motive is rising thanks to, many of the breaking and edgy innovations that happened in history that are in general delivered by big organizations or large companies with huge resources. Nowadays, more and more small companies have the same access to new tools, latest and modern technologies same as the big ones, promising that all companies can contribute in the competition for innovation. According to Pratap (2014) in an international journal acknowledged that *"The greater the cognitive distance and heterogeneity of knowledge inputs, the greater is the consequence for innovation ".* In a study research of contractors' selection by companies, was found that companies that need slighter technical complexity innovation for their IT process, they more rely on outsource appliers and outsource companies. As this technical difficulty and risk of uncertainty rose, more companies choose internal development.

2.2.4 Emphasis on Core Abilities

Besides the primary motives discussed for outsourcing, the cost and innovation related drivers, this motive can also be enormous if organizations and companies move or outsource all not-core activities and processes in the IT department and develop to advance and concentrate only on the core and most important ones. Choosing to outsource all of the not core functions and processes, companies and organizations will lower the cost for their development and maintenance and in the same time, will possess the same processes just outsourced, but developed with latest innovation technologies by an external contractor. Additionally, the company can focus on key and core resources, financially and managerially, in which the company is competing with the competitors in the industry. Attractive example in this regard, is the practice of Nike and Reebok companies that focus only on the core ability, the design and marketing, and all other processes and manufacturing activities are outsourced. In this process, most important thing for companies and organizations is to identify appropriately and precisely what are the core abilities and areas, and what "core" actually is. As seen in Figure 3, the structure of Sony company, its core ability, is the electromechanical miniaturization design and all other activates in their structure can be outsourced. Risk that can appear, related with outsourcing the activities, ~~that~~ are not core to a company strategy, is if the outsource applier enters the market itself as competitor. According to Pratap (2014), studies found that companies usually do not feel the risk or count the possibility that the outsourcer will appear on the market, and act as competitor.

Figure 3. The structure of SONY, an Outsourcing Company



Source: J. B. Quinn, Outsourcing Innovation: The New Engine of Growth, 2000.

2.3 Application Outsourcing (AO)

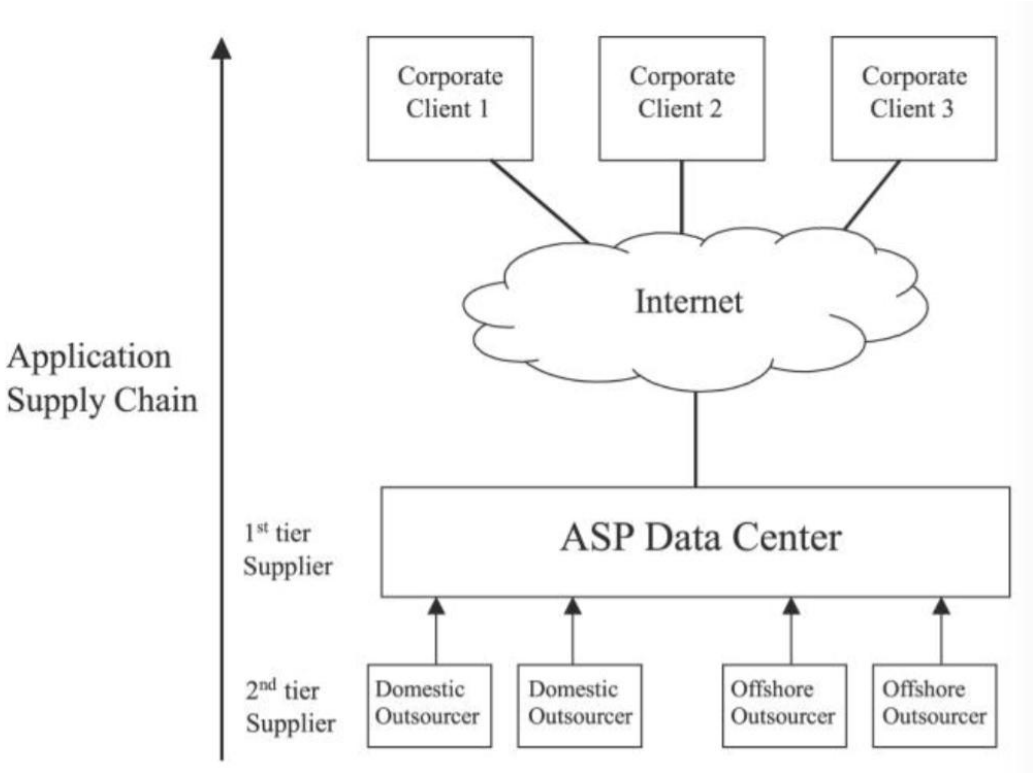
Application outsourcing (AO) stands of compilation of Application Service Provider (ASP) and Application Maintained outsourcing (hereinafter: AMO). The ASP and the AMO are subgroups of the AO market. The application provider is accountable for the management and the maintenance of the software applications. The differentiation between an ASP and an AMO is who essentially possess the application. An ASP remotely hosts and delivers packaged applications to the client from a central location. The client is efficiently rent the application on a per-user or per-use basis. An AMO keeps management for patented, packaged applications from whomever the client side or the provider side. Business process outsourcing BPO and information utilities providers are mainly concerned by economic and well-organized outsourcing for the greatly high-level but repetitive business processes. Processes can be as difficult and complicated as accounting or finance, or more repeated and frequent processes such as payroll. The provider is dependable for all of the processes linked with the business process. Platform IT outsourcing offers a range of data centre services, such as facilities management, on-site and off-site support services, data storage and security. Core difference for this form of outsourcing, is the transmission of facilities and resources from the client to the provider. The fundamental meaning of an ASP is to permit the client to cooperate only with the ASP for the services contracted. For this integration, central parts are prose cure, trustworthy data centre accommodations and experienced IT specialists who can manage and maintain the services. An ASP solution has many obligations. The ASP channel

must be capable to include choosing software vendor, system implementation, integration and ongoing support. These tasks will describe the development procedure of the ASP. An ASP is qualified of providing any type of software application, from e-mail and instant messaging applications to an ERP system that can manage, control or report. According to Palmatier (2001), an ASP must be capable to offer pre-packaged applications, support services and modify and adapt these services to the clients' needs.

2.4 ASPs as an international drift

Several authors defined the outsource procedure as a significant involvement by external providers of the physical or the human resources correlated with the complete or exact components of the information technology architecture in the user organizations, or more broadly, outsourcing of IS processes as the practise of contracting some or altogether of an organization's IS actions to an external provider (Soliman, 2003).

Figure 4. The relationship of ASPs with Clients and Offshore Outsourcers



Source: K. S. Soliman, A framework for global IS outsourcing by application service providers, 2003.

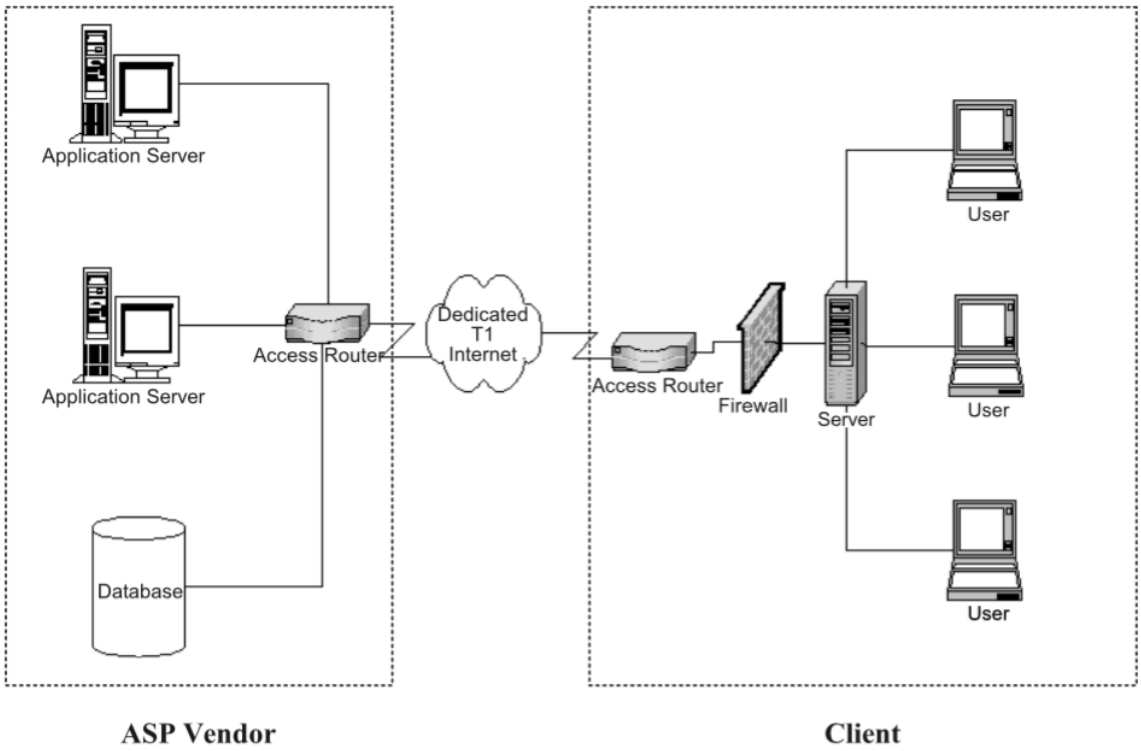
With the enormous development of the Internet, studies found that production costs benefits, transaction costs, asset specificity, internal knowledge, maturity of technology, ASPs value chain and application fit are the main aspects influencing the decision to outsource IS applications to service provider vendors. The international or global trend of outsourcing is in several methods: direct global outsourcing, global outsourcing via domestic consultant and global outsourcing via ASPs. The last method of global or international outsourcing via ASPs became so usual and common for companies because of the growth and expansion of the

Internet in the business world and the recent development in telecommunications technologies enabling the global outsourcing via ASP to become a viable option to many businesses and organizations. Researches define ASP as companies or businesses that distribute and administer applications and computer services from remote data centres to multiple users via the Internet. The data centres are owned by the contracted ASP or rented from a wholesale service provider. The relationship of ASPs with clients and customers and offshore outsourcers is seen in Figure 4. Example in this manner can be the Denver placed ASP that provides hospitality industry services, and switch off the development process in Bulgaria (Soliman, 2003).

Studies also reveals that approximately 70 percent of large organizations are very likely to use an ASP for e-commerce applications, and The Philips Group estimated that in Western Europe, ASP services were increased from $258 million in 2001 to $6.5 billion in 2006. The growth of usage and developing of ASPs resulted many benefits for the companies. The technical components, and ITs and ISs, of every organization should be updated every 1 to 2 years, the licensing fees, hardware and software installations, time needed for trainings of end users and employees is costly process for every company. In that manner, outsourcing internal applications lowers the costs and huge technological investments can be avoided. Therefore, exploiting the Internet as an application stage accelerates the utilization of new systems in reaction to market changes. Furthermore, global or international outsourcing IT applications by ASP, holds many promises for higher quality yet lower cost products. In order for ASPs to provide successful offshore outsourcing, clear proclamations of project prospects should be made. According to Soliman (2003), clear communication and mutual understanding of the project scope will enable clear results and measures. In cross cultural operations and differences, team meetings and tests should be done by strong project management team.

An ASP model of IT service delivery is shown on Figure 5. ASP providers host services to a wide range of industries and most common services that is dominating the ASP market can include business application hosting, ERP, e-commerce, customer relationship management CRM, supply chain management (hereinafter: SCM), digital content storage and wireless applications. Via the Internet, or other communication network these applications are accessed by the clients. Differentiations between ASP and traditional outsourcing are that ASP revenues are driven mostly by e-commerce, CRM and ERP applications, where traditional outsourcing focus more on software development and IT operational activities. Other difference is that traditional outsourcing installs the applications on client in-house server, where the ASP solution brings products and services and their function to be delivered within the Internet or some other communication channel (Chen & Soliman, 2002).

Figure 5. ASP Model of IT Service Delivery



Source: L. Chen & K. S. Soliman, Managing IT outsourcing: a value-driven approach to outsourcing using application service providers, 2002.

