Denis Lapin

Proposing a Cloud-based Operational Model for IT Infrastructure

Helsinki Metropolia University of Applied Sciences

Master's Degree

Industrial Management

Master's Thesis

20 November 2014

Helsinki Metropolia University of Applied Sciences

Author Title Number of Pages Date	Denis Lapin Proposing a Cloud-based Operational Model for IT Infrastructure 98 pages + 8 appendices 20 November 2014
Degree	Master's Degree
Degree Programme	Industrial Management
Instructor	Thomas Rohweder, DSc (Econ), Principal Lecturer Ziniada Grabovskaia, PhL, Senior Lecturer

This Master's Thesis investigates the possible use of Infrastructure as a Service (IaaS) service model in the case company and proposes a new cloud service based operational model for it. IaaS represents the service model where IT infrastructure is delivered to the customers through the network by the cloud service providers. The proposed operational model aims to addresses the needs for improving business agility and cost efficiency, as commissioned by the IT Infrastructure department of the case company.

The objective of this thesis is to review the current IT operational model existing in the case company and analyze possible impacts of the cloud services on the organization. The study is conducted using a case study research approach. The data collection includes methods such as scrutinizing the business requirements from the organization, its current operational model, examining the company documentation, and conducting a series of interviews and discussions with key stakeholders. The impact of the cloud services to organization was analysed with the help of a conceptual framework which was developed based on extensively selected academic articles and books.

The outcome of the thesis is a proposed cloud service based operational model. The proposed operational model is based on the Hybrid Cloud IT deployment model, a combination of the the Private Cloud IT (on-premises) and Private Cloud IT (off-premises) deployment models. This type of the Hybrid Cloud IT model is selected among the available alternatives by comparing benefits and challenges of each option, and also examined against the business requirements from the case company. The proposed operational model is described with the help of its key elements such as Organizational Structure, Governance, Sourcing, Operational processes, Configuration Management Database (CMDB) and Risk Analysis.

The outcome of the thesis helps the management of the case company in decision-making when taking cloud services into use. It provides the company-adjusted recommendations for the selection of a cloud deployment model and proposes a cloud service based operational model which could best suit the case company context. Many companies around the globe face similar challenges. This thesis provides an example of putting the IaaS service model into a real-life company context, and thus helps in adopting cloud service technologies.

Keywords	Cloud Computing, IaaS, Cloud Deployment Models, Organizational Structure, IT Governance, Sourcing, ITIL, ITSM processes, CMDB, Risk Analysis.

Contents

Acronyms

CITS	Corporate IT Services
IaaS	Infrastructure as a Service
SaaS	Corporate IT Services
PaaS	Software as a Service
CMDB	Configuration Management Database
CPU	Central Processing Unit
SLA	Service Level Agreement
MPLS	Multiprotocol Label Switching
CIO	Chief Information Officer
BPM	Business Process Management
HR	Human Resource Management
TMT	Top Management Team
PIT MT	Process and IT Management Team
Division MT	Division Management Team
ITMT	IT Management Team
BPM MT	Business Process Management Team
CCB	Customer Co-operation Board
CAT	Change Advisory Team
ARB	Architecture Review Boards
OLA	Operational Level Agreement
UC	Underpinning Contracts
ITSM	IT Service Management
ITIL	IT Infrastructure Library
KPI	Key Performance Indicators
ID	User Identifier
CMS	Configuration Management System

1 Introduction

This Thesis focuses on the development of a new operational model for Corporate IT Services (CITS) unit of the case company. The current operational model belongs to the traditional IT service mode and requires changes to include cloud scenarios. Traditional IT service mode typically includes management of the physical IT assets (servers and network equipment), management of the software on top of these IT assets, software licence management and user's support. Some of the activities in traditional IT service mode are often outsourced to the third party service provider(s).

The case company of this study is a Finnish energy company. It operates in the Nordic and Baltic countries, as well as in some European countries and Russia. The case company operates power plants and provides various energy related services. The company's main activities concentrate on the generation, distribution and sales of electricity and heat as well as related expert services. This Thesis focuses on one unit of the case company, Corporate IT Services unit (CITS). Corporate IT Services is an internal service unit providing IT infrastructure services to the company's business divisions. In addition, CITS is responsible for provisioning selected Enterprise Applications. This project on cloud services is done for the IT Infrastructure Team of the Corporate IT Services unit in particular.

1.1 Business Problem

In recent years, IT services from the cloud service providers have become more applicable for corporate use. The pricing model and fast commissioning of the infrastructure as a service (IaaS) by cloud service providers could solve many existing business problems of the traditional provisioning of IT services. These problems include lack of agility and slow service delivery of the IT hardware due to the slowness of the procurement process and required capital investments (Appendix 1). Thus, the business problem of this study is to investigate how to maintain and expand the case company Data Center in an economical and a functionally feasible way by utilizing the cloud technologies and cloud services.

Presently, the case company IT infrastructure team concentrates on handling IT capacity requests from internal business units. One of them is the provisioning of new virtual servers which can vary from days to several weeks, depending on the configuration, which becomes unacceptable in the current dynamic business environment. Another example is the allocation of additional capacity, where the delivery time is also quite long. Moreover, the IT capacity demands from internal users also fluctuate. All these

challenges, fluctuation in demand and slow provisioning times, point to the need for a new IT solution, with the cloud technologies as a promising choice.

1.2 Objective and Outcome

The aim of this study is to investigate the possible use of cloud computing for providing IT Infrastructure services in the case company. It is done by analysing how IT infrastructure team currently operates and what changes need to be done in order to take the cloud services into use. The objective of this Thesis is, thus, to propose a new cloud service based operational model for the IT Infrastructure Team. The new model should address the needs for improving business agility and cost efficiency of the IT infrastructure services.

The outcome of this thesis is a new cloud service based operational model proposed for future implementation in the case company. This operational model includes such key elements as Organizational Structure, Governance, Sourcing, Operational processes, Configuration Management Database (CMDB) and Risk Analysis (Table 2 A). The operational model is also examined against the case company business requirements for the cloud service based scenarios.

1.3 Scope of the Study

In this thesis, the emphasis is placed on: a) IaaS service model, b) analysis of the company's current operational model, c) the cloud deployments models suitable for the case company, d) the analysis of the business requirements for the selection of the cloud deployment model, and e) the proposal for new cloud service based operational model for IT infrastructure Team within the case company.

The proposal includes Organizational Structure, IT Governance, Sourcing, Operational Processes, CMDB and Risk Analysis. The Software as a service (SaaS) and Platform as a service (PaaS) cloud solutions are not discussed in this Thesis. Additionally, another unit, the Infra-structure support team, as agreed with the case company, lies outside the scope of this study, although it will also be affected by the introduction of cloud services.

2 Method and Material

This section describes the research approach, methods of data collection and analysis methods applied in this Thesis. Finally, the section presents the reliability and validity plan.

2.1 Research Approach

This Thesis applies a case study as its research approach. Yin (2003) defines a case study as “an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident” (Yin 2003: 13). In this Thesis, the study of a contemporary phenomenon corresponds to the inquiry about the use of cloud services for the case company and particularly by the Corporate IT Services unit (CITS) unit.

As indicated by Yin (2003), a case study approach “relies on multiple sources of evidence, with data needed to converge in a triangulating fashion” (Yin 2003: 14). This research approach allows for combining qualitative and quantitative data from various sources such as surveys, interviews, observations and other types of data. Another definition of the case study research is given by Woodside and Wilson (2003); it states that a “case study research is [an] inquiry focusing on describing, understanding, predicting, and/or controlling” the individual or a phenomenon (Woodside and Wilson 2003: 494). In this Thesis, the inquiry is focused on the investigation of a phenomenon taking place in a case study company.

Yin (2003: 105) suggests that, as one of the measures to strengthen validity and reliability of the case study research, researchers should maintain and refer to research protocols for guiding their studies from the research questions to conclusions. This approach is widely used in the research practice, where research designs act as guideline tools for researchers. They also help researchers to streamline their research work in order not to get lost in the amount of available data.

2.2 Research Design

The research design of this study includes five main stages in the investigation: business problem identification, current state analysis, best practice examination, building the proposal, and collecting feedback on the proposal. Figure 1 illustrates how the project is organized in this study and in which sequence these stages are executed.

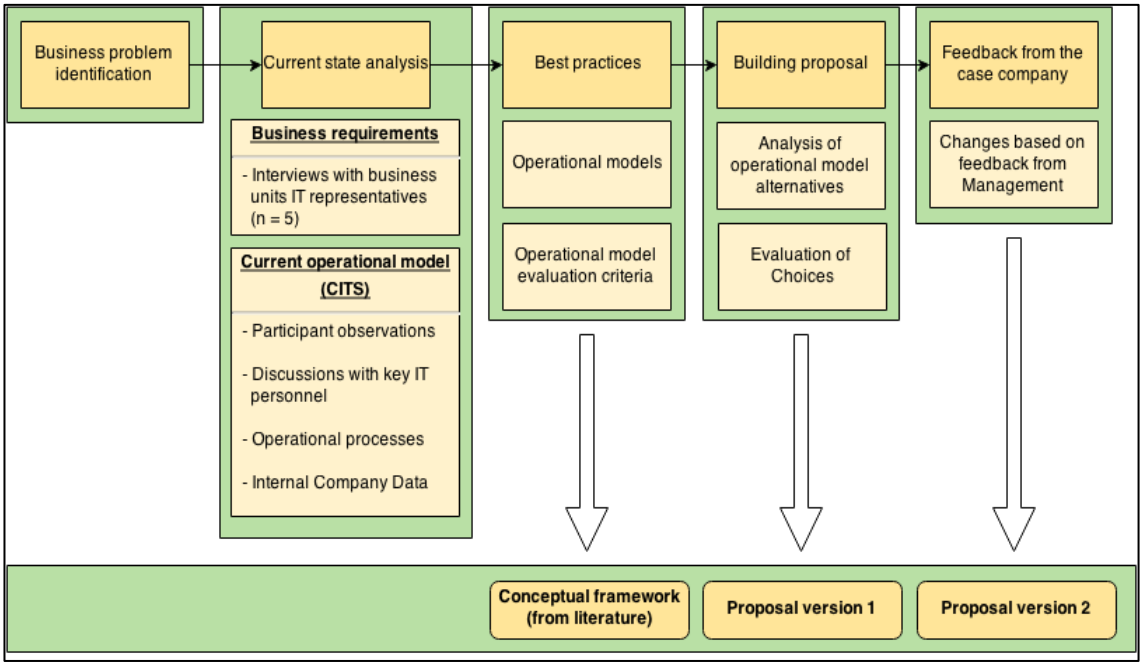

Figure 1. Research design in this study.

As seen from Figure 1, the research design starts with the identification of the business problem. In Step 2, the current state analysis focuses on the analysis of business requirements and the examination of the current operational model in the case company. Step 3 focuses on the search for best practice from the literature sources and covers the most important topics required for building the conceptual framework. In this step, the cloud computing is introduced, possible cloud deployment models are reviewed, and the key elements of these operational models are discussed. Section 3 ends with the formulation of the conceptual framework which is then applied for building the proposal. In Step 4, the operational model proposal is built, with the focus placed on the analysis of the case company data with the help of conceptual framework. As an outcome from this stage, a first version of the operating model proposal is drafted. In Step 5, the feedback from the management of the case company is collected. Changes to the initial version of the operational model from the feedback lead to the final operational model proposal.

2.3 Data Collection and Data Analysis Methods

In order to propose a new cloud service based operational model, this study collected the data in the following manner. First, the internal business requirements for cloud services were scrutinized. It was done by examining the existing (secondary) data collected in the case company. Second, the current operational model was investigated, first, by examining the case company documentation and, second, by conducting a

series of interviews and discussions in the case company. This data collection was focused on gaining knowledge on how IT organization operates currently and identifying the company requirements and expectations for the new operational model. After the initial model was drafted, the model was discussed in the interviews with two key stakeholders (Head of IT infrastructure Management and Infrastructure Development Architect) for getting feedback and building the final version of the new operational model. The data collection for the study is described in more detail below.

a) Secondary data

For collecting the business requirements for the new cloud services, the case company conducted five interviews with IT representatives of the internal business units. A total of forty two questions, grouped by ten categories were asked regarding the needs for the new cloud services. The interviews were held in the case company in the autumn 2013. The detailed analysis of this data by the researcher himself became a starting point for building the new operational model in this study.

Additionally, the case company conducted the internal study on the potential IaaS providers. It was done to analyse suitable offers on the market from the cost perspective to meet the case company business requirements. The best suitable cloud services providers (two public and two private) were reviewed. The researcher of the thesis participated in this analysis. The knowledge from this analysis affected the thesis's theory choices.

b) Case company documentation

For examining the current operational model, the researcher scrutinized the company documentation regarding the key elements of the operational model. These elements included: the Organisational Structure, IT Governance, Sourcing, Operational Processes, CMDB in the case company and Risk Analysis. Table 1 overviews the case company documentation used in the study.

Table 1. Case company documentation analysed in the study.

	Name of the document	**Amount**	**Description**
A	Case company's IT Governance Handbook.doc	22 pages	IT Governance, Operational Processes, Sourcing
B	ARIS – Tool	13 diagrams	Diagrams for Operational Processes

C	Organizational Structure		Company's web pages
D	Specific information security requirements for cloud services.doc	5 pages	Security requirements for cloud provider
E	Group Information security manual.doc	25 pages	Information security principles, Information security classification
F	New Server and Software Order.doc	2 pages	Process description
G	New Server and Software Order Diagram	1 diagram	Process diagram

c) Interviews and Discussions

The data includes a series of interviews and discussions conducted in the case company. It included interviews and discussions with Head of IT infrastructure Management and Infrastructure Development Architect. The CMDB related questions were discussed in the talk with a CMDB responsible person. The security regulations in the case company regarding to the management of the IT assets were discussed with Corporate IT Security Officer and Corporate IT Security Architect. Details of the interviews and discussion are shown in Table 2 below.

Table 2. Interviews and Discussions with the key personnel in this study.

Person	**Position**	**Topics**	**Dates**
A	Head of IT Infrastructure Management	- Setting up the goals for project - Comments about ongoing thesis project - CITS Infrastructure Team in IT Governance	- Jan 2013 - 18.02.2014 - 20.03.2014
B	Infrastructure Development Architect	- Evaluation of Cloud IaaS providers - How IT Infrastructure operates in the case company - CMDB in the case company	- 10.12.2013 - Jan 2014 - Feb 2014
C	CMDB responsible person	- How does CMDB configured in the case company	- Feb 2014
D	Corporate IT Security Officer and Corporate IT Security Architect	- Security practices in the company - Security practices with cloud services	- 8.04.2014

d) Benchmark

One case company benchmark was used in this study. The data for it was collected from an interview with the manager responsible for provisioning IT infrastructure for the case company business units. In that interview, the sub-process for delivering physical or virtual servers to the business customers was discussed as a benchmark for the IT Infrastructure Team. Details of the interview are shown in Table 3 below.

Table 3. Benchmark of the sub-process for delivering physical or virtual servers.

Person	Position	Topics	Duration	Date
A	Manager for IT Infrastructure provision	Server and Software Order process in IT Infrastructure Team	1.5 hours	20.01.2014

e) Feedback for building the final proposal for the operational model

For the development of the final proposal, the interviews with Head of IT infrastructure Management and Infrastructure Development Architect were organized. Their feedback was collected, analysed and used for building the final operational model. Details of the discussion are shown in Table 4 below.

Table 4. Feedback interviews for building the final proposal for the operational model.

Person	Position	Date
A	Head of IT Infrastructure Management	27.09.2014
B	Infrastructure Development Architect	27.09.2014

2.4 Validity and Reliability Plan

The validity and reliability are the two main concepts of the qualitative academic research. In qualitative research, validity relates to the produced outcome of the study which should address the research question initially defined. (Quinton and Smallbone 2006: 127) Validity also means that collected data should be accurate, and an interpretation of the data has to take into account various perspectives of the stakeholders participated in project. To provide a valid outcome, a researcher also needs to consider alternative explanations exisiting in the literature and given by relevant stakeholders in order to avoid the researcher bias. (Maxwell 1996: 109)

Reliability of the study relates to the results of the research which, for the reliable outcome, would be the same if another person conducted a research or if a research was done at a different point in time. (LeCompte and Goetz 1982: 32) Additionally, reliability of the thesis can be improved by using different data sources, different data collection methods and well documented research procedures. The collected data and literature analysis in this study will follow these validity and reliability requirements.

From the validity point of view, multiple discussions with the relevant company's personnel need to be organized in order to obtain the information about the company's and operations and practices. The business requirements for cloud services need to be collected internally with the help of an extensive study. An analysis of the current operational model need to be rooted in company documentation, as well as face-to-face interviews and discussions with all the parties involved. Additionally, a feedback from the key stakeholders needs to be taken for the reliable evaluation of the initial operational model proposal.

From the reliability point of view, the primary data needs to be collected from at least three sources, to meet the triangulation requirement of data collection methods (Dan et al. 2002: 4). There sources may include, for example, company documentation, interviews and discussions with the relevant stakeholders, benchmarking, and possible other data collection methods. In the study of the present type, in order to produce both, a reliable and valid outcome, a thorough analysis needs to be done also to ground the proposed model in the theoretical and best practice findings. The fulfilment of these requirements will give a good foundation for the proposed model.

The following section describes the results of the current state analysis of the case company; it was done with a special emphasis to meet the validity and reliability requirements discussed above.

3 Current State Analysis of Case Company IT Infrastructure

This section discusses the results of the business requirements analysis for the new cloud services in the case company. After that, it reviews the current operational model of the case company IT organization.

3.1 Business Requirements Analysis

In order to understand the needs for the new cloud services in the case company, business requirements were collected internally, from the five main business units of the case company (Section 2.3, Secondary data). The analysis of that data demonstrates different operations and different requirements for the cloud services proposed by the units. Yet five categories can be identified as key shared business requirements common for all business units. These business requirements include: Cost Efficiency, Agility, Functional requirements, Reliability and Security, and they are summarized below. The full analysis of business requirements is provided in Appendix 2.

Cost Efficiency

First, the results point that, currently, the customers are not satisfied with the existing price model for IT infrastructure services. The current price model is based on monthly fees charged to the business units for the virtual servers available to them from the case company's IT infrastructure team. The business units would like to have an hourly based fee charging for the usage of the virtual servers, and they believe that the current price model is not flexible enough to provide for it. They motivate it by the fact that often the customers are using virtual servers during the office hours only. The provision and de-provision of the virtual servers frequently enough creates a possibility for the customers to pay less for the allocated capacity. At the same time, it increases the efficiency of the used IT resources in the case company. Thus, cost efficiency makes one of the key business requirements cited by most internal customers.

Agility

Second, the results from the interviews indicate that capacity management is lagging behind in service delivery time. Currently capacity management is too slow, and the provision of personal access rights is also taking too much time. A faster service for capacity management and access rights is highlighted as the most important requirement by most of internal customers. They stress that servers with customized configurations need to be available in less than a week; while the most typical standard servers should be available in minutes. The customers are only ready to wait longer in the

special cases, where a customized configuration is needed; for these cases, manual provisioning by the IT service provider is an acceptable option. The customers also desired that the end users should have a possibility for self-service through the IT portal or CMDB interface which could reduce the time for IT infrastructure service delivery.

Functional requirements

Third, the widest group of the requirements for the new cloud services is made of functional requirements. These requirements can be divided into the three categories: *Requirements for the Cloud Provider*, *Integration Requirements* and *Management Requirements*.

In *Requirements for the Cloud Provider*, the following two issues were highlighted. First, the applications might have various technical needs such as high or low CPU, different memory sizes and a variety of storage capacity. Thus, the offerings by the cloud service provider should correspond to these needs related to the applications. Second, the auto scaling feature for cloud services should be available for the end users from the cloud service provider.

Integration Requirements focus on the integrations between the on-premises infrastructure and the cloud service provider. In the case company, most of the IT applications require integrations to the on-premises infrastructure due to a small number of isolated standalone applications. Nevertheless, the opinions of the business units were divided on this point. Two business units require all possible integrations with the cloud service provider, while the other three business units are satisfied with only some specifically supported protocols. One business unit also wishes to have a feature that would allow moving virtual servers between on-premises and the cloud provider data center.

Additionally, all the business units wish that the internal company's user credentials were used for working with the cloud services according to the company's current access management process. This will require integration of the cloud services with the case company's authentication servers. It will also require that all the provisioned IT resources located in the cloud environment would need to be visible in the company's configuration management database (CMDB). Therefore, the integration between CMDB and the cloud environment is required, which makes CMDB an important part of the cloud services.

Management Requirements describe how cloud services need to be managed in order to provide quality services to the business units. Business units have expectations for

Corporate IT Services (CITS) to manage the cloud infrastructure services in the same manner as IT Infrastructure team is currently doing for the existing traditional IT infrastructure services. One business unit suggested limiting the role of CITS to as small as possible for cloud service management. It was also required by the business units that the operational tools for the cloud service management should be available to the case company for management of the cloud-based IT assets. Operational tools should support the cloud infrastructure automation capabilities for easy deployment of the servers and applications, as well as the capabilities for configuration, orchestration and reporting of the cloud IT infrastructure. Additionally, operational tools should provide forecast for invoicing. Finally, all interviewees requested the maximum visibility for the new cloud services including resource monitoring information.

Reliability

In the context of the cloud services, reliability means the availability and accessibility of the IT services located in the cloud to the end user according to a Service Level Agreement (SLA). The main factors that affect the reliability of the provided cloud services were suggested by the experts, namely by the case company's IT infrastructure team. They include *the network connectivity*, *location of the cloud provider*, and *the performance of the cloud provider*.

Concerning *the network connectivity*, cloud providers currently offer two types of the network connections: the direct connection provided through dedicated network cables and the indirect one, through the internet. The direct connection is called MPLS and has higher reliability and security compared to the indirect Internet connection. Some cloud providers do not allow direct network connectivity due to security issues, while others make it possible through the partners' networks. Among the five business units, two customers demand the direct connectivity to the cloud provider, while the others are satisfied with the indirect connectivity option. The two customers asking for direct connectivity motivate it by stressing that quite often the applications require high data transfer capabilities which is impossible to get with the network connectivity through the Internet; in that particular case the MPLS connection is preferable.

As for *the location* of the cloud service provider, most of the business units agree that the preferable locations of the cloud providers are Finland or European Union (EU) countries. They motivate it by the fact that most of the business units located in Scandinavia or EU countries, except one business unit located in Russia.

Finally, regarding *the performance of the cloud provider*, the respondents stressed such characteristics of cloud service provider as network latency and maintenance windows, which should be taken into account while selecting the provider. Additionally, some business customers require highly reliable data storage from the cloud providers. These customers emphasize the importance of fully redundant round-the-clock data availability and a possibility to replicate data between at least two data centers.

Security

All five business units stressed that the security aspects when outsourcing services outside of the company need to be ensured according to the company's standards and policies. All insisted that the company's data security and compliance should be followed. If some sensitive data need to be used in the cloud services, the cloud provider should be a resident of the same country as the business unit. Finally, for the security reasons, the end users should have limited permissions for making customizations to the configurations of the provisioned servers in the cloud environment.

Summing up, the business requirements for the cloud services need to be prioritized and categorized, since fulfilling all the five business units' requirements, in an equally complete manner, will obviously be challenging, if possible at all. Therefore, this analysis categorized the existing business requirements into the *primary*, aimed at supporting business agility and cost efficiency, and the *secondary*, related to the functional, security and reliability requirements. The identification and prioritization of business requirements is needed as a basis for the holistic and grounded selection of the new cloud services model which is done in Section 3.3.

3.2 Analysis of the Current Operational Model

The operational model can be defined as a construct describing how an organization operates in order to meet its business objectives. At the same time, the operational model shows how the organization's strategy translates into a day-to-day delivery of services to its customers. Thus, the operational model can be considered as a very general definition which can be applied to any organization. In this study, the IT operational model term is applied to the analysis of how the case company's organization provides its IT services.

Generally speaking, an IT operational model can be considered as a construct breaking the organization and its activities into components that include some general operating modules of the organization such as the organization's structure, its operational

processes, its governance, sourcing and some other possible elements. Defining the operational model helps to understand how the organization operates and how it can be improved.

The sub-sections below discuss the elements of the company's current IT operating model including such elements as its organizational structure, IT governance, Sourcing, IT processes, Configuration Management Database and Risk Management. These elements were identified based on the results of data collection and the consultations with the key stakeholders from the case company. Later on, this approach was also strengthened the similar views on IT operating models evident in the literature. The five elements of the IT operating model are discussed below.

3.2.1 Organizational Structure

Presently, the organizational structure of the Corporate IT organization in the case company combines an arrangement of authority lines, rights and responsibilities of different teams within the organization. The organizational structure also determines how information flows between the teams and corresponds to the strategy and objectives of the organization. In the case company, as in any other companies with centralized organizational structure, the decision making power concentrates on the top management layer and decisions flow from the top to the bottom of the organization.

The company's IT activities are spread between Corporate IT and the IT departments of the business units. As it was mentioned earlier, the company has five business units. Corporate IT is responsible for common IT operations within the five business units. Figure 2 below shows the overview of the Corporate IT organization.

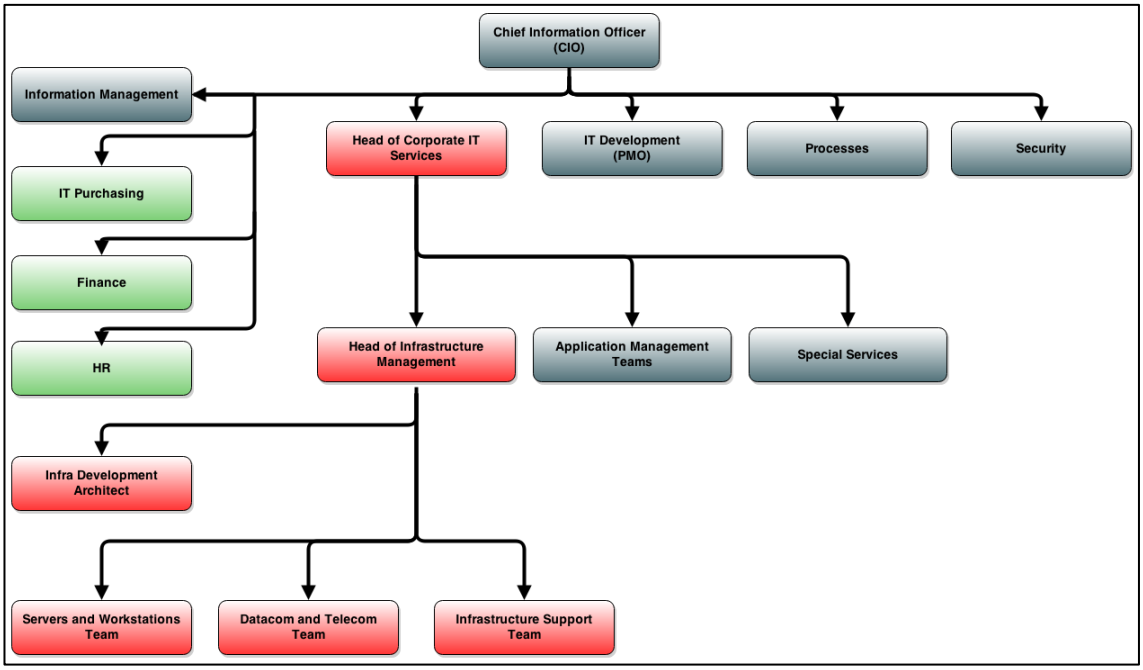

Figure 2. Corporate IT organization in the case company (Table 1 C).

As seen from Figure 2, the current company's Corporate IT organization has a highly centralized structure where the decisions flow downwards from the top. The red color marks the layers which will be affected by the cloud services and which are included in the focus of this study. In Figure 2, at the highest layer of this organizational structure, Chief Information Officer (CIO) is located. He has the highest responsibility and authority for the management of IT operations across the company. CIO is responsible for developing the information technology (IT) vision for the company and he leads the development of an IT governance framework which defines the working relations and sharing of IT assets among different IT teams within the corporation. In addition, CIO oversees the key IT operations within the company such as the development of corporate standards, technology architecture, technology evaluation, aligning IT with the business, and supervises financial aspects for IT. CIO reports to Senior Vice President, Corporate HR. CIO Office supports CIO and leads, guides and drives the development of IT processes, architecture, security, sourcing, IT development projects and BPM. CIO Office is also responsible for the company's wide IT&BPM governance, strategy development and implementation.

On the lower levels, the Corporate IT organization has Head of Corporate IT Services who is reporting to the company's CIO and leads the IT Infrastructure, Application Management and Special Services teams. The subordinate of Head of Corporate IT Services is Head of Infrastructure Management who leads the Servers and Workstations Team, Datacom and Telecom Team, and Infrastructure Support Team. Anoth-

er subordinate of Head of Infrastructure Management is Infra Development Architect who involved in all projects within Infrastructure department.

Inside the Corporate IT Services Infrastructure organization, there are three teams which will be affected by the cloud services most of all. These teams are Servers and Workstations Team, Datacom and Telecom Team, and Infrastructure Support Team. They all make parts of the Corporate IT Services Infrastructure organization. Figure 3 shows the three teams in the Corporate IT Services Infrastructure organization.

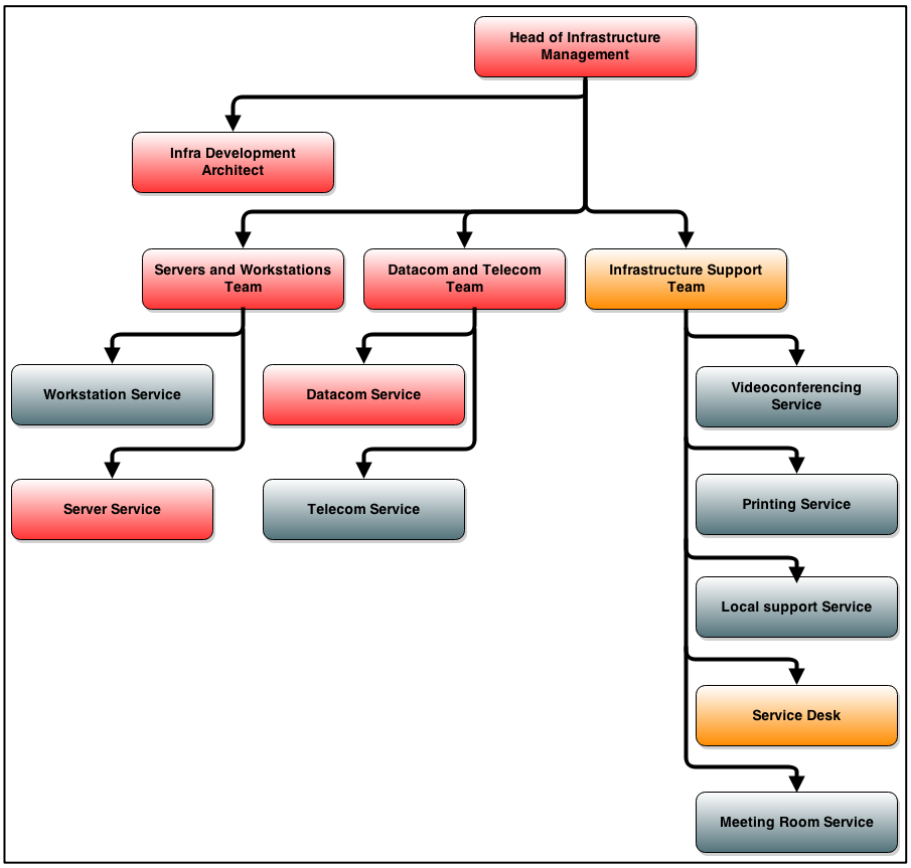

Figure 3. Corporate IT Services Infrastructure organization (Table 1 C).

As seen from Figure 3, Head of Infrastructure Management leads the Servers and Workstations, Datacom and Telecom, and Infrastructure Support Teams. Infra Development Architect works with these three teams on the different projects and reports to the Head of Infrastructure Management. The Server Service and Datacom Service teams are marked by the red colour. They will be affected by the cloud services in relation to capacity management activities. Server Service ensures that physical or virtual servers, data rooms, storage and workstations support the company's daily operations. Datacom Service provides local and external connectivity for the users via phones and networks at the office and outside. Additionally, Figure 3 shows two teams marked or-

ange. These are Service desk and Infrastructure support team which will also be affected by the cloud services. However, since it was agreed with the case company that these team lie outside the scope of this study, they are marked by the orange colour to show this exception.

Summing up, in the current organization the structure is based mainly on technical silos, which may not be fully suited to manage agile and rapidly provisioned cloud services due to many boundaries and responsibility layers between them. For a cloud scenario, instead of multiple technical silos, the organization may consider a single focal point for a collective cloud infrastructure expertise, which would reduce the amount of resources as well as the number of interactions for making the cloud specific decisions. Such a structure would speed up the decision making in the organization and enable a faster response to the business needs (Table 2 B). This observation related to the structure of the Corporate IT Services Infrastructure organization is discussed in more detail in the proposal in Section 5.

