Why Consumerization Affects IT Management

Esa Hietikko

Master's Thesis

UNIVERSITY OF
EASTERN FINLAND

Faculty of Science and Forestry

School of Computing

June 2014

UNIVERSITY OF EASTERN FINLAND, Faculty of Science and Forestry, Kuopio
School of Computing
Computer Science

Hietikko, Esa M.: Why Consumerization Affects IT Management
Master's Thesis, 71 p.
Supervisor of the Master's Thesis: PhD Niina Päivinen
June 2014

Abstract:

Standardization of information technology (IT) resources, such as devices and software, and the centralization of their acquisition have traditionally been essential guiding principles for IT management in organizations. Additionally, so called lockdown methods and usage restriction policies have been utilized in order to maintain the performance, information security, and compatibility of the IT resources.

In this master's thesis, we will first get familiar with the basic concepts, practices, and tools of IT management. After that, the thesis discusses what the consumerization of IT is, and how or why it affects to the IT management in organizations. The topic and the goal of this thesis are based on the observation that this far the research literature seems to have focused on researching the consequences that are caused by the consumerization of IT, although it is not yet clearly known what are the factors which cause those consequences.

This thesis is a literature review, and its purpose is to explore what are the consequences of the IT consumerization to the IT management, and more importantly, what are the underlying factors why the consumerization of IT affects the IT management. On the other hand, the aim of the literature review is also to either confirm or refute the observation that there is a gap in the research literature concerning the research of the factors why the consumerization of IT affects the IT management.

Eventually, this thesis suggests, based on the research literature and the author's contribution, that there are at least seven different factors, through which the consumerization of IT seems to affect to the IT management, and which help to explain *why* the consumerization of IT affects the IT management.

Keywords: Consumerization, IT Management

ITÄ-SUOMEN YLIOPISTO, Luonnontieteiden ja metsätieteiden tiedekunta, Kuopio
Tietojenkäsittelytieteen laitos
Tietojenkäsittelytiede

Hietikko, Esa M.: Miksi kuluttajistuminen vaikuttaa tietohallintoon

Pro gradu –tutkielma, 71 s.
Pro gradu –tutkielman ohjaaja: FT Niina Päivinen
Kesäkuu 2014

Tiivistelmä:

Tietoteknisten resurssien, kuten laitteiden ja ohjelmistojen standardointi ja niihin liittyvien hankintojen keskittäminen ovat perinteisesti olleet keskeisiä ohjaavia periaatteita organisaatioiden tietohallinnossa. Lisäksi tietohallinnossa on hyödynnetty ns. lukitusmenetelmiä ja käyttöä rajoittavia politiikoita, joiden avulla on haluttu ylläpitää käytössä olevien resurssien suorituskykyä, tietoturvallisuutta ja yhteentoimivuutta.

Tässä pro gradu –tutkielmassa tutustutaan ensin korkealla tasolla tietohallinnon peruskäsitteisiin, käytäntöihin ja työkaluihin. Sen jälkeen tutkielmassa syvennytään pohtimaan mitä on tietotekniikan kuluttajistuminen, ja kuinka tai miksi kuluttajistuminen voisi vaikuttaa organisaatioiden tietohallintoon. Tutkielman aihe ja tavoite perustuvat havaintoon siitä, että tutkimuskirjallisuus näyttäisi tähän saakka painottuneen kuluttajistumisen tietohallinnolle aiheuttamien seurauksien tutkimiseen, vaikka toistaiseksi ei vielä tunneta kovin hyvin niitä syitä, mitkä aiheuttavat havaittuja seuraamuksia.

Tutkielma on kirjallisuuskatsaus, jonka tarkoitus on selvittää mitä ovat kuluttajistumisen aiheuttamat seuraamukset tietohallinnolle ja ennen kaikkea mitä ovat ne syyt tämän taustalle, eli miksi kuluttajistuminen vaikuttaa tietohallintoon. Toisaalta kirjallisuuskatsauksen tavoitteena on myös vahvistaa tai kumota edellä mainittu havainto siitä, että onko syitä kuluttajistumisen vaikutuksista tietohallintoon toistaiseksi tutkittu kattavasti.