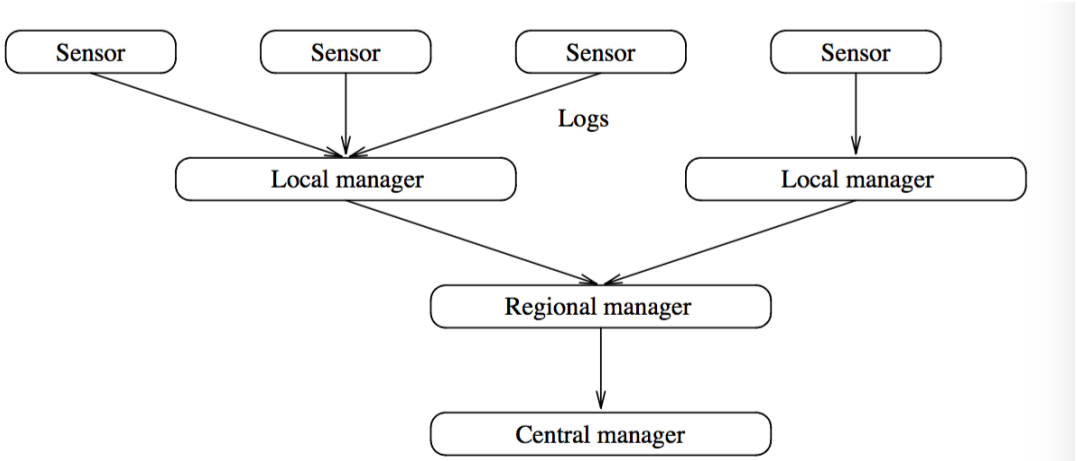
3 IS/IT SECURITY OUTSOURCING

3.1 Security Information Management (SIM) as an Outsourced Utility

The security of information systems and information technologies is an area that is sensitive and is a research topic that can be continuously investigated and studied. New security solutions and techniques were created when the expansion of the Transmission Control Protocol/Internet Protocol (hereinafter: TCP/IP) produced and led more frequent security harms. Exposures on computer's operating systems by the enlargement of the internet endorsed hackers to attack from system to system. Deficient access control measures directed to the formation and growth of intrusion detection systems (hereinafter: IDS). These IDS systems were created and settled to detect irregular and unusual performance of information systems and networks, specifying a crack of security program, and the core objective of this system is to notify operatives on the security condition of the implemented information system. By this system, misuse-detection and anomaly-detection techniques were established to investigate a data stream of the monitoring process of the information systems. In general, the activities that this system provides are just informative and do not protect and guard the information system or technology used from hackers or attack. In this manner, the security information management (hereinafter: SIM) detects and manage signals and alerts by recognition and prevention systems and further security tools and offer a complete analyse of the security state of the information system installed. The SIM is a must for all companies,

especially big corporations or enterprises, that possess complex IS or sensitive data information. SIM represents general information security industry expression, for the gathering of data, for example into log files, and presents a central source for analysis. However, the installation and implementation of this system requires advanced knowledge and can be demanding process to configure, maintenance and manage. Security information management platforms have developed through the years and are great platforms that can provide IT department managers a standardized assessment of the security state of its information systems (Debar &Viinikka, 2006).

Figure 6. Architecture of the SIM (Security Information Management) Platform



Source: H. Debar & J. Viinikka, Security information management as an outsourced service, 2006.

As Debar and Viinikka (2006) stated, this global view of the security state of an organization, that can be explored by the SIM platforms, should be connected to as many information systems that the company is operating and they need to correspond with one another. The architecture of the SIM platform as seen in Figure 6, is designed so sensors creates and stipulates logs to the local manager, which transmutes them in the Intrusion Detection Message Exchange Format (hereinafter: IDMEF) messages and from there just the determined IDMEF messages are communicated between the various SIM components.

3.2 Security Information Management (SIM) Functions

According to Debar and Viinikka (2006), main functions of a SIM platform are acquisition, contextual information management, alert correlation and reporting and exchanging. The acquisition function has a main object to deals with collecting and transporting proceedings to a central point for advanced processing. With push and pull collection techniques and mixture of protocols, this function of the SIM, protects the firewalls or other access control devices. Also, this function works with huge data flows and hundreds to thousands of actions per second are checked and send to the central platform. Sub-functions of the acquisition function are filtering, aggregation and normalization of the data. When huge quantity of cases information needs to be inserted in company's IT database, the acquisition function will

select which cases get inserted, and for regular case Strems is preferable to aggregate several identical cases as one. The normalization sub-function of the acquisition function, deals with safeguarding an unchanging representation of cases in company's database. There are distinctions in the identification settlements implemented by security tools for example intrusion detection systems or anti-virus systems. Different solutions can term the identical attack but with different marks. This sub-function, the normalization function of the acquisition process, is taking care and is guaranteeing that two cases can exemplify a same attack, and can add reference information to the marks, to ensure that internal indications and processes are appropriately acquired into account.

The contextual information management function, as second main function of the SIM, deals with signals and alerts and includes identification of the victim or the source of the attack, users and technologies affected. This function can contain network addresses or host names. The main responsibility of this function is to guarantee that each contextual data is correctly enclosed to hosts and users, and managing modifications in this data in order to up to date and precise. Alert correlation function has key responsibility to decide which of the placed alerts has priority and should be first sent to the security manager of the IS, so highest and most dangerous alerts will be realized first by importance. The importance or priority of alerts can vary, but with the role of ~~of~~ the acquisition process to ensure that the alerts are normalized to the IDMEF set of principles.

The last core function of the SIM, is the reporting and exchanging function which deals with interfaces for reading and pushing information. Operator real time, forensics analysis console and real time incident reporting are the interfaces that must be designed and provided.

3.3 Characteristics of IS/IT Security Outsourcing

3.3.1 General aspects for IS/IT Security Outsourcing

The area of security outsourcing process for companies and organisations is not satisfactorily researched topic making the outsource process different than the usual outsource, by the reason of the different organizational, legal, technical and risk aspects. Choosing to outsource the security functions of IS/IT, companies should take in consideration various considerations in which always the crucial element and most critical of significance is the confidentiality protection considering of the legal frameworks and due to it is an essential part for building trust among businesses, clients and corporate partners.

The outsourcing of security services, which can be indicated also as managed security services (hereinafter: MMS), involve outsourcing the security functions, physical and human, to an external supplier or administrational contributor who is specialized in the IS/IT security area. Companies and businesses can be very unenthusiastic for outsourcing the IS/IT services, considering it is a risky procedure and the process of outsourcing these functions carries its own risks. Studies and researches are showing that the IS/IT security services in Western Europe was projected to reach $1.4 millions of worth till the beginning of 2008, while in

2002 were projected just $548 million. What makes outsourcing IS/IT security functions that sensitive and on-going research topic, is in behalf of theoretical instruments like resource-based theory RBT, transaction cost theory TCT, resource dependence theory RDT or the agency cost theory ACT have not been applied in IS/IT security exploration and to study this practice can be extremely difficult. The practice of companies for agreeing to go for outsourcing can be delivered through cost analysis and the decision is driven for cost reduction or for putting emphasis on the core business activities for better efficiency. In the case of security outsourcing, this decision for companies can be more complicated by reason of (Karyda et al., 2006):

- there are not definite guidelines for it, and cannot be clear for companies or organizations, which security services can be outsourced, and which should be kept internal.

- IS/IT security functions can be vital asset for companies and can be of strong strategic importance.

- usual IS/IT outsourcing pronouncements are made by cost valuation or the ROI (return of investment) calculation. In the security IS/IT outsourcing process, these evaluations cannot be so straightforward.

- the IS/IT security functions carries out great confidentiality and privacy requirements, which are of critical importance for the outsourcing decision.

- nevertheless, which security functions are outsourced, and which are carried in-house, the risk still remains of the organization.

The strongest reason why companies choose to outsource IS/IT security functions, is due to the lack of knowledge, skills and intensive security experience, for efficient security management, specially for middle or small size organizations and companies. Tasks and security activities like, risk analysis, vulnerability assessment, information security risk assessment, network monitoring are some examples of security undertakings that can be outsourced. Other motive why companies are outsourcing IS/IT security functions, is the difficulty of holding and maintaining skilled employees in the security department, together with the high expenses of employing them. Also, companies and organizations should know that the IS/IT security area, is an area which requires knowledge of latest technology, both software and hardware, together with knowledge and awareness of the threats and attacks that are occurring, and the need for unceasing training and education for the employees. The IS/IT security services and functions that companies or organisations are more likely to outsource are (Karyda et al., 2006):

- intrusion monitoring

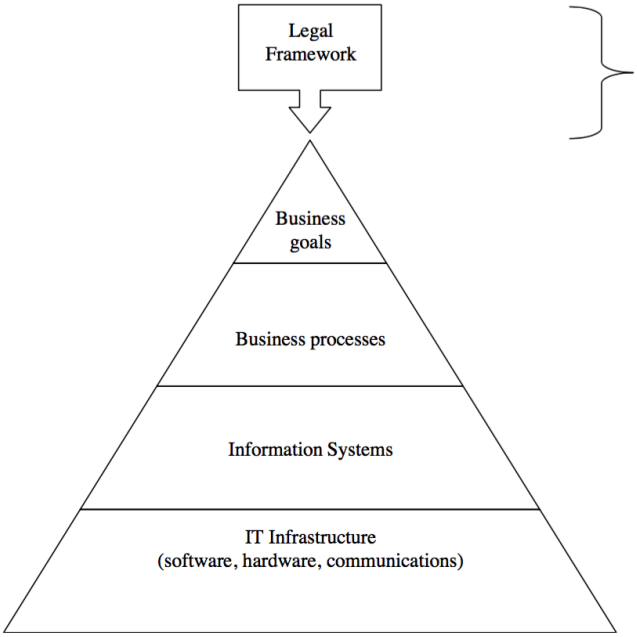
- e-mail virus and spam filtering

- penetration testing
- IT auditing
- firewall configuration and management
- virus protection
- intrusion detection systems management
- server management
- network monitoring
- security policy development and application
- security education and training
- security upgrades
- VPN management
- user access management
- data classification
- business process security

The installation of encryption security services as firewalls and VPNs, is complex and expensive process which requires an important level of expertise, are often outsourced to managed security service providers (hereinafter: MSSPs) as a cost effectual solution.

The management and monitoring of security systems is also a task that organizations often choose to outsource due to high requirements for employees. In Figure 7, is shown the socio-technical approach and framework which focus on the organizational, technical and legal dimension, and can assistance to answer the problematic outsource assessment (Karyda et al., 2006).

Figure 7. Socio-Technical Approach and Framework for Security Systems



Source: M. Karyda, E. Mitrou, & G. Quirchmayr, A framework for outsourcing IS/IT security services, 2006.

3.3.2 Organizational aspect of IS/IT security outsourcing

In the beginning all of the decisions, about what security functions to outsource and which would take in consideration, need to take into deliberation of the legal and regulatory requirements of the organizational context. For the security outsource preparations, privacy and confidentiality requirements are laid by the comparative legal framework which is of critical importance.

Information systems which are socio-technical systems of hardware, software, processes, data and users, operate and are used by organizations and companies with the resolution of accelerating and reaching business goals. IS use offer critical services of strategic significance, that is why the management of these IS services is very important for the business goals. Business objectives are creating the business processes, and they determine the role of IS/IT security and the security functions, therefore is determined the IS and the technical IT infrastructure that is required. Companies and managers of IT departments should have solid and strong security strategy associated with the business goals before outsourcing the functions.

Another characteristic for organizations, in this manner, when creating the IS/IT security strategy, is the relationship of IS/IT functions with the core business goal and objective. Close related IS/IT security functions to the core business strategy will deliver very limited opportunity for outsourcing the security functions, and vice versa if the core business objective is not so related with the security functions of the company, outsourcing can be considered with higher prospective. The main point is that the IS/IT security strategy should

always be considered in the highest strategy level of company's management style. Organizations that outsource IS/IT functions in long run and left the security risk external, might find themselves powerless to survive security risks and management if they decide to bring some functions in-house. This is as a result of the company's work culture is without security development and there is lack of security and privacy awareness of the employees.

When organizations decide to outsource the security functions to external provider, they need to investigate if all security functions should be outsourced to a single supplier or the security functions to be divided to multiple outsource suppliers. The decision to allocate the security functions to several companies brings more management costs and lower negotiation power, instead outsourcing functions to a single company is lowering the risks in situation of unfavourable results. In terms of pricing, organizations consider that paying contracted once-a-month fixed cost will avoid incremental and unknown costs. Side effects of outsourcing security services can arrive when the external supplier does not consider the organisational culture, internal relations and characteristics when developing applications or security strategies (Karyda et al., 2006).

Nassimbeni, Sartor, and Dus (2012) believe that organisational protection tools for security of the services covers policies, procedures and controls and should be developed and implemented by organizations to avoid threats and manage recovery activities. The tools and mechanisms for these actions may be in custom form of organisational arrangements, responsibility assignment and process reports. Reports and studies suggest that security risks and time manipulation can be lower when a trustful relationship is created with the external providers and education and training in security matters is gained.

3.3.3 Technical aspect of IS/IT security outsourcing

Since the security of IS/IT is in same line with the technological fast rate development of new IS/IT, not only the threats and risks are increasing, but security products and technologies development are appearing on the market very fast. Companies and organizations that are not IT driven cannot be in line with these changes, and that is the one key reason why organizations find complications in management of security IS/IT functions. At the same time the security outsource companies and providers face the same issue. They must be in line with the new technological developments and IS/IT security issues and should possess the most recent security systems and updates in order to keep in the race with the competitors. Functions, tools and services for data confidentiality and integrity, encryption mechanisms, authorization schemes and digital signatures, strong passwords, firewalls and antivirus software should always be with the appropriate latest and up to date techniques (Karyda et al., 2006).

3.3.4 Data protection and legal aspect, European data protection directive (EUDP)

The main protection tools in legal margin covers internet protocol (hereinafter: IP) rights and contracts. The contracts are the main protection of knowledge and data which are shared

among internal and external sources and parties, and are composed of precise and definite sections. Nevertheless, the effectiveness of the contracts lay on the legal and the jurisdictional environment in which a company operates and the data and IP violations are more likely to happen and appear on countries with weak legal systems (Nassimbeni et al., 2012).

The security, protection and privacy of personal data of companies and organizations is a challenging topic that had been discussed in the European Union countries for years, and several European countries produced data protection laws. The European data protection directive (hereinafter: EDPD) was generated considering there were variances in different European Union (hereinafter: EU) countries about data protection and the free flow of data. National and international legal frameworks, like the Organization for Economic Cooperation and Development (hereinafter: OECD) and the Council of Europe's Convention No. 108, do not determined strict standards for personal data managing.