3.2.2 IT Governance

In the case company, IT Governance embraces the processes that ensure the efficient use of IT resources in order to accomplish the company's goals. IT Governance also demonstrates how well the organization aligns its IT and business strategies together. Generally speaking, IT Governance makes sure that interests of all participants taken into account, applied processes provide a good way to measure IT performance, IT resources properly allocated, and risks are mitigated.

Currently, the case company's Corporate IT Governance helps and supports the company IT processes and services, drives and guides the IT users in moving towards a more unified way of working. It also defines how the aspects of IT work fit together, defines where and by whom decisions are made, and supports the employees working in the company business units in their understanding of how the company's IT operates. Figure 4 below shows the IT Governance of the case company.

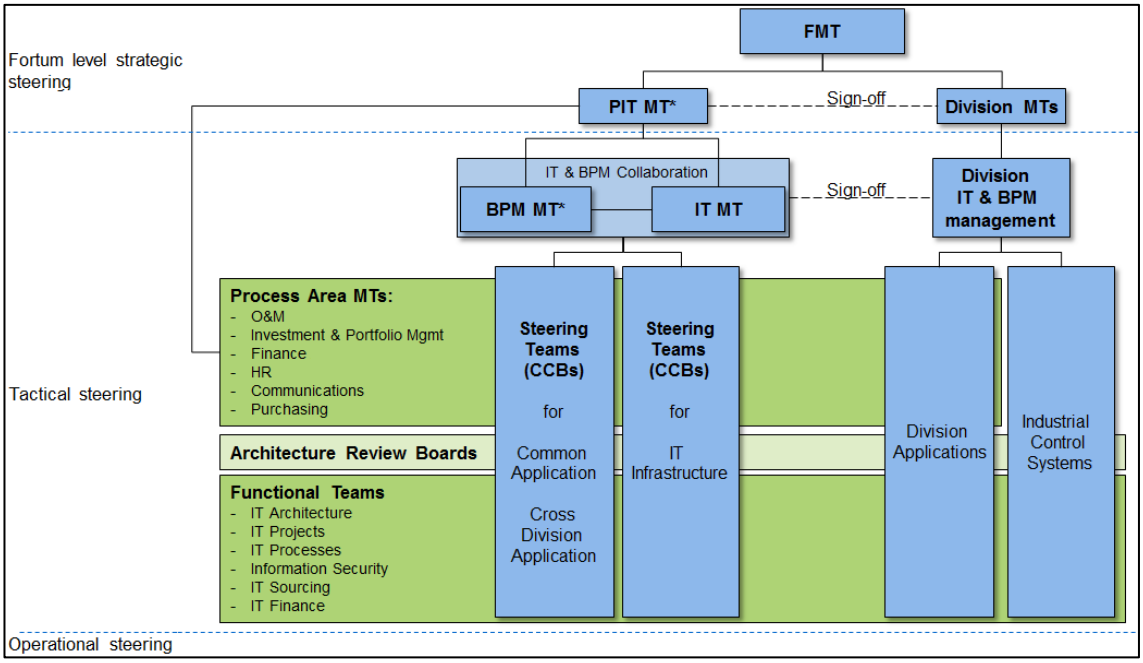

Figure 4. Corporate IT Governance in the case company (Table 1 A).

In Figure 4, IT Governance is illustrated as a system of collaboration between IT and the business units (divisions). IT Governance is divided by the three horizontal levels namely Strategic Steering Level, Tactical Steering Level and Operational Steering Level. The participants in that system are shown in different boxes in Figure 4.

On the first level of IT Governance, the strategic steering groups are located such as Top Management Team (TMT), Process and IT Management Team (PIT MT) and Division Management Teams (Division MTs).

At the strategic steering level, Top Management Team (FMT) is the highest IT decision making body in the case company. The key IT investments and principal decisions are made by the FMT. FMT sets the strategic direction to the company's IT and ensures that the case company's IT users have adequate information about the business goals and high level requirements. FMT approves the corporate level IT action plan and budget. The highest level Business Process Management and IT alignment are taken care by FMT.

On the same strategic steering level with FMT, Process and IT Management Team (PIT MT) is located. PIT MT is responsible for the case company's level strategic steering of IT&BPM. PIT MT ensures that the process and IT development leads towards the agreed targets. Division MTs perform similar functions for their divisions.

On the second level of IT Governance, tactical steering groups are located such as IT Management Team (ITMT), Business Process Management Team (BPM MT), Division IT and Business process management (BPM) Team, Process Area Management Teams, Functional teams, Architecture review boards, different Customer Co-operation boards (CCB) for various IT services and Infrastructure related activities. These divisions have their own internal management teams for handling the division's specific applications and industrial control systems.

On the tactical steering level, IT Management Team (ITMT) makes sure that the IT goals and the focus areas are defined in accordance with the business needs. It focuses on the strategic and tactical issues and leads the case company IT operations and development. The other main activities of ITMT include the approval of IT Governance, IT projects guidelines, IT architecture guidelines and IT sourcing guidelines for IT community, as well as CITS service catalogue and CITS pricing model. ITMT guides, follows and decides on major Functional Teams issues and proposals. Business Process Management Team (BPM MT) leads the development of BPM methods and tools and searches the company level synergies in business processes. The divisions have their own IT and BPM management teams which work in cooperation with Corporate IT Management and take care of the division's areas of the responsibility.

On the tactical steering level, Customer Co-operation Boards (CCBs) are formed in the areas which concern multiple Divisions or Functions. CCBs main work is to evaluate the requirements for IT in their responsibility area and initiate projects to plan, develop, test and implement IT services in order to fulfil the requirements for IT. CCBs approve of Project Charters and nominate Project Owners for planning, building, testing, and implementing new IT services in their responsibility area. CCBs also make decisions regarding the lifecycle of IT service after it has been taken into use. Typically, CCB approves the budget, content, time schedule, service level agreements, access rights principles, etc. CCBs can also nominate Change Advisory Team(s) (CAT(s)) for assistance in some projects. Different groups or a single person can act as CCB. Typically, one CCB handles multiple IT services.

Further on the same level, *Process Area Management Teams* support Corporate IT Services and Division's IT Services in general processes such as Operations and Maintenance, Investment and Portfolio Management, Finance, HR, Communications, Purchasing. *Corporate and Divisions* nominate Architecture Review Boards (ARBs) for

corporate and division level reviews and approvals. ARBs review such aspects of the proposed IT solutions as Process, Information and System.

Further on, *Functional Teams* oversee the common way of working of the case company's IT users. They ensure that the agreed practices are developed and taken into use. To achieve this purpose, CIO Office is coordinating and managing Functional Teams which are currently made of six teams: IT Processes, IT Architecture, IT Projects, IT Sourcing, Info Security and IT Finance. Main tasks of the Function Teams include planning, leading and managing various activities and projects in those fields.

Finally, IT Infrastructure Team, which makes the focus of this study, is presented in three different locations in the IT Governance diagram: first, in the IT Management (ITMT); second, in Steering Teams (CCBs) for IT Infrastructure, and third, in Architecture review boards. Head of Corporate IT Services participates in and reports to IT Management Team (1). ITMT makes decisions and approves of the cloud deployment, cloud pricing model and cloud service catalogue. Customer Co-operation Board (CCB) for IT Infrastructure (2) includes Head of CITS, Head of Infrastructure Team, Leaders of the sub-teams, Infrastructure Development Architect, and Division's IT representatives. Finally, IT infrastructure is involved in Architecture review boards (3) to support business units where the Infrastructure Development Architect participates (Table 2 A).

Summing up, in case the new cloud services are handled within the level of CCB (2) for IT Infrastructure, no changes will be necessary to the current IT Governance. In case the new cloud services become the responsibility of each division apart or a new CCB, some changes are required to the current IT Governance. These changes are discussed later in the proposal for the company IT Operational model in Section 5.

3.2.3 Sourcing

IT Sourcing makes part of the company's strategy focusing on how to deliver IT services to the business customers. IT services can be delivered by internal or external competences in alignment with business goals. Thus, the main target of the IT Sourcing is to select suitable internal or external human resources for the provision of IT services.

Presently, in order to provide services and create value for business customers, Corporate IT organization manages a wide range of vendors and service providers. In most of the cases, CITS acts as a middleman in the service delivery chain. Figure 5 illustrates how IT sourcing is presently organized.

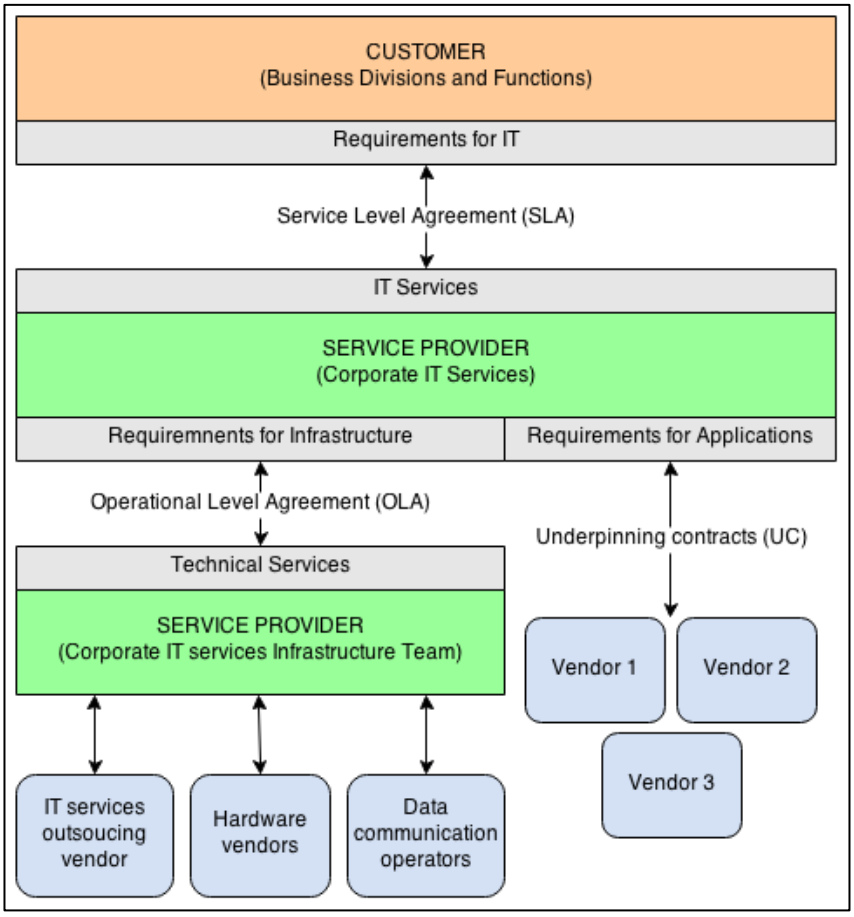

Figure 5. IT Sourcing in the case company (Table 1 A).

As Figure 5 shows, *Business Divisions and Functions*, marked orange, is the only customer for Corporate IT Services. They define requirements for IT Services that need to be delivered by CITS. All provided services are based on Service Level Agreements (SLAs) signed between CITS and its customers. SLA makes an essential part of service contract where the service is formally defined. In Corporate IT Services, SLAs determine the defined levels of service quality. Customer and CITS together decide which level of service quality should be used for each IT service. According to the customer requirements for particular IT services, CITS makes an Operational Level Agreement (OLA) with CITS Infrastructure Team. Operational Level Agreements are usually signed between IT Service Provider and another part of the same organization in order to provide service delivery to the customers. OLA defines the responsibilities of both sides of the agreement for provided services.

Correspondingly, Service Level Agreements between CITS and internal business customers match the agreement between the CITS Infrastructure Team and IT services outsourcing vendor. In IT services outsourcing, a vendor does all the technical work related to installation and maintenance of the hardware and software for the case com-

pany. It is a strategic partner for the case company in provisioning IT services to the end-users. The selection of the IT services outsourcing vendor is done through a tender once in a few years. The selected hardware vendors provide and support the requested hardware. Application vendors provide customer support for their products during their lifecycle through various communication channels. Data communication operators provide networking capabilities for the case company in various locations worldwide.

As shown in Figure 5, Corporate IT Services also have Underpinning Contracts (UC) with applications vendors. UC is a contract between an IT Service Provider and a third party in provisioning goods or services to the customers. It defines the targets and responsibilities of the service provider that are reflected in Service Level Agreements.

Summing up, the current sourcing structure does not include any cloud vendors or cloud maintenance provider in the service delivery chain. It means that for the cloud services, the way of decision making for sourcing is yet to be defined. There are two possible decision-making scenarios for sourcing: Business Divisions could directly make a deal with the cloud service provider, or CITS Infrastructure Team would sign the deal with the cloud service provider and acts as a cloud broker. Thus, it is also important to emphasize the role of the cloud maintenance provider. From the current sourcing perspective, the IT services outsourcing vendor which provides services for legacy infrastructure might also take up the cloud services maintenance responsibilities. Alternatively, another cloud maintenance vendor might be selected to add competition to the current IT services outsourcing vendor in maintenance services. These possibilities are further discussed in Section 5 when building a proposal for the case company.

3.2.4 Operational Processes

The case company's IT operational processes follow IT Service Management (ITSM) best practice and based on the IT Infrastructure Library (ITIL) framework. ITSM is a process-based practice that focuses on the delivery of IT services to the customers in a customer oriented manner (ITIL Glossary 2011). ITIL represents a practical framework for the design of ITSM processes based on the existing best practice. ITIL is used for identifying, planning, delivering and supporting IT services to the business customers (What is ITIL 2014). Figure 6 below illustrates the ITSM processes of the case company.

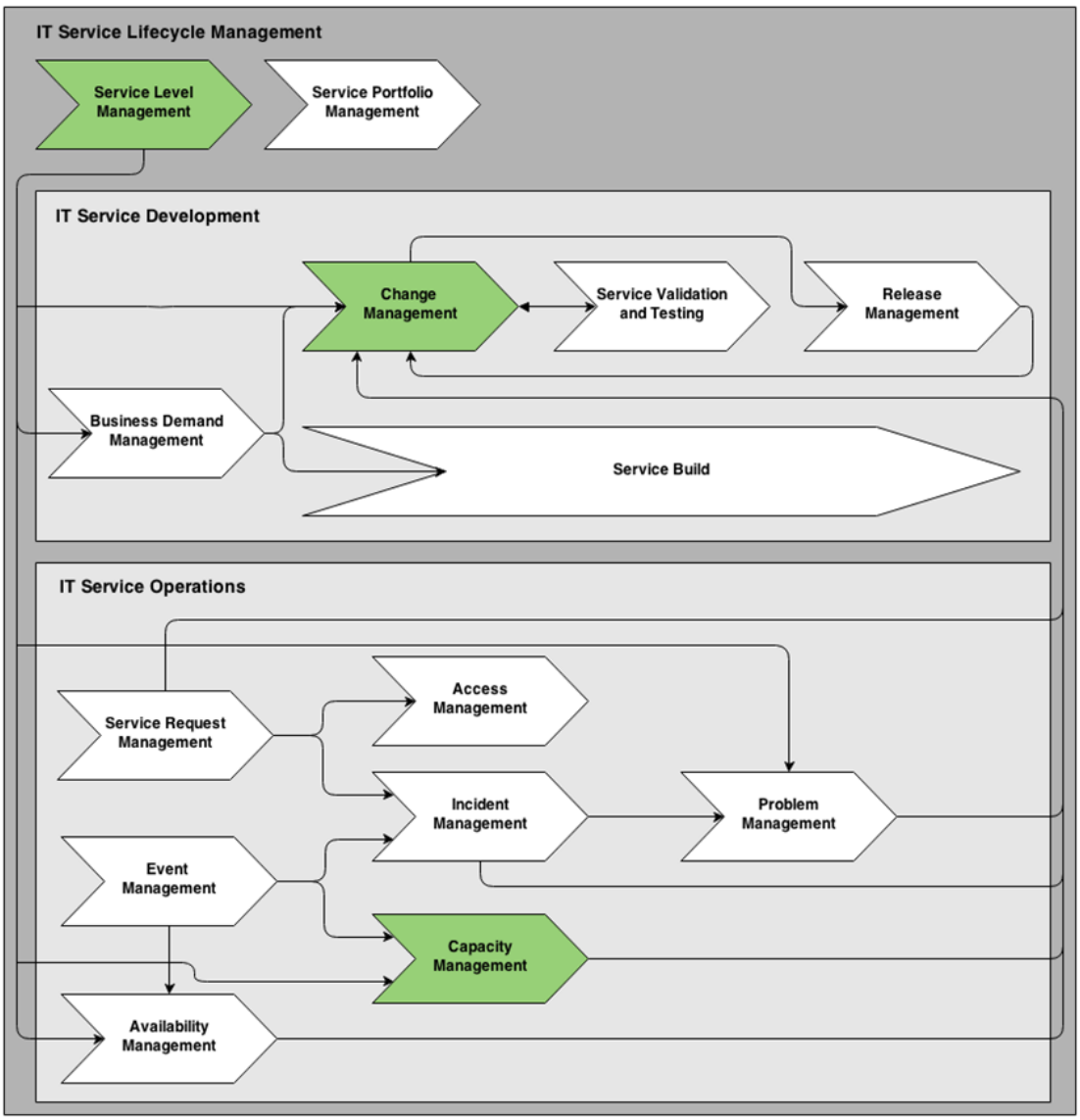

Figure 6. ITSM processes in the case company (Table 1 B).

As seen from Figure 6, the processes are illustrated as boxes connected to each other representing an ITSM framework in the case company. These processes are also divided into three main categories, namely IT Service Lifecycle Management, IT Service Development and IT Service Operations which are discussed below.

First, *Service Lifecycle Management* currently has two processes, Service Level Management and Service Portfolio Management. Service Level Management includes the activities which are required for managing relationships between the business stakeholders and the IT service provider after a new IT service is taken into use. Through Service Level Management the business requirements and IT service capabilities are kept aligned as agreed between the business stakeholders and the IT service provider. An objective of Service Level Management is to negotiate Service Level Agreements

between the IT provider and the customers. (ITIL Glossary 2011) IT services designed in consonance with the agreed service level targets in SLA. Service Level Management is also responsible for Operational Level Agreements (OLA) and Underpinning Contracts (UC) and their relevance.

In Figure 6, Service Level Management is marked by the green color. It indicates that this process will be affected by the cloud services in the case company (Table 2 A). This process is connected to Change Management, Business Demand Management, Capacity Management, Availability Management and Problem Management. After the new IT service is released to production, the measurement of performance indicators need to be done and compared with the existing Service Level Agreement for that IT service. If the measurement results do not correspond to SLA, some corrective action for IT Service is needed. There are two types of corrective actions: one where SLA change is needed and the other one where IT service needs to be changed. For the IT service change, the corrective action involves Change Management process, which does not include the root cause analysis. If the root cause analysis is required, the Problem Management process is used instead. Further on, if any new business requirements appear for IT service, the Business Demand Management process gets involved. If a forecast usage of IT Service indicates the possible effects on capacity or availability, Capacity Management and Availability Management processes are used (Table 1 B, Service Level Management Process diagram).

Currently in the case company, Service Level Agreement between Corporate IT Services and business customers needs to be changed to support the new cloud-based capabilities and levels of service quality. A contract with the cloud provider would correspond to that change in the Service Level Agreement. However, the measurement of the key performance indicators (KPIs) for comparison against SLA in cloud environment might be challenging, since it depends on the factors such as network latency and cloud environment performance. Additionally, a forecast of the IT service capacity and availability needs to take into account the cloud specific capabilities. There are might be limitations in extra capacity allocation and high availability might not be possible for the cloud-based SLA. These possibilities are further discussed in Section 5 when building a proposal for the case company.

As for Service Portfolio Management, it also belongs to Service Lifecycle Management category. Service Portfolio Management includes the activities required for identification and management of dependencies between individual IT Services throughout their

lifecycle. Service Portfolio Management ensures that the IT provider has the right portfolio of services to fulfill the customer's business requirements.

Secondly, the other block of the ITSM processes in Figure 6 is related to *IT Service Development*. There are five processes listed here in Figure 6, such as Business Demand Management, Change Management, Service Build, Service Validation and Testing, and Release Management.

Business Demand Management deals with the requirements for changing the current IT Services or developing some new IT Services.

Change Management is one of the most important processes in ITSM. It fulfils requirements for changing the current IT services or developing new IT Services. Solutions are managed as Changes. Service Level Management is marked by the green color in Figure 6. It indicates that this process will be affected by the cloud services in the case company. (Table 2 A) If a Change needs to be tested after implementation, the Service Validation and Testing process is involved. After Change is approved for release and is ready to be released, the Release Management is used. (Table 1 B, Change Management Process diagram)

In the current Change Management process, a Change Manager evaluates and estimates a Change. Change Manager assigns the Change to a System Developer, and System Developer implements the Change. (Table 1 B, Change Management Process diagram) In the cloud scenario, cloud awareness and skills would be required for these roles if the cloud environment is selected for Change implementation. Sometimes a Change does not need implementation, but rather needs the services of Infrastructure provider only. In that case, a request to the Infrastructure service provider is created and handled. Additionally, in the cloud scenario, the current Change Management Process in the case company does not take into account any self-service capabilities of the cloud infrastructure provisioning. Finally, in the cloud scenario at least two parties are involved in the provision of IT infrastructure, the cloud provider and the cloud maintenance provider. Thus, the current process would need structural changes based on that. These changes are discussed in Section 5 when building a proposal for the case company.

Further on along the IT Service development, Service Validation and Testing include all activities required to test that Change has been built as planned. Service Validation and Testing verify the Changes from Change Management during the lifecycle of the IT

service. Release Management includes the activities required to protect the production environment availability and performance when implementing the approved Changes. When a Change is ready for releasing, Release Management receives a Change from Change Management. The last process in IT Service Development block is Service Build. This process corresponds to Project Management for IT Service implementation. It includes the activities which are required to initiate, plan, execute, control and close the project for IT Service.

Thirdly, the final block in Figure 6 relates to *IT Service Operations*. This block contains seven processes are listed such as Event Management, Capacity Management, Availability Management, Service Request Management, Access Management, Incident Management and Problem Management.

Event Management detect and manages the events that occur from the Configuration Items (CI) related to the delivery of IT Service. A Configuration Item can be described as a record to configuration database about an IT asset or a combination of IT assets (ITIL Glossary 2011). CIs are typically configured to create events when availability or the performance of IT Service might be in jeopardy. If the identified event is an incident, the process moves to Incident Management. If the identified event is not an incident and can affect capacity or availability of IT Service, the process is directed toward Capacity Management or Availability Management.

Capacity Management includes activities for forecasting the usage of IT Service and ensuring that enough human and technological capacity is available for running the IT service in any given moment of time (ITIL glossary 2011). Capacity Request as an input for Capacity Management comes from Service Level Management or Event Management processes. In Capacity Management, a Capacity Request is configured as a Service Ticket. If the capacity related Change is required for that request, Change Management gets involved. After the capacity related Change is handled by the Change Management, the creator is notified and Service Ticket is closed. In the case company, the forecast usage of IT Service is done in Service Level Management. Capacity Management gets involved only if the forecast affects the capacity. (Table 1 B, Capacity Management Process diagram)

Capacity Management is marked by the green color in Figure 6. It indicates that this process will be affected by the cloud services in the case company. (Table 2 A) Currently, the existing Capacity Management process in the case company does not take cloud capabilities into account. In the current process, a Service Ticket has to be creat-

ed by the System Main User for System Manager. System Manager handles the capacity request and directs it to the Change Management (Table 1 B, Capacity Management Process diagram). In a typical cloud scenario, these steps can be avoided with the help of self-service IT infrastructure provision. In that case, Configuration Management Database should be updated automatically by the cloud solution. If the Capacity Request requires the custom configuration for the requested IT infrastructure resources, the current process suites the purpose. In the case if cloud service is involved, cloud awareness and related skills required for System Main User and System Manager. These changes to the Capacity Management are discussed in Section 5 when building a proposal for the case company.

Next, Availability Management includes activities for ensuring that IT service availability matches or exceeds the availability targets agreed in SLA. Availability process is organized in a similar way as the Capacity Management. Availability request comes from Service Level Management or Event Management. If changes to availability are needed, Change Management gets involved. After the availability related Change is handled by the Change Management, the creator is notified and Service Ticket for availability request is closed.

Next in Figure 6 is Service Request Management which is applied when the end-user asks for the IT service related help. Service Requests can be created by the users through two input channels such as a phone channel or a web based portal. Service Request can take a form of Incident Ticket for Incident Management or an Access Rights Ticket for Access Management. Additionally, Service Request might involve the Change Management if Change is required to fulfil the Service Request. The Service Desk belongs to Service Request Management and acts as the first line of support for Service Request from the end users.

Access Management is applied when end users request access to IT services. A Request for New User Identifier (ID) or Access Rights comes from Service Request Management. In some cases, the approvals of New User ID or Access Rights might involve several participants such as Manager, Access Manager or some another Approver.

Incident Management becomes relevant when IT Service is not working the way it was planned to work or it is severely degraded. An Incident is reported by the end-user with help of Service Request Management or can be detected by Event Management. If an Incident requires the root cause analysis, Problem Management gets involved. In case a Change is needed for an Incident, Change Management is used.

Finally, Problem Management is applied for the analysis of incidents and other information in order to reduce the number of the incidents and impact of incidents in the future. Problem Management gets involved when the root cause analysis of the Problem Ticket is needed by Incident Management or Service Level Management. When the root cause removal related Change is needed, Change Management is used.

Summing up, the current ITSM operational processes in the case company fulfil traditional IT service delivery, while lacks to support the cloud specific capabilities. The three current ITSM operational processes that fall in focus of this study, are Service Level Management, Change Management and Capacity Management. Some steps in these current processes might be avoided with the help of self-service cloud capability for the IT infrastructure provision. However, new cloud awareness and related skills will be required from the personnel involved in these ITSM processes. Finally, possible limitations in the cloud service delivery need to be taken into account.

3.2.5 CMDB in the Case Company

A Configuration Management Database (CMDB) is the information repository which holds the configuration data about the company's IT assets and the relationships between those assets (OGC 2000). IT assets might be described as the hardware or software components. Configuration data includes all possible records related to those assets. Examples of such records might be software licenses, invoicing data for customers, responsible persons, incidents or problems reported for IT asset, etc.

Presently, the case company has a very large number of IT assets and needs to keep track of them in an orderly manner. For that reason, the CMDB is actively used within the case company. After many years of implementation and use, the current CMDB is robust and reliable, but at the same time it is not dynamic enough for the cloud services. The information updates for IT assets in CMDB are mostly done manually. There is some limited automation exists which is used for automatic data collection about IT infrastructure resources over the network. In addition, the company's CMDB is interconnected with the current IT services outsourcing vendor's CMDB for synchronization. As a result, when an IT services outsourcing vendor updates some information related to IT assets within his own CMDB, this information automatically synchronized with the case company's CMDB. The established working practices and CMDB integration between the case company and IT services outsourcing provider makes difficult for the case company to change IT service outsourcing provider (Table 2 C).

Thus, the current version of CMDB does not support near real-time updates required for cloud scenarios. The case company's CMDB is very customized and based on the old version of the commercial CMDB product (Table 2 B). Due to that, there are no commercial solutions available for integration of the case company's CMDB with the cloud providers. Therefore, considerable changes and custom integrations will be needed in order to use the current CMDB with the cloud services. Alternatively, a new commercial CMDB product can be taken into use for the cloud scenarios. These needs will be discussed in Section 5 when building a proposal for the case company.

3.2.6 Risk Analysis

Risk analysis is an approach to identifying and assessing the aspects that may cause operational failures in provision of the IT services to the customers. From the risk analysis perspective, the case company currently operates in a low risk manner with IT assets. The case company has own Data Center which is located in Finland. All the IT hardware and software resources are located within that Data Center and belong to the case company. The Data Center is isolated from the outside with the help of physical and software firewalls. The network connection between the company's premises and the Data Center is also reliable and fast. The case company has established internal security rules and regulations for risk mitigation. Finally, integrations between the IT resources within the single Data Center are easy and do not bring any additional risks.

However, one of the challenges related to owing the Data Center is the fact that the maintenance of the own Data Center is extremely expensive. To manage the customer's capacity demands requires considerable capital investments into the IT Infrastructure such as purchases of the new servers and network equipment. Thus, Infrastructure as a service (IaaS) by cloud service providers creates an opportunity for the case company to lower the capital investments in IT Infrastructure. Such a change would require taking into use the cloud services from the public cloud providers or private (off-premises) cloud providers. But the utilization rate of the external cloud providers will depend on the amount of the applicable use cases. These challenges will be mentioned in Section 5.

3.3 Summary of the Current State Analysis

If summarized, the current Operational Model is used by Corporate IT Services Infrastructure Team to operate in the case company. The main activities of the IT infrastructure Team include provision of physical and virtual servers to the business units.

When the business requirements for the new cloud services are examined against the current Operational Model, this evaluation points to the challenges and benefits of the current operational model compared to the possible cloud-based IT operational model. If summarized, the results of *the business requirements* analysis can be combined into the five main topics: *cost efficiency*, *agility*, *functional requirements*, *reliability* and *security*. The key requirements are shown in Table 5 below.

Table 5. Summary of the Business Requirements.

Main topics	**Answers**
Cost Efficiency	- More flexible price model for provision of virtual servers - Hourly based charging - More frequent provision and de-provision of virtual servers will allow customers to pay less for capacity usage
Agility	- Faster capacity management in IT service delivery - Faster time for the provision of personal access rights - Faster service provisioning is demanded by the customers for o Standard servers provisioning (minutes) o Servers with customized configurations (<week) - A possibility for self-service through the IT portal or CMDB interface - Manual provision of servers with customized configurations is OK
Functional requirements	A. Requirements for Cloud Provider - The offerings by the cloud provider should have various technical options, such as high or low CPU, different memory sizes and variety of storage capacity - Auto scaling feature for cloud services
	B. Integration Requirements - Integration to on-premises infrastructure is required in most of the cases (approximately in 75% of the cases) o For all possible integrations o For some specific protocols - A possibility to move virtual servers between on-premises and the cloud provider data center - Internal company's user credentials used for working with cloud services according to the company's access management process o Integration of cloud services with the case company's authentication servers - Provisioned IT resources visible in the company's CMDB o Integration between CMDB and the cloud environment

	C. Management Requirements - Business units expect CITS to manage the cloud services o One business unit suggested to limit the role of CITS to as small as possible for cloud management - Operational tools for cloud management (automation, configuration, orchestration and reporting) - Operational tools providing better forecasts for invoicing - Full visibility for cloud services usage provided to the business units

Reliability	- Direct network (MPLS) connectivity (for two business units)
	  o Often the applications require high data transfer capabilities which is possible only with direct network (MPLS) connection
	  o Some cloud providers do not have that option
	- Alternative network connection through the Internet (acceptable for three business units)
	- Preferable locations of the cloud providers are Finland or EU countries
	- Network latency and maintenance windows taken into account when selecting the cloud service provider
	- Highly reliable data storage for some business customers
	  o With fully redundant round-the-clock data availability
	  o With data replication between at least two data centers

Security	- Security aspects when outsourcing services outside of the company according to the company's standards and policies - The company's data security and compliance need to be followed - If sensitive data is used in cloud services, cloud provider should be located in the same country as the business unit - Limited permissions for the end users to make customizations to the configurations of the provisioned servers in the cloud environment

The business requirements are identified and summarized in Table 5, will help to guide the search for the suitable operational model, as well as help to analyze the current IT operational model by pointing to its benefits and challenges. They also help to select and argue for the new IT Operational model for the cloud services.

As for the results of the current IT Operational model, they point to the following key five elements, namely: Organizational Structure, IT Governance, Sourcing, Operational Processes, CMDB and Risk Analysis. These key elements of the current IT Operational model are summarized in Table 6.

Table 6. Summary of the current IT Operational model.