Kirjallisuuskatsauksen ja kirjoittajan oman kontribuution pohjalta esitetään vielä lopuksi seitsemää vaikuttavaa osatekijää, joiden kautta kuluttajistuminen näyttäisi vaikuttavan tietohallintoon ja mitkä osaltaan selittävät *miksi* kuluttajistuminen näyttäisi vaikuttavan tietohallintoon.

Avainsanat: kuluttajistuminen, tietohallinto

Acknowledgements

I want to sincerely thank my employer Miradore Ltd for granting me a term of study-leave and the University of Eastern Finland for the M. Sc. thesis completion grant, which together made it possible to complete this thesis. I also would like to thank my thesis supervisor Niina Päivinen and inspector Marko Jäntti, who both provided excellent feedback and comments on my work.

List of Terms and Abbreviations

Term or Abbreviation	Description
Admin	Computer systems administrator, IT administrator, or administrator.
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.
Asset management (AM)	An activity or process responsible for tracking and reporting the value and ownership of assets throughout their lifecycle.
Configuration item (CI)	Configuration items (CIs) are basically abstractions or management units that are needed to manage the IT or service assets and components in a configuration management system (CMS).
Cloud	The terms cloud and cloud computing are very close to distributed computing, and when an information system is offered from a cloud, it means that the solution doesn't have to be installed for the users locally, but instead it can be remotely used on-demand by multiple users through web technologies.
Configuration management (CM)	Configuration management is the process responsible for capturing and maintaining information of how the IT infrastructure components are configured, and what are the relationships between the components throughout their lifecycle.
CMDB	Configuration management database.
CMS	Configuration management system.
Community cloud	Community cloud is an information system deployment model where the information system is provided from cloud using a shared, multi-tenant infrastructure.
Configuration Record	The information related to each configuration item is recorded in a configuration record.
Hardware asset management (HAM)	The management of hardware assets such as computers, printers, and other devices.
Help desk	Help desk provides IT users with information and support related to IT services.
IaaS	Infrastructure as a service.

Infrastructure management (IM)	Management process responsible of managing the components of an IT infrastructure, such as hardware and software assets and their configuration settings.
Internal cloud	A synonym for the *private cloud*.
ITIL	Information Technology Infrastructure Library (ITIL) is a widely known and generally accepted collection of documented IT management best practices.
IT	Information technology.
IT asset management (ITAM)	ITAM is the process of managing organizations hardware and software assets.
Information technology service management (ITSM)	Information Technology service management means the organizational abilities to provide value to customers through IT services. The activities may include integration and utilization of specialized people, processes, and tools.
Information technology service management foundation (itSMF)	Information technology service management foundation is an independent organization of ITSM professionals, which develops and promotes ITSM related best practices such as ITIL and arranges trainings and discussions.
Management agent	Management agent is a background application which runs on a managed device and is responsible for administering the device management task in the device. A management agent communicates with a management system's central server.
MoSCoW technique	The MoSCoW technique is a method for collecting and prioritizing requirements for an information system.
PaaS	Platform as a service.
PC	Personal computer.
Private Cloud	In the on-premise private cloud deployment model, an IS is exclusively hosted for the user organization within its own premises. The cloud is private because it is operated on a single-tenant infrastructure, which means that the system hardware, software, and database are dedicated for the use of particular user organization.
Public Cloud	In public cloud deployment, the IT solutions are always provided from off-premise data centers for users over the public Internet as a service, and the IT

	solutions are not hosted exclusively for the customers, but instead they are *multi-tenant* by their nature.
RQ	Research question.
SaaS	Software as a service.
SACM	Service asset and configuration management.
Software asset management (SAM)	SAM is a process of managing organization's software resources.
Service level agreement (SLA)	SLA is an agreement between the service provider and a customer, which describes and documents the IT service, the service targets, and specifies the responsibilities of the service provider and the customer.
Systems management	Systems management is the activity of identifying and integrating various products and processes in order to provide a stable and responsive IT environment.

Table of Contents

1 Introduction

The intention of keeping organizations' information technology (IT) resources, such as hardware and software components consistent, and reducing the range of tools that address the same purpose, are the guiding principles in *IT standardization*, which together with *centralization* has been the best practice for IT management over a decade for now [CC10, Pet08]. In the centralization concept, which is often employed in conjunction with the standardization, the decision-making power, ownership, and control over the IT resources are centralized to the organizations' IT departments.