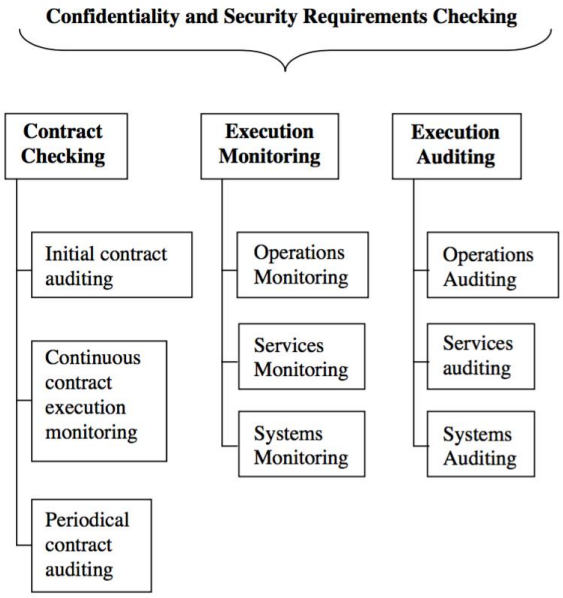
Outsourcing security functions are processes in which the external provider is operating with organizational or personal data. In that manner, the person or company need to define the purpose and means of data processing and has to comply with the specific requirements of the directive and implemented national law of the EU. Since, this process needs to be controlled, outsource of personal data must be organized in acquiescence with its requirements.

According to Jain, Singh and Verma (2002), subcontracted company working with personal company data should guarantee that the requirements regarding the grounds for processing are legal and the conditions for processing sensitive data are fulfilled. The subject of management concern by companies and organizations is that by outsourcing their data processing functions and processes, all responsibilities for being submissive with the directive would be mechanically reassigned to the service provider.

To safeguard that the confidentiality of data and high level security is succeeded, the outsourcing partner must implement all obligatory technological and organizational protections resulting in full access of control and monitor of the personal data, in written, formal and clear contract.

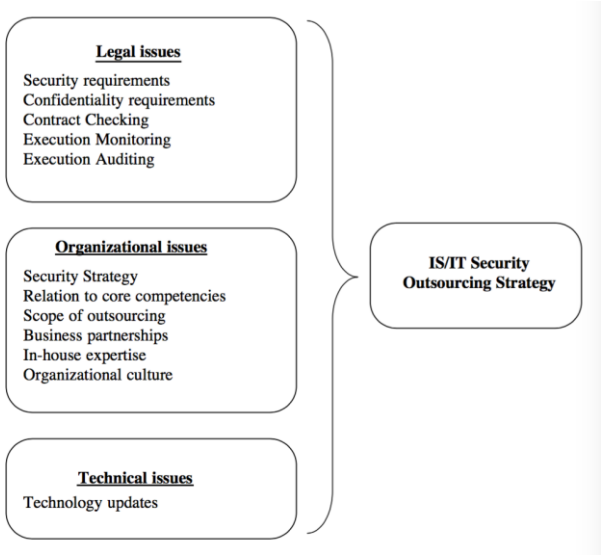
In Figures 8 and 9, it is shown the outsourcing framework can offer organizations a manageable and controllable principle and arrangement, with respects to the core legal necessities, outlined by the EDPD (Karyda et al., 2006).

Figure 8. Confidentiality and Security Requirements Checking



Source: M. Karyda, E. Mitrou, & G. Quirchmayr, A framework for outsourcing IS/IT security services, 2006.

Figure 9. IS/IT Security Outsourcing Strategy



Source: M. Karyda, E. Mitrou, & G. Quirchmayr, A framework for outsourcing IS/IT security services, 2006.

3.4 Service level agreements (SLA)

3.4.1 SLAs for protected IS/IT security outsourcing

In general form, the service level agreement or the SLA is a contract between a provider of a service and a customer, which quantifies that the minimum quality of service is provided and the service will meet client's or customer's business need. Diverse definitions and terms are synced for SLAs. It is an agreement which is negotiated and includes an upward understanding and consideration of the business needs on each side and should always give

outcome in compromise. SLA is a contract that measures the level of service in terms of metrics, which is designed to meet both parties needs and will represent a quality of the service that should be delivered. In the SLA distributed quality is the minimum satisfactory, due to higher quality commonly will cost more money. Anything beyond the minimum may be additional service and can be with unnecessary cost, but that minimum has to be acceptable and satisfactory for the customer. The service level agreements were created mainly from the dissatisfaction of the end users, especially of IT functions. It covers the realization of those functions and also should define the service for which end users were paying.

According to Hiles (1994), there has been improvement in attention in SLAs with the development of benchmarking, market testing and outsourcing considering processes in these fields should be done properly and the services must be defined before the start. SLAs can execute service management controls and service placement, aligning distributed service with consumer business objective.

Key advantage to the IT board in one company with initiating SLA is to clarify exactly what the customers' needs are and which elements are most important. SLA assists in concentrating on the consumer and in improving professionalism. Many organizations and companies do not have strict and unchanging business processes and their services are varying over the years because of changes of business objectives, market conditions, deadlines, priorities and cost benefit analysis. SLAs should recognize changing conditions and management processes with identification of real and current service requirements. This service management processes need to shield response, availability, performance and serviceability and commonly the key to accomplishment lies in successful problem management and escalation.

According to Hiles (1994), the service provider is the connection in the quality chain, on which the customer depends in order to distribute quality in turn to its customers. In that manner, it is recommended that SLAs should be clearly defined by reason of clear statements are fundamental. For example, is a multi-computer service accessible if one of the computers is down, or is the service accessible if only ten out of 500 users cannot access it. Business contracts will insurance business terms and commercial, profitable and marketable issues. Service level agreement SLA can cover:

- resolution of the SLA
- services Explanation
- service Hours and Maintenance slots
- service Availability
- performances
- peak period service – Variations
- volumes and deadlines

- restrictions and standards
- supportive services
- security
- contingency
- change Controls
- problem management and escalation
- service Level Monitoring
- service Level Reporting
- service regimes and priorities
- SLA Meetings

The service level agreement SLA, is also formal definition of the relationship and is strikingly described contract among two organisations, usually between the external supplier of the services, for example the ASP, and the customer. The importance of service level agreements relies on the the fact that outsourced security services will increase of when the organization's core business is facing also success, resulting that new challenges of services will be desired. In that manner, the complexity of new IT security services will provoke more control and quality of the service provider, and together the client company and the service provider, sign a service level agreement SLA in which the functionality of the services and the required service level is well described by standards of quality of service (hereinafter: QoS) (Jain et al., 2002).

SLAs are specific agreements and are related to particular functions of the outsourced processes. All parts of the SLA, should narrate to the master service agreement to guarantee and confirm a common value approach. Business security sections that must be integrated in the SLA can include information of the system name, devices and locations, restoration time-scale objectives, application owner, business continuity co-ordinator. The data provided in the outsourced process, should be presented in the agreement and all of the necessitated minimum standby requirement, firmware, operating system, network specifications, the standby assets, application recovery time, testing requirements etc.

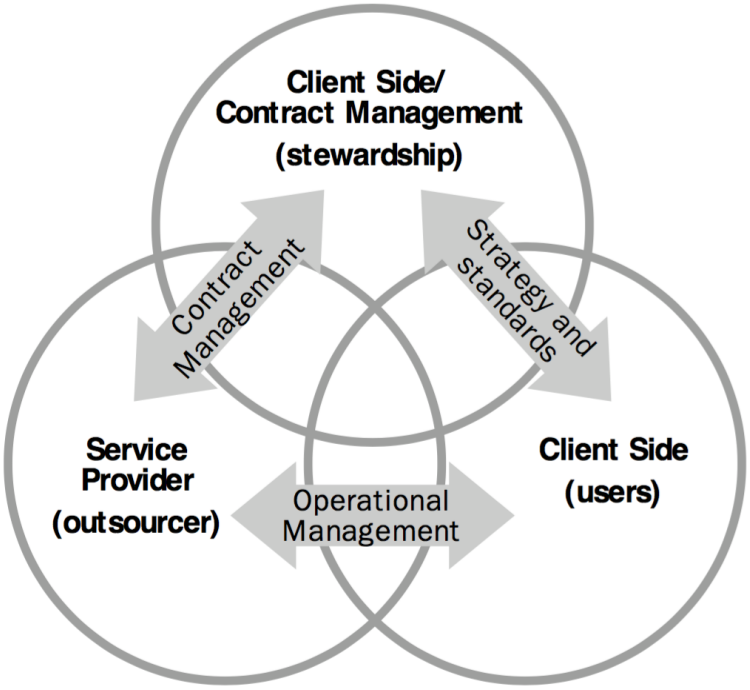
In the SLA, security specifications are not constructed or established on risk assessment or business impact analysis, and does not always contain details concerning backup strategies. Organizations should create and develop a business continuity plan founded by the risks and impacts on the core business. The confidential part of the agreement must have clear and sharp information and that security information can be used for the strict purposes written in the agreement, and not for disclosure to any third party without the previous scripted approval of the data holder.

According to Smith (1995), not a single agreement or strategy can promise and guarantee perfect accomplishment, except those who start it know what, when, and how to do it.

Practise can create workforces to be better, aware, prepared, competent, confident and comfortable. The golden rule for success is always: test, test, test.

According to Larson (1998), SLAs in outsourcing management are designed and created by three key participants, the steward (client-side contract manager), the service provider and the users, as shown in Figure 10. Their connections are contract management, strategy and standards management and operational management.

Figure 10. Key Participants in the SLA in Outsourcing Management



Source: K. D. Larson, The role of service level agreements in IT service delivery, 1998.

The responsibility of the client-side contract manager in the outsourcing contract is focused mainly on the measurement and reviewing of the service provider's performance in contradiction of the defined service levels. This manager is responsible for generating and maintaining the framework within where services are distributed and are exploited. Also, the contract manager is responsible for providing the contracted services, undertaking day-to-day operational difficulties and managing requirements and implementation of routine changes in harmony with the contract and standard. This manager is the chain among the service provider and the users and should focus also on the demand and supply of the contracted services. Performance measurement of service delivery with observance of the SLAs is accomplished operating the metrics of availability, reliability, serviceability, response and user satisfaction. Measurement of availability captures the percentage of the time that the contracted service arranged is really available and functioning over ~~a~~ defined measurement period. Reliability describes the frequency with which the planned service is withdrawn or crashes over a well-defined measurement period. Serviceability is a postponement of

reliability and processes the interval of available time and time lost between the point of service breakdown and service reinstalment. Response measures the time delay between a demand for service and the subsequent reply. Response time can be considered as turnaround time, transfer time or cycle time. User satisfaction is a measurement method of perceived performance relative to expectation. User satisfaction is frequently restrained by examination using a repeatable procedure to track modification over time.

By Larson (1998), the developing of SLA has three steps, project initiation, pilot SLA and the final phase of SLA and its development process. To develop SLAs that can be used on an on-going base, and not just a stack of valueless document, can be hard work and continuous work with the service provider. What would be defined is what the client would get.

By Hiles (1994), success or breakdown of a SLA depends of both parties. Explanations for SLAs failing can include insignificant measurements, insufficient definitions and unwieldy SLA documentation. The primary reason for failure is possibly lack of commitment from management or customers. SLAs can be expensive projects and they need resourcing.

3.4.2 Example of an ASL agreement, provided by Telecommunication Company

The SLA agreement for maintenance of network services has several parts, in which different aspects of the services provided is explained specifically in details. This SLA was delivered to me by a company, which insisted that the company name stays private. The outside ASP vendor offers these circumstances for the services for company X:

Action Line Help Service - Once a network is installed and operational, you have direct access to a core team of network experts, providing you with prompt responses to any inquiry related to: trouble isolation and resolution support, specific features/functions questions and general product-related questions.

Hardware Repair Service – After having determined that hardware is in need of repair or replacement, company X will work with the Customer to effect repair. The customer should use only company X certified spare parts for replacements. The customer will send the faulty equipment to company X for repair, using the Return Material Authorization (hereinafter: RMA) procedure. Replaced parts carry the longer of a ninety days' warranty or any remaining warranty on the part repaired or replaced. Upon installation of parts in the equipment, title to those parts will pass to the Customer at the time of installation. The parts replaced will become the property of an elastic network company (hereinafter: ECI). Turnaround time for repair or replacement of company X equipment will be up to fifty working days from the time it arrives to company X until it arrives back to the customer. Company X will not be held responsible for any delay beyond its reasonable control.

Software Repair Service – Following a request to company X Telecom Action Line expert, and after determination that the software is in need of repair, Company X will arrange speedy delivery of a software correction patch file or new point release as quickly as possible, if one

is already available to correct confirmed software deficiencies. Software deficiencies are defined only as those which are traffic affecting.

Extended Services – Set of services, extended to the Basic Services, which completes a full range of Maintenance Services to cover all customers' needs and requirements.

Fast Exchange Hardware Service – Company X will insure that a replacement item for the one identified as failed is available to the Customer at Company X Principal Service Centre for replacement. Company X will commit to deliver the needed item to the customer, prior to receiving the faulty item, within the agreed time frame. The same unit will be replenished within fifty working days. Fast Exchange Service will cover only those items that will be determined in the Maintenance Order Form.

On-Site Service – Company X will perform On-Site remedial repair service on the Contracted Equipment within the Service Area. The service is provided during the Contracted Service hours. Maintenance services may be provided at the Customer's locations outside the Service Area subject to a surcharge that will be applied as a fee per service event. Following a request for service from the Customer, Company X will attempt to resolve it through remote network access. If appropriate, Company X authorized maintenance representative will arrive at the Customer's location normally within three business days (within the Contracted Service Hours) of problem verification to rectify the problem, using the Customer's spare parts. Attendance at the Customer's site during times other than the Contracted Service Hours may be provided on a charge basis.

Extended Action Line – The service extends the Normal Business Hours Period to twenty-four hours per day seven days a week (including Public holidays) at the Company X Principal Service Centre. The service allows for a one-hour call back within the Contracted Service Hours instead of the normal two hours.