Main topics	Answers
Organizational Structure	- Corporate IT Services Infrastructure Team operates in the traditional IT approach o No cloud competences exist in the team o Team units operate separately from each other - Cloud services require joint structure of IT Services Infrastructure Team
IT Governance	- Case company's IT Governance is very well-defined and suitable for almost any traditional IT related activities and projects. - Changes to IT Governance are expected for cloud services o If the responsibility for new cloud services moves to the company's Divisions or to the new Customer Co-operation Board.
Sourcing	- The ways of decision making for sourcing in the case company o Decision making power for the cloud provider selection might be consolidated or prerogative of each division. - Additionally to current IT services outsourcing vendor for legacy environment, new vendor for maintenance of the cloud environment might add competition in maintenance services.
Operational Processes	- The current operational processes are defined for traditional IT service management and do not support the cloud scenarios. - Cloud services will affect to most of the ITSM processes, magnitude of change will depend on the selected cloud deployment model. - Service Level Management o Needs to consider the cloud-based capabilities and the levels of service quality for defining the Service Level Agreement (SLA). - Capacity Management o Will be affected by the self-service IT infrastructure provision capability of the cloud services. - Change Management o Needs structural changes due to the involvement of the Cloud Service Provider into IT service delivery. - Cloud awareness and skills are required for the personnel involved with the affected ITSM processes.
CMDB	- Case company owns large number of IT assets. - Company's current Configuration Management Database (CMDB) is robust and reliable, but not dynamic enough for the cloud services. - Information updates for IT assets in CMDB are mostly done manually - The changes and custom integrations are needed in order to use the current CMDB with the cloud services o Alternatively, a new commercial CMDB product can be taken into use, which would mean additional expenses and implementation challenges

Risk Analysis	- Case company currently operates in a low risk manner - Case company owns Data Center and all the IT assets Positive: o Data Center is highly safe and reliable o Integrations between the IT assets are safe and reliable Negative: o Maintenance of the Data Center is extremely expensive o Capital investments to fulfil the capacity demands are high - Some IaaS cloud solutions allow to lower the capital investments and maintenance costs for IT Infrastructure - Cloud solutions pose the risks related to confidentiality, integrity and availability of the company's data.

As seen from Table 6, five elements of the current IT Operational model describe how the company IT infrastructure Team currently operates and point to the changes needed to each of these elements for taking the cloud services into use.

From *the organizational structure* point of view, Corporate IT Services Infrastructure team operates in the traditional IT approach. At the moment, no cloud competences exist in the team. Server Service and Datacom Service teams will be the most affected by the cloud services. Those teams currently operate as separate units with their own responsibilities. In the cloud-enabled environment, both teams will need to work jointly to provide cloud services to the internal customers, since cloud technologies unify server hardware provisioning and networking in a single entity.

IT Governance in the case company is currently very well-defined and suitable for almost any traditional IT related activities and projects. If the responsibility for the new cloud services will reside in the Corporate IT Infrastructure team, no changes to the IT Governance are expected. Alternatively, the responsibility for new cloud services will move to the company's Divisions or to the new Customer Co-operation Board. In that case, the changes to the current IT Governance are needed.

Sourcing in the current operational model does not take into account the cloud services. It is yet unclear what will be the ways of decision making for sourcing in the case company and who will provide the maintenance services to the cloud infrastructure. Decision making power for the cloud provider selection might be consolidated or prerogative of each division in the case company. Another question is who will maintain the cloud environment and software on top of the cloud-based IT assets, current IT services outsourcing vendor responsible for legacy environment or a new vendor. A new vendor might add competition to the current IT services outsourcing vendor in maintenance services. Thus, the sourcing strategy especially needs to be defined.

The current *operational processes* in the case company are defined for traditional IT service management and do not support the cloud scenarios. Cloud services will affect to most of these processes, but the magnitude of change will depend on the selected cloud deployment model. In this study, three operational processes of the case company were selected for the impact analysis, namely Service Level Management, Capacity Management and Change Management. The Service Level Management needs to consider the cloud-based capabilities and the levels of service quality for defining the Service Level Agreement (SLA). The Capacity Management will be affected by the self-service IT infrastructure provision capability of the cloud services. The Change Management needs structural changes due to the involvement of the Cloud Service Provider into IT service delivery.

The case company owns *Configuration Management Database (CMDB)* due to a large number of company's IT assets. Presently, the company's CMDB is robust and reliable, but not dynamic enough for the cloud services. The information updates for IT assets in CMDB are mostly done manually. The current version of the company's CMDB does not support near real-time updates that usually required by the cloud services. The changes and custom integrations are needed in order to use the current CMDB with the cloud services. Alternatively, a new commercial CMDB product can be taken into use for cloud scenarios, which would mean additional expenses and implementation challenges for the case company.

From *the risk analysis* point of view, the case company currently operates in a low risk manner. The case company has its own Data Center and all the IT resources located within that Data Center belong to the case company. The Data Center is highly safe and provides reliable and fast network connections between the company's premises and the Data Center. Integrations between the IT resources within the single Data Center are also maintained a very low risk manner. However, the maintenance of the Data Center is extremely expensive. The capital investments needed to fulfil the customer's capacity demands are high. Infrastructure as a service (IaaS) provided the by cloud service providers might lower the capital investments and IT Infrastructure maintenance costs. Unfortunately, the cloud solution might also pose some risks related to confidentiality, integrity and availability of the company's data.

Based on the analyses of the business requirements and the current IT Operational model, the following key challenges and benefits can be indicated when considering the introduction of the cloud technology into the case company.

As for the current challenges, the provisioning and configuration of servers are mainly done manually. Adding the server and the operating system management layer on top of the compute resources requires several hours of outsourcing vendor's manual work which causes a long delivery time and costs in server provisioning process. Currently, the delivery time for server provisioning may last from days to weeks, depending on the configuration requested. For allocating additional capacity, the delivery time is shorter but it is still not short enough. Yet the number of virtual servers in the case company is significant. At the same time, the company is using many virtualization technologies that make the environment heterogeneous. These virtualization technologies require different tools, management procedures and thus add to increasing the costs. Automation and orchestration is not used other than as basic scripts to help in repeating the tasks; self-service ordering of capacity services is also not available. Capacity management and forecasting is done manually using Office tools by fetching data manually from the management and monitoring systems. Some business units started to use public cloud services with direct subscriptions in a non-regulated way which poses significant security risks to the company's data (Table 2 B).

As for the benefits of the current operational model, there is a number of positive features which need to be mentioned. First, the current IT services outsourcing vendor has the needed skills to provide quality services for installations, configurations and maintenance of the legacy environment. Such activities cannot be fully automated. Also IT services outsourcing vendor supports the case company's customers with technical expertise in troubleshooting. Another responsibility of the IT services outsourcing vendor includes keeping the company's CMDB up-to-date for the company's IT assets. The current IT services outsourcing vendor brings a lot of value to the company and cannot be excluded from the service delivery process.

These are some of the key points that the case company needs to take into account when opting for the cloud technology and choosing a suitable cloud deployment model. The identified business requirements and the changes needed to the current operational model will be applied for building the operational model in Section 5 of this study.

Next section discuss the findings from best practice in cloud deployment models and existing knowledge related to key elements of the IT infrastructure operational model.

4 Best Practice of the Operational Models for Cloud Computing

This section overviews best practice in cloud computing and discusses a possible structure of an operational model for providing IT Infrastructure services to the enterprise customers. First, it overviews cloud computing and its role in IT infrastructure provision in general. Second, it discusses four cloud deployment models suitable for the case company. Third, it discusses the key elements in the structure of an Operation model. Based on the findings, a Conceptual framework for the Operational model is developed.

4.1 Cloud Computing: General Overview

Various definitions exist for cloud computing. Mell and Grance (2009) from National Institute of Standards and Technology (NIST) give a definition which is most frequently used.

> *"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."* (Mell and Grance 2009: 1)

Halpert (2011) defines four minimum criteria for any computer model that can be qualified as cloud computing, namely *elasticity*, *multitenancy*, *economics* and *abstraction*. From the *elasticity* point of view, cloud computing allows to rapidly scale up or down the capacity of the provided service with little or no involvement of the customers. *Multitenancy* means that workload of the multiple users can be shared between the available hardware resources, which is one of the reasons for the economic benefits of cloud computing. From the *economics* perspective, the customer pays for the amount of time used to buy the resource. It allows the customers to use computer resources more efficiently and opens up opportunity to use high performance computing resources when needed. *Abstraction* can be defined as the ability of the cloud service provider to isolate the customer from the underlying logic of the provided IT service. (Halpert 2011: 2-3)

Mell and Grance (2009) define five essential characteristics of the cloud computing: *on-demand self-service, broad network access, resource pooling, rapid elasticity* and *measured service*. Two of those characteristics are the same as previously mentioned minimum criteria by Halpert (2011). *Rapid elasticity* belongs to the elasticity criteria, and *resource pooling* belongs to multitenancy by Halpert (2011). Resource pooling

means that the provided IT resources can be physically located at multiple geographical locations and act as the virtual components of the computation system. *On-demand self-service* allows the customers to request and obtain the IT resources automatically, without interaction with the service provider. *Broad network access* allows the multiple customers with different end device capabilities (PC, mobile phones, tablets) to access the IT resources. Broad network access can also limit the use of the cloud-based IT services due to the network latency. *Measured service* means that the cloud resource usage can be monitored, controlled and reported to the customer and service provider in transparent manner. (Mell and Grance 2009 : 1)

Taking cloud computing into use (off-premises cloud environment) allows IT organizations do not own the IT infrastructure which eliminates all possible expenses related to IT infrastructure. In this case, IT organizations rent the IT infrastructure in a subscription-based or a consumption-based way. This enables companies to pay only for the resources actually needed or used, and avoid paying for non-need resources, thus avoiding large capital investments into their IT infrastructure. Cloud computing also reduces the expenses for the software licensing and support costs which are substantial in the traditional IT model. These reductions in expenses are possible since the cloud provider shares the provided IT Infrastructure between multiple customers. The costs for the use of high-speed bandwidth are also shared between the customers. Eventually, the low startup costs for cloud services allow companies to access computing power and software development environments much quicker compared to the traditional IT model. (Krutz and Vines 2010: 36)

Presently, the companies providing cloud computing offer various kinds of delivery service models for cloud services to their customers. Literature commonly identifies three delivery service models for cloud computing. These models represent different levels of abstraction in provision of IT services by the cloud service provider. These three service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Software as a Service (SaaS) stands for delivering software applications over the Internet through the web-based interface. In this service model, the customer is usually abstracted from everything that is underneath of the application interface like a platform or infrastructure layers (Halpert 2011: 6).

Platform as a Service (PaaS) is a service similar to SaaS, but instead of an application use only, it represents an application development environment. PaaS provide cloud-

hosted development platform accessible via an Internet interface. The customer is able to develop their own cloud-based applications and host these applications on the cloud provider side. (Krutz and Vines 2010: 39-40)

Infrastructure as a Service (IaaS) represents the third type of cloud computing services. IaaS stands for a delivery of the IT infrastructure as a service to the customers through the network. IaaS provider, with the help of virtualization, divides the large physical infrastructure IT resources into small pieces which are available to the customers for purchase. The customers are able to access processing, storage, networks, and other computing resources. On top of those computing resources, the customers are able to deploy various operating systems and applications. In the IaaS model, the customers do not manage the cloud infrastructure but they have control over the operating systems, storage, applications, databases, and limited control of networking capabilities. In the cases where the operating system or software are included in the provisioned IT resources by the cloud service provider, the cost of the required license is added to the overall service cost or included as an additional expense. (Halpert 2011: 5) IaaS have similar benefits as other cloud service models. Dynamic infrastructure scalability allows IaaS customers to manage their requirements in an adaptive and financial beneficial way. In contrast to the traditional IT model which requires purchasing of hardware, software, internal and external human resources, and thus consumes a high amount of the company's financial capital, employing the IaaS model provides a possibility for a company to rapidly respond to the demand for IT resources in IT acquisition, implementation and maintenance activities. As a result, the number of IaaS vendors is quite high. (Krutz and Vines 2010: 42)

Additionally, cloud computing has its own deployments models. A deployment model is a way how the cloud service is deployed. Different deployment models are suitable for different workload and use cases. Presently, there are four deployment models most frequently referred to: *private, community, public,* and *hybrid.* The *community* deployment model corresponds to the cloud infrastructure which is shared between several companies, partners or organizations and supports this specific community. For the *private* deployment model, the cloud infrastructure may be located on-premises or off-premises of the case company. (Halpert 2011: 8) These deployment models are discussed in the next sections and later on analyzed from the operational model perspective. One of the models, namely the community deployment model, is not discussed in the report since this type of model is not suitable for the case company. The case com-

pany deployment model needs to serve only the internal customers and cannot be shared within any community.

4.2 Cloud Deployment Models

Cloud computing has several deployment models which represent unique ways of deploying the cloud services. They are the private, public and hybrid deployment models applicable to the case company and reviewed in following sub-sections. Private deployment model is presented by two location-based deployment options, called the Private Cloud IT (on-premises) and Private Cloud IT (off-premises). The public and hybrid deployment models are called the Public Cloud IT and Hybrid Cloud IT respectively. These deployment models have specific characteristics, own benefits and challenges discussed below.

4.2.1 Private Cloud IT (on-premises)

The private cloud (on-premises) is a private cloud computing environment deployed on the company's premises and owned by the company. This cloud computing environment intended only to be used by the employees of the company, so the consumers and the service provider work in the same company and have shared goals. The private cloud (on-premises) model offer similar benefits as widely known public clouds, at the same time it allows to keep greater control over the data and the process. Additionally, the private cloud (on-premises) provides the customers with excellent quality management of the cloud services due to the closer cooperation between the customers and internal service provider. For example, a customer can determine the priority of the particular workload and define availability requirements for a specific cloud-based IT service. The private cloud (on-premises) environment can be managed by the internal organization or a third party. The cloud environment maintenance provider can also be represented by the vendor of the private cloud solution. (Halpert 2011: 8)

In the past few years, the private cloud deployment was initiated by many large organizations around the world. Large organizations have the existing legacy IT infrastructure which can be utilized for deployment of the private cloud. Regarding the positive side of the private cloud, it allows the company to prepare for the future by moving the existing infrastructure into the cloud direction earlier and by enabling the organization to understand the cloud technologies without sacrificing control, governance, security and reliability of its IT resources. (Krutz and Vines 2010: 48) One of the drawbacks of this model is that the ability to control and operate the private cloud comes with the high expenses

that are similar to the traditional IT infrastructure. Another downside of the on-premises private cloud is its less elasticity and scaling due to its limitations in available hardware resources. This factor increases the capacity risks for the company.

4.2.2 Private Cloud IT (off-premises)

The private cloud (off-premises) is a private cloud computing environment deployed on the third party premises and owned by the cloud service provider. This deployment model belongs to the same type as private cloud (on-premises) deployment model. The private cloud (off-premises) deployment model has similar benefits as the private cloud (on-premises) deployment model namely good quality management of the cloud services and higher customization capabilities of the cloud environment.

The main benefit of the private cloud (off-premises) deployment model compare to private cloud (on-premises) deployment model is the customer company does not need to own a Data Center. The tasks related to the maintenance and hardware upgrades of the servers move to the responsibility of the cloud service provider. It allows a customer company's IT organization to concentrate on the management of the cloud services from the strategic and operational point of view. (Incisive Media 2013: 6) Private cloud (off-premises) deployment model also offers single-tenant cloud environment to the customers and thus reduce the risks associated with multi-tenancy. (Robinson et al. 2011: 1) Single-tenancy is described as provision of the dedicated hardware to the single customer which can be customized and independently operated from the other customers. (Halpert 2011: 81)

Unfortunately, a private cloud (off-premises) deployment model has multiple challenges. A control over the data and the process in the private cloud (off-premises) deployment model is worse compare to the private cloud (on-premises) deployment model due to the fact that company's data is stored and managed off-premises. Additionally, a private cloud (off-premises) deployment model has higher risks associated with the cloud service provider, privacy assurance and compliance regulations; these risks are further discussed in Section 4.3.6. (Incisive Media 2013: 7) Finally, a single-tenant solution of the private cloud (off-premises) deployment model is expensive, especially if offered by the respected private cloud service providers. (Marks and Lozano 2010: 33)

4.2.3 Public Cloud IT

The public cloud can be characterized as a cloud which is available to the public use, to any customer who is wishing to access it through the Internet. There are no re-

strictions as for who can use the cloud, as long as the terms and conditions accepted by the consumer and the payment model satisfy the customer. (Halpert 2011: 9) The public cloud infrastructure is owned and maintained by the cloud service provider. The cloud service provider hosts multiple customers and shares the IT resources dynamically between them. (Krutz and Vines 2010: 44-45)

There are many benefits of the public cloud such as on-demand dynamic provisioning, scalability, ability to pay per use for IT resources and related licenses, innovations and fast cloud evolving. (Krutz and Vines 2010: 45)

However, the public clouds also have multiple challenges. One of them is the assurances related to quality of service. The public cloud providers operate widely around the globe and do not heavily depend on the single customers. Due to that fact, the cloud providers offer small compensations for the failures in the cloud IT infrastructure. Thus, for many customers the impact of the downtime in the IT service might be much higher than the standard penalties stipulated by the pre-defined service level agreement. (Halpert 2011: 9) Furthermore, the public cloud might not fulfil the organization's specific needs for IT services such as some customized configuration requirements or desired service-level agreement (SLA) regarding the up-time availability. This forces the companies to avoid the use of the public cloud for business critical tasks. (Krutz and Vines 2010: 45)

Another challenge of the public cloud deployment model relates to security. The security in public cloud is lower compared to the other types of the cloud deployment models, since the cloud environment is shared between multiple independent customers. (Halpert 2011: 9) An access to the cloud environment is done through the Internet which creates the risks of data loss in communication. Additionally, the public cloud provides own mechanisms and standards for data security which limits the customers in controlling the data security in a personalized way. It adds to the concern related to data residency requirements, for some customers the data cannot resident outside of the country where it belongs. (Krutz and Vines 2010: 45)

4.2.4 Hybrid Cloud IT

The hybrid cloud model is a combination of different cloud models such as private (on-premises), private (off-premises) and public. It can also make a combination of physical and virtual resources. Some private cloud providers offer a mix of services such as the private cloud services, traditional hosting and co-location services. This mix of services

suites the customers with heterogeneous requirements for IT infrastructure. (Bittman 2012: 3)

The hybrid cloud combines benefits of all cloud models. The public cloud model brings economies of scale which are evident in cloud provider offerings, while the private cloud model better suits for workloads that require high reliability, security and quality of service. (Halpert 2011 : 9) In the hybrid cloud deployment model, an organization might deploy non-critical IT services in the public cloud, while keeping the critical ones in the private cloud (on-premises). The combination of the public and private clouds can be especially efficient when both of them are located in the same facility. (Krutz and Vines 2010: 49) The hybrid clouds may involve multiple cloud service providers. The key feature of the hybrid cloud model is a cloud bursting, which means the ability of the IT service to allocate more IT resources from the public cloud in the event of a spike in capacity demand. (Krutz and Vines 2010: 49)

However, the hybrid clouds have some challenges. The hybrid cloud often characterized as heterogeneous environment. Management of such environment might become very complex for an IT department. (Marks and Lozano 2010: 38) Additionally, integration of different cloud models to hybrid cloud requires the efforts and expertise of an IT department. The technologies for integration various cloud models exist, but these might be costly. (Hugos and Hulitzky 2010: 106) Finally, some cloud service providers offer hybrid cloud solutions. Such hybrid cloud solutions include private and public cloud environments based on the same technology platform and typically dedicated to single cloud service provider. These solutions create vendor lock-in or technology lock-in situations for the customers. (Hurwitz et al. 2009: 95-98)

Summing up, these four cloud deployment models namely private (on-premises), private (off-premises), public and hybrid have own benefits and challenges. An organization can choose to implement one or several cloud deployment models depending on the needs for the solutions provided by each model. For example, critical applications will require for more security, thus a private cloud model may be used. Also the private, public and hybrid deployment models can co-exist in single co-location facility. These deployment models typically favour certain operational models. Next the operational model and its elements are discussed.

4.3 Operational Model and Its Elements

The term ‘operating model’ has originally appeared in the corporate strategy literature. It relates to how the target organization operates in order to execute the company’s strategy and deliver services to its customers. De Vries et al. (2011), based on business-IT alignment framework (BIAF), emphasize that “the operating model creates a company-wide vision for process standardization and data centralization, and guides decisions about how a company implements processes and IT infrastructure” (De Vries et al. 2011: 1005).

An operating model term (in other contexts, operational model) can apply to any organization, business unit or the whole company. Operating models have the goal to align day-to-day operations with the company’s strategy to produce measurable results. Brown et al. (2008: 310) recommend that each company should have a business operating model which emphasizes the company’s strength to deliver value.

In spite of a wide use of operating models in various business fields, the structure of the IT operating model for enabled cloud computing is not yet widely defined in the literature. To define the structure of the IT operating model in this thesis, two advanced marketing materials from consulting companies were used. The first one defines the IT operating model as a combination of IT capabilities to support the needs of the business, internal competences and organizational structure, delivery mechanisms, decision rights and accountabilities (Strategy& Formerly Booz & Company 2014). The second source defines the IT operating model as a collection of key elements such as Governance, People, Processes, Capacity and Costs (Owen, Strategy2Life 2012). In the context of this thesis, the human capacity and associated costs can be related to the Sourcing element. Based on the findings from available materials and consultations with the Head of IT Infrastructure Team in the case company, an IT operating model was constructed from the following elements: an Organizational Structure, Operational Processes inside the organization, IT Governance, Sourcing, CMDB and Risk Analysis associated with the cloud services. These six elements are further investigated in this section as possible elements for the Operational model proposal for the case company.

4.3.1 Organizational Structure

The organizational structure can broadly be defines as a purposeful arrangement of the people for achieving some specific purpose (Hiriyappa 2009: 3). According to Child (1984), the components of the organizational structure include: a) allocation of tasks and responsibilities to individuals, b) defining formal reporting relationships and number

of levels in hierarchies, c) grouping together of personnel into teams, departments and to whole organization, d) design of systems to provide information flow between the teams in order to facilitate the decision-making process, e) delegation of authority and f) provision of the systems for performance measurement and employees rewarding (Child 1984: 5). Thus, the definitions of an organizational structure focus on the resources and functions of the organization, including the organizational layers, participants, their competences and responsibilities in the organization.

In the cloud computing, the choice of the organizational structure for cloud computing can be especially challenging since cloud computing represents a complex environment with many technologies involved. The IT organization needs to have technical knowledge in a wide range of these technologies in order to manage the cloud services. However, the most important change that cloud computing brings is the relationship between the business and the IT department in the consumption of IT resources. Both research and business literature suggest that cloud computing requires a much better understanding of the business requirements from the IT organization. (Anderson and Gtantz 2012: 5)

Oredo et al. (2014) emphasize that, in the addition to the changes in the consumption of IT resources, cloud computing will also affect the job roles, required competences and organizational structure, as compared to the traditional IT department. For identification of the new required competences, the following challenges of the cloud computing can be pointed out: a) availability and reliability of the cloud services, b) security and privacy concerns, c) portability, interoperability, integration with legacy system, d) vendor management, e) cultural resistance to changes in the organization, f) transition and execution activities with cloud services. (Oredo et al. 2014: 154,155)

Similarly, Anderson and Gtantz (2012) highlight that in transition to the cloud-enabled organization, all areas of the IT organization will be affected as for the required critical skills for cloud computing. These areas include Management functions, Project and Program Managers, Business Analysts, Application Development and Maintenance, IT Systems and Operations, Network and Telecom Management, Security Management, Help desk and End-user support (Anderson and Gtantz 2012: 6,7).

Summing up, based on the reviewed best practice and existing knowledge for the identified need for the new cloud computing competences, there are recommendations to either establish a new IT organization within the corporation, or to make considerable changes to the old IT organization, in case the new cloud services are planned. The

type of the cloud deployment model adopted by the company will determine the amount of efforts needed for the deployment and maintenance of the cloud services by the IT organization. It will also point to the new roles and responsibilities in that IT organization. Correspondingly, the magnitude of change to the current organizational structure needs to be seriously considered by the company making the choice of its cloud deployment model as one of the key factors in the coming change.

4.3.2 IT Governance

The governance term can be described as the activity which "ensures that policies and strategy are actually implemented and that required processes are followed correctly. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified". (ITIL Glossary 2011)

There are different types of governance existing in the enterprise environment. The most well-known are *Corporate Governance* and *IT Governance*. The Corporate Governance corresponds to all the processes, policies, management practices affecting the way how the corporation is controlled and managed. IT Governance, in its turn, is a subset of the Corporate Governance. It focuses on the information technology assets, their performance and managing the risks associated with them. The main goals of the IT Governance are to validate that the IT investments generate business value and to reduce the IT related risks. (Brisebois et al. 2007: 31)

For the IT governance of cloud services, some of best practice suggests the division into security oriented and the service oriented approaches. The first approach corresponds to *Information Security (InfoSec) Governance.* InfoSec Governance provides a strategic vision and guidance of the information security implementation in the organization. InfoSec governance applies to the data which is stored, processed and transmitted through the IT infrastructure. In the case of the cloud, the InfoSec governance takes more essential role due to the fact that data moves outside of the company's IT infrastructure. (Halpert 2011: 41-43) The second approach corresponds to *Service-Oriented Architecture (SOA) Governance.* The cloud services belong to the service-oriented architecture (SOA) due to their functionality. SOA governance breaks down software (service) elements and functions into the independent components that can be connected or redefined. The senior managers are recommended to rethink the approaches related to the control and governance procedures for all of the separate service elements in the SOA environment for cloud scenario. (Moeller 2013: 242,243,244)

The security and management issues discussed above need special consideration since cloud computing shifts a range of security challenges and responsibilities from the company's internal IT function to the cloud service provider. For the selection of the cloud service provider, the company's IT management would need to examine the security and privacy components of possible cloud service providers in the following areas: physical access to facilities, regulatory compliance, data location, data segregation, data recovery, investigative support, long term viability. (Moeller 2013: 166, 167) To ensure high security in protecting the access, transmission and storage of the company's data at the provider side, the company might reach these levels only through the legal contract (Service Level Agreement) with the cloud service provider mandating compliance with acceptable security standards. (Halpert 2011: 44)

The IT governance for cloud services needs to be defined since the cloud-based IT infrastructure is different from the traditional IT infrastructure. The cloud-based IT infrastructure implies several deployment models. Although these models may be similar, they have their specifics, especially for big organizations. For example, for on-premises cloud IT infrastructure the IT governance might not have significant changes. While for public or private it may include new roles and responsibilities and new security guidelines. The common changes to the all deployment models may include new methods how to measure the performance of the cloud-based IT services and new approach how to resolve any issues related to the cloud-based IT services.

Another reason why a separate IT governance model needs to be discussed is a new type of key attribute of the cloud IT governance, which is *self-service*. Wide options for self-service lead to the need for the employees to know the rules and regulations related to the cloud services. Thus, a set of clear written policies need to be developed. Additionally, the written set of the policies need to be communicated though the organization which can be done, for example, through organized trainings. Finally, the policies would also be needed in the automation process of provisioning the cloud services, called as "policy-driven" process. Provisioning of cloud services in the cloud environment is typically done through a web-based self-service portal. Accordingly, the policies need to be configured for the portal. (Muller 2011: 162,163)

Summing up, based on the reviewed best practice and identified challenges for the IT governance in cloud computing, several areas of the traditional IT governance may require most changes, namely Information Security (InfoSec) governance and SOA governance, cloud competences including the self-service part, new roles and respon-

sibilities, and new operational processes including measuring, reporting and taking action to resolve the identified issues. The type of the cloud deployment model adopted by the company will affect the amount of change needed to govern these areas. According to that choice, the magnitude of change to the current IT governance will become more visible to make a more precise plans and forecasts for the company planning the shift to cloud computing.

4.3.3 IT Sourcing

The IT sourcing belongs to the Strategic Sourcing field. The general practices from strategic sourcing are applicable to the cloud-based IT infrastructure services. (Bensch 2011: 101) Strategic sourcing is often defined as a procurement and supply management process which locates, qualifies and employs the suppliers that add value to the customer in accordance with business requirements. (Sollish and Semanik 2010: 1)

Strategic *sourcing process* applies to the sourcing projects as a best practice. This process allows company to coordinate the procurements with defined checks in order to justify costs and requirements. (Payne 2011: 11) Typical strategic sourcing process includes steps such as strategic planning, business requirements analysis, research about potential suppliers, solicitation (request for offer to the supplier(s)), supplier selection, negotiation and contracting, and contract administration. (Sollish and Semanik 2010 : 17; Payne 2011: 11) Sourcing decisions need to take into account overall performance of the supplier in the following criteria such as quality, delivery, customer service, product/service advancements and cost. (Maromonte 1998: 2)

Bensch (2011) focuses on the procurement/sourcing process of the cloud-based IT infrastructure services. Because the most common public IaaS offerings have standard pre-defined service agreements (SLAs), some steps in sourcing process might not be possible to execute such as solicitation, negotiation and contracting. Additionally, the billing methods might not be negotiable with public IaaS offerings. (Bensch 2011: 101)

Several sourcing decision options defined in the literature. Most known are *total outsourcing*, *total insourcing* and *selective sourcing*. Total outsourcing option is used when assets, staff and management for service delivery transfers to the third party vendor for more than 80 percent of the service budget. Contrary Total insourcing option means that provisioning and management of the service is mostly done in-house. Selective sourcing option means a combination of the internal and external sourcing options. (Dibbern et al. 2004 : 10)

Since large and complex organizations already have own IT infrastructure, internal competences and organizational processes in place the total outsourcing of the IT infrastructure services to the cloud service providers might be avoided by the optimization of internal efficiencies in the form of economies of scale, scope, management and organizational process flows. (Khan and Jameel 2010: 1073,1077)

Summing up, an IaaS service delivery to the customers is divided into two components such as managing physical IT infrastructure and operational activities related to management of the software on top of it. In the cloud services the management of physical IT infrastructure belongs to the total outsourcing or total insourcing depending on the deployment model. The management of the software on top of the provided hardware can be done though the total outsourcing, total insourcing or selective sourcing options. According to that the organizational sourcing decision option for management of physical IT infrastructure and sourcing decision option for management of the software are included into conceptual framework of this study.

4.3.4 IT Operational Processes

IT Operational Processes is part of the IT service management (ITSM) practice. IT service management (ITSM) refers to the implementation and management of the IT services by the IT service providers for the purpose to fulfil the requirements of the business. IT service management (ITSM) is a combination of the skilled human resources, defined processes and information technology assets. (ITIL glossary 2011)

The Information Technology Infrastructure Library (ITIL) is an approach for IT service management (ITSM) that aligns IT services with the needs of business. ITIL is a practical framework and a collection of the best practices for identifying, planning, delivering and supporting IT services to the business. (What is ITIL 2014) Best practice is a proven method of completing the task to produce a best possible result. The first version of the ITIL was developed by British Government's Central Computer and Telecommunication Agency in the 1980s. In the 1990s ITIL was widely adopted globally by the private organizations. (Knapp 2010: 9).

Marquis (2012) emphasise that ITIL processes are able to support the cloud operations without significant changes to them. At the same the ITIL methods used in the traditional IT Infrastructure Management require changes. By default ITIL is not optimized for fast service delivery, amount of changes and supplier management approach that cloud services offer. In the cloud scenario ITIL is used for improvement of service relia-

bility instead of component availability in the traditional IT. In the cloud scenario typically the external providers do most of the work related to the physical infrastructure management. Moving towards the cloud-based IT Infrastructure, the operational teams responsible for the legacy IT infrastructure need to change their operations towards the management of the services and managing service providers. (Marquis 2012: 1,2,3).

Based on the discussion with Head of the Infrastructure Team, three operational processes were selected as the focus of this thesis, namely Service Level Management, Capacity Management and Change Management.

ITIL defines *Service Level Management* as a process to ensure that IT services are provided to the customers with agreed conditions. Service Level Management process includes negotiation and making an agreement between the customer and supplier for the provision of the defined IT services. Such agreement called as Service Level Agreement (SLA) by ITIL. Service Level Agreement is a contractual obligation between the service provider and the customer which includes the targets for the IT services. Targets might include levels of availability, capacity, performance which is possible to measure and achieve by the IT service provider (Gallacher and Morris 2012: 78,79).