Recently, it has been noticed that people around the world have increasingly started to use mobile devices, cloud services, and other consumer technologies for working and accessing the organization IT resources like networks, e-mail etcetera. This trend is called *consumerization of IT* [GF11, HIJ12, Mor14].

Although the IT consumerization has been debated and researched pretty widely during the last few years, it has been identified that the focus of research has clearly been on researching the consequences of consumerization to organizations [OKBN13]. At the same time, surprisingly little research has been conducted to discover *why* the consumerization affects to organizations in terms of IT management.

The ambition of this thesis is to confirm the research gap, and on the other hand, to provide contribution to the question: "Why consumerization affects IT management?"

This thesis is structured as follows: chapter two describes how the thesis and the related work were conducted, chapter three introduces the essential IT management concepts, chapter four presents the tools and practices that have traditionally been used for IT management tasks, chapter five deals with the consumerization and the phenomena that belong under the umbrella of consumerization, chapter six describes why consumerization affects IT management, chapter seven introduces some management strategies that have been proposed to control the consumerization, and finally chapter eight concludes the thesis and summarizes the most important findings.

2 Research Design

This chapter describes how this thesis and the related work were conducted, and explains why the used approach was selected. Additionally, this chapter introduces the research questions, and reasons why they are considered important.

2.1 Motivation

The author of this thesis had about three years of working experience from documenting and developing IT infrastructure management systems before starting to work with this thesis. In this job, the author had noticed that there are numerous competing management systems and solutions which are used for the same purpose – for managing the IT infrastructure components, such as hardware and software components, their relationships, or the related IT services. However, these solutions often go with many different names, although they would have very similar kind of feature sets with each other. Therefore, it is sometimes difficult to understand, what would be the appropriate terms for calling the key tools and processes in IT management.

On the other hand, in his work, the author had also experienced the emergence of consumer devices and cloud services in the corporate IT environments, and heard the terms *Bring Your Own Device (BYOD)* and *Consumerization* quite often, but he really wasn't sure what they mean. Therefore, one goal of this thesis was to find more information of those concepts and also explore what kind of impact BYOD and consumerization might have to the management of IT infrastructure components in corporate environments, which have traditionally been very uniform and strictly regulated environments.

Thus, the intention of this thesis was to shape research questions and approach the topic in an academic way. During the research process, it was found out that there is already some debate going on about what are the consequences of consumerization for

IT management, but the discussion seemed to be missing the point *why* consumerization affects to the IT management. Therefore, that was selected as the emphasized approach for this thesis.

This gap in the research had been also been notified by Ortbach & al. [OKBN13], who stated: "*Overlooking the research undertaken in the area of IT consumerization, there is a clear focus on the consequences of the trend, for the most part in order to estimate the pros and cons for individuals and organizations*". In their own research, Ortbach & al. aimed to fill this gap by explaining the causal relations and reasons why people adopt consumer technologies for work, but the reasons why consumerization of IT affects IT departments and IT service providers doing IT management still remain largely undiscovered.

2.2 Research Questions

This section introduces the four research questions (RQ) that were shaped based on the preconception about the thesis topic.

RQ1: What are the key terms, processes, and management concepts related to IT management, and what are their industry accepted definitions?

RQ2: What kind of tools or systems are typically used to automate or manage the IT management processes?

RQ3: What does IT consumerization mean, and what are its consequences to the IT management?

RQ4: Why the consumerization of IT does affect IT management?

Why these research questions were considered as important? The research question one is important, because the currently available IT infrastructure management systems and solutions are called with very many names, such as asset management systems, configuration management systems, IT management systems, IT service man-

agement systems, IT systems management solutions, remote monitoring and management systems, systems management solutions etcetera, but in fact, many of them have overlapping or even identical feature sets. This makes it really difficult to compare the systems with each other and decide what is actually needed to perform certain IT management routines. Therefore, it is logical and justified to start the thesis by getting familiar with the key concepts and their relationships to each other.

Answering the RQ2: "*What kind of tools or systems are typically used to automate or manage the IT management processes?*" is a prerequisite for answering the RQ4, because we cannot evaluate how consumerization affects to IT management if we don't first get familiar with the IT management concepts.