Software Upgrade – This service provides customers with new versions of software as they become available for the hardware they have purchased and have under contract. Performance improvements and technology updates are supplied in order to keep the network up-to-date with changes or improvements made during the life-cycle of the products. Company X will send the customer one master set of each new major Company X licensed software revision (such revisions normally being shipped with new Company X equipment), including the management system. The Software Upgrade service supplies continuing improvements to the functionality of our products and ensures successful operation throughout the network life-cycle.

Preventive Maintenance Service – As networks are becoming more advanced and complex, they are also more critical to business success. In order to prevent future failures and discrepancies in the equipment, company X offers the Preventive Maintenance & Inspection service. It is recommending using this service once a year, in order to maximize the maintenance of the equipment. company X service engineer will visit annually, to inspect

each site. The engineer will inspect the current company X site installation status and will perform a preventative maintenance routine according to the product type procedure. To prevent traffic disruption, the preventative maintenance routine will be performed only upon full customer authorisation.

Spares Management – The Spares Management program maximizes the operating efficiency through a reliable program that is devoted to decreasing the cost of spare parts and maximizing equipment availability. By implementing our Spares Management program, you outsource your entire spare parts logistics process to ECI. We will consult with you to build a plan that meets your business goals and objectives. This comprehensive service provides continuous monitoring and automatic replenishment of parts as well as intelligent inventory management. Replacement units are shipped within twenty-four working hours of receiving the request call. This service is available 7x24x365.

Tailored Services -Additional services specially customised to customer's needs and requirements.

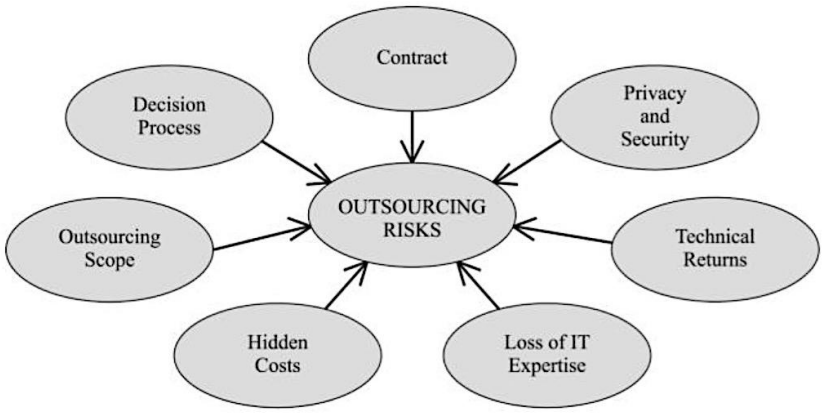
3.5 Outsourcing Security Risk Factors

Risk factors interconnected with privacy and security concerns are recognized and proven that can be enormous. Analytical and sensitive privacy and security parts that should be taken into account are corporate policies, audit and controls and host government laws and regulations. Organizations and businesses involved in IS/IT outsourcing should have a comprehensive and explicitly acknowledged corporate policy on defending and protecting individual privacy and data security. In same time, the outsource contract or the SLA should be closely tied to these policies in order to reduce or decrease conceivable risks of privacy and security contravention. A United States senator said "*In my view, American companies which are outsourcing consumer data to foreign countries must assume responsibility for the data".* An uninterrupted and continuous on-going audit and control functions and mechanisms are essential for protection of individual privacy and security of the corporate data. Because IS/IT security outsourcing regularly implicates access to corporate data to the outside vendors or outsiders, the requirement for audit and control becomes predominantly more serious and critical.

According to Tafti (2005), organizations and businesses should constantly and continuously monitor how outside providers is managing corporate data and how they handle the data access, usage, storage, sharing and transmission.

For companies this can be very challenging and strong process since verifying regulatory agreement, data protection and access can be difficult and different among different organizations and countries for reducing risks of incidents related to privacy and data security. On Figure 11, are shown different points that are affecting the risk for information technologies outsourcing.

Figure 11. Outsourcing IT Risks, Framework Outline



Source: M. H. A. Tafti, Risks factors associated with offshore IT outsourcing, 2005.

Two important key risks connected with outsourcing, are the risk of dropping skills key to competing for the upcoming and the risk of creating the outsourcing transfer at the least suitable time in an industry's development. Companies often are attracted to outsourcing as a means to discharge increasing competitive pressure. If businesses fail to consider the long term implications, they can breakdown possible future opportunities for short term advantage. Companies strategies also need to know when in an industry's evolution and where along its value chain the economics favour outsourcing. Companies should be conscious how this inclines to modification over time, especially in technology marketplaces.

According to disruptive innovation specialists, the serious transition is when the market changes from the stage where most customers remain to desire more functionality than is currently offered to the point where the majority of customers arise to see themselves as being over served with features. This is the stage at which the product quickly becomes a commodity and where the primary basis of competition swings to aspects of the value proposition beyond technology, such as price, speed, convenience and customization.

Leavy (2004) believes that outsourcing as a strategy has the latent to push competitiveness and value creation in many means beyond the constricted objective of cost decrease. Accomplishing greater focus, scaling without mass, fuelling disruptive innovation and enabling strategic repositioning are just four of the many encouraging options that outsourcing as a strategy can offer and support. Managers will always need to ask themselves whether the timing is accurate and also what strategic skills and capabilities they might be setting at risk.

IT/IS outsourcing being a growing worldwide method, has become a widespread phenomenon and is very common strategy process among large companies. In a study for IT outsourcing risks and worries in large companies, was found that SLAs or contract

agreements and its specifications can be a huge risk for companies. These documentations should contain every process element and the fear that something will be missed is rising among large companies. Other important uncertainties would be the loss of competence the customer may experience and the uncertain qualification of the provider's workforce. Other risk in importance is the inability to adapt to innovative technologies, which suggests that doubts refer to providers' personal or human characteristics rather than to their technical skills. Another result in the study is the low ranking for possible IS staff opposition (Gonzales, Gasco, & Llopis, 2005).

The major factor in this manner, which can significantly reduce the risks of privacy and security contravention, is the existence of laws and regulations, like the EUDP. When companies are outsourcing security IS/IT functions to foreign countries can face some problems. Specific data security and privacy protection laws, regulations or tools are still not yet provided by many countries. Data safekeeping and protection, together with the privacy of information technology processes and information technology designs are still very sensitive issues, which are not controlled or monitored in many businesses and companies (Tafti, 2005).

Table 1. Outsourcing Risks and Factors by Categories

Outsourcing risk categories	Risk factors within category
Outsourcing contract	Service level agreement Non-performance penalties Baseline measures Contract length Flexibility Post-outsourcing Standard contract
Privacy and security	Corporate policy Audit and control Host government laws and regulations
Decision process	Management involvement IT department
Outsourcing scope	Total outsourcing selective outsourcing
Diminished technical returns	Same IT staff loss of key employees No access to new technology Inability to define new architecture
Hidden costs	Beyond baseline services Vendor search costs Transition costs Post-outsourcing costs
Loss of IT expertise	Sacrificed IT knowledge Inability to rebuild IT Contract negotiations

Source: M. H. A. Tafti, Risks factors associated with offshore IT outsourcing, 2005.

Enforcement of laws and regulations may still be less than satisfactory due to several explanations involving corruption and ineffectiveness of those who interpret and enforce the law. Also, diversity and inconsistency of foreign laws and regulations compared to the home laws and regulations of the organization operating in security and privacy manner of corporate data can be seen. On Table 1. are shown the outsourcing risks and factors in categories, for example if the risk of outsourcing contract is affecting the process, that risk can be seen either in the service level agreement or in a standard contract. (Tafti, 2005).

According to Doomun (2008), managing and re-establishing an own IS/IT architecture of organizations and companies, which outsource security functions and they are handled and controlled by outside party, can be very challenging and hard process. The International Organization for Standardization (hereinafter: ISO), or the ISO standards are global security frameworks which increase importance on the need, not only for good security control, and the capability of validation.

On Table 2. are shown examples of different ISO and International Electro Technical Commission (hereinafter: IEC) information technology security standards. The ISO/IEC 27002:2013 determines guidelines and over-all principles for initiating, implementing, maintaining and improving IS/IT security management in organizations and businesses. The ISO/IEC 27005 standard is designed and constructed with techniques to cover the information technology and information security risks and its management. Other standards shield the information technologies and information systems measurements, scopes and direction. The standards cover best practices of control objectives and controls of information security management (International Organization for Standardization, 2013).

Table 2. Examples of ISO/IEC Information Technology Security Standards

Type	**Description**
ISO/IEC 27001	Information technology - Security Techniques: Security Management System (ISMS)
ISO/IEC 27002:2013	Information technology - Security Techniques: Code of practice for information security controls
ISO/IEC 27003	Information technology - Security techniques: Information security management system implementation guidance
ISO/IEC 27004	Information technology - Security techniques: Information security management — Measurement
ISO/IEC 27005	Information technology - Security techniques: Information security risk management

Source: International Organization for Standardization, 2013.

By outsourcing security services, companies are exposed of increased risks to organization's information system by unauthorised access, or risks of the system being broken, transformed or destroyed due to increased number of operators with access to the system. Sensitive information and trade secrets may disclosure, leading to damage or loss of the competitive advantage aspect with the competitors. That is why companies should use security frameworks and standards, because the advantages can be seen by provided outsourcing security that is consistent and constant by international standard.

By Doomun (2008), reliable, robust and repeatable IS security model and advanced security monitoring, management and maintenance are other advantages of used security standards and frameworks. Since the technology is changing very fast, legal requirements and laws for privacy and protection are considered as an ordinary must in every country. Also, as a result of the fast changing technological environment, protection and privacy are crucial factors for corporations and companies to compete with each other and grow their business. In that manner, the outsourcing productiveness should adopt a strong integrated and dynamic approach that adopts security and privacy in every process including three levels of security, the technical security guidelines, risks examination and the compliance and evaluation standards, together with the management of the information security. On Table 3., are shown the security process levels in outsourcing agreement.

Outsourcing process layer	Requirements
Compliance	
Regulatory framework	Strong copyright, intellectual property management and protection, privacy and global outsourcing security laws
Law enforcement	Penalties, information security culture
Security standards	Information security benchmarks, global security intelligence, independent auditing and review of security level
Risk	
Threats	Security from internal threats, limited and controlled access rights, confidentiality and non-disclosure agreements, security training and awareness
Technology	
Data and network security	Technological solutions like firewalls, anti-virus at various levels, backups, advance encryption methodologies, authentication and access controls, biometrics, active IDS, VPN, Server-level clustering/Storage area network, real-time monitoring and management, security of wireless devices. Activity auditing technology
Process protection	24 h network monitoring, guidelines on the usage of official assets, real time analysis and response, disaster recovery plans and business continuity
Physical protection	24 h premises security, closed-circuit camera in the workplace, multi-level code access, fire suppression systems
	Service and security level agreements

Table 3. Security Levels in Outsourcing

Source: M. R. Doomun, Multi-level Information System Security in Outsourcing Domain, 2008.

4 RESEARCH ON IS/IT SECURITY OUTSOURCING AWARENESS OF SLOVENIAN COMPANIES

4.1 Research introduction and respondents' observation

To perform my research on IS/IT security outsourcing awareness or perception, I managed and performed structured qualitative interviews for my exploratory research with companies operating in the IT and telecommunication industry and also with one service provider (hereinafter: SP) for security solutions and services. The companies I chose to contact and interviewed, are companies that are offering IS/IT or telecommunication services and are in general many years on the market in Slovenia.

The companies also are experienced in outsourcing IS/IT services and possess knowledge and understanding of the overall process. I chose structured interviews with standardized questionnaire, considering the companies that I have chosen to interview are mainly big companies operating in the IT or telecommunication industry in Slovenia, and flexibility in reaching them must be considered. To provide a complete perspective of the topic, I chose questions that are more general about the outsourcing principal, but also stricter and detailed questions about IT security outsourcing.

The questions that I provided for the interviews were formulated and created by me, from my own perspective and ideas that I got by all the critical literature reviewed for my research. The structured questionnaire can be seen in Appendix B. To have more clear picture about the IS/IT security outsource awareness, I also interviewed one service provider, to see how this area is seen on the side of service providers. In the following are companies' responses to my questions and they are exploratory examined.

Respondent company 1 – **Telemach**

The respondent is director in the networking department and is in charge for all network operations and decisions in Telemach. Telemach is the fastest growing mobile operator and a leading cable operator in Slovenia, which also offers cable services in Bosnia and Herzegovina, Serbia, Montenegro, Macedonia and Croatia through the international platform OTT and United Group. On Figure 12, is shown company's logo.

Figure 12. Telemach Company Logo

Source: Telemach, Telemach Company Logo, 2016.

The respondent aimed that the company is operating for 17 years in Slovenia, in the ISP, cable and mobile telecom industry. The company is positioned as a first cable company in Slovenia. Moreover, Telemach is the second company in the country for ISP services and is in the top three companies for mobile services.