A company that buys IaaS service from a cloud service provider typically accepts the standard Service Level Agreement from the provider or negotiate a new agreement. For mission-critical applications a company need to negotiate an SLA that includes penalties for cloud service provider in case of service delivery failure. Additionally, company needs to have own ability to monitor the IT service for verification of the requirements defined in SLA. (Hurwitz et al. 2009: 31) In some cases, company also needs to have ability to make changes to the SLA during the service lifecycle. (Hausman et al. 2013: 20) Typical SLAs with cloud service provider includes response times, availability of the service, uptime target for a service and response times in the case of service failure. Customer needs to take into account possible service downtime, lines of the responsibility on the cloud service provider side, cost of the downtime for the customer in the case of service failure, known incidents in the past with the selected cloud service provider. (Hurwitz et al. 2009: 242)

ITIL defines *Capacity Management* as a process to ensure that the capacity of IT services and IT infrastructure meets the current and future needs of the customers in a cost-effective and timely manner. Capacity Management is used for prediction of the future capacity requirements and ability to fulfil them in order to prevent possible service failures. (Gallacher and Morris 2012: 119) Capacity Management applies to the IT

services during their lifecycle. IT department identifies the capacity requirements for a new IT services, adjusts the capacity for existing IT services in a case of changes and optimizes the capacity based on the cost and future needs. (EMC Education Services 2012: 376) Capacity Management also supports decision making for server consolidation, hardware procurement, and service level management. (Stenzel et. al 2010: 68)

Hausman et al. (2013) highlight that in the cloud scenario the Capacity Management personnel no longer need to focus on the infrastructure components. Instead, capacity management personnel need to understand the performance data and limitations of the cloud-based IT assets in order to meet the rising demands of the business. Capacity management personnel also need to understand the costs associated with the resource allocation in the cloud environment in order to plan for the capacity. (Hausman et al. 2013: 21) Additionally, Marquis (2012) states that in the cloud scenario the Capacity Management process will transform from management of the traditional IT components to the management of the services. The IT component delivery is characterized by the long lead time, while the IT service delivery is near real-time. Removing excess capacity becomes a critical task by the capacity management personnel. (Marquis 2012 : 2)

ITIL defines *Change Management* as a process for controlling the lifecycle of the all changes and making possible to execute the changes with minimum disruption to the IT services. A Change term can be defined as “the addition, modification or removal of anything that could have an effect on IT services”. (ITIL glossary 2011) The management of changes needs to be controlled in order to provide a quality service to the business customers. (Gallacher and Morris 2012: 163) A Change Management has two main objectives. The first objective is to keep in order the changes meanwhile reduce the negative impact to the IT services such as amount of incidents, disruption to the services and possible rework. The second objective is to ensure that changes are recorded to the Configuration Management System (CMS), “prioritized, planned, tested, implemented, documented and reviewed in controlled manner”. (Gallacher and Morris 2012: 164) Some examples of IT related changes are changes in IT infrastructure, IT architecture, documentation and processes, as well as the changes to IT services during their lifecycle. (Gallacher and Morris 2012: 165)

In the cloud scenario, a Change Management process needs to handle the high number of changes and adapt to the shorter time frames for the change implementations, since cloud computing is characterized as the dynamic environment. (Marquis 2012: 1-

3) Hurwitz et al. (2009) highlight that changing configurations or patching in the cloud environment becomes more challenging due to virtualization technologies and cloud provider specific procedures. It is important that a cloud provider includes the support options in the contract to manage the changes. (Hurwitz et al. 2009: 207, 239) Additionally, the changes to the physical infrastructure components by the cloud provider should follow deployment schedule defined in SLA. However, these changes might be influenced by the cloud provider policies. (Otsuka and Lutfiyya 2011: 134)

Summing up, three ITIL-based operational processes used in the case company namely Service Level Management, Capacity Management and Change Management were selected for the impact analysis of the cloud computing to these processes. Based on the reviewed articles, cloud computing will make impact on these operational processes to some extent. The impact will depend on the cloud deployment model and cloud computing utilization rate in the case company. Accordingly, an impact to the Service Level Management, Capacity Management and Change Management processes is included into the conceptual framework of this study.

4.3.5 CMDB and the Cloud Services

Configuration Management Database (CMDB) is the main component of the Service Asset and Configuration Management (SACM) process. The SACM process is defined by the ITIL framework. This process ensures that IT assets required for service delivery are controlled, and accurate information regarding to those assets is stored and available when needed. The information about the IT assets contains the details of how these IT assets are configured and interconnected. CMDB stores that information throughout the lifecycle of the IT assets. (ITIL Glossary 2011)

Configuration Management Database (CMDB) contains a collection of the configuration items (CI). Those configuration items represent the elements of the IT infrastructure that are managed as the service assets. The examples of the service assets are physical and virtual servers, as well as knowledge about those servers by the support team. The information about the interconnections between the service assets stored to the CMDB and helps to understand how those elements depends on each other. Additionally, this information supports the identification of the impact regarding the changes in single service asset. (Gallacher and Morris 2012: 189)
In the distributed environments such as the cloud environments, management of the IT assets is challenging due to the fact that those assets might be located at various loca-

tions. That is the reason why the use of the CMDB by the organization is important in the management of the cloud-based assets. (Gallacher and Morris 2012: 188)

Due to the dynamic characteristic of the cloud environment, the configuration data, relationships and dependencies between the configuration items in CMDB can be represented as "*real-time IT service model*". Compare to the *traditional IT service model*, where configuration data typically stored once when an IT service goes to production mode, a real-time IT service model describes an IT service at any moment of time during the execution. The CMDB for the traditional IT infrastructure is not capable to manage near real-time data due to the limited performance and functional capabilities. For that reason, a company that wishes to leverage the power of the CMDB needs to have a CMDB that supports real-time IT service model. (Colville 2011: 1, 6)

There are commercial CMDB implementations that support cloud-based IT assets and exist on the market from vendors like Microsoft, BMC, HP, etc. Each CMDB implementation typically acts as part of the configuration management system (CMS). CMS governs the data in more federated way compare to the CMDB. (Gallacher and Morris 2012: 190) CMS also helps to manage the cloud resources more efficiently by providing additional functional capabilities to the CMDB, such as defining the policies for service models and enabling the automation of the tasks. (Curtis and Colville 2011: 3)

An overview of the commercial CMDB solutions supporting cloud-based IT assets for private or public cloud deployment models has been conducted in order to understand the available options for the case company. Four available options were identified and described below.

First option, many big *public cloud service providers* do not offer dedicated CMDB solutions; they provide simple repository of the data about IT infrastructure elements in web-based format. Additionally, these public cloud service providers have capabilities for custom integrations with the customer's CMDB solutions through the Application Programming Interface (API).

Second option, many *private cloud service providers* offer CMDB solutions dedicated to their own cloud environments. For example, Microsoft offers "Service Manager CMDB" solution which is a component of the System Center suite. System Center suite fully supports only Microsoft Private Cloud and Microsoft Public Cloud (Azure). (Flynn et al. 2009: 337, 340) (Turpijn 2013)

Third option, *some cloud service providers* offer CMDB solutions that are dedicated to their own cloud environment and also capable to work with other cloud environments that are based on the same technology platform. For example, HP offers "Universal CMDB" solution which is part of the HP Cloud Service Automation (CSA) Foundation suite. It is applicable to HP Private Cloud and other public clouds using OpenStack technology. (Hewlett-Packard Development Company, L.P. 2011: 31) (Jackson 2013)

Fourth option, *independent third party CMDB solutions* support public or private cloud service providers, or both. For example BMC software offers "BMC Atrium CMDB" solution which is a component of the Cloud Lifecycle Management suite. Cloud Lifecycle Management suite can be used with many private or public cloud service providers. (BMC Software 2014: 2) Another example, CloudAware company offers CMDB solution which supports public cloud service providers like Amazon AWS and GCE (Google Compute Engine), as well as internally-located virtualized environments based on the WMware technologies. The CloudAware CMDB solution is located on the cloud and can be accessed through the Internet. (CloudAware 2014: 3)

Summing up, CMDB has to support "real-time IT service model" in order to work with the cloud-based IT assets. Additionally, an overview of the commercial CMDB solutions identified four possible deployment options for CMDB namely on-premises, off-premises or cloud-based. Finally, a type of the cloud deployment model adopted by the company might affect the complexity of the integration between the company's CMDB and the cloud environment(s). According to that the requirements for company's CMDB, suitable deployment option for CMDB, and integration complexity between the company's CMDB and the cloud environment(s) are included into conceptual framework of this study. Integration in that context means gathering the information about cloud-located IT infrastructure assets and interconnections between them, as well as to storing and keeping this information up to date.

4.3.6 Risk Analysis

Risk analysis is a method which is able "to define what may happen in the future, assess associated risks and uncertainties". (Aven 2012: 2) Some examples of risks: risk of the accidents, risk of the possible nature disasters, risk of the electricity outages in the Data Center, etc. In today's world the systems become complex and difficult to maintain and the consequences of the possible failures are high. Risk analysis plays important role in management of the complex systems. The companies need to identify and categorize possible risks in order to develop preventive measures and make the

right decisions. Based on the risk analysis the best alternative is chosen, which has lowest amount of possible failures and highest profitability. (Aven 2012: 2-3,13,28)

Cloud computing represents a complex environment and has many risks to consider. It is advisable to perform a risk analysis to the selected cloud environment(s). Risk analysis typically is done once before taking the cloud environment(s) into use and constantly repeated afterwards as a practice in Risk Management process, which is a part of Business Continuity Planning. Halpert (2011) emphasizes that many risks applicable to the cloud environment(s) are similar to the risks in the traditional hosted and outsourced IT environments. Additionally, these risks differ depending on the type of the cloud services and cloud deployment model. Cloud computing also introduces some specific risks associated with the *cloud service provider(s)*, *data sensitivity* and *compliance requirements*. (Halpert 2011: 26-27,131) Similarly, Krutz and Vines (2010) identify that the cloud computing creates the risks to the *privacy assurance* and *compliance regulations*. (Krutz and Vines 2010: 125)

From the *privacy assurance* point of view, due to the fact that private (off-premises) and public cloud services located outside of the company's premises, a company has limitations to control these cloud services. Additionally, a company might suffer financially from the possible privacy losses which can result to the loss of company's credibility. It is important for the company to have the correct security measures in the cloud environment(s). (Krutz and Vines 2010: 127)

Information security of the data can be represented by three tenets namely *confidentiality*, *integrity* and *availability*. Confidentiality is the prevention of the data from disclosure to unauthorized person(s). Integrity is the prevention of the data from modifications by unauthorized person(s) or by accident. Availability refers to the stability and reliability of the IT infrastructure and network connectivity. (Krutz and Vines 2010: 125-127) Accordingly, to protect the company's data from loss of confidentiality, integrity and availability, the proper *cloud access controls* need to be in place. More valuable company's data, more intense cloud access controls are needed. Additionally, accountability has to be a part of the cloud access controls. The measures for mitigation of the access violations might include regular backups of the company's data, technological solutions for robustness of the cloud IT infrastructure like RAID technology and data replication between at least two Data Centers, business continuity planning process in place, fault tolerance and insurance. (Krutz and Vines 2010: 145-146)

For mitigation of the security risks also important to understand the possible threats and vulnerabilities in the cloud IT infrastructure and network connectivity. A threat is an event that can be a reason for the damage to the IT infrastructure environment or loss of confidentiality, availability and integrity. Vulnerability is a flaw in the environment that might become a cause of the threat. Reducing the vulnerabilities in the environment helps to reduce the risks. (Krutz and Vines 2010: 141) Most known key threats to cloud computing include: a) abuse and nefarious use of cloud computing, b) insecure application programming interfaces, c) malicious insiders d) shared technology vulnerabilities, e) data loss/leaks, f) Account, service, and traffic hijacking, g) Unknown risk profile. (Cloud Security Alliance 2010: 8-14)

From the *compliance regulations* point of view, sometimes companies need to follow the various compliance regulations and privacy laws when dealing with sensitive data. Cloud service provider should be compliant to these regulations in order to be a suitable partner for these companies. The compliance regulations and privacy laws might be common or vary in different countries. (Krutz and Vines 2010: 127-128) Additionally, customers need to plan for the possible new regulations that are coming directly to the cloud service providers in future by the legal authorities. (Halpert 2011: 144) Development of international regulations regarding to cloud services is consensus-driven and long-time process. (Ernst & Young 2011: 30)

From the *cloud service provider risks* point of view, there are certain risks exist with the cloud service providers. First, cloud service providers depend on the partners that provide network connectivity, premises and other services. A customer needs to identify the partners of the cloud service provider in order to analyse the risks associated with them. (Chee et. al 2010: 149) Second, quality of the cloud service providers needs to be assessed. Cloud service provider might discontinue the service or go out of the business, so a customer has to find out how long and how well a cloud service provider can provide quality services. Finally, customer needs to have business continuity plan ready for possible risks associated with the cloud service provider. Chee et. al (2010) point out that “safest” cloud service providers are the companies that fall into two categories such as cash-rich providers like Amazon or Microsoft, and the companies with high expertise and technological advantages. (Chee et. al 2010: 151-152)

Summing up, based on the reviewed best practice for risk analysis and risks associated with the cloud computing, it was identified that additionally to the risks associated

with the traditional hosted and outsourced IT environments, cloud computing introduces new specific risks related to the privacy assurance, compliance regulations and cloud service provider(s). According to that, the magnitude of risks associated with privacy assurance, compliance regulations and cloud service provider(s) are included into conceptual framework of this study.

4.4 Conceptual Framework for Operational Model

In this study, the main elements for cloud-based IT Operational model have been identified and discussed based on the consultations with the case company's representative (Head of IT Infrastructure Team), reflected in Section 3, Current State Analysis; and based on the findings from existing knowledge and best practice. The identified six elements of the Operational model, as well as the deployment models discussed above, are summarized into the conceptual framework intended for the analysis of the cloud options for the case company. The framework is illustrated in Figure 7 below.

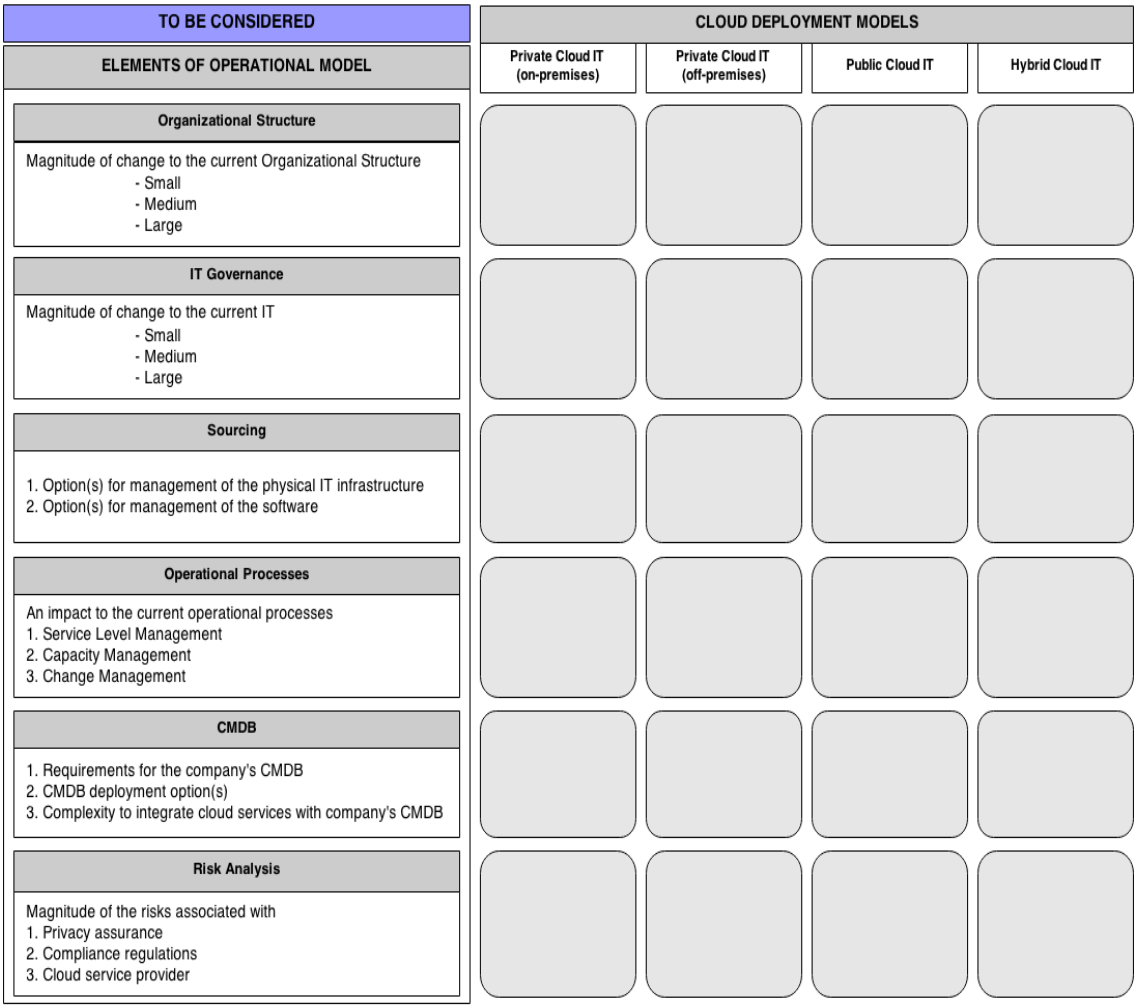

Figure 7. Conceptual Framework for the selection of cloud-based IT Operational Model.

As seen from Figure 7, conceptual framework is shown as a matrix table. Four columns of the table correspond to the cloud deployment models applicable to the case company, such as Private Cloud IT (on-premises), Private Cloud IT (off-premises), Public Cloud IT and Hybrid Cloud IT. These cloud deployment models represent different ways of cloud service delivery and included into the conceptual framework as the main topics for analysis and comparison.

The horizontal rows of the conceptual framework represent the six elements of the Operational model, namely an *Organizational Structure*, *IT Governance*, *Sourcing*, *Operational Processes*, *CMDB* and *Risk Analysis*. These elements need to be considered when choosing a cloud deployment model.

In addition to the six elements indicated in the Operational model, the conceptual framework was extended with some additional evaluation points, or critical components. These evaluation points support the analysis of the cloud-based IT Operational models and include: a) *a magnitude of change* to the current Organizational structure, b) *a magnitude of change* to the current IT Governance, c) the *sourcing options* for management of company's IT assets (physical and software), d) *an impact of the cloud computing* to the current Operational processes, such as Service Level Management, Capacity Management and Change Management, e) *the requirements* for company's CMDB to support cloud-based IT assets, *the suitable deployment option(s)* for CMDB, and *the degree of complexity* to integrate cloud-based IT assets with company's CMDB, f) *a magnitude* of risks associated with privacy assurance, compliance regulations and cloud service provider.

These points were necessary in order to evaluate and justify the selection of a particular Operational and Deployment model for the case company, which is done later in the thesis. This evaluation will be done following the system of "traffic lights" (*high - medium - low*), based on the findings from the current state analysis (Section 3), evidence from best practice (Section 4), and consultations with the case company (Section 5). The key questions will be indicated in full separately. The results will be merged into a Proposal for the IT Operational model for the case company described in Section 5 below.

5 Building the Operational Model Proposal

This section argues for a particular choice of a deployment and operational model for the case company. It starts with the evaluation of the cloud alternatives applicable to the case company, following the logic of the conceptual framework and checking against the business requirements from the case company. When the best suitable cloud deployment model is selected, its operational model is described and proposed to the case company.

5.1 Evaluation of Cloud Alternatives

The evaluation of the of the cloud alternatives in this paper means the grounded comparison of the advantages and challenges of each possible model for the case company. As possible alternatives for the case company, the four cloud deployment models are evaluated, namely: *Private Cloud IT (on-premises), Private Cloud IT (off-premises), Public Cloud IT* and *Hybrid Cloud IT*.

The evaluation is based on the business requirements revealed in the CSA and the elements of the Operational model built on the findings from the best practice related to each of the models. *Business requirements* include: *Cost Efficiency, Agility, Functional Requirements, Reliability and Security.* Elements of *the Operational model* include: changes to *the Organizational structure*, changes to *the IT Governance*, *Sourcing* options for management of the company's IT assets (physical and software), possible impact of cloud computing on *the Operational processes*, requirements and deployment options for the company's *CMDB*, and magnitude of unique *Risks* associated with cloud services.

The evaluation of each deployment model follows the system of "traffic lights" (high - medium - low). The results of the evaluation for each cloud deployment model are summarized into tables below.

5.1.1 Private Cloud IT (on-premises)

The first operational option available for the case company is Private Cloud IT (on-premises) deployment model. The cloud computing environment in this model is deployed on the company's premises, owned by the company and intended only to be used by the employees of the company. The detailed description of the Private Cloud IT (on-premises) deployment model is available in Section 4.2.1. Specific characteristics, benefits and challenges of the Cloud IT (on-premises) deployment model that

support the evaluation are summarized in Appendix 4 (Table 1). The evaluation results of the Private Cloud IT (on-premises) deployment model are shown in Table 8 below.

Table 8. Evaluation of the Private Cloud IT (on-premises) Operational Model.

	TO BE CONSIDERED	IT OPERATIONAL MODEL Private Cloud IT (on-premises)
	Business requirements from case company 1. Cost efficiency 2. Agility 3. Functional requirements 4. Reliability 5. Security	1. Fulfill partly (cost of the service is high, own Data Center) 2. Fulfill partly (Limitations due to available IT capacity) 3. Fulfill partly (Limitations due to available IT capacity) 4. Fulfill partly (Limitations due to the single Data Center) 5. Fulfill
ELEMENTS OF OPERATIONAL MODEL	**Organizational Structure** Magnitude of change to the current Organizational Structure - Small - Medium - Large	**Small** 1. New competences and roles are required 2. No integration is required with off-premises cloud service provider
	IT Governance Magnitude of change to the current IT Governance - Small - Medium - Large	**Small** 1. No significant changes 2. Some updates to the documentation
	Sourcing (cloud-based IT assets) 1. Option(s) for management of the physical IT infrastructure 2. Option(s) for management of the software	1. 3rd party (current vendor), case company owns Data Center 2. 3rd party (new vendor)
	Operational Processes An impact to the current operational processes 1. Service Level Management 2. Capacity Management 3. Change Management	1. Small (No additional tasks with data management off-premises) 2. High (Management of own Data Center) 3. Small (does not involve the private cloud provider)
	CMDB 1. Requirements for the company's CMDB 2. CMDB deployment option(s) 3. Complexity to integrate cloud services with company's CMDB	1. CMDB should support "real-time IT service model", have performance and functional capabilities for near real-time data management, and capabilities for the integration with selected cloud environment. 2. On-premises 3. Complexity - Medium (cloud environment is fully configurable, might be easier to purchase a commercial solution with build-in integration capabilities)
	Risk Analysis Magnitude of the risks associated with 1. Privacy assurance 2. Compliance regulations 3. Cloud service provider	1. Small (cloud environment needs to be properly configured) 2. Same as for the traditional model 3. Small (cloud environment support from cloud provider is required)

As seen from Table 8, the evaluation criteria for the Private Cloud IT (on-premises) model include seven categories, displayed as the horizontal rows. First category represents the business requirements from the case company. Other six categories represent the elements of the operational model defined in the conceptual framework, namely an *Organizational Structure*, *IT Governance*, *Sourcing*, *Operational Processes*, *CMDB* and *Risk Analysis*. Each area includes the questions to be answered for an evaluation of the deployment model.

The Private Cloud IT (on-premises) model does not fulfill the business requirements for the Cost Efficiency, Agility, Functional requirements and Reliability due to the specific characteristics of this deployment model, limitations to the available IT capacity and high costs associated with the IT capacity management for the company's own Data Center. The business requirements for the Agility and Reliability are fully fulfilled with the certain cloud providers.

A magnitude of change to the current *Organizational Structure* of the case company for the Private Cloud IT (on-premises) deployment model is *Small*. New cloud related competences are needed for the case company and new cloud specific roles need to be defined. No integration with off-premises cloud service provider(s) is required.

A magnitude of change to the current *IT Governance* of the case company for the Private Cloud IT (on-premises) deployment model is *Small*. Some general cloud-related changes will effect to the functional activities and company documentation of the case company. From the *Sourcing* perspective, the management of the physical IT infrastructure remains to be done by the current third party outsourcing vendor, and management of the software on top of the cloud-based IT infrastructure proposed for the new outsourcing vendor.

From the *Operational Processes* perspective, three ITSM operational processes are in the focus of the evaluation, namely *Service Level Management*, *Change Management* and *Capacity Management*. An impact to the Service Level Management and Change Management by the cloud computing in the Private Cloud IT (on-premises) deployment model is *Small*. The internal SLAs are easier to define and maintain by the Service Level Management. The management of the cloud environment on-premises does not involve the cloud provider which eliminates additional steps in the Change Management process. An impact to the Capacity Management by the cloud computing is *High*. The company continues to manage the IT capacity for the own Data Center. Additionally, new cloud specific tasks and management of the cloud environment are added to the Capacity Management.

The requirements for the company's CMDB include: a) support of the "real-time IT service model", b) performance and functional capabilities for near real-time data management, c) capabilities for integration with selected cloud environment. The best deployment option for the company's CMDB is on-premises, because the company continues to own the Data Center. The complexity for integration is *Medium* due to the

available high customization capabilities of the on-premises cloud environment. Alternatively to the current company's CMDB, new commercial CMDB product with built-in integration capabilities might be taken into use.

The magnitude of the risks associated with the Privacy Assurance, Compliance Regulations and Cloud Service Provider is *Small.* The deployment of the cloud environment on-premises gives full control over the data and process to the case company which eliminates the cloud related risks.

Summing up, the Private Cloud IT (on-premises) deployment model fulfills one out of the five business requirements of the case company. It makes a *low* impact to the company's current working practices and has the *lowest* risks associated with the Privacy Assurance, Compliance Regulations and Cloud Service Provider. The detailed evaluation of the Private Cloud IT (on-premises) deployment model is available in the Appendix 5. The following section evaluates the Private Cloud IT (off-premises) deployment model in the same manner.

5.1.2 Private Cloud IT (off-premises)

The second operational option available for the case company is Private Cloud IT (off-premises) deployment model. The cloud computing environment in this model is deployed on the private cloud provider's premises and IT hardware belongs to the cloud provider. The private cloud provider loans the cloud-based IT assets to the customers for certain period of time. The cloud-based IT resources might be dedicated to the single customer or shared between multiple customers, single-tenant or multi-tenant environments. The detailed description of the Private Cloud IT (off-premises) deployment model is available in Section 4.2.2. Specific characteristics, benefits and challenges of the Cloud IT (off-premises) deployment model that support the evaluation are summarized in Appendix 4 (Table 1). The evaluation results of the Private Cloud IT (off-premises) model are presented in Table 9 below.

Table 9. Evaluation of the Private Cloud IT (off-premises) Operational Model.

TO BE CONSIDERED	IT OPERATIONAL MODEL Private Cloud IT (off-premises)
Business requirements from case company 1. Cost efficiency 2. Agility 3. Functional requirements 4. Reliability 5. Security	1. Fulfill partly (cost of the service is high - single-tenant solution) 2. Fulfill 3. Fulfill partly (auto-scaling unavailable, integration requirements) 4. Fulfill 5. Fulfill partly (case company has limited control over the data)
ELEMENTS OF OPERATIONAL MODEL **Organizational Structure** Magnitude of change to the current Organizational Structure - Small - Medium - Large	**Medium** 1. New competences and roles are required 2. Additional competences are required for the integration with the off-premises cloud environment 3. Vendor management
IT Governance Magnitude of change to the current IT Governance - Small - Medium - Large	**Medium** 1. InfoSec governance should be extended 2. Updates to the policies and documentation
Sourcing (cloud-based IT assets) 1. Option(s) for management of the physical IT infrastructure 2. Option(s) for management of the software	1. cloud service provider 2. cloud service provider or 3rd party (new vendor)
Operational Processes An impact to the current operational processes 1. Service Level Management 2. Capacity Management 3. Change Management	1. Medium (possible to negotiate custom SLA with cloud provider) 2. Medium (additional tasks for IT resources allocation / de-allocation) 3. Medium (cloud provider gets involve to the Change Management)
CMDB 1. Requirements for the company's CMDB 2. CMDB deployment option(s) 3. Complexity to integrate cloud services with company's CMDB	1. Same as for the Private Cloud IT (on-premises) deployment model. Some private cloud providers offer cloud-compatible CMDB as a service, integration with company's CMDB might be easier. 2. On-premises / co-location at cloud provider site 3. Complexity - Medium (private cloud vendors allow the customization of the cloud environment, might be easier to purchase a commercial solution with build-in integration capabilities)
Risk Analysis Magnitude of the risks associated with 1. Privacy assurance 2. Compliance regulations 3. Cloud service provider	1. Medium (off-premises, single-tenant solution) 2. Medium (private cloud provider should be compliant to the local and international compliance regulations and privacy laws) 3. Medium (Risk assessment of the cloud service provider has to be done and business continuity plan ready for the possible risks)

As seen from Table 9, the evaluation criteria for the Private Cloud IT (off-premises) model are the same as for the Private Cloud IT (on-premises) deployment model. The evaluation criteria include eight categories, business requirements from the case company and seven elements of the operational model defined by the conceptual framework.

The Private Cloud IT (off-premises) deployment model does not fulfill the business requirements for the Cost Efficiency, Functional requirements and Security due to the specific characteristics of this deployment model, limitations to the integration capabili-

ties, security concerns for the use of the sensitive data off-premises, and high costs associated with the single-tenant cloud environment. The business requirements for the Agility and Reliability are fully fulfilled with the certain cloud providers.

A magnitude of change to the current *Organizational Structure* of the case company for the Private Cloud IT (off-premises) deployment model is *Medium*. Compare to the Private Cloud IT (on-premises) deployment model, additional competences are required for vendor management and integration with the off-premises cloud environment.

A magnitude of change to the current *IT Governance* of the case company for the Private Cloud IT (off-premises) deployment model is *Medium*. Compare to the Private Cloud IT (on-premises) deployment model, InfoSec governance should be extended additionally, as the company's data moves to off-premises. From the *Sourcing* perspective, the management of the physical IT infrastructure for cloud-based IT assets moves to the responsibility of the private cloud provider. The management of the software on top of the cloud-based IT infrastructure can be done by the private cloud provider or a new outsourcing vendor.

From the *Operational Processes* perspective, three ITSM operational processes are evaluation, namely *Service Level Management*, *Change Management* and *Capacity Management*. An impact to the Service Level Management, Capacity Management and Change Management by the cloud computing in the Private Cloud IT (off-premises) deployment model is *Medium*. The new SLAs should be defined with the private cloud provider and outsourcing vendor for the maintenance services. The private cloud providers are flexible in negotiation of the SLA, which supports the Service Level Management. Capacity Management no longer requires the management of the IT capacity for the company's Data Center extensively, but introduces additional tasks for IT resources allocation and de-allocation from the private cloud provider. The private cloud provider also gets involved to the Change Management which makes the Change Management more challenging.

The requirements for the company's CMDB in the Private Cloud IT (off-premises) model are the same as in the Private Cloud IT (on-premises) deployment model. The possible deployment options for the company's CMDB are on-premises and co-location at the private cloud provider site. The complexity for integration is *Medium* due to the medium customization capabilities of the off-premises private cloud environment. Some private cloud providers offer cloud-compatible CMDB product as a service, integration

between company's current CMDB solution and provider's CMDB product might be easier.

The magnitude of the risks associated with the Privacy Assurance, Compliance Regulations and Cloud Service Provider is *Medium.* The deployment of the cloud environment off-premises premises introduces new risks to the Privacy Assurance, Compliance regulations and Cloud Service Provider. The private cloud providers offer single-tenant cloud environment and allow implementation of the access controls. The risk analysis should be done for the private cloud provider and business continuity plan ready for the possible risks.

Summing up, the Private Cloud IT (off-premises) deployment model fulfills two out of the five business requirements of the case company. It makes a medium impact to the company's current working practices and has medium risks associated with the Privacy Assurance, Compliance Regulations and Cloud Service Provider. Additionally, the company's CMDB might be synchronized with the private cloud provider's CMDB solution, which makes the integration of the company's CMDB with the cloud-based IT assets easier. The detailed evaluation of the Private Cloud IT (off-premises) deployment model is available in the Appendix 6.

5.1.3 Public Cloud IT

The third operational option available for the case company is Public Cloud IT deployment model. The cloud computing environment in this model is deployed on the public cloud provider's premises and IT hardware belongs to the cloud provider. The public cloud provider loans the cloud-based IT assets to the customers for certain period of time. The cloud-based IT assets are typically shared between multiple customers and available for the public use. The detailed description of the Public Cloud IT deployment model can be found from Section 4.2.3. Specific characteristics, benefits and challenges of the Public Cloud IT deployment model that support the evaluation are summarized in Appendix 4 (Table 1). The evaluation results of the Public Cloud IT deployment model are presented in Table 10 below.

Table 10. Evaluation of the Public Cloud IT Operational Model.