RQ3 is important, because consumerization of IT as a phenomenon is quite new, and therefore it has many different definitions in different contexts of use. Additionally, it is important to review what is already known about the consumerization, before rushing to make more research. It is also necessary to define the consumerization of IT carefully, because otherwise it might be difficult to say we mean by that.

Ultimately, the RQ4: "*Why the consumerization of IT affects IT management?"* is important, because it contributes a new approach to a so far lightly covered area of consumerization research. The better we can understand the causes of the impact that consumerization has to the IT management, the better we can understand and react to the consequences that are the causal result of those causes.

2.3 Groundwork

This stage of thesis work included two parts: first, the exploration of the key terms, processes, concepts that are related to IT management, and second, the studying of the automation tools and their deployment models, as stated in RQ1 and RQ2. Because Information Technology Infrastructure Library *(ITIL)* [itSMF07] is a widely known and generally accepted collection of documented IT management best practices, it was selected as the theoretical framework for getting familiar with the key concepts, processes, and terminology that are related to IT management work in practice.

The IT management related concepts, processes, and terms that are relevant to this thesis, are introduced in the chapter three, which is mainly based on different volumes of ITIL. However, it is good to notice that the amount of presented concepts in this thesis is very limited, because it is possible to identify a countless number of different management activities that belong under the umbrella of IT management, but they all aren't necessary to be discussed within the scope of this thesis. The included terms and concepts were selected because they were regarded as most relevant and beneficial for dealing with the topic of this thesis.

In addition to introducing the key terms, processes, and concepts that are related to the IT management, this phase of the thesis work also included the research on IT management automation tools, and their deployment models. This phase was conducted by exploring the literature and the tools that are currently available on the markets. The results of this stage are presented in the chapter four.

2.4 Literature Review

After exploring the main terms, processes, and concepts as stated by RQ1, the conceptual framework started to get shape, and it was easier to plan how to search information to research the RQ3 and RQ4. Additionally, researching the RQ2 provided better understanding over the automation tools and their different deployment models, which gave good indications of what could be the ways how consumerization of IT might affect to the IT management. In other words, the literature review for answering the RQ 3 and RQ4 was planned after researching the RQ1 and RQ2, because before that it was difficult to conceptualize and understand all the different concepts and their relationships.

Building on the acquired knowledge, this stage of the thesis work aimed to answer the RQ3 and RQ4. This phase of the research was conducted as a literature review, in order to confirm the gap in the existing research literature. The information for these questions were searched from Nelli (a national information retrieval portal, for accessing extensive electronic resources including databases, online journals, electronic books,

and dictionaries) and Google Scholar. The search was conducted by using the following search phrases and their reasonable combinations:

- Asset management
- Asset and configuration management
- Bring Your Own Device
- Configuration management
- Consumerization
- Consumerization challenges
- Consumerization of IT
- Device management
- Heterogeneity of devices
- IT consumerization
- IT management
- IT management practices
- Management system
- Management tools
- Shadow IT
- Systems management
- Workstation management

The search results were then evaluated based on their title and summary or introduction, whichever was available. The found material was included in the literature review if it was considered to be related to the topic of this thesis, and more specifically if it provided information for answering the RQ3 or RQ4. Additionally, all publications published before 2004 were excluded from the literature review, because they were not believed to contribute this thesis, because the consumerization as a concept was initially recognized in 2004 [MNOT04].

Based on the inclusion criteria, the following publications were included in the literature review (see *table 1: Included literature*). The selected publications and their contribution to the thesis topic are discussed in the remaining chapters in this thesis.