On the question what type of IS/IT services the company is outsourcing the respondent said that the company is outsourcing the BRM services, more particular the support services in the BRM. Services for ERP, CRM, BPR, data operations or networking are all developed in house, or in company's group level. On the question for the contracting and the service level agreement SLA for the outsourcing services, the respondent does not provide knowledge, does a specific, accurate and reliable contract is existing. Also, the outsourced BRM support service is uncertainly measured, controlled or verified and the respondent said that he does not have enough information for that part. What are the reasons and expectations, why an organization or a business should outsource the IS/IT security services was the next question. The respondent aimed that if a project in the security functions or services in the company need or require special knowledge, and the cost of labour is high with specific delivery time for the project is needed the company can outsource the security IS/IT operations. In normal operating and day to day activities, the responded said that the IS/IT security functions should be kept internal. On the question can IS/IT security outsourcing lower the fixed costs or turn fixed costs to more variable costs, the respondent said that he believes from practise, that outsourcing IS/IT services always lowers the general fixed costs, and the highest parameter for that believe is that lower costs for salaries and labour is the first thing that lowest the fixed monthly costs. The respondent believes that more expertise in technology innovation or software or better access for knowledge can be transferred to company in-house employees by the outsourced company by day-by-day and shared working.

Speaking of outsource companies and SP, the respondent said that if a serious operating service provider is taking the security operations, newest and up-to-date hardware, software, network and security outsourcing model will be preparing and by all necessary means, from staff to technology will be provided for sure. Risk factors that IS/IT security outsourcing can bring to company's internal work, that the respondent believes can appear, are the risk factor of information leaking, the time required to learn the new infrastructure before the work is taken over, having multiple problems with the outsourcing partner and have troubles replacing with another. In general speaking, the respondent aimed that the most beneficial motive for the company that he is working to choose to outsource the IS/IT security function, will be the cost saving motive.

Respondent company 2 – **Siopti**

The respondent is the CEO of an organization in the information and technology industry that provides professional IS/IT services. Siopti is operating for nine years in the IT and networking industry in Slovenia and offers installation, maintenance and support services. On Figure 13, is shown company's logo.

Figure 13. Siopti Company Logo

Source: Siopti, Siopti Company Logo, 2016.

The company is outsourcing BPR services, and the respondent said that more specifically, the outsourced BPR services are coupled with accounting services and network communication services for interconnection backup site with the company's main site. For the outsourced services, the respondent said that contractual service level agreement SLA is not very specifically defined. The company is communicating and co-operating with the outsource vendor weekly, and a specific signed contract or agreement is not done. The respondent said that if a communication problem happens or an issue and problem with the services performed occur, probability for changing the vendor can be increased. In this manner, the respondent said that, there is no critical outsource factor that can damage company's work, considering none of the crucial company's function are outsourced, and replacing a service provider can be easily done in a reasonable time frame.

On the question, how the outsourced service is measured, controlled or verified by both parties, the respondent said that most importantly is measuring response time, when request is issued and the response time is the main evaluating consideration. For example, the respondent said that in case of network interconnection, a continually checking performance is done on a 24h basis. On the question, what are the main reasons and expectations that a business or organizations can see for outsourcing security IS/IT services, the respondent said that competences and expertise in the main company goal are must, a lean organization should focus on core competences rather than building up non-essential function and in that manner security IS/IT services can be considered. In line with this question, the next one on which security services a company can outsource and which should keep internal, the respondent said that the most important is to understand which security functions are connected to the main revenue generation. After complete understanding of the key functions, security functions can be more simply to be defined, and outsourcing them can be considered.

The outsourced BPR services are mostly accelerated with up-to-date technologies and qualified knowledge from the outsource vendor, said the respondent. The outsourced services lower the overall company costs and the respondent pointed that the outsourced costs can be predictable and in general he believes that outsourcing non-essential services can lower the fixed costs of the company. In outsourcing IS/IT security services, the respondent believes that can lead the company to focus to its core mission which will helps in-house employees to develop better expertise and knowledge and not loose time with unimportant aspects for running the business. On the question, how the service providers (SPs) that offer security services are prepared with hardware, software and network infrastructure, as well as business

services that are necessary for the security outsourcing model, the respondent aimed that IS/IT security service providers are not well prepared. Also, he assumed that security outsource providers should develop more in the security focus area, and in the moment of speaking, security IT providers are offering very basic security services. Risk factor that are appearing, when a company chooses to outsource the IS/IT security services, is that is a sensitive service and that the company can be dealing with security vendor that lacks expertise and is not able to tailor solutions to your specific needs. On the question, what is the most beneficial motive for outsourcing security services, the respondent said that is for sure lowering the operational costs, and lowering the operational costs is the main drive for outsourcing the security model across the board.

Respondent 3 – **Telekom Slovenije**

The respondent is one of the managers in the IT central department of the company, and more particularly, is working in the network department with the network operations. Telekom Slovenije is operating since 1991 and that is more than 25 years. Telekom Slovenije d.d., together with its subsidiary companies, is integrated provider and main communication services provider in Slovenia. The respondent said that, the company is a leader in the introduction and integration of new generations of mobile and fixed communications together with certain multimedia content. On Figure 14, is presented company's logo.

Telekom Slovenije is outsourcing several different services. The respondent said that the company is outsourcing the support hardware and software services for the network maintenance, the training for the IT staff and some managed security services. The outsourced services are all contracted with specific, accurate and reliable contract. The respondent discussed that most important and challenging factors for the SLA or contract with the outside vendor are to define how reliable is the service, the response time factor, the information leakage and the poor information security study.

Figure 14. Telekom Slovenije Company Logo

Source: Telekom Slovenije, Telekom Slovenije Company Logo, 2016.

In that manner, the respondent said that the outsourced IS/IT security services are controlled, measured and verified, and track record of the actions performed is constantly tested by internal staff.

The reasons and expectations why the company choose to outsource security services, specifically the managed IT security services, are that the company is always provided with up-to-date technology on the services that are not in the core strategy of the business, said the respondent. On the question which IT security functions are suitable for outsourcing and which should be kept internally, the respondent said that internally are kept all security functions that are related to all network operations, and the outsourced managed security services are for the users/clients. In that approach, the respondent said that the managed IT security outsourced functions accelerate the organization with latest technology and qualified outside workers with excellent knowledge.

Outsourcing IT managed security services enables the company to lower fixed costs, and as the respondent state, the company prefer to use the pay as grow business model for their type of services. On the question is IT security outsourcing brings more expertise to company in-house employees, the respondent said that technology innovation, better software management and superior access for knowledge are even visible improvements by practise. The outsourced IT managed services are controlled, and all operations that are outsourced are using the IS 27001 standards for information security management, said the respondent.

Next topic deliberated is about the risk factors for IS/IT security outsourcing and the arguments for implementing IS/IT security outsourcing. The respondent said that risk factors for security outsourcing are many but some of the most important is the leak of company information. Other risk factor is the trust, and the break of the intellectual property right. The respondent said that if a company does not possess the knowledge for effective security model of the IS and IT functions and does not have all the required up-to-date technology for the hardware and software implementation, can consider outsourcing to an outside vendor or service provider. On the question what is the most beneficial motive on which the company decided to outsource the security services, as managed security services designed for end users or clients, the respondent said that new services, which need to be highly secured and implemented with the latest technology, need to be presented to clients often and regularly and that is the main motive on which the company outsourcing the security services to outside provider, considering it is not a core business area and investing on it internally, it is not of best interest for them.

Respondent 4 – **ELES**

The respondent is working in the IT department of the company, which is operating for more than 20 years. The public company ELES, Ltd., Electricity Transmission System Operator (ELES) has the exclusive right to perform the public service of the transmission network system operators in Slovenia. On Figure 15, is visible company's logo.

Figure 15. ELES Company Logo

Source: ELES, ELES Company Logo, 2016.

The respondent said that the outsourcing is part of the company IS/IT infrastructure and support services for the hardware and software and the implementation of it are outsourced. A specific, accurate and reliable contracting SLA is defined for the outsourced services, and also the respondent delivered an example script of it written in Slovenian language, which can be seen in Appendix C.

The factors and parameters which are the most important and challenging for the SLA are "response time and high quality of support", the respondent said. Also, the outsourced services which are provided and specified in the SLA are measured, controlled and verified by both parties in the agreement and according to it, the respondent addressed that with the IT tool for Information Technology Infrastructure Library (hereinafter: ITIL) processes – Maximo, the services are tracked and measured. The respondent does not provide noteworthy knowledge on the reasons and expectations why a business or an organizations turn their IS/IT security services to outsourcing.

Which IT security functions are suitable for outsourcing and which should be kept internally was the next question, and the respondent stated that planning processes can be outsourced to an external vendor or service provider, as a result of the planning process is a crucial step of the company's security model and the outsourced vendor will pose all the required knowledge, practise, expertise and the newest technology. Also, the penetration tests and quality assurance process can be outsourced, said the respondent. The processes and operations that the company outsource accelerate the company with up-to-date technological solutions and the IT stuff that is employed by the outsourced vendor for that services are qualified experienced workers, said the respondent. Lowering the fixed costs is also one aspect of the benefits of outsourcing, which also enables the company to have more variable costs by turning some of the fixed to more variable.

The respondent also addressed that by IS/IT security outsourcing the company in-house employees are with better and additional new access to technology innovation, considering the outsourced vendor is always providing latest technological solutions, by which the in-house employees are acquiring. The next question on how service providers are prepared to deliver appropriate hardware, software, network infrastructure as well as business services that are necessary for the security outsourcing model, the respondent said that in specific IT security resolution and difficulties, the providers are not satisfactorily and sufficiently

educated and experienced. Some examples, which the respondent stated are that firewalls and data encryption, can be concluded in the SLA and in practice, without proper planning process.

Risk factors for IS/IT security outsourcing that the respondent addressed are the trust and the references. The most beneficial motive that can drive companies to outsource the security operations for their IT departments or the security of their products is the better knowledge for the in-house employees and the better and stronger planning strategy for future operations, said the respondent.

Respondent 5 – **Stelkom**

The respondent is working in the sales department and also working with management and administration activities in Stelkom, a telecommunication service provider that is operating since 2003, more than 10 years on the Slovenian market. The company provides superior services and network access with great quality as a long-term solution for Slovenia and the region, focusing in telecommunication area and the company is positioned as alternative Telco service provider. On Figure 16, is indicated company's logo.

Figure 16. Stelkom Company Logo

Source: Stelkom, Stelkom Company Logo, 2016.

The company is outsourcing mainly the ERP processes and partial CRM operations. The respondent does not provide solid response to the question does an accurate and reliable contract or SLA is existing for the outsource operations, but addressed that the most important and challenging factor for the contract is the verification of services and the ability to trust your vendor about what is signed and negotiated in the contract. The respondent stated that no specific criterion is designed for measuring, controlling and verification of the outsourced operations and it is still under consideration that process.

Reason and expectation that drives the outsourcing process and the company is seeking for outsourcing the security IS/IT services, the respondent said that inside the company there cannot be so well educated and practised employees that can be hired for low cost in regular method. By obtaining outsource vendor for security services, the external service provider can bring the same and the needed knowledge, by lowest cost. Which operations should be kept internally and not be outsourced in security manner was the next question, and the respondent stated that it is different for every special security solution to problem or IT or

data security function, and that at the moment of writing, it is still very internally decided and depends on the sensitivity of the function and their vitality for the company.

The company's respondent believes that IT security outsourcing processes can accelerates a business or an organization with the up-to-date technologies and qualified knowledgeable workers and employees. With already done investigations and analyses by the company, the respondent stated that the IS/IT security outsourcing, can enables an organization or a business to lower fixed costs, and in their practise that is the case. Also, the respondent addressed that IT security outsourcing can brings more knowledge and capability to company's in-house employees and also better technology innovation, software management of it and superior access for information.

The preparation and knowledge of the IT security services providers, the respondent stated that in terms of hardware, software, network infrastructure they must be prepared quite well. "Biggest risk factor is human factor in form of people without having enough knowledge" said the respondent on the question what is the biggest risk factor for IS/IT security outsourcing. The most beneficial motive, on which companies choose to outsource the IT security operations, that the respondent is addressed is that raising understanding and better and knowledgeable awareness in the company's IT staff about what is secured and with what technologies and methods.

Respondent 6 – **Masterline International**

The respondent from this company is working in the sales department, and more particularly is the director of sales. Masterline International d.o.o. is a company operating and offering services in the telecommunications, energy and consulting. The company is operating for 20 years and is one of the leading providers of telecommunication and security equipment for Slovenian power distribution companies. On Figure 17, is presented company's logo.

Figure 17. Masterline International Company Logo

Source: Masterline International, Masterline International Company Logo, 2016.

The company is outsourcing mostly network communication services. On the question, does a specific, accurate and reliable contracting SLA is defined for the outsourced operations the respondent does not provide strong argument, but stated that the most important factors and parameters for a IS/IT outsource contracting are the respond time and the time frame of eliminating an error from the time when error appears. The respondent said that in general, they are not working with security services, with outside vendors or providers, and the security polices and model is build and implemented internally, considering the company is

distributing and supplying security equipment to clients. In this company, the respondent addressed that every process and activity in the security model of the company is built internally, and all IT security functions are in-house maintained.

On the question, does IT security outsourcing bring more expertise to company in-house employees like technology innovation, software management or better access for knowledge, the respondent aimed that in her knowledge, she considers that companies which outsource security IT functions has already educated and experienced staff, and the security functions are already well defined and structured, ~~so~~ the in-house employees and the outsourced working staff are in line with knowledge and practice. Also, the respondent said that the service providers, which offer security IT functions, are dealing very slowly with hardware, software or network solutions for supporting the securing operations, mainly as a result of lack of knowledge.

The risk factors for IS/IT security outsourcing that the respondent stated is that most of the applications outsourced connected with security are critical and sensitive to company's mission, and without proper control as possible, can affect the overall security status of the company operating. The most beneficial motive, on which companies choose to outsource the security IT functions, is to get higher level of security that can be enabled within the company and the level of trust that brings the outsourced vendor to the in-house working level.