TO BE CONSIDERED	IT OPERATIONAL MODEL Public Cloud IT
Business requirements from case company 1. Cost efficiency 2. Agility 3. Functional requirements 4. Reliability 5. Security	1. Fulfill partly (cost of the service is low - multi-tenant solution, out coming data traffic from cloud provider is costly) 2. Fulfill 3. Fulfill partly (integration requirements) 4. Fulfill 5. Fulfill partly (case company has limited control over the data)
ELEMENTS OF OPERATIONAL MODEL **Organizational Structure** Magnitude of change to the current Organizational Structure - Small - Medium - Large	**Medium** 1. New competences and roles are required 2. Additional competences are required for the integration with the off-premises cloud environment 3. Vendor management
IT Governance Magnitude of change to the current IT Governance - Small - Medium - Large	**High** 1. InfoSec governance should be extended (multi-tenant environment) 2. Limitations in SLA, more controls need to be in place 3. Updates to the policies and documentation
Sourcing (cloud-based IT assets) 1. Option(s) for management of the physical IT infrastructure 2. Option(s) for management of the software	1. cloud service provider 2. 3rd party (new vendor)
Operational Processes An impact to the current operational processes 1. Service Level Management 2. Capacity Management 3. Change Management	1. Medium (difficult to negotiate custom SLA with cloud provider) 2. Medium (additional tasks for IT resources allocation / de-allocation) 3. Medium (cloud provider gets involve to the Change Management)
CMDB 1. Requirements for the company's CMDB 2. CMDB deployment option(s) 3. Complexity to integrate cloud services with company's CMDB	1. Same as for the Private Cloud IT (on-premises) deployment model. 2. On-premises 3. Complicity - Medium (limited customization of the cloud environment, but full featured API interface. Might be easier to purchase a commercial solution with build-in integration capabilities)
Risk Analysis Magnitude of the risks associated with 1. Privacy assurance 2. Compliance regulations 3. Cloud service provider	1. High (off-premises, multi-tenant solution, available to the public use) 2. High (public cloud provider might not be compliant to the local compliance regulations and privacy laws) 3. Medium (Risk assessment of the cloud service provider has to be done and business continuity plan ready for the possible risks)

As seen from Table 10, the evaluation criteria for the Public Cloud IT model are the same as for the previously discussed deployment models. The evaluation criteria include eight categories, business requirements from the case company and seven elements of the operational model defined by the conceptual framework.

The Public Cloud IT deployment model does not fulfill the business requirements for the Cost Efficiency, Functional requirements and Security due to the specific characteristics of this deployment model, limitations to the integration capabilities, security concerns for the use of the sensitive data off-premises, and costs associated with the out

coming data traffic from the cloud provider. For the purposes where high amount of out coming data traffic is not needed, the price per hour is lowest among the deployment models. The business requirements for the Agility and Reliability are fully fulfilled.

A magnitude of change to the current *Organizational Structure* of the case company for the Public Cloud IT deployment model is *Medium*. The required competences and additional roles are the same as for the Private Cloud IT (off-premises) deployment model.

A magnitude of change to the current *IT Governance* of the case company for the Public Cloud IT deployment model is *High*. IT Governance for Public Cloud IT deployment model should define the suitable use cases for the cloud services, due to the limitations in the pre-defined SLAs of the public cloud providers. Additionally, the InfoSec governance should be extended, as the company's data moves to the multi-tenant and available to the public use environment off-premises. From the *Sourcing* perspective, the management of the physical IT infrastructure for cloud-based IT assets moves to the responsibility of the public cloud provider. The management of the software on top of the cloud-based IT infrastructure proposed to the new outsourcing vendor, as the public cloud providers do not offer such service.

From the *Operational Processes* perspective, three ITSM operational processes are evaluated, namely *Service Level Management*, *Change Management* and *Capacity Management*. An impact to the Service Level Management, Capacity Management and Change Management by the cloud computing in the Public Cloud IT deployment model is *Medium*. The new SLA is challenging or impossible to negotiate with the public cloud provider, as the public cloud providers typically offer pre-defined SLA to their customers. Capacity Management no longer requires the management of the IT capacity for the company's Data Center extensively, although introduces additional tasks for IT resources allocation and de-allocation from the public cloud provider. The public cloud provider also gets involved to the Change Management which makes the Change Management more challenging.

The requirements for the company's CMDB in the Public Cloud IT model are the same as in the Private Cloud IT (on-premises) deployment model. The proposed deployment option for the company's CMDB is on-premises, although the cloud-based option also available. The complexity for integration is Medium. Public cloud providers limit the customization of the cloud environment, but offer full featured API interface for custom integration.

The magnitude of the risks associated with the Privacy Assurance, Compliance Regulations can be evaluated as *High,* and for the Cloud Service Provider as *Medium*. The Public Cloud IT model has the *highest* risks for Privacy Assurance, as it represents the multi-tenant environment which is available to the public use through the Internet. The public cloud providers operate internationally and might not be compliant with the local compliance regulations and privacy laws. The risk analysis should be done for the public cloud provider and business continuity plan ready for the possible risks.

Summing up, the Public Cloud IT deployment model fulfills two out of the five business requirements of the case company. It makes a *medium* to *high* impact to the company's current working practices and poses *high* risks associated with the Privacy Assurance and Compliance Regulations. The detailed evaluation of the Public Cloud IT deployment model is available in the Appendix 7.

5.1.4 Hybrid Cloud IT

The fourth and last option available for the case company is the Hybrid Cloud IT deployment model. The Hybrid Cloud IT deployment model is a mixture of the three deployment models, namely the Private Cloud IT (off-premises), Private Cloud IT (on-premises) and Public Cloud IT. The detailed description of the Hybrid Cloud IT deployment model can be found from Section 4.2.4. Specific characteristics, benefits and challenges of the Hybrid Cloud IT deployment model that support this evaluation are summarized in Appendix 4 (Table 1).

Generally speaking, Hybrid Cloud IT deployment model combines the benefits of all deployment models, but at the same time it has specific challenges. One of the main challenges corresponds to the proper segregation of the workloads between the different deployment models. The segregation of the workloads must take into account the company's data characteristics defined by Information security, such as confidentiality, integrity and availability. The evaluation results of the Hybrid Cloud IT deployment model are presented in Table 11 below.

Table 11. Evaluation of the Hybrid Cloud IT Operational Model.

TO BE CONSIDERED	IT OPERATIONAL MODEL Hybrid Cloud IT
Business requirements from case company 1. Cost efficiency 2. Agility 3. Functional requirements 4. Reliability 5. Security	1. Fulfill partly (cost of the service is average - own Data Center, integration and management costs) 2. Fulfill 3. Fulfill 4. Fulfill 5. Fulfill
ELEMENTS OF OPERATIONAL MODEL **Organizational Structure** Magnitude of change to the current Organizational Structure - Small - Medium - Large	**High** 1. New competences and roles are required 2. Additional competences are required for the integration with the off-premises cloud environments 3. Vendors management
IT Governance Magnitude of change to the current IT Governance - Small - Medium - Large	**High** 1. InfoSec governance should be extended (multiple cloud providers) 2. Limitations in SLA, additional controls need to be in place 3. Updates to the policies and documentation
Sourcing (cloud-based IT assets) 1. Option(s) for management of the physical IT infrastructure 2. Option(s) for management of the software	1. cloud service providers & 3rd party (current vendor) 2. 3rd party (new vendor)
Operational Processes An impact to the current operational processes 1. Service Level Management 2. Capacity Management 3. Change Management	1. High (management of the multiple cloud providers) 2. High (management of the multiple cloud providers) 3. High (cloud providers gets involve to the Change Management)
CMDB 1. Requirements for the company's CMDB 2. CMDB deployment option(s) 3. Complexity to integrate cloud services with company's CMDB	1. Same as for the Private Cloud IT (on-premises) deployment model. 2. On-premises 3. Complexity - High (multiple cloud providers, might be easier to purchase a commercial solution with build-in integration capabilities)
Risk Analysis Magnitude of the risks associated with 1. Privacy assurance 2. Compliance regulations 3. Cloud service provider	1. Small (company's data and workloads should be properly segregated between the different deployment models) 2. Small (same as for the Privacy Assurance risks) 3. Medium (Risk assessment of the cloud providers has to be done and business continuity plan ready for the possible risks)

As seen from Table 11, the evaluation criteria for the Hybrid Cloud IT model are the same as for the previously discussed deployment models. The evaluation criteria include eight categories, business requirements from the case company and seven elements of the operational model defined by the conceptual framework.

The Hybrid Cloud IT deployment model does not fulfill the business requirements for the Cost Efficiency. The case company continues to own the Data Center which is expensive. Additionally, the integration and management of the multiple cloud environments are costly. However the proper segregation of the workloads between the cloud

environments can decrease the operational expenses. The business requirements for the Agility, Functional Requirements, Reliability and Security are fully fulfilled.

A magnitude of change to the current *Organizational Structure* of the case company for the Hybrid Cloud IT deployment model is *High.* The required competences and additional roles are the same as for the Private Cloud IT (off-premises) deployment model. Additionally, the management of the multiple deployment models requires additional competences.

A magnitude of change to the current *IT Governance* of the case company for the Hybrid Cloud IT deployment model is *High.* The IT Governance should cover all aspects of the different deployment models. From the *Sourcing* perspective, the management of the physical IT infrastructure for the company's Data Center remains to be done by the current outsourcing vendor. The management of the physical IT infrastructure for the cloud-based IT assets moves to the private and public cloud providers. The management of the software on top of the cloud-based IT assets proposed to the new outsourcing vendor.

From the *Operational Processes* perspective, three ITSM operational processes are evaluated, namely *Service Level Management*, *Change Management* and *Capacity Management*. An impact to the Service Level Management, Capacity Management and Change Management by the cloud computing in the Hybrid Cloud IT model is *High.* The SLAs with the multiple cloud providers and software maintenance vendor should be negotiated, defined and managed. For public cloud providers SLA should be properly assessed and managed. The Capacity Management becomes more complex in order to manage IT capacity located at the multiple cloud providers. The Change Management becomes extremely challenging, as the multiple cloud providers get involved to the Change Management process.

The requirements for the company's CMDB in the Hybrid Cloud IT model are the same as in the Private Cloud IT (on-premises) deployment model. The proposed deployment option for the company's CMDB is on-premises, as the case company continues to own the Data Center. The complexity for integration is *High*, due to the required integration with the multiple cloud environments. In the Hybrid cloud scenario, a new commercial CMDB product which is compatible to work with the various cloud environments might be the best choice for the case company.

The magnitude of the risks associated with the Privacy Assurance and Compliance Regulations can be evaluated as *Small*, and for the Cloud Service Provider as *Medium.* The proper segregation of the company's data and workloads between the different deployment models makes possible to decrease the risks for the Privacy Assurance and Compliance Regulations to Small. The risk analysis should be done for the cloud providers and business continuity plan ready for the Cloud Service Provider's risks.

Summing up, the Hybrid Cloud IT deployment model fulfills four out of the five business requirements of the case company. It makes a *high* impact on the company's current working practices, has small risks associated with the Privacy Assurance and Compliance Regulations and has medium risks for the Cloud Service Provider. The detailed evaluation of the Hybrid Cloud IT deployment model is available in the Appendix 8. The following section compares the previously described deployment models with the help of the current state analysis and consultations with the case company representatives.

5.2 Evaluation of the Choices

In the previous section, four cloud deployment models were evaluated against the case company operational context and requirements. The evaluation results of the cloud deployment models are combined into the table to show the comparison of the cloud deployment modes and select the best suitable cloud deployment model for the case company. The evaluation results, summarized in Table 12 below, are presented following the system of "traffic lights" (*high - medium - low*) for better visibility in the comparison and selection. The detailed evaluations of the deployment models can be found in Appendixes 5,6,7,8.

Table 12. Comparison of the cloud deployment models.

TO BE CONSIDERED	CLOUD DEPLOYMENT MODELS			
	Private Cloud IT (on-premises)	Private Cloud IT (off-premises)	Public Cloud IT	Hybrid Cloud IT
Business requirements from the case company 1. Cost efficiency 2. Agility 3. Functional requirements 4. Reliability 5. Security	1. Fulfill partly (cost is high) 2. Fulfill partly 3. Fulfill partly 4. Fulfill partly 5. Fulfill	1. Fulfill partly (cost is high) 2. Fulfill 3. Fulfill partly 4. Fulfill 5. Fulfill partly	1. Fulfill (cost is average) 2. Fulfill 3. Fulfill partly 4. Fulfill 5. Fulfill partly	1. Fulfill partly (cost is average) 2. Fulfill 3. Fulfill 4. Fulfill 5. Fulfill
ELEMENTS OF OPERATIONAL MODEL				
Organizational Structure Magnitude of change to the current Organizational Structure - Small - Medium - Large	Small	Medium	Medium	High
IT Governance Magnitude of change to the current IT Governance - Small - Medium - Large	Small	Medium	High	High
Sourcing (cloud-based IT assets) 1. Option(s) for management of the physical IT infrastructure 2. Option(s) for management of the software	1. 3rd party (current vendor) 2. 3rd party (new vendor)	1. Cloud service provider 2. Cloud service provider or 3rd party (new vendor)	1. Cloud service provider 2. 3rd party (new vendor)	1. 3rd party (current vendor) and Cloud service provider(s) 2. 3rd party (new vendor)
Operational Processes An impact to the current operational processes 1. Service Level Management 2. Capacity Management 3. Change Management	1. Small 2. High 3. Small	1. Medium 2. Medium 3. Medium	1. Medium 2. Medium 3. Medium	1. High 2. High 3. High
CMDB 1. Requirements for the company's CMDB 2. CMDB deployment option(s) 3. Complexity to integrate cloud services with the company's CMDB	1. "Real-Time IT service model" support. CMDB should have performance and functional capabilities for near real-time data management, and capabilities for integration with the selected cloud environment 2. On-premises 3. Complexity - Medium	1. Same as for the Private Cloud IT (on-premises) Possible to integrate company's CMDB with the private cloud provider's CMDB 2. On-premises or co-location at the private cloud provider's site 3. Complexity - Medium	1. Same as for the Private Cloud IT (on-premises) 2. On-premises 3. Complexity - Medium	1. Same as for the Private Cloud IT (on-premises) 2. On-premises 3. Complexity - High
Risk Analysis Magnitude of the risks associated with 1. Privacy assurance 2. Compliance regulations 3. Cloud service provider	1. Small 2. Same as with tradition model 3. Small	1. Medium 2. Medium 3. Medium	1. High 2. High 3. Medium	1. Small 2. Small 3. Medium
	Choice 1	**Choice 2**		**Choice 3**

As seen from Table 12, the selection among the four deployment models, namely Private Cloud IT (on-premises), Private Cloud IT (off-premises), Public Cloud IT and Hybrid Cloud IT, is based on the combination of the following prioritized criteria: a) fulfillment of the business requirements (as much as possible), b) the lowest possible risks associated with Privacy Assurance, Compliance Regulations and Cloud Service Provider, c) the impact of the cloud computing on the Organizational Structure, IT Governance and Operational Processes (as low as possible), d) CMDB integration with the cloud-based IT assets (as less complex as possible). (Table 2A, 2B)

First, the Private Cloud IT (on-premises) deployment model has the worst evaluation results for the business requirements. However, the actual number of missing capabilities is low and might be acceptable by the case company. The missing capabilities of the Private Cloud IT (off-premises) deployment model are the limitations to the available hardware resources of the case company, no data replication between at least two data centers and no auto-scaling of the cloud services. Based on the other evaluation categories, the Private Cloud IT (on-premises) deployment model would be the first choice for the selection. (Table 2A, 2B) (Appendix 5)

Second, the Private Cloud IT (off-premises) deployment model has the medium evaluation results for the business requirements. This deployment model does not have the auto-scaling of the cloud services. Additionally, the company's data security policies limit the use of Private Cloud IT (off-premises) model for storing and processing sensitive data. The risks associated with Privacy Assurance, Compliance Regulations and Cloud Service Provider are higher compared to the Private Cloud IT (on-premises) and Hybrid Cloud IT modes, but lower compare to the Public Cloud IT model. The other evaluation results are worse compared to the Private Cloud IT (on-premises) model, but better compared to the other deployment models. Thus, the Private Cloud IT (off-premises) model would be the second choice for the selection.(Table 2A, 2B) (Appendix 6)

Third, the Public Cloud IT deployment model has similar evaluation results as the Private Cloud IT (off-premises) model. The Cost Efficiency is affected by the extra costs for the out coming data traffic from the public cloud provider. The functional requirements affected by the limited connectivity options since some public cloud providers do not offer the MPLS connection. The high risks associated with the Privacy Assurance and Compliance Regulations limit the use of the Public Cloud IT model by the case company, as only non-sensitive or low-sensitive data might be used in this deployment

model. Additionally, the Public Cloud IT model has some unique capabilities like auto-scaling of the cloud services, high scalability, innovativeness and others. These capabilities might be utilized by the case company without the explicit selection of the Public Cloud IT model and integration with the company's legacy environment. Thus, the Public Cloud IT deployment model cannot be chosen due to the limited number of use cases for the case company. (Table 2 A, B) (Appendix 7)

Fourth, the Hybrid Cloud IT deployment model fulfills most of the business requirements and has low risks associated with the Privacy Assurance and Compliance Regulations, as it combines the benefits of the all deployment models. An impact of the cloud computing to the Organizational Structure, IT Governance and Operational processes for the Hybrid deployment model is the highest compared to other deployment models. Since the Hybrid Cloud IT model represents a heterogeneous environment, management of the multiple cloud environments becomes a complex task for the IT organization. Additionally, the integration of the company's CMDB with the several cloud environments requires a lot of efforts and expertise. Thus, the Hybrid Cloud IT deployment might be the third choice for the selection and a target for the future.
(Table 2 A, 2B) (Appendix 8)

Summing up, four cloud deployment models were compared and three of them were proposed as a possible selection in the following order. First choice would be the Private Cloud IT (on-premises) deployment model, the second choice would be the Private Cloud IT (off-premises) deployment model, and the third choice would be the Hybrid Cloud IT deployment model.

However, considering the options of the case company realistically, the best suitable cloud deployment model for the case company could be a combination of the Private Cloud IT (on-premises) and Private Cloud IT (off-premises) deployment models, in other words *the Hybrid Cloud IT deployment model without Public Cloud IT option*. This model combines the benefits of the two deployment models and requires fewer efforts for the deployment, integration and management compare to the full Hybrid Cloud IT deployment model. The Public Cloud IT deployment model might be utilized by the case company separately, without the integration with the legacy IT Infrastructure environment. The following section describes the operational model proposal to the case company in detail.

5.3 Operational Model Proposal to the Case Company

The operational model proposal to the case company is made of: a) evaluation of recommended deployment model, b) evaluation of meting business requirements, and 3) evaluation of the challenges for each element of the operational model in this choice.

Recommended deployment model

The recommended deployment model consists of for a combination of *two deployment models*, *Private Cloud IT (on-premises) and Private Cloud IT (off-premises)*. This combination of the deployment models has evident benefits for the case company and the challenges that need to be addressed, as summarized in Table 13.

Table 13. Benefits and Challenges of the proposed deployment model against other models.

Benefits	**Challenges**
- Decreased capital investments for the case company - Full control over the data and process on-premises - Both single-tenant and multi-tenant options from private cloud provider allow to decrease the overall costs - Customization capabilities of the cloud environment off-premises and negotiable SLAs - Excellent quality management, security and reliability for on-premises cloud environment - Procurement process of the case company can be optimized to manage the customer demands	- Segregation of the workloads and data between the Private Cloud IT(on-premises) and Private Cloud IT (off-premises), single-tenant and multi-tenant environments - Risks associated with cloud provider, privacy assurance and compliance regulations should be assessed and mitigated - MPLS connectivity to the private cloud provider is needed

As seen from Table 13, the case company can utilize the available private provider's IT capacity in order to balance the fluctuated demands of the internal customers and decrease the capital investments for the own Data Center. Additionally, a procurement process for the company's own Data Center can be optimized since the IT hardware might be ordered and waited while using the IT capacity from the private cloud provider located off-premises. The full control over the data and process on-premises allows the case company to manage the business critical tasks with excellent quality management, security and reliability.

Based on the findings, the case company can be recommended to utilize single-tenant and multi-tenant options from the private cloud provider located off-premises in order to decrease the overall costs, although a segregation of the workloads and data between the deployment options is challenging. The customization capabilities of the cloud environment off-premises support the integration with the legacy system and on-premises cloud environment. The SLA should be negotiated with the private cloud provider in order to mitigate the risks associated with the privacy assurance, compliance regulation and cloud service provider. Additionally, the risk analysis of the private cloud provider should be done. The private cloud provider with MPLS connectivity should be selected in order to fulfill the business requirements of the case company.

Fulfillment of business requirements

If summarized, the fulfillment of business requirements in the proposed deployment model can be evaluated as shown in Table 14 below.

Table 14. Evaluation of the proposed deployment model vs business requirements.

Business requirements	**Results of the analysis**
Cost efficiency	**Partly fulfils** - Price per hour is high ○ management and ownership of the Data Center is costly ○ single-tenant option from cloud provider is expensive
Agility	**Fully fulfils** - Some private cloud providers don't fully fulfil the requirements ○ private cloud provider should be properly evaluated
Functional Requirements	**Fulfils (almost)** - Auto-scaling of the cloud services unavailable - Scalability not as high as in the Public Cloud
Reliability	**Fully fulfils** - MPLS connectivity to the private cloud provider is required - Single-tenant cloud environment is used for critical workloads
Security	**Fully fulfils** - Security controls have to be in place for the off-premises cloud environment - Data and workloads segregation between the deployment options is required

As seen from Table 14, the proposed deployment model fulfills the business requirements from the case company for Agility, Reliability and Security. The involvement of the Private Cloud IT (off-premises) deployment model significantly improves the Agility for the IT capacity management. Functional requirements are almost fulfilled, except

the auto-scaling of the cloud services is not available for the proposed deployment models. The Cost Efficiency is not significantly better compare to the current IT service provision, but the multi-tenancy and self-service make the overall price per hour acceptable by the end users.

Challenges for the six elements of the operational model

a) *Changes to the Organizational Structure*

Changes to the Organizational Structure are evaluated following the logic Oredo et al. (2014). He argues that the cloud computing requires from the IT organization some general competences and competences specific to the off-premises cloud environment. Therefore, to demonstrate the changes to the Organizational Structure, first, the general cloud related competences required from the new IT organization (as recommended by Oredo et al. 2014: 157) are evaluated. These challenges are summarized in Table 15 below.

Table 15. The challenges of the cloud computing for the IT organization.

(1) Changes to the Organizational Structure	
Cloud related competences required	**Challenges**
General	- Availability and reliability of the cloud services - Transition and execution activities with the cloud services - Portability and interoperability - Cultural resistance to changes in the IT organization
Specific for the off-premises environment	- Security and privacy concerns - Vendor management o evaluation of the cloud service providers o negotiation and maintenance of the SLAs o integration of the cloud service providers to the company's processes

As seen from Table 15, the cloud computing requires new competences specific to the off-premises cloud environment. *Availability and Reliability* of the cloud services mean that a disaster management process needs to take into account the cloud capabilities, SLA with the cloud service provider should be properly defined (with availability and performance guarantees). *Transition and execution activities* mean the ability to understand the different cloud environments (on-premises, off-premises, single-tenant and multi-tenant) and segregate the workloads between them by the personnel. *Portability* and interoperability of the IT services mean the competences for the integration of the cloud environment with the legacy system, as well as the portability of the existing IT

services from the legacy system to the cloud environment. *Cultural resistance* to the changes in the IT organization means that the IT department personnel should be able to see the opportunities in the changes by the cloud computing with the help of the trainings and competence development activities. *Security and privacy* concerns require competences for the configuration and management of the cloud environments. *Vendor management* includes assessing the cloud service providers, negotiating and maintaining the SLAs, as well as incorporating the cloud service provider into the company's IT service delivery process (developed from Oredo et al. 2014: 157). Additionally, new cloud technology skills are required from the IT service development teams.

Changes to the Organizational Structure also include changes to the roles affected by the cloud computing. Changes to the roles in the IT organization are shown in Table 16.

Table 16. The current roles affected by the cloud computing and new proposed roles.

(1) **Changes to the Organizational Structure**	
Changes to the roles	**Details**
The current roles affected by the cloud computing	- Security and Compliance Manager o Security and privacy concerns - Provisioning Manager o Availability and reliability of the cloud services - Vendor Manager o Vendor management - Training Manager o Cultural resistance to changes in the IT organization - Capacity Planner (becomes a Cloud Analyst) o Transition and execution activities with the cloud services - IT Infrastructure Architect (becomes a Cloud Architect) o Portability and interoperability
The new roles proposed	- Cloud Administrator - Cloud Developer(s)
A MAGNITUDE OF CHANGE	**MEDIUM / HIGH** amount of changes

As seen from Table 16, the roles affected by the cloud computing come from the challenges of the cloud computing for the IT organization. Additionally, two new roles are proposed, Cloud Administrator and Cloud Developer(s). Cloud Administrator should be responsible for the overall cloud infrastructure and management of the cloud environment. The cloud developers should implement all possible cloud integrations with the

legacy applications and develop automation workflows as suggest by Lees. (2012: 12) These new roles might be outsourced to the third party outsourcing vendor, which will manage the software on top of the cloud-based IT assets. A Magnitude of change to the current IT organization is defined as *Medium* to *High.*

b) Changes to IT Governance

Changes to the current IT Governance which come with the new Hybrid deployment model are summarized in Table 17 below.

Table 17. Changes to the IT Governance.

(2) **Changes to IT Governance**	
Changes	**Details**

General	- New roles and responsibilities
	- New methods how to measure the performance of the cloud-based IT services
	- New approach how to resolve any issues related to the cloud-based IT services
	- A self-service attribute of the cloud computing
	  ○ set of clear policies to the end-users
	  ○ organized trainings to the end-users
	  ○ built-in policies to the automation process

Specific for the off-premises environment	- InfoSec governance has to be extended
	  ○ security policies should define which workload or company's data might be stored or managed off-premises
	  ○ access controls have to be implemented in order to support the security policies

OUTCOME	**MEDIUM** amount of changes

As seen from Table 17, the general changes to the IT Governance will affect to the roles and responsibility, some functional activities and company documentation. Additionally, new built-in policies to the automation process should be implemented in order to support the governance of the cloud-based IT assets. The current structure of the IT Governance, described in the CSA, will remain the same and the decisions will be done within the Customer Co-operation board for the IT infrastructure. (Table 2 B) In addition to the general changes to the IT Governance, the security policies should define what workloads and company's data might be used off-premises.

c) Changes to Sourcing Options

Changes to the sourcing options for the management of the physical IT infrastructure and software on top of the cloud-based IT assets are summarized in Table 18 below.

Table 18. Sourcing options for the case company.

(3) **Changes to Sourcing Options**	
Sourcing Options	**Details**
Management of the physical IT infrastructure	- The current third party outsourcing vendor proposed for the management of the physical IT infrastructure and software on the legacy system
	- The management of the physical IT infrastructure for the off-premises IT assets moves to the responsibility of the private cloud provider
Management of the software on top of the cloud-based IT assets	- A new third party outsourcing vendor is proposed

As seen from Table 18, a private cloud provider will take a responsibility for the management of the IT infrastructure located off-premises and new third party outsourcing vendor is proposed for the management of the software on top of the cloud-based IT assets. The technical tasks for the cloud environments also will be done by the new third party outsourcing vendor. The practices from the strategic sourcing are applicable to the selection of the suppliers. The best suppliers should be located, compared, qualified and employed in accordance to the business requirements and justified price. (Section 4) The sourcing structure of the case company will remain the same and new service level agreements (SLAs) will be defined between the Corporate IT Services Infrastructure Team and the new selected suppliers. The provision of the cloud-services for the company's internal customers will be consolidated by the Corporate IT Services Infrastructure Team. Additionally, Corporate IT Services Infrastructure Team should provide the guidelines to the company's divisions for the use of the services from the public cloud providers, if the unique capabilities of these providers are demanded.

d) Changes to the Operational (ITSM) Processes

Changes to the three ITSM operational processes are summarized in Table 19 below.

Table 19. Three ITSM operational processes affected by the cloud computing.

(4) Changes to the Operational (ITSM) Processes	
ITSM Processes	**Details**
Service Level Management	- New SLA with for the management of the physical IT infrastructure has to be negotiated and defined - New SLA has to be defined with the new third party outsourcing vendor for the management of software on top of the cloud-based IT assets (on-premises, off-premises) - Monitor the IT service for the verification of the requirements defined in SLAs - Make changes to the SLAs during the IT service lifecycle (private cloud provider, new third party outsourcing vendor)
OUTCOME	**MEDIUM / HIGH** amount of changes
Capacity Management	- Legacy tasks (Capacity planning, Procurement of the hardware resources) - Cloud related tasks ○ Understanding of the performance data and limitations of the cloud-based IT assets ○ Understanding the costs associated with the resource allocation from the private cloud provider (off-premises) in order to plan for the IT capacity ○ Removing excess capacity ○ Management of the services built on top of the cloud-based IT assets ○ Partial management of the cloud environment(s)
OUTCOME	**MEDIUM / HIGH** amount of changes
Change Management	- Cloud related tasks (general) : ○ manage high number of changes ○ adapt to the shorter time frames ○ changes are stored to the company's CMDB (CMDB integration with cloud-based IT assets is required) - Cloud related tasks (off-premises) : ○ Private cloud provider specific procedures have to be taken into account ○ Support options have to be available to the customer from private cloud provider (to resolve any issues that might occur in the Change Management process)
OUTCOME	**MEDIUM** amount of changes

In Table 13, first, an impact of the cloud computing for selected Hybrid deployment model on the Service Level Management is reviewed. The case company should negotiate and define the Service Level Agreements with cloud service provider and new third party outsourcing vendor. SLA should include the penalties for the possible ser-

vice delivery failures that satisfy the case company. Mission critical applications should be deployed on-premises, so the case company has some flexibility in the negotiation of the SLA with private cloud provider. Private cloud providers are also flexible in the negotiation of the SLA and consensus could be found. The case company should establish the practices to monitor the cloud-based IT services for the verification of the requirements defined in SLAs. If the changes are required to the SLAs for some IT services, the case company might negotiate the new SLAs or move affected IT services from the private cloud provider's site to on-premises. An impact to the Service Level Management is defined as Medium to High.

Second, an impact of the cloud computing for selected Hybrid deployment model on the Capacity Management is reviewed. The case company continues to manage the tasks related to the legacy environment, such as Capacity planning and procurement of the IT hardware resources. The use of the IT capacity from the private cloud provider while waiting for the ordered IT hardware resources significantly speed-ups the internal Capacity Management process. The Capacity Management personnel should be able to understand the performance data and limitations of the cloud-based IT assets, as well as the costs associated with the resource allocation. The Capacity Management also should concentrate on the management of the services built on top of the cloud-based IT assets, especially in the measuring of their performance. On the contrary, a self-service in the cloud environment and properly implemented automation should reduce the amount of efforts from the Capacity Management personnel. The possible structural changes to the Capacity Management process are discussed in the Section 3. An impact to the Service Level Management is defined as Medium to High.

Third, an impact of the cloud computing for selected Hybrid deployment model on the Change Management is reviewed. The case company should manage high amount of changes and adapt to the short time frames for the change implementations. A self-service in the cloud environment and properly implemented automation should support the Change Management process in these tasks. The changes also should be recorded to the company's CMDB in order to make the Change Management process functional. For the off-premises cloud environment, the cloud provider specific procedures, such as maintenance windows or limitations of the cloud environment should be considered, and support options need to be available to the customer. (Possible structural changes to the Change Management process were mentioned in Section 3). An impact to the Change Management is defined as *Medium.*

e) Changes to CMDB of the case company

Changes to *CMDB of the case company* are summarized in Table 20. These changes include recommendation of best suitable deployment option for company's CMDB and integration complexity evaluation of company's CMDB with the cloud-based IT assets.

Table 20. Recommendations for the CMDB integration with the cloud-based IT assets.

(5) Changes to CMDB of the case company	
CMDB integration with cloud-based IT assets	**Details**
Requirements for the company's CMDB - The analysis of the current company's CMDB has to be done	- CMDB should support "Real-time IT service model" o Real-time IT service model describes an IT service at any moment of time during the execution - CMDB should have performance and functional capabilities for near real-time data management - CMDB should have the capabilities for an integration with the selected cloud environment(s) and possible future integrations with the public cloud providers.
Deployment option	- On-premises (company continues to own the Data Center)
Integration complexity with cloud-based IT assets **Medium**	- The private cloud providers offer full customization for the cloud environment (on-premises) and limited customization for the cloud environment (off-premises) - Some private cloud providers offer cloud-compatible CMDB product as a service which can be synchronized with the current company's CMDB - Alternatively, a new commercial cloud-compatible CMDB product has to be selected and taken into use

As seen from Table 20, the company's CMDB should have specific capabilities in order to work with the cloud services. The current company's CMDB does not have these capabilities and might not be capable to support these capabilities with modifications. An assessment of the current company's CMDB should provide information about the feasibility of these modifications.