Publication
Cosgrove T., Colville R. J. (Gartner, 2010) *Organizations Are Increasing PC Lockdown*.
Costello T., Prohaska B. (IEEE Computer Society, 2013) 2013 Trends and Strategies, *IT Professional*, pp. 61-63
Cummings J., Massey A. P., Ramesh V. (2009), *Web 2.0 Proclivity:* Understanding How Personal Use Influences Organizational Adoption, Operations and Decision Technologies Department, Indiana University
Disterer G., Kleiner C. (University of Applied Sciences and Arts, Hannover, Germany, 2013) BYOD Bring Your Own Device, *CENTERIS 2013 - Conference on ENTERprise Information Systems / ProjMAN 2013 - International Conference on Project MANagement / HCIST 2013 - International Conference on Health and Social Care Information Systems and Technologies*
Geyer M., Felske F. (ACM, 2011) Consumer toy or corporate tool: the iPad enters the workplace. *Interactions*, Volume 18, Issue 4, pp. 45-49
Harris J., Ives B., Junglas I. (2012) IT Consumerization: When Gadgets Turn Into Enterprise IT Tools. *MIS Quarterly Executive*, Volume 11, Issue 3, pp. 99-112
Morabito V. (Springer International Publishing Switzerland 2014), *Trends and Challenges in Digital Business Innovation*, Chapter 5, pp. 89-109.
Niehaves B., Köffer S., Ortbach K., Katschewitz S. (European Research Center for Information Systems 2012) *Towards an IT Consumerization Theory – A Theory and Practice Review*, Working Paper No. 13
Niehaves B., Ortbach K., Köffer S. (ACM 2013) IT consumerization under more difficult conditions – Insights from German local governments, *The Proceedings of the 14th Annual International Conference on Digital Government Research*, pp. 205-213
Parsi K., Laharika M. (2013) A Comparative Study of Different Deployment Models in a Cloud, *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 5, pp. 512-515
Walters R. (SaaSID 2013), Bringing IT out of the shadows, *Network Security*, Volume 2013, Issue 4, pp. 1-20

Table 1: Publications included in the literature review

2.5 Own Contribution

Almost all tasks related to this thesis were on the sole responsibility of the thesis author, including the topic selection, definition of inclusion criteria for the literature review, the literature review, making conclusions, and the actual authoring of this written thesis. In addition to that, the own contribution shows particularly well in chapters six and eight, which contain a lot of the author's own thoughts besides those which were

derived from literature. However, the inspector (Ph. D. Marko Jäntti) and the supervisor (Ph. D. Niina Päivinen) of this thesis provided valuable support by proof-reading and commenting the thesis.

3 IT Management Concepts

This chapter presents the key IT management concepts that are essential to understand when discussing about the management of an organizations' IT resources. The presented concepts are: *IT Asset Management* (ITAM), *Configuration Management* (CM), *Change management*, *Systems management*, and *IT Service Management* (ITSM). This chapter also attempts to explain the relationships of these concepts to each other, and describe the role and possible sub-processes of each concept. Additionally, one goal of this chapter is to familiarize the reader with the key concepts and terminology of IT and IT infrastructure management, and introduce the key publications where more information can be found.

3.1 Administrators

A *computer systems administrators* or *IT administrators* are professionals who are familiar to many who have used the IT resources, such as workstations or printers of some enterprise or organization. The IT administrators (or *admins)* are typically the "magicians" who can almost mystically wipe away any IT-related problems when IT users run into troubles with the IT. But how do they do that, and what are actually the duties of an IT administrator? That is something which isn't so obvious – although it is not magic after all.

> According to [Web14]: *"Computer system administrators install, maintain, and support an organization's information technology systems. They test system components to ensure that computers, software, and network equipment function seamlessly together. System administrators may be in charge of the company's LAN, WAN, intranet, or Internet systems. Some administrators focus on specialist roles such as network security, IT audit, or system upgrade research."*

A common example of such a specialist role, especially in bigger organizations, is the role of the *service asset manager* [OGC11a, pg. 315]. The service asset manager is basically an IT administrator whose responsibility is firstly: to manage organization's

IT resources through their entire lifecycle including procurement, assignation, utilization, renewal, and disposal, and secondly: to plan, implement, and staff the related asset management processes and workflows.

Another example of such specialist role is the *help desk operator* who specializes in providing information and support services to IT users who encounter problems with IT. Thus, when people have difficulties with IT, they usually contact to *help desk* or *service desk* which then helps to resolve the reported *incident*. According to ITIL® glossary [HR11], incident is an unplanned interruption to an IT service, or a reduction in the quality of an IT service. Incidents are caused by *problems* which are the cause of one or more incidents.

Hence, we understand that the IT administrators have a lot of duties ranging from financial planning to testing software and providing support for the IT users, and many of their duties are not visible outside the IT department. Anyway, the bottom line is that there is a great number of duties and responsibilities to take care of.