Respondent 7 – **VIRIS** (Service Provider (SP) for IT security services)

Viris d.o.o. is a company which primarily focus on providing security services. The company offers development, consulting and improvements on setting up information systems and security solutions grounded on up-to-date technological platforms. The services that the company is providing include security reviews, penetration testing, consulting about Information and Computer Security and implementation of security solutions in an Information system, both with hardware and software solutions. On Figure 18, is indicated company's logo.

Figure 18. Viris Company Logo

Source: Viris d.o.o., Viris Company Logo, 2016.

The respondent is working as operational manager in the company and said that the company is actively working from 2005 in the IT industry in Slovenia. Additionally, the respondent stated that the company estimates 20% market share in Slovenia. On the question what type

of security services the company offers to companies, the respondent lists that they offer to customers Information Security services as System Security Review, Penetration testing, Application Security Reviews, Source Code Security Review, trainings and other. The respondent said that contracting and SLAs are commonly written, but besides the strong signed contracts, most important in the operations outsourced is the quality of service, considering that it is the main factor that defines an executor and fulfils customer's expectations.

The security services that the company is providing, are always measured, controlled and verified by both parties and every project signed for client has its scope and objectives and at the end of the project, both parties execute verification. The reasons and expectations on which customers choose them as a service provider for security IT functions, is owing to Viris always offer high-level skill services. The respondent said, "Customers have usually absence of great level knowledge, by combining with our expertise, the in-house employees always gain more". To perform excellent security IT services, the respondent said that to be up with the technology and knowledge, they always invest in the company infrastructure and employees. The outsourcing of security IT functions, the respondent stated that, companies are facing lower fixed costs because they are preventing security incidents, the security awareness is highly increased, and that in time can lower company's costs.

On the question is IT security outsourcing brings more expertise to company's in-house employees like technology innovation, software management or better access for knowledge, the respondent said "We believe that we provide knowledge to our clients and customers and different prospective of information security that help customers with technology innovation and software management". For providing effective security solutions, the respondent stated that they have their own infrastructure and they are well prepared for the services, and that is a must and necessary for executing security projects. The risk factors for IS/IT security outsourcing and basic arguments for implementing IS/IT security outsourcing was the next topic discussed. The respondent aimed that the biggest risk for outsourcing is trust. High level of confidentiality is necessary for both parties. Arguments for outsourcing are in objectivity of services and in high level of information security knowledge. The respondent also stated that most beneficial motives on which companies choose to outsource security functions, is to have strong and sharp IT security model with latest technology and knowledge, and also to lower costs of investing in their in-house assets.

4.2 Research key findings and analysis

To show my research findings analysis with graphical representations in tables, I separated them in several tables by different parameters of analyzing. In the following are tables where company's responses to my structured questionnaire are separated by characteristics of answers.

On Table 4, are shown my researched companies separated by industry of operating in Slovenia in the interest of I assumed that the industry of operating is an important question considering different industries without core IS/IT technological operations will be out of focus for this research. How many years are actively existing and operating on the Slovenian market was important for my research, in behalf of the years of experience is the knowledge and practice in the IS/IT area and companies that are actively operating on the market for more than ten years, possess understanding and professional knowledge. In addition, the products and services they are offering.

On Table 5, are shown characteristics of the type of services that the companies outsource, since I desired to study what type of outsourced functions are in company's business model. In addition, the SLA or contract provided and the level of measuring, controlling and verifying of services outsourced.

On the Table 6, are shown the IS/IT security outsource characteristics separated by reasons for outsourcing IS/IT Security, IT security functions internally vs. outsourcing development and preparedness of technology and knowledge from IT security outsource vendors.

On Table 7, are shown the risk factors of IT security outsourcing that the companies believe are rising when they choose to outsource, the cost benefit parameter as a driver for cutting costs and the main motive for organizations and companies for IT security outsourcing.

Table 4. Researched Companies separated by Industry and Years of operating in Slovenia and their Products and Services

Company	**Industry of Operating**	**Years' operating**	**Products/Services Offering**
Telemach	Telecommunication	17 years	Cable services, Internet Services, Provider services and Telecommunication services
Siopti	Information Technology and Network	9 years	Professional Information Technology Services (Installation, Maintenance and Support)
Telekom Slovenije	Telecommunication	+25 years	Provider and Communication services
Eles	Information Technology and Telecommunication	+20 years	Public Services of Transmission Network System Operator
Stelkom	Telecommunication	13 years	Telecommunication services
Masterline International	Telecommunication and Information Technology	20 years	Telecommunication security equipment for Slovenian power distribution companies

table continues

continued

Viris	Information Technology	11 years	System Security Review, Penetration Testing, Application Security Reviews, Source Code Security Review, Trainings and other

Table 5. Researched Companies separated by Types of outsourced services, Contracting method and Level of measuring, controlling and verifying of Services Outsourced

Company	**Outsourced Services**	**Level of contracts or SLA for the services**	**Level of measuring of services outsourced**
Telemach	Support for business relationship management (**BRM**)	Weak level of answer for SLA or contract agreement	Unsatisfactory level of answer for measuring, controlling or verifying of outsourced services
Siopti	Business relationship management (**BRM**), Accounting Services and Network Communication Services	Satisfactory level of answer. Not specific SLAs, more contact personal agreement with the organizations	Efficient level of measuring, controlling or verifying – **response time and performance**
Telekom Slovenije	Support for Network Maintenance (Hardware & Software), Staff Training and **Managed Security Services**	Weak level of answer for SLA or contract agreement	Efficient level of measuring, controlling or verifying – **reliable service, response time, information leakage, security information status**
Eles	Support for hardware and software	Satisfactory level of answer. SLA provided for the research (**Appendix C**)	Efficient level of measuring, controlling and verifying – response time, quality level of support for the hardware and software
Stelkom	Enterprise resource planning (**ERP**) and partial customer relationship management (**CRM**) services	Weak level of answer for SLA or contract agreement	Unsatisfactory level of answer for measuring, controlling or verifying of outsourced services
Masterline International	Network Communication Services	Weak level of answer for SLA or contract agreement	Efficient level of measuring, controlling or verifying – **response time and time duration of successfully remove of error**
Viris	**Offering Information Security services** for clients	Weak level of answer for SLA or contract agreement	Efficient level of measuring, controlling or verifying – **quality of service, customer's expectations and execution verification**

Table 6. Researched Companies separated by their Reasons or Expectations for Outsourcing IS/IT security, Internal vs. Outsourcing developed and Preparedness of Outsource Vendors

Company	Reasons for outsourcing IS/IT Security	IT Security functions, outsourcing vs. in-house	Technology preparedness
Telemach	Efficient delivery time, less costs for labour, special knowledge required for IT security	All IT security functions are developed internally	N/A
Siopti	Lean organization that focuses on core competences, rather than building security IT functions	Key decision is understanding of core competences, than deciding which should be outsourced	Mostly prepared
Telekom Slovenije	To stay up-to-date with technology that is not of core business function	Internal development of functions related to network operations. Outsourcing security services for clients	Prepared
Eles	Weak level of answer for reasons for IT security outsourcing	Outsourcing penetrations tests and planning of the security model	Prepared
Stelkom	To get the best security services for lower costs	Depends of company's internal structure	Prepared
Masterline International	Organization with strong IT Security model, developed by professionals	All IT security functions are developed internally	Prepared
Viris	Lack of high skilled security services	Internal all critical to core business	Prepared

Table 7. Researched Companies separated by Risk factor, Cost drive and Motive for IT Security Outsourcing

Company	Risk Factors of IT Security Outsourcing	Cost-beneficial Drive	Motive for outsourcing security services
Telemach	Information leaking, time required to learn the infrastructure, troubles replacing outsource vendors	Lowering labour fixed costs	Cost savings

table continues

continued

Siopti	Dealing with security SP's lacks expertise and solutions for specific needs	Lowering fixed costs by making labour and investment costs more predictable	Lowering the operational costs
Telekom Slovenije	Information leaks, intellectual property rights, trust	Lowering fixed costs	To be up-to-date with technology and ability to introduce new services to clients
Eles	Trust and References	Lowering fixed costs	Better knowledge for in-house employees and security planning
Stelkom	Human factor – employees without knowledge	Lowering fixed costs	Greatest awareness of security among in-house employees
Masterline International	Access of company's mission and critical application	No answer for cost reduction provided	Higher level of security and trust
Viris	Trust and confidentiality	Lowering fixed costs, by preventing security incidents	High level of information security knowledge

CONCLUSION

The purpose of this thesis was to investigate and define the perception and awareness of Slovenian companies, which operate in industries like telecommunication, information technology or mobile networking and communication, on IS/IT Security Outsourcing. The selected companies researched are regularly in-line with many security functions of their operations. Mainly considering their products or services must be followed up with the latest security solutions and they must offer to their clients strong and sharp secured services. In that manner, it was investigated their perception or awareness for outsourcing the security functions.

I managed to provide structured interview with survey questionnaire with two of the top three main mobile operators in Slovenia, Telekom Slovenije and Telemach, and with five other companies (ELES, Siopti, Masterline International and Stelkom) that operate for more than 10 years in Slovenia and are very successful in the telecommunication, information technology, and network communication industries. To have a perspective on IS/IT security outsourcing with both parties, I managed to provide an interview also with an ASP for security services, Viris.

The interviewed companies showed an effective knowledge on outsourcing, and they all have experience in outsourcing particular functions for their business. In general, the interviewed companies are mainly outsourcing support functions and solutions for their business utilities. Support functions for business relationship management BRM, support functions for network maintenance and support for the hardware and software are the services that were stated by several interviewed companies. Therefore, I conclude, from the answers, that the owners of the telecommunications networks are mainly interested in outsourcing support services for the hardware and software of their networks. Services like enterprise resource planning ERP, customer relationship management CRM and trainings for the in-house employees were also stated.
From the interviewed companies just Telekom Slovenije, the biggest communication provider in Slovenia, indicates that they outsource security functions, but for clients and customer's services. Implicating that the organizational security model and structure is in-house developed and maintained, but the security solutions of their services are managed by security ASPs in order to provide the latest and up-to-date security solutions for their products and services. On the level for SLAs and contracting awareness, the interviewed companies showed weak level of responses, pointing out that the contracts agreement are not in best knowledge and detailed and strong SLAs were provided just from two of the interviewed companies. Addressing next on the level of responses for measuring, controlling or verifying of the services outsourced was very efficient, and all of the interviewed companies measure and control the outsource functions, without strong contracting guidelines.

The researched companies provided similar responses for the reasons and expectations for which they will outsource IS/IT security functions and main resolutions for it were the efficient delivery time of first-rate security services, less costs for investing in in-house labour and to be up-to-date with technology that is not of core business function. They all believed that IS/IT security outsourcing service providers SPs are prepared with the latest technology and knowledge for securing IS/IT functions.

From the researched companies, I cannot conclude strong argument on which IT security functions should be outsourced and which should be internally development considering companies showed mixed opinions, but key argument is that key decision on this topic is understanding of core competences on the IT functions, and then deciding which to outsource. I conclude that owners of the telecommunication networks have a different approach in this respect, for example in Telemach all IT security functions are developed internally.

On the cost investigation for outsourcing IT security functions, I conclude that the researched companies are assuming that the most cost-beneficial drive is lowering the fixed costs and lowering labour investments. As for the motive for using security outsourced services only two respondents, Telemach and Siopti are finding in cost savings. The main motive for other companies is to stay with latest up-to-date technology and possess better in-house knowledge.

My research findings showcase that companies are still not very familiar and do not have great knowledge and experience with the IT security outsourcing method, and still it is a topic on which supplementary researches could be done. On the Slovenian market, I conclude that companies operating in telecommunication industries are the ones that have best expertise in this issue. Furthermore, the IS/IT security outsourcing is a sensitive process, and still Slovenian companies are not familiar with the benefits of it. Because, the Slovenian IS/IT market it is not a giant, ASPs are not in big competition, and the ones that outsource security functions, are doing it to the ones that are in solid functioning.

Further researches could be done on exploring which are the security functions that are outsourced the most, and which parameters are crucial on companies' decision for going in for it. With the constant change of technology, new security solutions are rising daily and every IS/IT department of companies operating must follow it. In that manner, IS/IT security outsourcing, even with the risks that can occur, can be still a solid and effective solution for having strong and secured IS/IT company or offer services or products that are always highly secured.

REFERENCE LIST

1. Ashford, W. (2012, July). Best Practise in Outsourcing Security. *ComputerWeekly*. Retrieved May 29, 2016, from http://www.computerweekly.com/feature/Best-practice-in-outsourcing-security

2. Axelrod, C. W. (2004). *Outsourcing Information Security: Computer Security Series*. Norwood: Artech House.

3. Chen, L., & Soliman, K. S. (2002). Managing IT outsourcing: a value-driven approach to outsourcing using application service providers. *Logistics Information Management, 15*(3), 180-191.

4. Corbett, M. F. (2004). *The Outsourcing revolution, why it makes sense and how to do it right*, New York: Kaplan Publishing.

5. Debar, H., & Viinikka, J. (2006). Security information management as an outsourced service. *Information Management & Computer Security*, *14*(5), 417-435.

6. Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125-8.

7. Doomun, M. R. (2008). Multi-level information system security in outsourcing domain. *Business Process Management Journal*, *14*(6), 849-857.

8. DTI. (2004). *Information Security Breaches Survey and Technical Report* - Trade and Industry department, London.

9. *ELES.* Official Web-site of the company and company's logo. Retrieved June 18, 2016, from http://www.eles.si

10. Frost, C. (2000). Outsourcing or increasing risks. *Balance Sheet, 8*(2), 34-37.

11. Gonzales, R., Gasco, J., & Llopis, J. (2005). Information systems outsourcing risks: a study of large firms. *Industrial Management & Data Systems, 105*(1), 45-62.