In this thesis, two questions have been asked from the researcher by the IT infrastructure management team to support IT decision-making. First, what is *the best suitable deployment option* for cloud environment (on-premises or off-premises). Second, *how complex an effort could be to integrate the company's internal CMDB with the cloud environment(s)*. To address the first question, the best deployment option for the company's CMDB is on-premises, as the case company continues to own the Data Center

and CMDB is very valuable asset. Regarding the second question, as believed by the Curtis and Colville (2011: 3, 4), integration between the cloud environments and CMDB is possible due to a standardized cloud architecture. Cloud environments use specific technologies, limited set of hardware and software, and standard delivery mechanisms. Therefore, in this proposal, an integration complexity of the company's CMDB with the cloud-based IT assets is defined as *Medium*. The on-premises cloud environment can be fully customized and private cloud providers offer some limited customization to their cloud environment, which supports the integration. Although, the easiest way for the integration would be to use the cloud compatible CMDB solution at the private cloud provider's site and synchronize the current company's CMDB with that particular solution.

Alternatively, if the case company is willing to integrate the public cloud deployment model into the operational model later on, a new commercial cloud compatible CMDB solution could be recommended to be selected. In that case, the case company has two choices. First, the case company should select a CMDB solution which supports multiple cloud platforms. Second, the case company should make strategic choice to the direction of the particular cloud (technology) platform. The CMDB solutions which support a particular cloud (technology) platform, unfortunately, create vendor or technology lock-in situation for the customer. At the other side, the CMDB solutions supporting multiple cloud technologies are often not mature enough to fulfill the customer's requirements.

a) Risk Analysis of the proposed Hybrid deployment model

The last element of the proposed operational model is *risk analysis*, which includes the cloud specific risks associated with Privacy Assurance, Compliance Regulations and Cloud Service Provider. These risks are summarized in Table 21 below.

Table 21. Summary of the Risk Analysis for the proposed operational model.

(6) Risk Analysis of the proposed Hybrid deployment model	
Risk Analysis (Cloud specific risks)	**Details**
Privacy Assurance	**Benefits of the proposed deployment model** - On-premises cloud environment ○ No risks over the data and control managed ○ Allows to establish all desired access controls and eliminate the risks to confidentiality, integrity and availability - Off-premises cloud environment ○ Private cloud providers allow customization of the cloud environment to some extent, which allows the companies to implemented proper access controls ○ Single-tenant and multi-tenant options have to be utilized in order to balance the costs and company's requirements
	Challenges of the proposed deployment model - Off-premises cloud environment ○ Limited control over the data and process ○ Risks regarding to the network connectivity have to be considered - Off-premises and on-premises cloud environment ○ Cloud environment has to be properly configured
Magnitude of the risks	**SMALL/MEDIUM**
Compliance Regulations	**Benefits of the proposed deployment model (on-premises)** - Full control over the sensitive data - Case company can follow the compliance regulations and privacy laws without dependency on the cloud service provider
	Challenges of the proposed deployment model (off-premises) - The case company has limited control over the data and process - The private cloud provider should be compliant to the compliance regulations and privacy laws in order to be used for storage and processing of the company's sensitive data - The company needs to plan for the possible new regulations that are coming directly to the cloud providers in future by the legal authorities
Magnitude of the risks	**SMALL/MEDIUM**

Cloud Service Provider	**Challenges of the proposed deployment model (off-premises)** - Cloud service providers depend on the partners that provide network connectivity, premises and other services ○ Risk analysis of the cloud provider partners should be done

	Recommendations
	- Cloud solution should be chosen from the respected and qualified cloud provider
	  ○ Cloud provider should provide support services and up-dates to the product in future
	  ○ Risk analysis of the cloud service provider should be done
	
	- Business continuity plan has to be in place for the case company
	
	- "Safest" cloud service providers
	  ○ cash-rich providers like Microsoft, IBM, etc
	  ○ providers with high expertise and technological advantages

Magnitude of the risks	**SMALL/MEDIUM**

As seen from Table 21, first, the risks associated with the Privacy Assurance can be evaluated as *Small* to *Medium.* The company's data and workloads should be properly segregated in order to keep the Privacy Assurance risks low. The on-premises cloud environment should be used for the business critical workloads and management of the sensitive data, less critical workloads and low sensitive data might use the single-tenant cloud environment located off-premises, and non-critical workloads and non-sensitive data might use multi-tenant cloud environment located off-premises. The proper access controls have to be implemented and deployed in order to reduce the possible risks to the confidentiality, integrity and availability of the company's data. Additionally, accountability has to be a part of the cloud access controls. All the actions of the individuals need to be logged and traceable. Finally, both on-premises and off-premises cloud environments should be properly configured and latest patches should be continuously installed in order to decrease the vulnerabilities of the environments.

Second, the risks associated with the Compliance Regulations can be evaluated as *Small* to *Medium*. Since the case company store and manage some company's data off-premises at the private cloud provider's site, a private cloud provider should be compliant to the compliance regulations and privacy laws that are applicable for that data in the country of IT assets residency. Additionally, a case company needs to plan for the possible new regulations that are coming directly to the private cloud provider in future by the legal authorities.

Finally, the risks associated with the Cloud Service Provider can be evaluated as *Small* to *Medium.* A proper risk analysis should be done for the private cloud provider and its partners, and for the provider of the cloud environment deployed on-premises. Additionally, the case company should regularly make the back-ups of the important company's data located off-premises to reduce the risks associated with the off-premises environment. A business continuity plan should also be developed in order to mitigate the possible risks associated with the Cloud Service Provider.

Summing up, the proposal for the case company includes the recommendation of *the Hybrid deployment model,* which mostly *meets the business requirements* set by the case company, and the evaluation of changes to each element in *the IT operational model* for the Hybrid cloud scenario. Based on these evaluations, the Hybrid Cloud IT deployment model requires some changes, especially visible in the Organizational Structure of the IT Infrastructure Team and IT Governance. These changes include: a) for the Organization Structure, the additional competences for the current roles and new cloud specific roles, b) to the IT Governance, a new approach how to manage the cloud services and what need to be considered. On top of them, Sourcing strategy needs to be re-defined for the management of the physical IT infrastructure and software, since the cloud computing makes a big impact on it. The Hybrid cloud scenario will also require the changes to the operational processes in the Service Level Management, Capacity Management and Change Management. Additionally, it will require the change in the CMDB to integrate the cloud-based IT assets. Finally, it also calls for specifying the risks identified in the Risk Analysis for the proposed operational model.

This proposal building included the feedback received from the company inbuilt in the evaluations. It was received when the model was finalized and was interwoven into the fabric of the proposal, along with other company input).

6 Conclusions

This section contains the summary of the study, practical implications for the proposed operational model and next possible steps for the future operational model development. It also contains the evaluation of the study by comparing the outcome with the initial research objective. Finally, validity and reliability of the study are discussed.

6.1 Summary

The main goals of this thesis were to explore the possible use of cloud computing by the case company IT infrastructure team and to propose the cloud service based operational model for applying the selected deployment model in the case company. A proposed model targeted to improve the business agility and cost efficiency of the case company.

The current state analysis (CSA) points to the five main categories of the business requirements for the cloud based IT Infrastructure services which arise from the case company context and based on the business requirements of the business units. The categories of the business requirements include the Cost Efficiency, Agility, Functional Requirements, Reliability and Security. The current state analysis also identifies the key elements necessary to be included in the case company operational model in order to provide IT services and meet the case company needs in the cloud scenario. These key elements are Organizational Structure, Governance, Sourcing, Operational processes, Configuration Management Database (CMDB) and Risk Analysis.

Based on the current state analysis, the focused search for existing knowledge and best practice is done. The focus is placed on exploring the four possible deployment models suitable for the case company, and the key elements in the related operation models. The evaluated cloud deployment models in this study are the Private Cloud IT (on-premises), Private Cloud IT (off-premises), Public Cloud IT and Hybrid Cloud IT. In each of these four models, the six elements identified as parts of the IT operational model in the CSA, are explored and discussed separately.

For building the operational model proposal tailored to the case company, an evaluation of the cloud deployment models is done with the help of the constructed conceptual framework and business requirements revealed in the CSA. The results of the elevations are summarized for each model which allows to compare them and select the one that suits best the requirements from the case company. The company feedback for the recommended model is interwoven in the proposal building stage.

Based on the evaluation and feedback from the management, the final choice of the operational model points to the combination of the Private Cloud IT (on-premises) and Private Cloud IT (off-premises) deployment models, in other words to the Hybrid Cloud IT deployment model. The proposed model combines the essential benefits of the two deployment models. It would also meet best the business requirements and significantly improves Business Agility and, to some extent, Cost Efficiency of the case company IT Infrastructure services. As an additional choice, the case company could also consider the use of the Public Cloud IT deployment model separately, if done without the integration to the information system.

The proposed the Hybrid Cloud IT deployment model requires some changes to the current IT operational model in the case company, first of all, changes the Organizational Structure of the IT Infrastructure Team and IT Governance. These changes include: a) for the Organization Structure, the additional competences for the current roles and new cloud specific roles, b) to the IT Governance, a new approach how to manage the cloud services and what need to be considered. In addition, Sourcing strategy needs to be re-defined for the management of the physical IT infrastructure and software, since the cloud computing makes a big impact on it. It includes the changes to the operational processes in the Service Level Management, Capacity Management and Change Management. Additionally, the Hybrid Cloud scenario requires for the change in the CMDB to integrate the cloud-based IT assets. Finally, it also calls for specifying the risks in the Risk Analysis for the operational model.

The proposed cloud service based operational model was presented to the management of the case company. (Table 3A) The feedback from the management was positive and case company is planning to employ the findings from the thesis in their practices.

6.2 Practical Implications and Next Steps

This study helps the management team to select among available cloud deployment models and provides detailed information for decision-makers on the possible implementation of cloud computing to the company's IT operations.

The next step, as soon as the cloud-based IT operational model is selected, is to provide guidelines for implementation of the chosen Hybrid Cloud IT deployment model. The case company needs to investigate particular technical solutions available on the market and develop detailed plans for the implementation. The implementation could

be divided into two parts: the deployment of the on-premises cloud environment and the integration of the off-premises cloud environment from the private cloud provider with on-premises cloud environment. Here the strategic decision is needed to select the cloud technology platform since the on-premises cloud environment needs to be compatible with the off-premises cloud environment. Alternatively, a third party integration technology could be used, but this choice would significantly increase the costs. The same concerns is that the selection of the CMDB product needs to support both environments and also legacy environment.

Another management concern may relate to segregation of the data and workloads between the on-premises and off-premises cloud environments. Such segregation could be based on the criticality of the workload and data characteristics. The data characteristics, currently used by the case company, are applicable, such as confidentiality, integrity and availability. In order to define which data or workload can be used off-premises and which should stay on-premises, a broader analysis of the case company's IT software assets needs to be conducted.

As for the future steps, the case company might also investigate a possibility to move the IT hardware assets from own Data Center to a co-location facility of the private cloud provider in order to reduce the costs associated with the IT infrastructure. Co-location at the private cloud provider eliminates the necessity to own the Data Center. However, the risks associated with the co-location also need to be carefully assessed.

6.3 Project Evaluation

This section evaluates the outcome of this project compared against the research objective defined at the beginning of this study. Additionally, validity and reliability of the thesis are evaluated and compared to the plan which was defined in Section 2.4.

6.3.1 Outcome vs the Objective

The main objective of this thesis was to propose a new cloud service based operational model for IT Infrastructure Team within the case company. The proposed model had to address the needs for improving business agility and cost efficiency of the IT infrastructure services.

The outcome of this thesis is an IT operational model for the cloud scenario described in Section 5.3, which is based on the Hybrid Cloud IT deployment model. The selected Hybrid Cloud IT deployment model combines the Private Cloud IT (on-premises) and

Private Cloud IT (off-premises) deployment models. A proposed operational model fits the combination of these deployment models and is evaluated to improve business agility (significantly) and cost efficiency (non-significantly) of the case company. In this sense, the outcome of this thesis reaches its initial objective.

In this thesis, two questions have been asked from the researcher by the IT infrastructure management team to support IT decision-making. First, what is *the best suitable deployment option* for cloud environment (on-premises or off-premises). Second, *how complex an effort could be to integrate the company's internal CMDB with the cloud environment(s)*. To address the first question, the best deployment option for the company's CMDB is on-premises, as the case company continues to own the Data Center and CMDB is very valuable asset. Regarding the second question, integration between the cloud environments and CMDB could be possible due to a standardized cloud architecture, since cloud environments use specific technologies, limited set of hardware and software, and standard delivery mechanisms. Therefore, for the selected Hybrid scenario, an integration complexity of the company's CMDB with the cloud-based IT assets is assessed as *Medium*. The on-premises cloud environment can be fully customized and private cloud providers offer some limited customization to their cloud environment, which supports the integration. Although, the easiest and most convenient way for the integration would be to use the cloud compatible CMDB solution at the private cloud provider's site and synchronize the current company's CMDB with that particular solution.

Thus, the study described the key aspects of the new cloud service based operational model and assessed the changes from the cloud computing to each element of the operational model for the case company. Additionally, it can be considered that the proposed operational model answered most of the management questions that were raised at the beginning of the project.

6.3.2 Validity and Reliability

The thesis has been done following the case study research approach, by the qualitative research methods. Therefore, the examination of its validity and reliability makes an essential part of the research approach. The validity and reliability plan was created and described in Section 2.4 of the thesis, for the purpose to support the introspection afterwards.

In qualitative research, validity can be measured by questioning whether the outcome of the thesis gives an answer to the research question. In this study, the research question corresponds to the main objective of the thesis. The proposed cloud service based operational model achieves the main objective of this thesis and thus can be considered to address the research question set at the beginning. Additionally, the data collected for the study needs to be accurate and interpretation of the data should avoid the researcher bias. It could be done in many ways including, for example, by considering alternative explanations in the literature and by involving the relevant stakeholders. Both ways were used in this study: the data was accumulated from the trusted sources such as internal company's data, extensively selected academic articles and books. Finally, the proposed cloud service based operational model was presented in verbal and written format to the case company and accepted by the commissioners.

Reliability in qualitative research can be measured by questioning whether the results of the research were the same if another person conducted this research or if the research was done at a different point in time. In this project, it is very likely that the results of the research conducted by another researcher could be the same if the same data sources were used. The data sources such as interviews and discussions with the stakeholders, review of the company documentation, and the internal benchmark would mostly probably lead to the same or similar conclusions. The fundamental aspects of the cloud computing technology from academic articles and books would also support the same or similar outcome. However, if the research was done at a different point in time, the current company's operational model might be different and a proposed cloud based operational model could then differ. For technology topics, the time issue is critical since tools and available solutions constantly evolve.

Additionally, the reliability of the thesis can be improved by using different data sources, data collection methods and maintaining a well-documented research process. In this project, four different data collection methods have been used in the end, namely interviews and discussions with the relevant company's stakeholders, extensive survey for gathering business requirements for cloud services, the analysis of the company documentation, and an internal benchmark of one operational process. Research process was also developed in detail in advance and then executed accordingly.

To increase reliability and validity of the outcome, more interviews and discussions in the case company would definitely benefit the evaluations and might lead to more con-

crete recommendations and more fine-tuning to the needs of the case company. It was not however possible due to the limited access of the researcher acted as an outside expert for the case company. This fact, however, may also have a positive side, as selection and recommendation of a particular model for the case company was free on a possible researcher bias. Finally, the validation sessions for the proposal should have been done more extensively and involve more stakeholders in the case company, and done at the end of the study. This was not possible due to the specific project constrains of this rather extensive project. All these facts, without any doubt, reduce the reliability and validity of its outcomes. Still it needs to be noted that the proposal, even when presented as not yet fully completed, was accepted by the commissioners of the case company.

At the end of the study, it could be added that many companies around the globe currently face similar challenges as the case company, when they aim at improving the agility and cost efficiency of their IT infrastructure services. These challenges could be overcome by considering cloud infrastructure as a service (IaaS) for use. This study can help such companies by providing an example evaluating one selected cloud based scenario in one company context.

References

AXELOS (2014). What is ITIL. *AXELOS ITIL.* Available from <http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx> [Accessed May 27, 2014].

Anderson, C. and Grantz, J. (2012). Climate Change: Cloud's Impact on IT Organizations and Staffing. *International Data Corporation.* Available from < http://www.microsoft.com/en-us/news/download/presskits/learning/docs/idc.pdf > [Accessed May 5, 2014].

Aven, T. (2012). *Foundations of Risk Analysis (2nd Edition).* Hoboken, NJ: John Wiley & Sons, Inc.

Bensch, S. (2011). How to procure cloud computing solutions: a manageable value network approach. *International Conference on Management of Emergent Digital EcoSystems. Nov. 21,* 99-106.

Bittman T. J. (2012). *Design Your Private Cloud With Hybrid in Mind.* Gartner Inc.

BMC Software (2014). BMC Cloud Lifecycle Management. *BMC Software.* Available from <http://documents.bmc.com/products/documents/39/81/453981/453981.pdf > [Accessed June 23, 2014].

Brisebois, R., Boyd, G. and Shadid Z. (2007). What is IT Governance? and why is it important for the IS auditor. *The IntoSAI IT Journal.* Available from <http://www.intosaiitaudit.org/intoit_articles/25_p30top35.pdf> [Accessed May 5, 2014].

Brown, W. A., Laird, R., Gee, C. and Mitra, T. (2008). *SOA Governance: Achieving and Sustaining Business and IT Agility*. Boston, MA: Pearson Education.

Chee, B. and Franklin, C. (2010). *Cloud Computing. Technologies and Strategies of the Ubiquitous Data Center.* Boca Raton, FL: CRC Press. Taylor & Francis Group, LLC.

Child, J. (1984). *Organization: A Guide to Problems and Practice*. 2nd ed. London: SAGE Publications Ltd.

CloudAware (2014). CMDB - Datasheet. *CloudAware.* Available from <http://www.cloudaware.com/files/datasheets/CMDB%E2%80%94Datasheet.pdf> [Accessed June 23, 2014].

Cloud Security Alliance (2010). Top Threats to Cloud Computing V1.0. *Cloud Security Alliance.* Available from <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf> [Accessed June 23, 2014].

Colville, R. (2010). Cloud Environments Need a CMDB and a CMS. *Gartner Inc.*

Curtis, D. and Colville, R. (2011). Issues and Recommendations for Synchronizing CMDB and Real-Time IT service models. *Gartner Inc.*

Dan, R., Arthur, M., David, P. and Frank, B. (2002). The creation of knowledge through case study research. *Irish Journal of Marketing*. Vol. 23 (2), 1-17.

De Vries, M., van der Merwe, A., Kotze, P. and Gerber, A. (2011). A Method for Identifying Process Reuse Opportunities to Enhance the Operating Model. *IEEE International Conference on Industrial Engineering and Engineering Management*. *Dec. 6-9.*

Dibbern, J., Goles, T., Hirschheim, R., Jayatilaka, B. (2004). Information Systems Outsourcing: A Survey and analysis of the Literature. *ACM SIGMIS Database*. Vol. 35 (4), 6-102.

EMC Education Services (2012). *Information Storage and Management: Storing, Managing, and Protecting Digital Information in Classic, Virtualized, and Cloud Environments.* 2nd Edition. Hoboken, NJ: John Wiley & Sons, Inc.

Ernst & Young (2011). Cloud computing issues and impacts. *Global Technology Industry Discussion Series.,* 1-55. Available from < http://www.ey.com/Publication/vwLUAssets/Cloud-computing_issues_and_impacts/$File/Cloud_computing_issues_and_impacts.pdf > [Accessed June 23, 2014].

Flynn, D., Lownds, P. and Vredevoort, H. (2012). *Microsoft Private Cloud Computing.* Somerset, NJ: John Wiley & Sons, Inc.

Gallacher, L. and Morris, H. (2012). *ITIL Foundation Exam Study Guide.* Somerset, NJ: John Wiley & Sons, Inc.

Gallivan, M. and Oh, W. (1999). Analyzing IT Outsourcing Relationships as Alliances among Multiple Clients and Vendors. Systems Sciences. *HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference*. *Jan. 5-8*, 1-15.

Halpert, B. (2011). *Auditing Cloud Computing – A Security and Privacy Guide*. Hoboken NJ: John Wiley & Sons.

Hausman, K., Cook, S. and Sampaio, T. (2013). *Cloud Essentials: CompTIA Authorized Courseware for Exam CLO-001.* Somerset, NJ: John Wiley & Sons, Inc.

Hewlett-Packard Development Company, L.P. (2011). HP Cloud Service Automation: Concepts Guide. *Hewlett-Packard*, 1-36. Available from <http://h21007.www2.hp.com/portal/download/files/unprot/CloudSystem/HP_CSA_201_Concepts_Guide.pdf> [Accessed June 23, 2014].

Hiriyappa, B. (2009). *Organizational Behavior*. Daryaganj, Delhi: New Age International Publishers.

Hurwitz, J., Bloor, R., Kaufman, M. and Halper, F. (2009). *Cloud Computing For Dummies.* Hoboken, NJ: John Wiley & Sons, Inc.

Incisive Media (2013). The off-premise private cloud: The third way for agile: Research paper. *Incisive Media* Available from <

http://www.fasthosts.co.uk/downloads/white-papers/computing-research-off-premise-cloud.pdf> [Accessed May 5, 2014].

ITIL.org (2011). ITIL glossary. *ITIL.org.* Available from < http://www.itil.org/custom/glossaren/> [Accessed May 5, 2014].

Jackson, J. (2013). HP updates IT automation suite for cloud deployments. *IDG Consumer & SMB.* Available from <http://www.pcworld.com/article/2038632/hp-updates-it-automation-suite-for-cloud-deployments.html> [Accessed June 23, 2014].

Khan, F. and Jameel, A. (2010). Economics of Infrastructure Management and Selective Sourcing. Management of Innovation and Technology (ICMIT), *2010 IEEE International Conference, June 2-5*, 1073-1078.

Knapp, D. (2010). *The ITSM Process Design Guide.* Ft. Lauderdale, FL: J. Ross Publishing

Krutz, R. L. and Vines, R. D. (2010). *Cloud security: A Comprehensive Guide to Secure Cloud Computing*. Indianapolis, IN: Wiley Publishing.

LeCompte, M. and Goetz, J. (1982). Problems of Reliability and Validity in Ethnographic Research. *Review of Educational Research*, 52: 31–60.

Marks, E. A. and, Lozano, B. (2010). *Executive's Guide to Cloud Computing.* Hoboken, NJ: John Wiley & Sons.

Maromonte, K. (1998). *Corporate Strategic Business Sourcing*. Westport, CT: Greenwood Publishing Group.

Marquis, H. (2012). How ITIL Helps Cloud Computing. *Global Knowledge Training LLC.* 1-3. Available from < http://www.globalknowledge.net/mea-shared-content/documents/Decision_Brief_Cloud_and_ITIL.pdf > [Accessed April 6, 2014].

Marquis, H. (2007). ITIL And The Evolution CMDB. *Business Communication Review. Feb.,* 54-57. Available from < http://www.webtorials.com/main/resource/papers/BCR/paper118/02marquis.pdf> [Accessed April 6, 2014].

Maxwell, J. (1996). *Qualitative Research Design: An Interactive Approach*. Thousand Oaks, CA: SAGE Publications Ltd.

Mell, P. and Grance, T. (2009). The NIST Definition of Cloud Computing. *National Institute of Standards and Technology.* Available from < http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf> [Accessed April 6, 2014].

Moeller, R. (2013). *Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL.* Somerset, NJ: Wiley Corporate F and A.

Muller, H. (2011). *On Top of the Cloud: How CIOs Leverage New Technologies to Drive Change and Build Value Across the Enterprise.* Hoboken, NJ: John Wiley & Sons, Inc.

Office of Government Commerce. (2000). ITIL Service Support. London: The Stationery Office.

Oredo, J. and Njihia, J. (2014). Challenges of Cloud Computing in Business: Towards New Organizational Competencies. *International Journal of Business and Social Science.* Vol. 5, 150-160.

Otsuka, H. and Lutfiyya, H. (2011). Using Strategy Trees in Change Management in Clouds. *Network and Service Management (CNSM), 7th International Conference., Oct. 24*, 133-142.

Owen S. (2012). Principles to consider when you design a new operating model. *Strategy2Life.* Available from < http://strategy2life.com/2012/10/15/operating-model-design-principles/> [Accessed April 14, 2014].

Payne, J. (2011). *Managing Indirect Spend: Enhancing Profitability Through Strategic Sourcing.* Hoboken, NJ: John Wiley & Sons, Inc.

Quinton, S. and Smallbone, T. (2006). *Postgraduate Research in Business: A Critical Guide.* London: Sage Publications.

Robinson, N., Valeri, L. and Cave, J. (2011). *The Cloud: Understanding the Security, Privacy and Trust Challenges.* Santa Monica, CA: RAND Corporation.

Sollish, F. and Semanik, John. (2010). *Strategic Global Sourcing Best Practices.* Hoboken, NJ: John Wiley & Sons, Inc.

Stenzel, J., Cokins, G., Schubert, K., Hugos, M., Betancourt, R., Farrell, A., Flemming, B. and Hujsak, J. (2010). *CIO Best Practices: Enabling Strategic Value With Information Technology.* 2nd Edition. Hoboken, NJ: John Wiley & Sons, Inc.

Strategy& Formerly Booz & Company (2014). IT Operating Model and Governance. *Strategy& Formerly Booz & Company.* Available from <http://www.strategyand.pwc.com/global/home/what_we_do/services/it/service-areas/world-class-it/display/it-operating-model-governance> [Accessed April 14, 2014].

Turpijn T. (2013). Deploying a VM to Windows Azure with Orchestrator leveraging the Service Manager CMDB. *Microsoft Corporation.* Available from <http://blogs.technet.com/b/privatecloud/archive/2013/07/25/deploying-a-vm-to-windows-azure-with-orchestrator-leveraging-the-service-manager-cmdb.aspx> [Accessed June 23, 2014].

Woodside, A. and Wilson, E. (2003). Case study research methods for theory building. *Journal of Business & Industrial Marketing*. Vol. 18 (6/7), 493-508.

Yin, R.K. (2003) *Case Study Research: Design and Methods.* 3rd ed. Thousand Oaks, CA: Sage Publications.

Appendix 1. The case company's procurement process

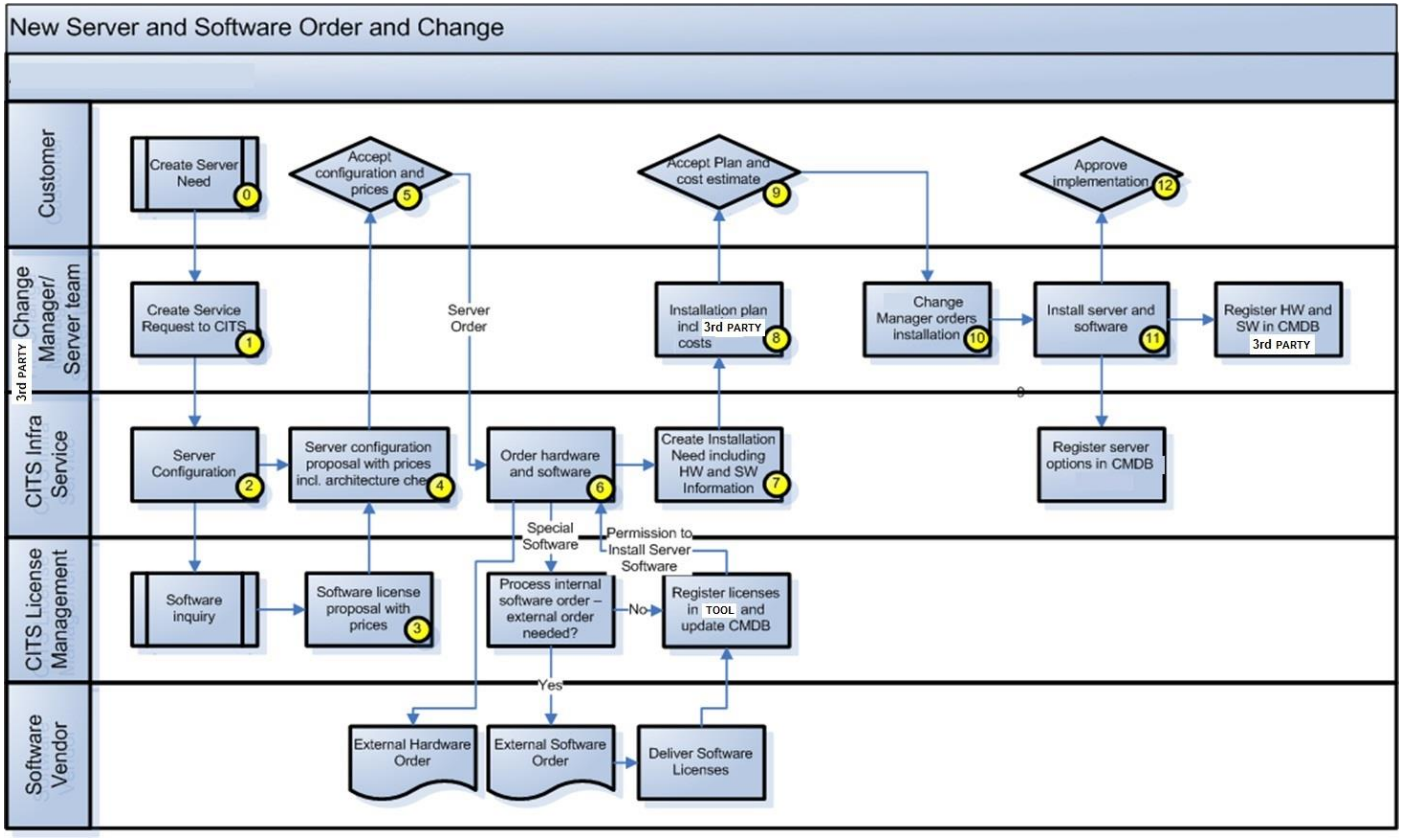

Figure 4. The case company's procurement process.

Appendix 2. Analysis of the Business requirements

Table 1: Business requirements from the case company's divisions.

		UNIT1		UNIT2		UNIT3		UNIT4	
General Questions		**Answer:**	**Longer explanation:**	**Answer:**	**Longer explanation:**	**Answer:**	**Longer explanation:**	**Answer:**	**Longer explanation:**
Have you evaluated or even tried IaaS cloud services in your division already?		**No**	SaaS only	**No**		**No**		**Yes**	We are testing with ***
What are the main reasons for your division to consider using cloud computing? (e.g. provisioning time, self service, elasticity, scale out..)			Elasticity and price, turn off servers when they are not needed		Missing or poor delivery of service in-house		Scalability, self-service and to get better price and quality	**all the above**	Drivers have been to move test servers in cloud and run them only when we need them and not 24/7 which creates savings. We might sometimes need a lot of processing power but not all the time. Later we would like to use cloud provider as a disaster recovery site.
Do you expect the cloud initiative to significantly impact one or more business processes? How?		**No**		**No**	Not significantly	**No**	Not significantly but some. I'll see that SaaS will give us much more than pure IaaS	**Yes**	Long term business planning might benefit from better processing resources. Big Data and Cloud go hand in hand and there might be something revolutionary happening in the future even for energy industry.
What are your biggest concerns for the cloud services today?			Integrations to other different services inside company, Information security, Large data amount, which might prevent moving the application to cloud services		performance managment		Security and availability if problem in Internet		We need some amount of governance while still keeping the service as agile as possible. There needs to be a management interface available (self service portal) for getting systems running and setting the schedule when to run systems. We might need some "playground" too where users could start servers themselves. How to keep this all in some order? If cloud would not have these privileges, it does not make much sense. NSA will listen and we leak our intelligence… Though we might need keep our stuff in own data center which is operated by the third pary. NSA might request date from the third party anyhow?
Could you describe a typical use cases where you would need a server from cloud services?		**Yes**	Test environments that do not contain confidential information --> not too many	**No**	There is no typical use case. There could be some exceptions like where the temporary setups with no integrations etc.	**Yes**	When capacity is needed quickly		I would like to setup my test environments in cloud and eventually all the rest too, maybe apart from the 24/7 systems. This means the typical use case would be to move current systems in cloud. I would need cloud servers then every morning or when the system is set to work. We need some system to manage the deployments too to make this scheduling happen.

Which are the main security concerns for your business related to cloud services?			Information confidentiality		1) The information classification needs to be done 2) The requirement from based on the classification shall be understood then put into the project/implementation 3) Proper ASP/Cloud contracts shall be created and implemented. Also containing things like - Physical protection - Network protection - Hardening and other protections - Vendor personnel - Access and authentications - Encryption - Routines and processes - Incident management 4) Secure integrations shall be build based on classification (users/AD, business data, metering etc.) 5) Cloud systems shall be managed the same way as internal application. (IE ITSM, contacts, finance etc.) 6) It must be clear responsibility about the information and controlled in contracts etc.: - When closing a Cloud service - What happens if the service provider go bankruptcy for example - What happens if there is information leakage, who is responsible for what - Restore of data, responsibility etc. 7) Third party data must me controlled and secured. Like personal data, secret geographical data etc.		Is our data safe and secure and what happens when you stop to use the service. Is all information deleted.		We don't manage the Private Keys or security groups correctly. Instances might run without patches, though the management system could perhaps force the instance to be patched before putting it into a security group which has open ports. I don't know if such a system exists.

Have you identified business risks if cloud services are utilized?			Availability of the servers	**Yes**	Se above	**No**			Worst cases are that business information leaks outside or that a system is not available when needed. Impact varies greatly.
What kind of cloud service are you mainly interested? (Private, Public or Hybrid)			Mainly Private or Hybrid, but also public if it works		The ones that we cannot find internally --> Ok, could you name one		All		Public, we would go with VPC (Virtual Private Cloud)

Current virtual server service									
Are you satisfied with the current price of virtual servers?			Price of virtual servers is OK, Moving test databases to PaaS is more expensive, maintanance provider service is for is a **big part of the service price** for databases	**Yes**		**No, please specify why not**	Capacity management is failing		The price of running a service 24/7 is competitive, but for office hours only, it's too much.
Are you satisfied with the current invoicing grounds (per/month) of virtual servers?		**Yes**	Ok	**Yes**		**Yes**			No, it should be per hour or even minute like Azure does it.
Are you satisfied with the current delivery time virtual servers?		**No, please specify why not**	Working with normal process is not possible, when escalating it then servers come within decent time. Personal access rights delivery time is too long.	**No, please specify why not**	Satisfied time would be five working days	**No, please specify why not**	Takes way too long time to get it		No, and especially the PAR process are too slow.
Cloud service requirements									
Performance and capacity									
What percentage of your use cases will be using totally isolated stand alone resources?			0 %		1%?				We can do some preliminary tests without connection back, but to do anything meaningful, we need the connection and integrations to work towards internal systems. So, the percentage is 0%.

What are the performance characteristics of typical applications?			Light processor usage, but heavy IO usage. However these DBs probably can not be moved to the cloud		?		High IO and CPU usage		Mostly they are idling. When running the simulations/optimizations, CPU is needed. Business might run multiple optimizations during a day, while one optimization run might take from 1-10 minutes. During this time, the application consumes all the resources. It is bursty.
What would be a typical amount of data is moving per application to/from cloud?			Large amount of data, data communication availability would be crucial		?		not evaluated, consider buying CRM solution as a SaaS		I have not measured this, but I would guess it around 10-50MB daily.
What are your requirements for storage availability and durability?			Critical, but more important is security		None/per case		0,9998		I have no significant storage requirements. Applications don't need to store static files, but require mostly a database. I would run the production systems on cloud provider environment which is replicated between two availability zones.
Storage - do you require data replication between data centers?			Not necessarily, if this is the way to secure the data availability then yes		See information classification		Depends on the case		See above.
What degree of resource isolation is required for security and compliance? (e.g. in public IaaS)			-		See information classification				I don't know who sets these up. I don't see any problem running services on a shared platform.
Do you have any requirements to encrypt data stored in cloud? (in transfer, at rest?)			Most likely		See information classification		Not at the moment but maybe in the future.		Data should be transferred with secure methods, for example with SFTP. The data should encrypted on virtual drives. This should be easy to do with the standard operating system resources.
Data connection									
What are the network connection requirements for your applications? (For example, Direct mpls, or vpn over internet)			Because the large amount of traffic, most likely dedicated connection to in-hous infrastructure would be needed		The applications seldom or never has that kind of requirements		Direct and VPN		The applications are integrated with other internal systems, basically it is only internal connections which would now need to be extended over the Internet with VPN.

Authentication and security									
What are the security requirements for e.g. access to your applications?			Integration to in-house authentiation database would be the only solution, because application usage requires single sign on.		See information classification		Company's access manage-ment has to be followed		Access is granted for business purposes. The authenti-cation is not strong though.
Do you expect to use com-pany's user identity when connecting to your applica-tions in cloud?			Yes		Yes, so integrations with in-house authenrication system is needed		Why not		No, but it will come there in the long run.
Do you need to give access to external employees?			Yes		Yes		Yes		Yes, for example consultants from the application vendor.
What are your security aspects when you are outsourcing services out-side of the company?			See above.				company's standards		To be honest, I feel Virtual private cloud would be as much part as company as is the company's own datacenter. It is just a question to take it into use with some good practices.
Integrations									
What kind of integration do you need from cloud to on premise infrastructure? E.g. special protocols or other company's application level, full infrastructure integration)			Servers would be needed as they would be in-house Data center		Depending on implementation, special protocols support is need-ed		Probably special protocols sup-port is needed		
Do you expect to move virtual servers between the cloud and on premise infrastructure automatical-ly?			Yes		?		Possible		No.
Provisioning									
How quickly would you like to be able to get new resources?			2-5 days would be enough		Depending on service --> Explana-tion		asap		The faster, the better. If we think about the billing by the minute, I would like make it so that we have an API call to the cloud for provisioning a server from a template and we would have a running server in under a minute. Currently cloud service providers provision a new linux server in 2-3 minutes and Win-dows server in a bit longer time while getting access to a Windows takes more than 15 minutes.
How often do will you need to provision or deprovision resources?			Minimal need		Depending on service				Depends a lot of the system, but ideally provision the system in the morning and deprovision in the evening.

Do you see that provisioned servers should be visible in CMDB?			Yes		Same as others, tag some metadata		Yes		I would like to have them visible somewhere, I am not sure if CMDB is the correct location, but at least the magical cloud management system should display this information.
What would in your opinion be the best way to request new service (i.e. server resource)?			Possibility to a self service		Depending on service --> My it portal?		Self service portal		A server is just a building block. A server itself does not do anything. It must be tied to some service/system. The magical management system should allow users to define services and give the possibility to set some servers in the system to provide for example application services or database services. If a user wants a server, she creates a new system (dummy system #2487 for example) and adds a server within this system. User could then do what ever she likes with the server, make it a new template for what ever purpose. So, the good way of provisioning a server would be to allow users the possibility to provision servers with the magical management system.
What capabilities will you need to self service? (e.g. just standard servers with limited set of capabilities, or do you need additional software, OS roles, self-service load balancer, or firewall openings, or is partly manual provisioning fine?)			Yes		Depending on service		All listed but Firewall settings should be left out (too risky)		I would like to see some predefined server templates where users could start from. In basic case, users will need to set some parameters like the amount of disk and what kind of a server (micro, small, large etc.) they need, keys and firewall openings. Maybe there could be some predefined firewall openings, that is, security groups available.
Do you need configurable auto-scaling?			Yes, with self service. Timing would be critical		Yes, but in practice just an service for the future		Yes		We don't have such systems which would need this.
Operation and management									
What are the operational tools that are needed for event/performance management, configuration, change management, monitoring, logging, etc.?			Yes		Depending on service, from none to all				The magical management system should be able to keep up with the systems so that if they crash during the schedule they should be running, it is trying to recover them. Essentially, the magical management system would run a Chef or a Puppet master role. With these Chef/Puppet recipes we would initiate systems every time the same way. If we need changes, changes are either put in a Recipe or the deployment script is modified. Recipes would of course be kept in a version control system.

How willing are you to commit to cloud service providers operating model, e.g. maintenance schedules?			No, maintenance breaks need to be agreed		How should it be done otherwise?		Depends		This of course depends about the IaaS vendor. The systems in the cloud should always be designed without a single point of failure since one server can stop to exists if it fails, but this is of course a decision which should be put in the SLA between the cloud service provider and company's IT department.
What are the business' expectations for CITS to manage the cloud infrastructure services? (skills, resources, service management, reporting, billing, instructions,…)			Same as before		Could be discussed depending on what company's internal department is willing to do		Should be self service and Corporate IT Services department role should be small as possible		Of course I would not like all divisions rolling with their own magical management system. We need a consolidated system to handle the deployments. Maybe divisions could create the Chef/puppet scripts and the management system would give access to those deployments only and all the needed statistics etc. CITS might need to be the master account owner and then give accounts to divisions and handle the invoicing.
What kind of visibility do you require to the cloud services, resources and configurations? (performance, capacity, monitoring, alerts)			Would be good for a system manager to see for example performance of the server		Depending on service and information classification. Some Cloud services must be controlled in detail other more "loose"		All possible		Most IaaS vendors have pretty nice health status screens available but it would be nice to have some health info for my own instances too.
What kind of billing you would like - pay per use (hour, daily) or standard monthly pricing? How much visibility and control do users need over usage, costs and possible chargebacks?			Per day invoicing		Needs to be discussed with the business. Needs to be looked upon when the service model with the vendor is setup		Pay per use		I would like per hour or if vendor support it, by minute pricing.
Do you need to monitor the cloud resources as part of business process monitoring?			-		Depending on service, mostly no		Yes		We are not currently doing this, but I would not see it as a bad thing to have.
Do you have any requirements to customize the cloud service?			Possibly		Hm… well depends on how well the service suits the demands?		Could be		No.
Special questions									
Does it matter where the cloud resources and business data resides? (e.g. within Finland, EU, doesn't matter)			Most likely Finland, definitely at least in EU		Depending on information classification. Some data must never be accesses from "other" counties of citizen. Some data is open		Prefer EU		We are not operating with any personal data, such as social security numbers so I don't think this matters really.

Do you have any legal or regulatory issues that have impact when selecting cloud vendor/service or locations of services?			Most likely Yes		See above		Could be		I don't have any.
Pilot									
Do you have a candidate for piloting the cloud infra service?			No		No	No			We have a plan how to test with IaaS from cloud service provider. First we get familiar with how to get data in out cloud and manage the resources. Next we setup some dummy service there and see how it responds to get familiar with encrypting drives etc. Then we are putting a copy of the Test application and see how the optimization goes and whether we get any better results of running it there in the cloud.

Appendix 3. The case company's (current) ITSM operational processes

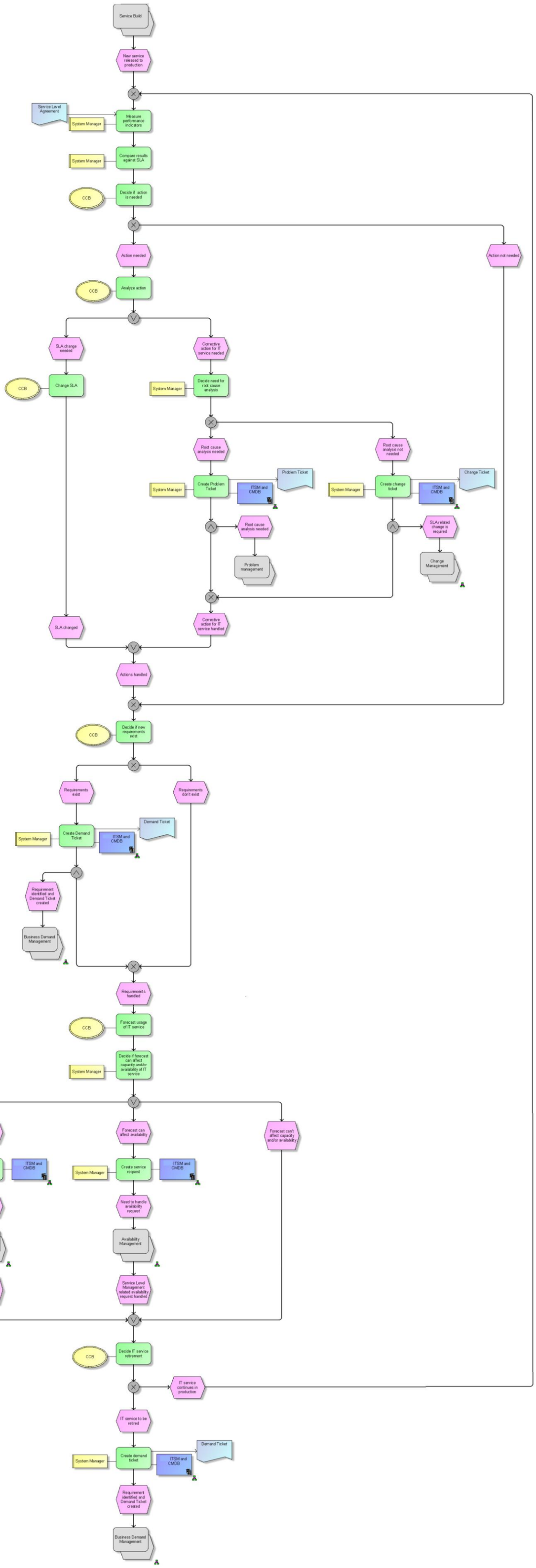

Figure 1. Service Level Management.

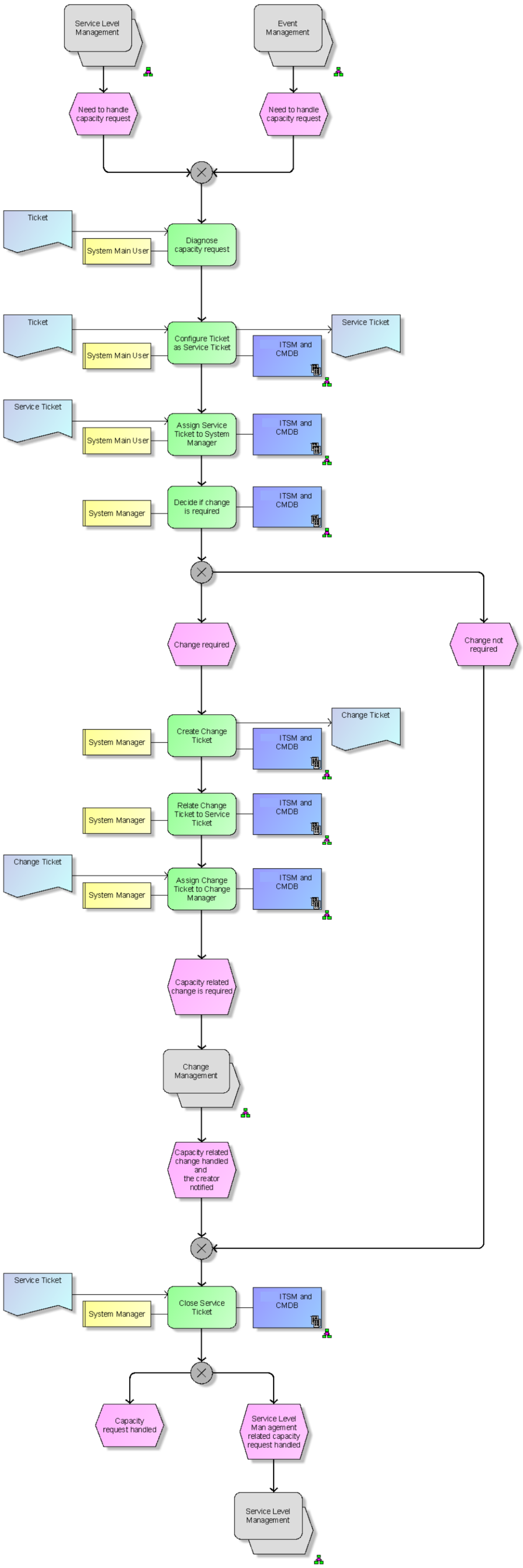

Figure 2. Capacity Management.

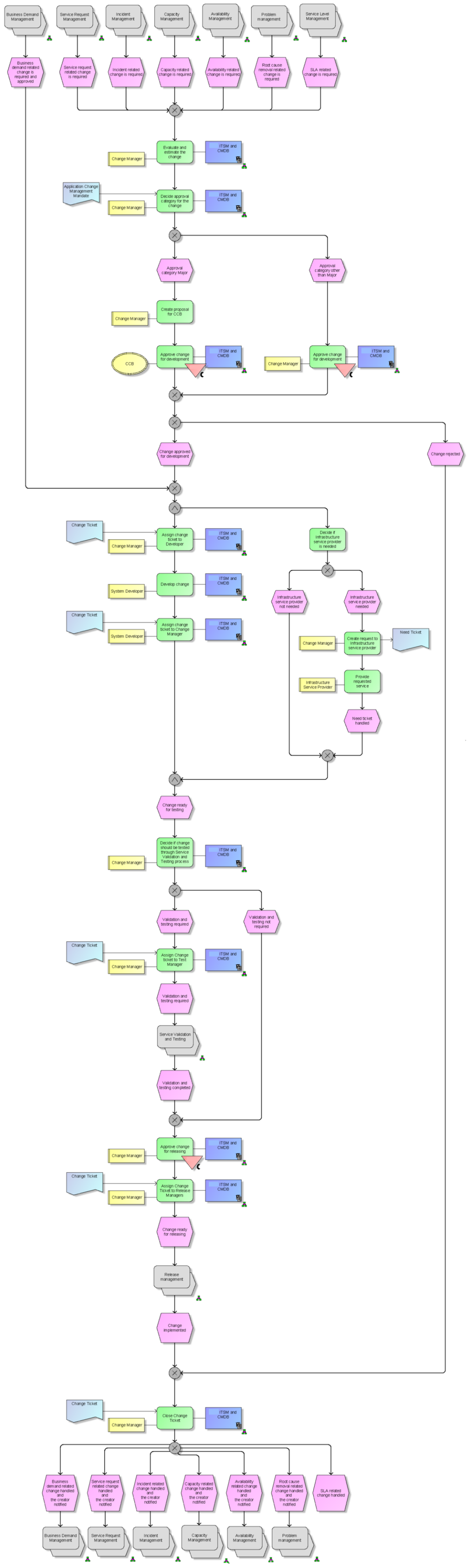

Figure 3. Change Management.

Appendix 4. Existing Knowledge and Best Practice Analysis

Table 1: Benefits and Challenges of the Cloud deployment models.

Cloud deployment model	Benefits	Challenges
Private Cloud IT (on-premises) - Deployed on-premises of the case company, IT hardware belongs to the case company - Data Center is owned by the case company	- Cloud environment is dedicated to the case company - Full control over the data and process - Single-tenant environment removes the risks associated with multi-tenancy - Excellent communication between the end-customers and IT service provider (same company) - High customization of the cloud environment and internal SLA - Excellent quality management of the cloud services - Excellent Security and Reliability of the IT infrastructure assets - The case company has the existing legacy IT infrastructure which can be utilized for the deployment of the private cloud - No connectivity to off-premises is required - Allows the company to prepare for the future by moving the existing infrastructure into the cloud direction	- High costs associated with operating own Data Center - Limitations in hardware resources decrease the elasticity and scaling capabilities of the environment - Procurement process of the IT capacity is challenging (Capital investments are required, procurement process is slow)
Private Cloud IT (off-premises) - Deployed on private cloud provider's premises, IT hardware belongs to the private cloud provider - Available options for Connectivity are Internet or MPLS	- No ownership or decreased use of the company's the Data Center, reduces the operational expenses and capital investments - Single-tenant environment, eliminates the risks associated with multi-tenancy - Private cloud providers offer the customization of the cloud environment and negotiable SLA - Good quality management of the cloud services - Good Security and Reliability of the IT infrastructure assets	- Single-tenant environment is expensive - Limited control over the data and process, as the company's data stored and processed off-premises - The risks associated with cloud provider, privacy assurance and compliance regulations exist - Multi-tenant cloud environment is offered by some cloud providers. It reduces the price, but increases the risks associated with Privacy. - Additional connectivity (MPLS) to the private cloud provider is needed

Public Cloud IT - Available to the public use through the Internet, to any customer - Deployed on the public cloud provider's premises, IT hardware belongs to the public cloud provider - Typical connectivity is though the Internet (some public cloud providers offer the MPLS connectivity through the partner's networks)	- No ownership or decreased use of the company's the Data Center, reduces the operational expenses and capital investments - Cost advantage due to economies of scale - Some public cloud providers offer the single-tenant environment (more expensive option) - Most flexible on-demand dynamic provisioning - High scalability - Ability to pay per use for IT resources with related licenses - Innovations and fast cloud evolving - Some public cloud providers offer also single-tenant cloud environment which reduces the privacy assurance risks, but increases the price.	- Multi-tenant environment (higher risks due to shared IT resources) - Limited control over the data and process, as the company's data stored and processed off-premises - Low customization of the cloud environment and in most of the cases non-negotiable SLA - Quality management of the cloud services is lowest compare to the other cloud deployment models (cloud providers offer small compensations for the failures in the cloud IT infrastructure) - Security and Reliability of the IT infrastructure assets are lowest compare to the other cloud deployment models. (multi-tenant environment for public use, no possible audits, limitations for the data encryption, Internet connectivity option is not reliable for critical tasks) - The risks associated with cloud provider, privacy assurance and compliance regulations exist - Additional connectivity to the public cloud provider is needed
Hybrid Cloud IT - A combination of the different cloud models: private (on-premises), private (off-premises) and public - A combination of the physical and virtual resources - Might include: the cloud services, traditional hosting and co-location - The combination of the public and private clouds can be especially efficient when both are located in the same facility - The hybrid clouds may involve multiple cloud providers.	- All benefits of the cloud deployment models combined to the Hybrid Cloud IT (critical tasks are executed on the private (on-premises) cloud, less critical tasks are executed on the private (off-premises) cloud, and non-critical tasks are executed on the public cloud) - Cloud bursting is the ability of the IT service to allocate more IT resources from the public cloud in the event of a spike in the IT capacity demand	- Heterogeneous environment, management becomes a complex task - Integration of the different cloud models to hybrid cloud requires extra efforts and expertise - Technologies for integration of the various cloud models are expensive - Vendor lock-in or technology lock-in situation for the customer (cloud providers offer dedicated hybrid cloud solutions)

Table 2: Elements of the Cloud Operational Model

Elements of the Cloud Operational Model (Definitions)	**Fundings from literature**
Organizational Structure - Allocation of tasks and responsibilities to individuals - Defining formal reporting relationships and number of levels in hierarchies - Grouping together of personnel into teams, departments and to whole organization - Design of systems to provide information flow between the teams - Delegation of authority - Provision of the systems for performance measurement and employees rewarding	- The IT organization needs to have technical knowledge in a wide range of technologies in order to manage the cloud services - Relationship between the business and the IT department changes in the consumption of IT resources - Cloud computing requires a much better understanding of the business requirements from the IT organization - For identification of the new required competences, following challenges of cloud computing are pointed out: General competences: a) portability, interoperability b) cultural resistance to changes in the organization c) transition and execution activities with cloud services Additional (off-premises) competences: d) vendor management e) integration with legacy systems f) availability and reliability of the cloud services g) security and privacy concerns - In transition to the cloud-enabled organization, the areas of the IT organization will be affected as for the required critical skills: General - IT Systems and Operations - Network and Telecom Management - Security Management - Help desk and End-user support IT service development: - Management functions - Project and Program Managers - Business Analysts - Application Development and Maintenance The collaboration between those areas needs to be functional and efficient.

IT Governance - Activity which "ensures that policies and strategy are actually implemented and that required processes are followed correctly." (ITIL Glossary 2011) - Governance includes - defining roles and responsibilities - measuring and reporting - taking actions to resolve any issues identified (ITIL Glossary 2011) - IT Governance focuses on the information technology assets, their performance and managing the risks associated with them	- General changes to the IT Governance include: - New roles and responsibilities - New methods how to measure the performance of the cloud-based IT services - New approach how to resolve any issues related to the cloud-based IT services - Self-service is a new key attribute of the IT service delivery - Set of clear written policies need to be developed for the end-users (rules and regulations, limitations of the cloud environment and the points of contract for the support) - Written sets of policies need to be communicated through the organized trainings - The policies should be built-in to the automation process of provisioning the cloud services - Service-oriented architecture (SOA) governance has to be applied to the cloud-based IT services - InfoSec governance is especially essential for the private (off-premises), public and hybrid deployment models - Strategic vision and guidance of the information security imple mentation in the organization - Security guidelines have to be defined for the end-users - The case company in order to establish IT governance for cloud-based IT assets must - Examine the security and privacy components of cloud service providers - Mandate compliance with acceptable security standard through the legal contract (Service Level Agreement) with the cloud service provider
Sourcing - The general practices from strategic sourcing are applicable to the cloud-based IT infrastructure services (Bensch 2011: 101) - Strategic sourcing is a procurement and supply management process which locates, qualifies and employs the suppliers that add value to the customer in accordance with business requirements (Sollish and Semanik 2010: 1)	- Sourcing decisions need to take into account overall performance of the supplier in the following criteria: quality, delivery, customer service, product/service advancements and cost (Maromonte 1998: 2) - The public IaaS offerings have standard pre-defined service agreements, some steps in sourcing process might not be possible to execute: solicitation, negotiation, contracting, and in some cases the billing methods (Bensch 2011: 101) - Total outsourcing of the IT infrastructure services for large companies with own Data Center might be avoided by the optimization of internal efficiencies (Khan and Jameel 2010: 1073,1077)
Operational processes - ITIL is a practical framework which describes the operational processes for identifying, planning, delivering and supporting IT services to the business.	General to all ITIL-based operational processes: - ITIL processes are able to support the cloud operations without significant changes. Instead, ITIL methods used in the traditional IT Infrastructure Management require changes. (Marquis 2012: 1,2,3). - ITIL is not optimized for fast service delivery, amount of changes and supplier management approach that cloud services offer. (Marquis 2012: 1,2,3). - ITIL operations change from traditional infrastructure management tasks towards the management of the services and managing service providers.

	Service Level Management Definition: Service Level Management ensures that IT services are provided to the customers with agreed conditions. Service Level Management process includes negotiation and making an agreement between the customer and supplier for the provision of the defined IT services. Service Level Agreement (SLA) includes the targets for the IT services that need to be measured and met (the levels of availability, capacity, performance which is possible to measure and achieve by the IT service provider) Cloud computing related: - For mission-critical applications a company needs to negotiate an SLA that includes penalties for cloud service provider in case of service delivery failure - Company needs to have own ability to monitor the IT service for verification of the requirements defined in SLA - Cloud vendor management personnel need to have ability to make changes to the SLA during the service lifecycle to support the changes in the service level requirements.
	Capacity Management Definition: Capacity Management is a process to ensure that the capacity of IT services and IT infrastructure meets the current and future needs of the customers in a cost-effective and timely manner. Efficient prediction of the future capacity requirements prevents the possible service failures. Capacity Management applies to the IT services during their lifecycle. Capacity Management also supports decision making for server consolidation, hardware procurement, and service level management. Cloud computing related: - Capacity Management personnel need to understand the performance data and limitations of the cloud-based IT assets, as well as the costs associated with the resource allocation in the cloud environment in order to plan for the capacity - Capacity Management process will transform from management of the traditional IT components to the management of the services - The IT component delivery is characterized by the long lead time, while the IT service delivery is near real-time. - Removing excess capacity becomes a critical task by the capacity management personnel.

	Change Management Definition: Change Management is a process for controlling the lifecycle of the all changes and making possible to execute the changes with minimum disruption to the IT services Main objectives of the Change Management: a) keep in order the changes that arise in the business environment meanwhile reduce the negative impact to the IT services such as amount of incidents, disruption to the services and possible rework b) ensure that changes are recorded to the Configuration Management System (CMS), "prioritized, planned, tested, implemented, documented and reviewed in controlled manner" (Gallacher and Morris 2012: 164) Cloud computing related: - Change Management process needs to handle the high number of changes and adapt to the shorter time frames for the change implementations - Changing configurations or patching becomes more challenging due to virtualization technologies and cloud provider specific procedures. - Support options from the cloud provider are required
CMDB - Configuration Management Database (CMDB) is the main component of the Service Asset and Configuration Management (SACM) process, defined by ITIL - SACM process ensures that IT assets are controlled, and accurate information regarding to those assets is stored and available when needed. - CMDB stores the information about the IT assets through out their lifecycle, how these assets configured and interconnected.	- Use of the CMDB with the cloud-based IT assets is especially important, as the cloud IT assets might be located at various locations (Hybrid cloud deployment model) - In the cloud scenario, the configuration data, relationships and dependencies between the configuration items in CMDB represented as a "real-time IT service model" - In the cloud scenario, The CMDB for the traditional IT infrastructure is not capable to manage near real-time data due to the limited performance and functional capabilities. - Configuration Management System (CMS) governs the data in more federated way compare to the CMDB and advisable to be used with the cloud-based IT assets - Overview of the commercial CMDB solutions, compatible with the cloud-based IT assets: - Most of the public cloud providers do not offer CMDB solutions - Many private cloud providers offer CMDB solutions dedicated to their own cloud environments - Some cloud providers offer CMDB solutions that are dedicated to their own cloud environment and also capable to work with other cloud environments that are based on the same cloud (technology) platform. - Independent third party CMDB solutions support public or private cloud service providers, or both. The commercial CMDB solutions might be deployed on-premises, off-premises, or cloud-based.

Risk Analysis - Method which is able "to define what may happen in the future, assess associated risks and uncertainties"	General for the Risk Analysis: - Cloud computing represents a complex environment and has many risks to consider - Risk analysis typically is done once before taking the cloud environment(s) into use and constantly repeated afterwards - Many risks applicable to the cloud environment(s) are similar or almost the same as the risks in the traditional hosted and outsourced IT environments

	Privacy assurance risks
	
	- Company has limited control over the data and process in the Private Cloud IT (off-premises) and Public Cloud IT deployment models
	  - Company might suffer financially from the possible privacy losses that can result in the loss of company's credibility
	
	- Information security of the data represented by three tenets:
	  - Confidentiality is the prevention of the data from disclosure to unauthorized person(s)
	  - Integrity is the prevention of the data from modifications by unauthorized person(s) or by accident
	  - Availability refers to the stability and reliability of the IT infrastructure and network connectivity (guarantee of service, performance and up time)
	
	- To protect the company's data from loss of confidentiality, integrity and availability, the proper cloud access controls need to be in place
	  - Accountability has to be a part of the cloud access controls
	
	- For mitigation of the security risks important to understand the possible threats and vulnerabilities in the cloud IT infrastructure and network connectivity

	Compliance regulations risks - Companies need to follow the various compliance regulations and privacy laws when dealing with sensitive data - Cloud service provider should be compliant to these regulations - The compliance regulations and privacy laws might be common or vary in the different countries. - Customers need to plan for the possible new regulations that are coming directly to the cloud service providers in future by the legal authorities.

	Cloud service provider risks
	
	- Cloud service providers depend on the partners that provide network connectivity, premises and other services (customer should analyze the risks associated with these partners)
	
	- Quality of the cloud service providers needs to be assessed
	  - How long and how well a cloud service provider can provide quality services
	
	- Customer needs to have business continuity plan ready for possible risks
	
	- "Safest" cloud service providers fall into the categories:
	  - Cash-rich providers like Amazon or Microsoft
	  - Companies with high expertise and technological advantages

Appendix 5. Detailed Evaluation of Private Cloud IT (on-premises) deployment model

Table 1

Evaluation category: Business requirements	
The Private Cloud IT (on-premises) deployment model is evaluated against the business requirements of the case company in five categories: *Cost Efficiency*, *Agility*, *Functional Requirements*, *Reliability* and *Security*.	
Cost efficiency	The Private Cloud IT (on-premises) deployment model offers to the customers desired capabilities such as *flexible price model, hourly based charging, frequent provision* and *de-provision of virtual servers*. Unfortunately ownership of the Data Center by the case company is extremely expensive, and overall price per hour is high. As an outcome, The Private Cloud IT (on-premises) deployment model **partly fulfills** the requirements for Cost Efficiency.
Agility	The Private Cloud IT (on-premises) deployment model provides general cloud computing capabilities such as a *self-service* and *faster service provisioning* with the help of built-in automation. Unfortunately Private Cloud IT (on-premises) deployment model comes with limitations to the available hardware resources, which makes the capacity management process slow in some cases. The case company has to procure the hardware resources and make the capital investments in order to manage the IT capacity. As an outcome, The Private Cloud IT (on-premises) deployment model **partly fulfills** the requirements for Agility.
Functional Requirements	The Private Cloud IT (on-premises) deployment model *does not fulfill* some business requirements from the case company. The auto-scaling of the cloud services requirement cannot be fulfilled, as it is available only in the Public Cloud IT deployment model. As an outcome, the Private Cloud IT (on-premises) deployment model **partly fulfills** the functional requirements.
Reliability	The Private Cloud IT (on-premises) deployment model *does not fulfill only one* business requirement from the case company. This deployment model does not offer the data replication between at least two data centers. The case company owns only one Data Center. This capability is useful for safety of the critical data in the case of the accident or natural disaster with the single Data Center. As an outcome, the Private Cloud IT (on-premises) deployment model **partly fulfills** the requirements for Reliability.
Security	The Private Cloud IT (on-premises) deployment model **fully fulfills** the business requirements of the case company, because the company's data stays on the company's premises.
Conclusion	**Partly fulfills** the business requirements of the case company.

Table 2

Evaluation category: Effect on the case company organizational structure	
The Private Cloud IT (on-premises) deployment model is evaluated as for its effect on the current organizational structure of the case company *(roles and responsibilities).*	
General changes by cloud computing	Cloud computing in general requires the new competences and roles *from the IT organization* in the following activities: transition and execution activities with cloud services, portability and interoperability of the IT services, cultural resistance to changes in the IT organization. Additionally, the IT service development for cloud environment differs from

	the traditional IT service development and requires *the competences* from the personnel involved in the IT service development.
Changes to Management of the physical IT assets	The roles associated with the management of the physical IT assets on the company's Data Center remain the same.
Organizational actions for the changes	The trainings need to be organized for the case company's IT personnel. New roles need to be defined.
Conclusion	Compared to the other deployment models, a magnitude of change to the current organization structure is **Small**.