12. Goodwin, B. (2004, January). Companies are at risk from staff ignorance. *ComputerWeekly*. Retrieved May 30, 2016, from http://www.computerweekly.com/feature/Companies-are-at-risk-from-staff-ignorance

13. Gottschalk, P., & Solli-Sæther, H. (2006). Maturity model for IT outsourcing relationships. *Industrial Management & Data Systems, 106*(2), 200-212.

14. Hiles, A. N. (1994). Service Level Agreements: Panacea or Pain? *The TQM Magazine*, *6*(2), 14-16.

15. International Organization for Standardization. (2013). *The ISO/IEC 27002:2013 standard 2013*. Retrieved June 19, 2016, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

16. Jain, G., Singh, D., & Verma, S. (2002). Service level agreements in IP networks. *Information Management & Computer Security*, *10*(4), 171-177.

17. Karyda, M., Mitrou, E., & Quirchmayr, G. (2006). A framework for outsourcing IS/IT security services. *Information Management & Computer Security*, *14*(5), 403-416.

18. Larson, K. D. (1998). The role of service level agreements in IT service delivery. *Information Management & Computer Security*, *6*(3), 128-132.

19. Laudon, K. C., & Laudon, J. P. (2015). *Management Information Systems: Managing the Digital Firm* (14th ed.) Essex: Pearson.

20. Leavy, B. (2004). Outsourcing strategies: opportunities and risks. *Strategy & Leadership, 32*(6), *20-25.*

21. *Masterline International.* Official Web-site of the company and company's logo. Retrieved June 18, 2016, from http://www.masterline-international.com/en/

22. Mezak, S., & Hilliard, A. (2016). *Outsource or Else!: How a VP of Software Saved his Company.* Redwood City, California : Accelerance Inc.

23. Nassimbeni, G., Sartor, M., & Dus, D. (2012). Security risks in service offshoring and outsourcing. *Industrial Management & Data Systems*, *112*(3), 405-440.

24. Nosworthy, J. (2000). Implementing Information Security in the 21st century – do you have the balancing factors? *Computers and Security*, *19*, 337-47.

25. Palmatier, G. (2001). *ASP Configuration Handbook: A Guide for ISPs*. Rockland: Syngress Publishing Inc.

26. Pratap, S. (2014). Towards a framework for performing outsourcing capability. *Strategic Outsourcing: An International Journal*, *7*(3), 226-252.

27. Proctor, K. S. (2011). *Optimizing & Assessing Information Technology – Improving Business Project Execution*, (1st ed.) New York: Wiley.

28. Quinn, J. B. (2000). Outsourcing Innovation: The New Engine of Growth. *Sloan Management Review*, *41*(4), 13.

29. Rainer, R. K., & Cegielski, C. G. (2012). *Introduction to Information Systems - International Student Version* (4th ed.) New York: John Wiley & Sons Inc.

30. Rainer, R. K., Prince, B., & Cegielski, C. G. (2013). *Introduction to Information Systems - Supporting and Transforming Business* (5th ed.) New York: John Wiley & Sons Inc.

31. Renkema, T. J. W. (2000). *The IT Value Quest* (1st ed.) New York: John Wiley & Sons Inc.

32. Rouse, M. (2010). Application Service Provider (ASP). *Tech Target*. Retrieved March 16, 2016, from http://searchsoa.techtarget.com/definition/application-service-provider

33. *Siopti*. Official Web-site of the company and company's logo. Retrieved June 18, 2016, from http://www.siopti.com

34. Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

35. Smith, R. (1995). Business continuity planning and service level agreements. *Information Management & Computer Security*, *3*(3), 17-19.

36. Soliman, K. S. (2003). A framework for global IS outsourcing by application service providers. *Business Process Management Journal*, *9*(6), 735-744.

37. *Stelkom.* Official Web-site of the company and company's logo. Retrieved June 18, 2016, from http://www.stelkom.si/en/

38. Tafti, M. H. A. (2005). Risks factors associated with offshore IT outsourcing. *Industrial Management & Data Systems*, *105*(5), 549-560.

39. *Telekom Slovenije*. Official Web-site of the company and company's logo. Retrieved June 18, 2016, from http://www.telekom.si

40. *Telemach*. Official Web-site of the company and company's logo. Retrieved June 18, 2016, from http://telemach.si

41. Tuban, E., Volonino, L., & Wood, G. R. (2013). *Information Technology for Management: Advancing Sustainable*, Profitable Business Growth (9th ed.) New York: John Wiley & Sons Inc.

42. *Viris d.o.o.*. Official Web-site of the company and company's logo. Retrieved June 18, 2016, from https://www.viris.si

APPENDIXES

TABLE OF APPENDIXES

Appendix A: List of Abbreviations

Table 1. List of Abbreviations

Abbreviation	Meaning
IT	Information Technology
IS	Information Systems
IT/IS	Information Technologies and Information Systems
IS/IT	Information Systems and Information Technologies
ERP	Enterprise Resource Planning
CRM	Customer Relationship Management
SP	Service Provider
ASPs	Application Service Providers
ASP	Application Service Provider
ROI	Return on/off Investment
RBT	Resource Based Theory
TCT	Transaction Cost Theory
RDT	Resource Dependence Theory
ACT	Agency Cost Theory
VPN	Virtual Private Network
SLA	Service Level Agreement
SLAs	Service Level Agreements
CBIS	Computer Based Information System
SaaS	Software as a Service
AO	Application Outsourcing
BPO	Business Process Outsourcing
AMO	Application Maintenance Outsourcing
SCM	Supply Chain Management
IP	Internet Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
ITIL	Information Technology Infrastructure Library
IDS	Intrusion Detection Systems
SIM	Security Information Management
IDMEF	Intrusion Detection Message Exchange Format
MMS	Managed Security Services
MSSPs	Managed Security Service Providers
EDPD	European data protection directive
EU	European Union
OECD	Organization for Economic Cooperation and Development
QoS	Quality of Service
RMA	Return Material Authorization
ECI	Elastic network company
ISO	International Standards Organization
IEC	International Electro technical Commission

Appendix B: Structured Interview Survey questionnaire

- Describe how long your business or organization is operating, and in which industry is, what is the position level on the market?
- Define what types of Information Technology or Information Systems (IT/IS) your business or organization outsources? (ERP, CRM, IT Security services, BPR, Network communication services, Data operations etc.)
- Is a specific, accurate and reliable contracting SLA, defined for the outsourced services? – By your opinion, what are the factors and parameters you consider most important/challenging for the SLA for IS/IT security outsourcing and why? (Prices, verification of services, track of services etc.)
- How the outsourced IS/IT security services are measured, controlled and verified by both parties in the agreement?
- What are the reasons/expectations for which your business or organization turn to IS/IT security outsourcing?
- Which IT security functions are suitable for outsourcing and which should be kept internally?
- Is IT security outsourcing processes accelerates your business or organization with up-to-date technologies and qualified knowledge workers?
- Is IT security outsourcing, or IT/IS outsourcing, enables your business or organization to lower fixed costs or turn fixed costs more to variable costs?
- Is IT security outsourcing brings more expertise to company in-house employees like technology innovation, software management or better access for knowledge?
- How are service providers prepared to provide hardware, software and network infrastructure, as well as business services that are necessary for the security outsourcing model?
- What are risk factors for IS/IT security outsourcing and basic arguments for implementing IS/IT security outsourcing?
- In your opinion what would be the most beneficial motive for your business from using security-outsourcing services?

Appendix C: SLA Example in Slovenian Language, provided by ELES, Ltd., Electricity Transmission System Operator (ELES)

DOGOVOR O NIVOJU IZVAJANJA STORITEV

1. DEFINICIJA POJMOV

Storitve so naročnikove storitve, ki jih naročnik izvaja za svoje uporabnike

Storitve podpore in vzdrževanja so storitve, izvajalca, namenjene podpori in vzdrževanju strojne in programske opreme opredeljene v pogodbi s katero naročnik izvaja storitve za svoje uporabnike.

Katalog storitev je evidenca storitev s pripadajočimi opisnimi podatki.

Nivo storitev je določen način izvajanja storitve podpore in vzdrževanja, kjer so zajeti parametri, način in čas izvajanja storitev podpore in vzdrževanja.

Storitveni center (SC) je enotna vstopna točka za komunikacijo med izvajalcem in naročnikom.

Komunikacijski kanal, je oblika komunikacije med naročnikom in enotno vstopno točko SC izvajalca. Te oblike so:

- telefon, GSM,
- elektronska pošta,
- portal.

Vsi našteti komunikacijski kanali so dvosmerni.

Informacija je skupek dejstev, ki se nanašajo na posamezno storitev in opisujejo stanje te storitve ali z njo povezanih dogodkov.

Dogodek Sprememba stanja, ki je pomembna s stališča upravljanja storitve ali konfiguracijskega elementa. Izraz se uporablja tudi kot opozorilo ali obvestilo, ki ga kreira storitev, konfiguracijski element ali orodje za spremljanje. Dogodek praviloma zahteva odziv osebja zadolženega za obratovanje IKT in pogosto temu sledi vpis incidenta.

Incident je dogodek, ki pomeni nenačrtovano prekinitev ali zmanjšanje kakovosti storitve. Incident je tudi napaka v konfiguracijskem elementu, ki še ne vpliva na storitev, kot je okvara ene komponente sistema, zmanjša pa zanesljivost storitve.

Zanesljivost je merilo ki pove koliko časa zmore storitev ali nek konfiguracijski element delovati brez prekinitve. Običajno se meri kot povprečni čas med odpovedma (MTBF) ali kot povprečni čas med izpadoma storitve (MTBSI). Izraz se lahko uporablja tudi za opredelitev verjetnosti, da bo storitev delovala kot zahtevamo.

Vpliv – je pojem oz. objektivno merilo s katerim se določi vpliv posameznega dogodka na poslovanje oz. uporabo storitve. Z vplivom lahko določimo, koliko dogodek vpliva na delovanje storitev in poslovanje.

Nujnost – je pojem oz. objektivno merilo s katerim določamo, kako hitro je potrebno odpraviti incident in zagotoviti ponovno normalno delovanje storitve.

Prioriteta – je pojem oz. objektivno merilo s katerim na osnovi določene nujnosti in vpliva določimo vrstni red reševanja incidentov, problemov,storitvenih zahtev in zahtev za spremembo. Prioriteto določi naročnik na podlagi vpliva in nujnosti.

Problem je nepoznan vzrok za nastanek enega ali več incidentov na storitvah.

Problemski tip je klasifikator problematike, s katerim določimo vrsto aktivnosti in z generičnimi parametri opredelimo vsebino problematike. Na osnovi problemskega tipa se določi ali je klic naročnika vezan za incidente oz. zahteve, z njim opredelimo tudi specifičnosti iz kataloga storitev vezane na različne ravni storitve.

Znana napaka je odkrit vzrok za nastanek incidentov. Znana napaka je tako rekoč rešitev problema, ki ponuja začasno ali stalno rešitev.

Storitveni zahtevek je uradni zahtevek uporabnika za neko storitev. Na primer: zahtevek za informacijo ali nasvet, zahtevek za odpravo incidenta, zahtevek za rešitev problema, zahtevek za novo storitev. Storitveni zahtevek je lahko vezan na zahtevek za spremembo kot del procesa reševanja zahtevka.

Zahteva za spremembo, sprememba je zahteva, kjer naročnik poda zahtevo za dodajanje nove funkcionalnosti in vsebine oz. s katero se spremeni, doda ali odvzame funkcionalnost ali vsebina obstoječe storitve. Sprememba pomeni tudi spreminjanje kapacitete in razpoložljivosti storitve. Spremembe se klasificirajo na osnovi obsega in se lahko obravnavajo kot projektno delo. Spremembe niso standardne storitvene zahteve. Sprememba pomeni tudi kreiranje novih storitev.

Odzivni čas je čas v katerem se prijava incidenta, prijava problema, storitvena zahteva in zahteva za spremembo vpiše v sistem, klasificira, določi osnovna problematika, storitev, sistemski sklop ali okvarjena strojna oz. programska oprema. Po izteku tega časa mora izvajalec storitve kompetentno pristopiti k odpravi incidenta oz. k zagotavljanju izvedbe storitvene zahteve. Mejnik odzivnega časa je povratna informacija naročniku, ki vsebuje:

- zaporedno številko odprtega incidenta, problema, zahteve za spremembo oz. storitvene zahteve, ki je hkrati tudi identifikacijska številka za nadaljnjo komunikacijo;
- podatke o določitvi storitve, okvarjenega sistemskega sklopa, strojne ali programske opreme;
- določena mora biti prioriteta, kot derivat med vplivom in nujnostjo
- določena mora biti generična vsebina problematike

Čas obratovanja določi časovni interval razpoložljivosti storitve naročniku. Časovni roki za izračun SLA parametrov tečejo samo znotraj tega časovnega intervala.

Pomoč naročniku je nasvet ali interaktivno spremljanje uporabe storitve, ki ga izvajalec posreduje naročniku. Pomoč naročniku vključuje tudi prenos izvajalčevega znanja.

Programska oprema je vsa programska oprema, ki mora biti nameščena na strojni opremi (postavljenem v delovno okolje) za izvajanje storitev.

Odbor za analizo in odobritev sprememb, je skupina, ki je določena stalno oz. se zasedba te skupine spreminja glede na kompleksnost spremembe. V skupini sodelujejo člani naročnika in izvajalca, ki s svojimi kompetencami lahko presodijo kakšen vpliv bo imela sprememba na obstoječe stanje storitev in na poslovanje.