Table 3

Evaluation category: Effect on the case company IT Governance	
The Private Cloud IT (on-premises) deployment model is evaluated as for its effect on the IT Governance of the case company.	
General changes by cloud computing	Cloud computing in general requires changes to the current IT governance. Some of general changes include: a) new roles and responsibilities, b) new methods how to measure the performance of the cloud-based IT services, c) new approach how to resolve any issues related to the cloud-based IT services. A self-service attribute of the cloud computing also introduces the changes, such as a set of clear policies and organized trainings to the end-users, and built-in policies to the automation process of provisioning the cloud services. Additionally, Service-oriented architecture (SOA) governance has to be applied to the cloud-based IT services. The current IT governance of the case company already has SOA governance in place and does not require the big efforts for SOA governance implementation.
Changes to InfoSec governance	The minor updates to the current company's InfoSec governance.
Conclusion	The management of the company's data on-premises reduces the number of needed changes to IT Governance of the case company. IT Governance also remains the same from structural point of view, as the changes will only affect to the functional activities and company documentation. (Table 2 A) Compared to the other deployment models, a magnitude of change to the current IT governance is **Small**.

Table 4

Evaluation category: Effect on the case company Sourcing strategy	
The Private Cloud IT (on-premises) deployment model is evaluated as for its effect on the Sourcing strategy of the case company.	
Changes to management of physical IT infrastructure	The cloud computing does not bring any significant changes to the management of the physical IT infrastructure of the case company and current third party outsourcing vendor fulfills the requirements of the case company.
Changes to management of software	The current third party outsourcing vendor manages the software on the legacy system and has competences for the management of the software on top of the cloud-based IT assets. Alternatively, a new vendor for the management of the software on top of the cloud-based IT assets might add competition to the maintenance services against

	the current third party vendor. (Table 2 B).
Conclusion	The current third party outsourcing vendor proposed for management of the physical IT infrastructure and management of the software for the legacy system. For the management of the cloud environment and software on top of the cloud-based IT assets, a new third party outsourcing vendor is proposed.

Table 5

Evaluation category: Effect on the case company operational (ITSM) processes	
The Private Cloud IT (on-premises) deployment model is evaluated as for its effect on the current operational (ITSM) processes of the case company.	
Service Level Management	Service Level Management process does not require from the case company to negotiate a Service Level Agreement with the private cloud provider located off-premises. An internal service level agreement is easier to define, and the monitoring of the cloud-based IT assets on-premises is simpler. Compared to the other deployment models, an impact of the cloud computing to the Service Level Management for the Private Cloud IT (on-premises) deployment model is **Small**.
Capacity Management	Capacity Management is used in the management of the case company's Data Center. In addition, a capacity management has to manage the new tasks associated with cloud computing, such as understanding of the performance data and limitations of the cloud-based IT assets, and management of the services built on the cloud-based IT assets. Additionally to these general tasks, the management of the cloud environment becomes a responsibility of the case company. Compared to the other deployment models, an impact of the cloud computing to the Capacity Management for the Private Cloud IT (on-premises) deployment model is **High**.
Change Management	Change Management process for the cloud computing in general has to manage high number of changes and adapt to the shorter time frames for the change implementations. Additionally, Change Management has to ensure that changes are stored to the Configuration Management Database (CMDB), so the CMDB integration with cloud-bases IT assets is required. The deployment of the Private Cloud IT on-premises does not involve the cloud provider in the management of the physical IT infrastructure, which discards the miscommunication issues and private cloud provider specific procedures from the Change Management process. Compared to the other deployment models, an impact of the cloud computing to the Change Management for the Private Cloud IT (on-premises) deployment model process is **Small**.

Table 6

Evaluation category: Effect on the case company CMDB.	
The Private Cloud IT (on-premises) deployment model is evaluated as for its effect on the current Configuration Management Database (CMDB) of the case company.	
Requirements for CMDB	The current company's CMDB does not support the cloud-based IT assets and based on the old version of the commercial CMDB product. The company's CMDB should support the "real-time IT service model" in order to work with the cloud-based IT assets, have enough performance and functional capabilities to manage near real-time data in the cloud environment, and have the capabilities for the integration with selected cloud environment. An internal analysis of the company's CMDB should provide the information about the possibility to integrate the current company's CMDB with the selected cloud solution.
CMDB deployment option	CMDB can be deployed on-premises, off-premises or cloud-based. The best deployment option for is on-premises, as the company continues to own the Data Center.
Complexity to integrate cloud services with company's CMDB	If the case company's CMDB is suitable for integration with cloud-based IT assets, the integration complexity is **Medium**. The private cloud vendors offer technical support and customization to their cloud environment for the integration. Alternatively, a new commercial CMDB product can be taken into use with built-in integration capabilities.

Table 7

Evaluation category: Risk Analysis of the Private Cloud IT (on-premises) deployment model	
The Private Cloud IT (on-premises) deployment model is evaluated as for its effect on the company's risks associated with the Privacy Assurance, Compliance Regulations and Cloud Service Provider.	
Privacy Assurance	Full control over the data located on-premises allows the case company to establish all possible access controls to eliminate the risks to confidentiality, integrity and availability. However, cloud environment has to be properly configured in order to eliminate the possible threats and vulnerabilities. As an outcome, a magnitude of the risks associated with Privacy Assurance is **Small**.
Compliance Regulations	A control over the sensitive data located on-premises allows the case company to follow the compliance regulations and privacy laws without dependency on the cloud provider. As an outcome, a magnitude of the risks associated with Compliance Regulations is the **same as for the traditional IT service model**.
Cloud Service Provider	Full control over the data located on-premises eliminates almost all the risks, except one. The selected cloud solution should be chosen from the properly selected cloud service provider. Cloud service provider should provide the support services and updates to the product in future. Additionally, risk analysis of the cloud service provider has to be done and business continuity plan ready for the possible risks. Compared to the other deployment models, a magnitude of the risks associated with Cloud Service Provider is **Small**.

Appendix 6. Detailed Evaluation of Private Cloud IT (off-premises) deployment model

Table 1

Evaluation category: Business requirements	
The Private Cloud IT (off-premises) deployment model is evaluated against the business requirements of the case company in five categories: *Cost Efficiency*, *Agility*, *Functional Requirements*, *Reliability* and *Security*.	
Cost efficiency	The Private Cloud IT (off-premises) deployment model offers to the customers the desired capabilities. Unfortunately the price per *single-tenant* environment is high. Some private cloud providers also offer *multi-tenant* environment with better price point, but the multi-tenant cloud environment has higher privacy assurance risks and not be suitable for some workloads. As an outcome, the Private Cloud IT (off-premises) deployment model **partly fulfills** the requirements for Cost Efficiency.
Agility	The Private Cloud IT (off-premises) deployment model **fully fulfills** the business requirements of the case company. Additionally, not all private cloud service providers fully fulfill the requirements for Agility, as their practices in provision of the cloud-based IT resources vary.
Functional Requirements	The Private Cloud IT (off-premises) deployment model does not fulfill some requirements. *Auto-scaling* of the cloud services is not available in this deployment model. The *transition technologies* are required for moving the virtual servers between on-premises and the private cloud provider Data Center in most of the cases. In the case of integration between existing on-premises Data Center and private cloud provider located off-premises, the *security* has to be considered. As an outcome, the Private Cloud IT (off-premises) deployment model **partly fulfills** the functional requirements.
Reliability	The Private Cloud IT (off-premises) deployment model **fully fulfills** the business requirements from the case company with the special conditions. A *direct MPLS connectivity* with the private cloud provider located off-premises is required to provide reliable connection. Additionally, a *single-tenant environment* is required as it provides higher reliability compare to the multi-tenant environment.
Security	In this deployment model, case company has limited control over the data and process, as the data stored and managed off-premises. The company's data security policies do not allow to use sensitive data off-premises, which limits the use of deployment model. (Table 2 D) Additionally, the private cloud provider should be located in Finland or in EU countries. As an outcome, the Private Cloud IT (off-premises) deployment model **partly fulfills** the requirements for Security.
Conclusion	**Partly fulfills** the business requirements of the case company.

Table 2

Evaluation category: Effect on the case company organizational structure	
The Private Cloud IT (off-premises) deployment model is evaluated as for its effect on the current organizational structure of the case company *(roles and responsibilities).*	
General changes by cloud computing	In addition to the general requirements for IT organization defined for the Private Cloud IT (on-premises) deployment model (Appendix 5, Table 2), the management of the cloud-based IT assets located off-

	premises requires additional competences in following areas: a) integration with legacy system, b) increased security and privacy concerns, c) increased availability and reliability concerns, d) vendor management (negotiation and maintenance of the SLA).
Changes to Management of the physical IT assets	Maintenance of the physical IT infrastructure for the cloud-based IT assets moves to the responsibility of the private cloud provider and reduces the efforts of the company's internal workforce.
Organizational actions for the changes	The trainings need to be organized for the case company's IT personnel. New roles need to be defined.
Conclusion	Compared to the other deployment models, a magnitude of change to the current organization structure is **Medium**.

Table 3

Evaluation category: Effect on the case company IT Governance	
The Private Cloud IT (off-premises) deployment model is evaluated as for its effect on the IT Governance of the case company.	
General changes by cloud computing	All the changes to the IT Governance, applicable to the Private Cloud IT (on-premises) deployment model (Appendix 5, Table 3) apply to the Private Cloud IT (off-premises) deployment model.
Changes to InfoSec governance	InfoSec governance has to be **extended**, as the company's data moves off-premises.
Conclusion	A structure of IT Governance remains the same as the changes will only affect to the functional activities and company documentation. (Table 2 A) Compared to the other deployment models, a magnitude of change to the current IT governance is **Medium**.

Table 4

Evaluation category: Effect on the case company Sourcing strategy	
The Private Cloud IT (off-premises) deployment model is evaluated as for its effect on the Sourcing strategy of the case company.	
Changes to management of physical IT infrastructure	The management of the physical IT infrastructure for the cloud-based IT assets moves to the responsibility of the private cloud provider. The current third party outsourcing vendor continues to manage the physical IT infrastructure for legacy system.
Changes to management of software	The current third party outsourcing vendor continues to manage the software on legacy system.
Conclusion	The private cloud provider or a new outsourcing vendor is proposed for management of the software on the cloud-based IT assets in order to add a competition in the maintenance services against the current third party outsourcing vendor. (Table 2 B).

Table 5

Evaluation category: Effect on the case company operational (ITSM) processes	
The Private Cloud IT (off-premises) deployment model is evaluated as for its effect on the current operational (ITSM) processes of the case company.	
Service Level Management	Service Level Management process requires from the case company to negotiate a Service Level Agreement (SLA) with the private cloud provider for the management of the physical IT infrastructure located off-premises. Additionally, a new SLA has to be defined with the private cloud provider or a new third party outsourcing vendor for the management of the software on top of the cloud-based IT assets. Finally, the case company should have a possibility to monitor the IT service for the verification of the requirements defined in SLA, as well as make changes to the SLA during the service lifecycle. The private cloud providers are more flexible in the negotiation and maintenance of the SLA than public cloud providers. Compared to the other deployment models, an impact of the cloud computing to the Service Level Management for the Private Cloud IT (off-premises) deployment model is **Medium**.
Capacity Management	Capacity Management should support the following tasks associated with cloud computing, such as understanding of the performance data, limitations of the cloud-based IT assets, costs associated with the allocation of resources and management of the services built on top of the cloud-based IT assets. In addition, removing excess capacity becomes a critical task by the capacity management personnel. On the contrary, the management of the physical IT infrastructure and cloud environment moves to the responsibility of the private cloud provider and reduces the efforts of the capacity management personnel. Compared to the other deployment models, an impact of the cloud computing to the Capacity Management for the Private Cloud IT (off-premises) deployment model process is **Medium**.
Change Management	Change Management process for the Private Cloud IT (off-premises) deployment model has the same general requirements from the cloud computing as for the Private Cloud IT (on-premises) deployment model. (Appendix 5, Table 5) Additionally, a private cloud provider is involved into the Change Management process, as it manages the physical IT infrastructure. The private cloud provider specific procedures have to be taken into account and support options have to be available to the customer to resolve any issues that might occur in the Change Management process. Compared to the other deployment models, an impact of the cloud computing to the Change Management for the Private Cloud IT (off-premises) deployment model process is **Medium**.

Table 6

Evaluation category: Effect on the case company CMDB.	
The Private Cloud IT (off-premises) deployment model is evaluated as for its effect on the current Configuration Management Database (CMDB) of the case company.	
Requirements for CMDB	The requirements for company's CMDB in the Private Cloud IT (off-premises) deployment model are the same as in the Private Cloud IT

	(on-premises) deployment model. (Appendix 5, Table 6) Additionally, some private cloud providers offer cloud-compatible CMDB product as a service which can be integrated with the case company's CMDB.
CMDB deployment option	The possible deployment options for the CMDB are on-premises and co-location at the private cloud provider site (off-premises).
Complexity to integrate cloud services with company's CMDB	If the case company's CMDB is suitable for integration with cloud-based IT assets, the integration complexity is **Medium**. The private cloud vendors offer technical support and customization to their cloud environment for the integration. Alternatively, a new commercial CMDB product can be taken into use with built-in integration capabilities.

Table 7

Evaluation category: Risk Analysis of the Private Cloud IT (off-premises) deployment model	
The Private Cloud IT (off-premises) deployment model is evaluated as for its effect on the company's risks associated with the Privacy Assurance, Compliance Regulations and Cloud Service Provider.	
Privacy Assurance	The case company has limited control over the data located off-premises, so the risks related to the network connectivity have to be considered. The Private Cloud IT (off-premises) deployment model offers single-tenant cloud environment, which decreases the privacy assurance risks than compare to multi-tenant environments. The Private Cloud IT (off-premises) deployment model also has capabilities for customization, which allows the case company to implement the proper access controls for reduction or elimination of the risks to the confidentiality, integrity and availability. Compared to other deployment models, a magnitude of the risks associated with Privacy Assurance is **Medium**.
Compliance Regulations	Typically, a control over the sensitive data has to follow the compliance regulations and privacy laws. The case company has limited control over the data located off-premises. The private cloud provider should be compliant to the compliance regulations and privacy laws in order to be used for storage and processing of the sensitive data. Additionally, the case company needs to plan for the possible new regulations that are coming directly to the cloud providers in future by the legal authorities. Compared to the other deployment models, a magnitude of the risks associated with Compliance Regulations is **Medium**.
Cloud Service Provider	A limited control over the data and process off-premises introduces the new risks. First risk corresponds to private cloud provider dependency on the partners that provide network connectivity, premises and other services. Second risk corresponds to quality of the private cloud provider, how long and how well the private cloud provider can provide the quality services. The case company should assess the risks associated with the private cloud provider and its partners. Additionally, the risks associated with the cloud service provider identified for the Private Cloud IT (on-premises) deployment model (Appendix 5, Table 7) also apply to the Private Cloud IT (off-premises) deployment model. Risk analysis of cloud service provider has to be done and business continuity plan ready for the possible risks. Compared to the other deployment models, a magnitude of the risks associated with Cloud Service Provider is **Medium**.

Appendix 7. Detailed Evaluation of Public Cloud IT deployment model

Table 1

Evaluation category: Business requirements	
The Public Cloud IT deployment model is evaluated against the business requirements of the case company in five categories: *Cost Efficiency*, *Agility*, *Functional Requirements*, *Reliability* and *Security*.	
Cost efficiency	The Public Cloud IT deployment model offers to the customers all required capabilities. The *price model* is flexible and *price per hour* is lowest among the deployment models, as the public cloud providers have cost advantage due to economies of scale. At the same time the public cloud providers charge the customers for the out coming data traffic. In the case of high amount of data is required to be transferred from the public cloud provider to the customer, the price increases significantly. Additionally, some public cloud providers offer single-tenant environment with higher price. Two from the five business units of the case company requested high amount of out coming data traffic from the cloud provider. Due to that fact, the Public Cloud IT deployment model **partly fulfills** the requirements for Cost Efficiency.
Agility	The Public Cloud IT deployment model **fully fulfills** the business requirements of the case company. On-demand dynamic provisioning, high scalability, innovations and fast cloud evolving makes it a *best choice* from the Agility perspective.
Functional Requirements	The Public Cloud IT deployment model does not fulfill some of the requirements. The *transition technologies* are required for moving the virtual servers between on-premises and the public cloud provider environments in most of the cases. The moving data from public cloud provider to on-premises might become expensive, as the public cloud providers charge for out coming data traffic. Not all public cloud providers offer the *MPLS connectivity* option, the default Internet connectivity reduces the reliability of the cloud services. In the case of integration between on-premises Data Center and public cloud provider (off-premises), the *security* becomes a big concern. As an outcome, the Public Cloud IT deployment model **partly fulfills** the functional requirements.
Reliability	The Public Cloud IT deployment model fully fulfills the business requirements from the case company. Two business units of the case company demanded the *MPLS connectivity* to the cloud provider. Some public cloud providers do not offer the direct MPLS connectivity, which reduces the Reliability. Additionally, the *network latency*, *maintenance windows* and *multi-tenancy* need to be taken into account, as they might affect to Reliability. As an outcome, the Public Cloud IT deployment model **fulfills** the requirements for Reliability **with conditions** mentioned above.
Security	The Public Cloud IT deployment model has lowest Security compare to the other deployment models. The case company has limited control over the data and process, as the company's data stored and processed off-premises. The public cloud environment is multi-tenant, typically accessed through the Internet and available for the public use, which introduces additional risks. The public cloud providers do not allow the audits of their Data Centers and have limitations for deployment of the proper access controls. As an outcome, the Public Cloud IT deployment model **partly fulfills** the requirements for Security.
Conclusion	**Partly fulfills** the business requirements of the case company.

Table 2

Evaluation category: Effect on the case company organizational structure	
The Public Cloud IT deployment model is evaluated as for its effect on the current organizational structure of the case company *(roles and responsibilities).*	
General changes by cloud computing	All the competences defined for the Private Cloud IT (off-premises) deployment model (Appendix 6, Table 2) are applicable to the Public Cloud IT deployment model.
Changes to Management of the physical IT assets	Maintenance of the physical IT infrastructure for the cloud-based IT assets moves to the responsibility of the public cloud provider and reduces the efforts of the company's internal workforce.
Organizational actions for the changes	The trainings need to be organized for the case company's IT personnel. New roles need to be defined.
Conclusion	Compared to the other deployment models, a magnitude of change to the current organization structure is **Medium**.

Table 3

Evaluation category: Effect on the case company IT Governance	
The Public Cloud IT deployment model is evaluated as for its effect on the IT Governance of the case company.	
General changes by cloud computing	All the changes to the IT Governance, applicable to the Private Cloud IT (off-premises) deployment model (Appendix 6, Table 3) apply to the Public Cloud IT deployment model.
Changes to InfoSec governance	The Public Cloud IT deployment model has the **highest risks** associated with the security. The preventive measures should be implemented in to the InfoSec Governance.
Conclusion	A structure of IT Governance remains the same as the changes will only affect to the functional activities and company documentation. (Table 2 A) Compared to the other deployment models, a magnitude of change to the current IT governance is **High**.

Table 4

Evaluation category: Effect on the case company Sourcing strategy	
The Public Cloud IT deployment model is evaluated as for its effect on the Sourcing strategy of the case company.	
Changes to management of physical IT infrastructure	The management of the physical IT infrastructure for the cloud-based IT assets moves to the responsibility of the public cloud provider. The current third party outsourcing vendor continues to manage the physical IT infrastructure for legacy system.
Changes to management of software	The current third party outsourcing vendor continues to manage the software on legacy system. The public cloud providers do not offer the maintenance services for the software.
Conclusion	A new outsourcing vendor is proposed for management of the software on the cloud-based IT assets in order to add a competition in the maintenance services against the current third party outsourcing vendor. (Table 2 B).

Table 5

Evaluation category: Effect on the case company operational (ITSM) processes	
The Public Cloud IT deployment model is evaluated as for its effect on the current operational (ITSM) processes of the case company.	
Service Level Management	Service Level Management process requires from the case company to negotiate the Service Level Agreement (SLA) with the public cloud provider or accept the pre-defined SLA for the management of the physical IT infrastructure (off-premises). Public cloud providers in most of the cases provide pre-defined SLA which is non-negotiable. The SLA might be negotiable, if the customer is willing to make a big order. If it is not possible, the company should assess the pre-defined SLA. Additionally, a new SLA has to be defined with the new third party outsourcing vendor for the management of the software on top of the cloud-based IT assets. The case company should have a possibility to monitor the IT service for the verification of the requirements defined in the SLAs for IT infrastructure and software maintenance services, as well as make changes to the SLAs if possible during the service lifecycle. Compared to other deployment models, an impact of the cloud computing to the Service Level Management for the Public Cloud IT deployment model is **Medium**.
Capacity Management	Capacity Management should support the same tasks associated with cloud computing for the Public Cloud IT deployment model process as for the Private Cloud IT (off-premises) deployment model. (Appendix 6, Table 5) Accordingly an impact of the cloud computing to the Capacity Management for the Public Cloud IT deployment model is **Medium**.
Change Management	Change Management process for the Public Cloud IT deployment model has the same requirements from the cloud computing as for the Private Cloud IT (off-premises) deployment model. (Appendix 6, Table 5) As an outcome, an impact of the cloud computing to the Change Management for Public Cloud IT deployment model is **Medium**.

Table 6

Evaluation category: Effect on the case company CMDB.	
The Public Cloud IT deployment model is evaluated as for its effect on the current Configuration Management Database (CMDB) of the case company.	
Requirements for CMDB	The requirements for company's CMDB in the Public Cloud IT deployment model are the same as in the Private Cloud IT (on-premises) deployment model. (Appendix 5, Table 6)
CMDB deployment option	The company's CMDB might be deployed on-premises or cloud-based. The proposed deployment option for the CMDB is on-premises, as the case company continues to own the Data Center.
Complexity to integrate cloud services with company's CMDB	If the case company's CMDB is suitable for integration with cloud-based IT assets, the integration complexity is **High**. The public cloud vendors offer limited customization to their cloud environment which makes an integration challenging. Alternatively, new commercial CMDB product can be taken into use with built-in integration capabilities.

Table 7

Evaluation category: Risk Analysis of the Public Cloud IT deployment model	
The Public Cloud IT deployment model is evaluated as for its effect on the company's risks associated with the Privacy Assurance, Compliance Regulations and Cloud Service Provider.	
Privacy Assurance	The same risks for the Private Cloud IT (off-premises) deployment model (Appendix 6, Table 7) apply to the Public Cloud IT deployment model. Additionally, the Public Cloud IT deployment model has highest risks for the Privacy Assurance compare to other deployment models, as it represents the multi-tenant environment which is available to the public use through the Internet. The public cloud providers also do not allow the audits of their Data Center and might limit the customers in deploying the access controls on top of the cloud environment. On the contrary, the public cloud providers might offer the single-tenant cloud environment and MPLS connectivity for extra cost, which reduces the privacy assurance risks. Compared to other deployment models, a magnitude of the risks associated with Privacy Assurance is **High**.
Compliance Regulations	The same risks for the Private Cloud IT (off-premises) deployment model (Appendix 6, Table 7) apply to the Public Cloud IT deployment model. Additionally, the public cloud providers might not be compliant with the local compliance regulations and privacy laws, as they are typically multi-national providers. Compared to other deployment models, a magnitude of the risks associated with Compliance Regulations is **High**.
Cloud Service Provider	The risks for the Private Cloud IT (off-premises) (Appendix 6, Table 7) and Private Cloud IT (on-premises) (Appendix 5, Table 7) deployment models apply to the Public Cloud IT deployment model. Additionally, the public cloud providers might not disclose the information regarding to their partners, which makes the risk analysis of the partners impossible. Typically the cash-rich public cloud providers have lower risks compare to others. Compared to other deployment models, a magnitude of the risks associated with Cloud Service Provider is **Medium**.

Appendix 8. Detailed Evaluation of Hybrid Cloud IT deployment model

Hybrid Cloud IT deployment model consists of the Private Cloud IT (on-premises), Private Cloud IT (off-premises) and Public Cloud IT deployment models.

Table 1

Evaluation category: Business requirements	
The Hybrid Cloud IT deployment model is evaluated against the business requirements of the case company in five categories: *Cost Efficiency*, *Agility*, *Functional Requirements*, *Reliability* and *Security*.	
Cost efficiency	The Hybrid Cloud IT deployment model offers to the customers all required capabilities. The *price model* is flexible and *price per hour* is average with the proper segregation of the workloads between the various deployment models. The case company should properly utilize single-tenant and multi-tenant options in order to balance the costs and company's requirements. Additionally, the increased management costs and costs associated with the integration of the multiple cloud deployment models have to be taken into account. As an outcome, the Hybrid Cloud IT deployment model **in overall fulfills** the requirements for Cost Efficiency.
Agility	The Hybrid Cloud IT deployment model **fully fulfills** the business requirements of the case company.
Functional Requirements	The Hybrid Cloud IT deployment model **best fulfills** the business requirements of the case company.
Reliability	The Hybrid Cloud IT deployment model **fully fulfills** the business requirements from the case company. The *MPLS connectivity* should be used for the Private Cloud IT (off-premises) deployment model and *Internet connectivity* is enough for the Public Cloud IT deployment model.
Security	The Hybrid Cloud IT deployment model **fully fulfills** the business requirements from the case company. The company's data has to be *properly segregated* between the deployment models based on the security policies of the case company.
Conclusion	**Fully fulfills** the business requirements of the case company.

Table 2

Evaluation category: Effect on the case company organizational structure	
The Hybrid Cloud IT deployment model is evaluated as for its effect on the current organizational structure of the case company *(roles and responsibilities).*	
General changes by cloud computing	All the competences defined for the Private Cloud IT (off-premises) deployment model (Appendix 6, Table 2) are applicable to the Hybrid Cloud IT deployment model. The Hybrid Cloud IT deployment model represents a heterogeneous environment, which makes the management of such environment extremely challenging.
Changes to Management of the physical IT assets	Maintenance of the physical IT infrastructure for the cloud-based IT assets moves to the responsibility of the company's internal workforce, private and public cloud providers.

Organizational actions for the changes	The trainings need to be organized for the case company's IT personnel. New roles need to be defined. An integration of different cloud deployment models to Hybrid Cloud IT deployment model requires additional competences.
Conclusion	Compared to the other deployment models, a magnitude of change to the current organization structure is **High**.

Table 3

Evaluation category: Effect on the case company IT Governance	
The Hybrid Cloud IT deployment model is evaluated as for its effect on the IT Governance of the case company.	
General changes by cloud computing	The changes to IT Governance for the Private Cloud IT (off-premises) (Appendix 6, Table 3) and Public Cloud IT (Appendix 7, Table 3) deployment models are applicable to Hybrid Cloud IT deployment model.
Changes to InfoSec governance	The preventive measures should be implemented in to Infosec Governance for the Private Cloud IT (off-premises) and Public Cloud IT deployment models.
Conclusion	As the hybrid environment represent heterogeneous environment, a magnitude of change to the current IT governance is **High**.

Table 4

Evaluation category: Effect on the case company Sourcing strategy	
The Hybrid Cloud IT deployment model is evaluated as for its effect on the Sourcing strategy of the case company.	
Changes to management of physical IT infrastructure	The current third party outsourcing vendor continues to manage the physical IT infrastructure on-premises. The management of the physical IT infrastructure for the cloud-based IT assets at the Private Cloud IT (off-premises) and Public Cloud IT deployment models moves to the responsibility of the private and public cloud providers.
Changes to management of software	The current third party outsourcing vendor continues to manage the software on legacy system.
Conclusion	A new outsourcing vendor is proposed for management of the software on the cloud-based IT assets in order to add a competition in the maintenance services against the current third party outsourcing vendor. (Table 2 B).

Table 5

Evaluation category: Effect on the case company operational (ITSM) processes	
The Hybrid Cloud IT deployment model is evaluated as for its effect on the current operational (ITSM) processes of the case company.	
Service Level Management	Service Level Management process requires from the case company to negotiate the SLA for the management of the physical IT infrastructure located off-premises with the private cloud provider and accept the pre-defined SLA from public cloud provider. The case company does not have too many use cases for the Public Cloud IT deployment model and negotiation of the SLA is not possible. The company

	should assess the pre-defined SLA of the public cloud provider against the company's requirements. Additionally, a new SLA has to be defined with the new third party outsourcing vendor for the management of the cloud environment deployed on-premises and software on top of the cloud-based IT assets located at the different deployment models. The case company also should have a possibility to monitor the services of the cloud providers and software maintenance vendor for verification of the requirements defined in SLA, as well as to make changes to these SLAs during the service lifecycle if providers allow it. The workload for the Hybrid Cloud IT deployment model related to the defining, negotiating, assessing and managing the SLAs increases. Compared to other deployment models, an impact of the cloud computing to the Service Level Management for the Hybrid Cloud IT deployment model is **High**.
Capacity Management	Capacity Management should support the tasks associated with company's own Data Center and the cloud computing. All the tasks defined for the Private Cloud IT (on-premises) (Appendix 5, Table 5) and Private Cloud IT (off-premises) (Appendix 6, Table 5) deployment models apply to Hybrid Cloud IT deployment model. As the management of the multiple cloud deployment models becomes complex and requires a lot of efforts, an impact of the cloud computing to the Capacity Management for the Hybrid Cloud IT deployment model process is **High**.
Change Management	Change Management process for the Hybrid Cloud IT deployment model has the same considerations as for the Private Cloud IT (off-premises) deployment model. (Appendix 6, Table 5) Heterogeneous environment makes the change management even more challenging. This requires awareness of the management personnel about the differences in the deployment models and their specifics. As an outcome, an impact of the cloud computing to the Change Management for the Hybrid Cloud IT deployment model process is **High**.

Table 6

Evaluation category: Effect on the case company CMDB.	
The Hybrid Cloud IT deployment model is evaluated as for its effect on the current Configuration Management Database (CMDB) of the case company.	
Requirements for CMDB	The requirements for company's CMDB in the Hybrid Cloud IT deployment model are the same as in the Private Cloud IT (on-premises) deployment model. (Appendix 5, Table 6)
CMDB deployment option	The proposed deployment option for the Hybrid Cloud IT deployment model is on-premises, as the case company continues to own the Data Center.
Complexity to integrate cloud services with company's CMDB	If the case company's CMDB is suitable for integration with cloud-based IT assets, the integration complexity is **High**. The Hybrid Cloud IT deployment model represents a heterogeneous environment, which increases the complexity of the integration compare to other deployment models. In the Hybrid cloud scenario, a new commercial CMDB product compatible to work with the various cloud environments might be the best choice for the case company. Unfortunately, the most of the

	commercial CMDB solutions for the Hybrid Cloud IT deployment model available on the market are dedicated to the particular cloud providers or to the cloud technologies, which creates a vendor or technology lock-in situation for the customer. In the case of taking new commercial CMDB product in to use, the case company should make a strategic choice into the direction of the particular technology or cloud vendor.

Table 7

Evaluation category: Risk Analysis of the Hybrid Cloud IT deployment model	
The Hybrid Cloud IT deployment model is evaluated as for its effect on the company's risks associated with the Privacy Assurance, Compliance Regulations and Cloud Service Provider.	
Privacy Assurance	The same risks for the Private Cloud IT (off-premises) (Appendix 6, Table 7) and Public Cloud IT (Appendix 7, Table 7) deployment models apply to the Hybrid Cloud IT deployment model. If the data and workloads are segregated properly between the different deployment models, a magnitude of the risks associated with Privacy Assurance is **Small**.
Compliance Regulations	The same risks for the Private Cloud IT (off-premises) (Appendix 6, Table 7) and Public Cloud IT (Appendix 7, Table 7) deployment models apply to the Hybrid Cloud IT deployment model. If the data is segregated properly between the different deployment models, a magnitude of the risks associated with Compliance Regulations is **Small**.
Cloud Service Provider	The risks for the Private Cloud IT (on-premises) (Appendix 5, Table 7), Private Cloud IT (off-premises) (Appendix 6, Table 7) and Public Cloud IT (Appendix 7, Table 7) deployment models apply to the Hybrid Cloud IT deployment model to some extent. The data and workloads segregation between the different deployment models reduce the risks. Additionally, a magnitude of the risks associated with the cloud providers might be decreased with the proper risk analysis of the cloud providers. Typically the cash-rich or technology-leading cloud providers have lower risks compare to other providers. As an outcome, a magnitude of the risks associated with Cloud Service Provider is **Medium**.