Odprava incidenta pomeni zagotovitev prvotno določenega delovanja storitve z zagotavljanjem končne ali pa nadomestne rešitve.

Vzdrževanje so standardne vnaprej določene aktivnosti s katerimi se zagotavlja kvalitetno delovanje opreme in storitev, kot tudi preventivno odkrivanje vzrokov za nastanek incidentov ali pa potreb za izvajanje sprememb v smislu povečanja kapacitete. Aktivnosti vezane na redno vzdrževanje se izvajajo in dokumentirajo v sklopu izvajanja storitvenih zahtev.

Delovniki so vsi dnevi od ponedeljka do petka, ki niso v Republiki Sloveniji priznani kot praznik.

Prazniki so dnevi, ki so v Republiki Sloveniji priznani kot dela prosti dnevi.

2. IZVAJANJE PODPORE IN VZDRŽEVANJA

Opis storitev podrobneje opredeljuje storitve, ki so predmet te pogodbe.

Dosegljivost strokovnjaka izvajalca

- dajanje informacij povezanih s posamezno storitvijo in opremo,
- pomoč naročniku pri uporabi storitve in opreme.

Sprejem in odprava incidentov

- prijava incidentov preko želenega komunikacijskega kanala
- sprejem incidentov in dokumentiranje vsebine problematike
- vezava incidentov na specifično storitev, sistemski sklop, sistem in opremo
- določanje problemskega tipa incidentov
- reševanje incidentov – vzpostavitve normalnega delovanja storitve
- poročanje o incidentu (vzrok, kako se je incident odpravil..)

Reševanje problemov

- prijava problemov
- proaktivno odkrivanje in odpravljanje problemov
  - analiza trendov dogodkov na sistemih in sistemskih sklopih
  - priprava predlogov za izboljšave
- reaktivno odkrivanje in odpravljanje problemov
  - odkrivanje problemov in dokumentiranje vsebine
  - raziskovanje problematike
  - pripravo podlag za odpravo vzrokov iz problematike

Izvajanje storitvenih zahtev

- prijava storitvenih zahtev
- sprejem zahtev in dokumentiranje vsebine
- klasifikacija zahtev glede vsebine
- vezava storitvenih zahtev za specifično storitev, sistemski sklop, sistem in opremo
- izvajanje zahtev na obstoječih storitvah, sistemskih sklopih, sistemih in opremi
- dokumentiranje izvedenih storitev

Izvajanje zahtev za spremembo

- prijava zahtev za spremembo
- sprejem in dokumentiranje zahtev za spremembo
- kategorizacija zahtev za spremembo glede na obseg in kompleksnost
- vezava zahtev za spremembo na specifično storitev, sistemski sklop, sistem in opremo
- določanje prioritete sprememb
- analiza zahtev za spremembo glede na obstoječe stanje – organiziranje odbora za analizo in odobritev sprememb.
- določanje vpliva sprememb glede na izvajanje obstoječih storitev in poslovanje
- planiranje izvedbe spremembe skupaj z naročnikom
- razvoj spremembe
- testiranje spremembe
- implementacija spremembe
- stabilizacija spremembe in izobraževanje naročnika
- dopolnitev obstoječe dokumentacije storitve, sistemskega sklopa, sistema in opreme glede na spremembo.

Redno vzdrževanje in upravljanje

- redni pregled in spremljanje delovanja opreme, sistemov in storitev
- vzdrževanje obstoječih skript posameznih storitev
- izvajanje posodobitev in nameščanje varnostnih popravkov po navodilih proizvajalca na najnovejšo verzijo oz. na verzijo dogovorjeno z naročnikom

- izdelava mesečnih poročil o izvajanju vzdrževanja in stanju sistemskih sklopov, sistemov, opreme in storitev.
- stalen avtomatski nadzor nad delovanjem sistemskih sklopov in sistemov.

Nadomestna oprema

- Izvajalec bo za naročnika imel v pripravljenosti nadomestno opremo.
- Nadomestna oprema bo zadovoljevala takojšnjo zamenjavo okvarjene opreme vsakega sistema, ki je predmet vzdrževanja te pogodbe.
- Izvajalec bo nadomestno opremo uporabil, zamenjal takoj v primeru, da ugotovi okvaro na produkcijski opremi.
- Izvajalec bo zamenjavo izvedel v skladu z parametri ravni storitve.

Poročanje o izvajanju storitev

- izvajalec bo mesečno zagotavljal poročila o izvajanju storitev podpore in vzdrževanja in stanju storitev, sistemskih sklopov in sistemov. Poročilo o opravljenih storitvah je obvezna priloga k računu. Izvajalec enkrat letno pripravi skupno poročilo o delovanju sistema in izvajanju storitev

3. KOMUNIKACIJA IN KONTAKTNI PODATKI

Naročnik prijavi storitveni zahtevek preko enega izmed komunikacijskih kanalov:

- telefon: _____
- e-pošta: _____
- portal: _____

Odzivni čas in čas za rešitev prične teči od trenutka prijave napake s strani naročnika.

Ponudnik kontaktrira naročnika preko enega izmed sledečih komunikacijskih kanalov:

- telefon: 01 473 2020
- e-pošta: sos-itk@eles.si

4. NIVO IZVAJANJA STORITEV.

Določanje prioritete izvajanja storitev

Tabela 2. Določitev stopnje nujnosti

Stopnja nujnosti	**Opis**
URGENTNO	• Prizadet je sistem oz. storitev in je ni mogoče več uporabljati. • Uporaba sistema ali storitve je zahtevana v najkrajšem možnem času. • Od časa ponovne vzpostavitve delovanja sistema ali storitve je odvisno nadaljnje izvajanje poslovanja oziroma zagotavljanje dogovorjene kvalitete poslovanja v podjetju.
NUJNO	• Prizadet je sistem ali storitev vendar je uporaba možna v omejenem obsegu, omejeni funkcionalnosti oz. omejeni kapaciteti. • Sistem deluje v razpoložljivem načinu (namesto v visoko razpoložljivem načinu). Obstaja bojazen, da se bo izgubila funkcionalnost tudi rezervnega sistema. • Poslovanje je moteno, • Delovanje storitve ali sistema je časovno občutljivo
STANDARDNO	• Na sistemu ali storitvi je odkrita napaka. • Poslovanje je lahko moteno vendar delovanje storitve ali sistema ni časovno občutljivo.
NIZKO	• Kategorija se dodeljuje dogodkom in zahtevam, ki ne vplivajo na poslovanje. V primeru, ko je incident odpravljen in je potrebno opazovanje ali nadaljnje raziskovanje.

Tabela 3. Določitev stopnje VPLIVA

Stopnja vpliva	**Opis**
IZREDEN	• Dogodek ali zahteva ima vpliv na delovanje storitve, od katere je v odvisno veliko število uporabnikov oz. ima veliko poslovno pomembnost. • Uporaba storitve je onemogočena vsem uporabnikom. • Poslovanje je lahko ogroženo ali onemogočeno.
VISOK	• Dogodek ali zahteva ima vpliv na delovanje storitve, od katere je v tem trenutku odvisno samo del uporabnikov oz. ima delno veliko poslovno pomembnost. • Uporaba storitve je onemogočena večini uporabnikov. • Poslovanje je omejeno.
NORMALNO OMEJEN	• Dogodek ali zahteva ima omejen vpliv. • Uporaba storitve je omogočena, vendar je dogodek omejen na določen sistemski sklop ali del programske opreme. • Dogodek je lahko omejen tudi na skupino uporabnikov, v celoti pa je večini uporaba storitve omogočena. • Poslovanje je lokalno omejeno.
LOKALEN	• Dogodek ali zahteva ima izredno omejen vpliv na posameznega uporabnika ali na posamezen del sistemskega sklopa, strojne oz. programske opreme.

Tabela 4. Matrika za določanje PRIORITETE na podlagi nujnosti in vpliva

VPLIV/NUJNOST	**Nizko**	**Standardno**	**Nujno**	**Urgentno**
Izreden vpliv	4	2	1	1
Visok vpliv	4	3	2	1
Normalno omejen	4	3	2	2
Lokalen	4	4	3	3

Čas obratovanja storitev in odzivni časi:

Tabela 5. Dosegljivost strokovnjaka izvajalca

Čas za odzivnost	**Čas za odgovor**	**Čas obratovanja**
30 minut	4 h	Delavnik 7:00 – 17:00

Tabela 6. Sprejem in odprava incidentov

Prioriteta	**Opis**	**Čas za odzivnost**	**Čas do rešitve**	**Čas obratovanja**
1	Kritično	1 h	4 h	Delavnik 7:00 – 17:00
2	Visoka	1 h	4 h	Delavnik 7:00 – 17:00
3	Srednja	4 h	24 h	Delavnik 7:00 – 17:00
4	Nizka	4 h	24 h	Delavnik 7:00 – 17:00

Tabela 7. Reševanje problemov

Prioriteta	**Opis**	**Čas za odzivnost**	**Čas do rešitve**	**Čas obratovanja**
1	Kritično	1 h	4 h	Delavnik 7:00 – 17:00
2	Visoka	1 h	4 h	Delavnik 7:00 – 17:00
3	Srednja	4 h	24 h	Delavnik 7:00 – 17:00
4	Nizka	4 h	24 h	Delavnik 7:00 – 17:00

Tabela 8. Izvajanje storitvenih zahtev

Prioriteta	**Opis**	**Čas za**	**Čas do**	**Čas obratovanja**

		odzivnost	**rešitve**	
1	Kritično	1 h	24 ur	Delavnik 7:00 – 17:00
2	Visoka	1 h	24 ur	Delavnik 7:00 – 17:00
3	Srednja	4 h	5dni	Delavnik 7:00 – 17:00
4	Nizka	4 h	5dni	Delavnik 7:00 – 17:00

Tabela 9. Izvajanje zahtev za spremembo

Prioriteta	**Opis**	**Čas za odzivnost**	**Čas do rešitve**	**Čas obratovanja**
1	Kritično	1 h	24 ur	Delavnik 7:00 – 17:00
2	Visoka	1 h	24 ur	Delavnik 7:00 – 17:00
3	Srednja	4 h	5dni	Delavnik 7:00 – 17:00
4	Nizka	4 h	5dni	Delavnik 7:00 – 17:00

Tabela 10. Redno vzdrževanje in upravljanje

Opis	**Čas za odzivnost**	**Čas do rešitve**	**Čas obratovanja**
Analiza sistema	1 dan	5 dni	Delavnik 7:00 – 17:00
Nameščanje nove verzije programske opreme	1 dan	5 dni	Prazniki in delavnik 17:00 – 7:00
Nameščanje kritičnih popravkov programske opreme	4h	1 dan	24/7

5. POGODBENA KAZEN ZA IZVAJANJE PODPORE IN VZDRŽEVANJA,

Če je izvajalec po svoji krivdi v zamudi z izpolnitvijo svojih obveznosti, ima naročnik pravico zahtevati od izvajalca pogodbeno kazen. Pogodbena kazen se izračunava če se storitve ne izvajajo časovnih okvirjih dogovorjenimi s to pogodbo. Pogodbeno kazen je dolžan izvajalec plačati naročniku v roku 8-ih dni od datuma izstavitve zahtevka za plačilo kazni oz. se znesek lahko pobota z izstavljenim računom če se stranki tako dogovorita.

Pogodbena kazen za neizvajanje storitev v dogovorjenih časovnih rokih za posamezne storitve je:

Tabela 11. Dosegljivost strokovnjaka izvajalca

Čas za odzivnost	**Čas za odgovor**
Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€

Tabela 12. Sprejem in odprava incidentov

Prioriteta	**Opis**	**Čas za odzivnost**	**Čas do rešitve**
1	Kritično	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 20€
2	Visoka	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 20€
3	Srednja	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€
4	Nizka	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro10€

Tabela 13. Reševanje problemov

Prioriteta	**Opis**	**Čas za odzivnost**	**Čas do rešitve**
1	Kritično	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 20€
2	Visoka	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 20€
3	Srednja	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€
4	Nizka	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€

Tabela 14. Izvajanje storitvenih zahtev

Prioriteta	**Opis**	**Čas za Odzivnost**	**Čas do rešitve**
1	Kritično	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€
2	Visoka	Za vsako začeto prekoračeno uro 5 €	Za vsako začeto prekoračeno uro 10€
3	Srednja	Za vsako začeto prekoračeno uro 10€	Za vsako začet prekoračen dan 5€
4	Nizka	Za vsako začeto prekoračeno uro 5€	Za vsako začet prekoračen dan 5€

Tabela 15. Izvajanje zahtev za spremembo

Prioriteta	**Opis**	**Čas za Odzivnost**	**Čas do rešitve**
1	Kritično	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€
2	Visoka	Za vsako začeto prekoračeno uro 5€	Za vsako začeto prekoračeno uro 10€

tabela se nadaljuje

nadaljevanje

3	Srednja	Za vsako začeto prekoračeno uro 5€	Za vsako začet prekoračen dan 10€
4	Nizka	Za vsako začeto prekoračeno uro 5€	Za vsako začet prekoračen dan 10€

Tabela 16. Redno vzdrževanje in upravljanje

Opis	**Čas za odzivnost**	**Čas do rešitve**
Analiza sistema	Za vsako začet prekoračen dan 5€	Za vsako začet prekoračen dan 10€
Nameščanje nove verzije programske opreme	Za vsako začet prekoračen dan 5€	Za vsako začet prekoračen dan 10€
Nameščanje kritičnih popravkov programske opreme	Za vsako začeto prekoračeno uro 5€	Za vsako začet prekoračen dan 20€