In relatively small organizations, where the amount of IT resources to be managed is low and which employ only a small group of IT administrators, it is rather common that the organizations are working on an ad-hoc basis without formal and documented processes. It is understandable that the small organizations don't wish to invest a lion's share of money into *enterprise resource planning* (ERP) systems or costly IT management tools. However, when the organization size grows and the number of IT staff and components arise, the demand for a systematic way of working raises rapidly.

In order to understand how the entire process of IT management can be systematically organized in any size of organizations, we will next get familiar with some basic concepts or processes which are the essential building blocks of organized IT management.

3.2 Asset and IT Asset Management

Earlier, we learned that asset is something comparable to a resource. Next, we will give a more comprehensive definition for the asset, because it is one of the most important terms related to the process of managing IT infrastructure components, and it must be therefore discussed thoroughly. ITIL, which is the most widely adopted systematic and professional best practice framework to the management of IT services, defines the asset as follows [HR11]:

"Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service. Assets can be one of the following types: organization, process, knowledge, people, information, applications, infrastructure, or financial capital."

What we should learn from this definition is that the assets can be of many types, either tangible or intangible, and they contribute to the delivery of services. The *asset management* process, on the other hand, is defined as follows [HR11]:

> *"An activity or process responsible for tracking and reporting the value and ownership of assets throughout their lifecycle."*

What is especially important in this latter definition is that it emphasizes the tracking and reporting of the assets' value and ownership through their entire *lifecycle*. If we now would try to understand the concept of *IT Asset Management (ITAM),* we could say, based on the ITIL definitions, that:

> *ITAM is process of tracking and reporting the value and ownership of such IT resources that are needed to deliver IT services, through their whole lifecycle.*

At this point, one could ask what we mean with the lifecycle, and what are those IT resources that are needed to deliver the IT services. The answer of course depends on the offering of organization's IT services, and the desired level of management and control – but in general, organizations are usually interested in tracking and reporting

physical (e.g. devices), logical (e.g. software), and contractual (e.g. financial information) assets from purchase to disposal – with a varying amount of lifecycle stages in between of those. In fact, the lifecycle management of physical assets e.g. computers and network equipment is often called *Hardware Asset Management* (HAM), whereas the lifecycle management of software applications and licenses is called *Software Asset Management* (SAM), and usually the term asset management is a collective term that is used to refer to those both.

Anyway, as it was stated earlier, organizations need a systematic, and preferably an automated way or system for identifying, inventorying, tracking, and reporting their assets (i.e. service resources) reliably, accurately, and in a timely manner, because the ITAM basically forms the foundation for the higher level IT management activities. For example, it would be quite impossible to plan or assess the feasibility of new services if resources and capabilities are not accurately known to the service provider organization. But if the resources and capabilities are well-known, then it is possible to figure out how they could be combined in order to establish a new services.

In other words, the purpose of ITAM is to translate IT assets such as hardware, software, and immaterial property into an understandable and easy-to-use form, which supports the other IT management functions such as financial and technological planning, maintenance of day-to-day operations, and governance of the entire IT management. Additionally, the secondary mission of ITAM is to coordinate how people and processes collaborate and exchange information during the IT service production.

3.2.1 Different Types of Asset Information

What kind of information organizations could, or perhaps should collect concerning their assets? That naturally depends on the organizations' strategy and operations, but here are some examples of what different types of asset information exist:

- An inventory of owned assets e.g. hardware, software, and infrastructure components, and their characteristics or properties. These can be gathered manually or discovered automatically using discovery technologies.

- What is the value of the owned assets? The value information, or purchase price is often registered manually when an assets are acquired.
- Who owns or is responsible for the assets?
- Where the assets are physically located?
- Contractual, financial, lease, license, warranty, invoice, vendor and supplier information and contracts that are related to the assets.
- What are the different asset statuses during the asset's lifecycle?

3.3 Configuration Management

Within ITIL [OGC11a, pp. 118-121], the asset management and the configuration management concepts are actually discussed as one, *service asset and configuration management* (SACM) process, because in practice, these two processes always go hand in hand. In this thesis, however, we will discuss these processes separately in order to emphasize the different responsibilities, functions, and aspects that must be considered in the management of organizations' IT resources.

As the asset management process is responsible for governing the management of organizations' IT resources, the *Configuration Management* (CM) process is responsible for tracking and reporting the physical and logical structure of the resources, the use of the resources, and mapping the inter-relations of the resources or components. Thus, the configuration management is a process responsible for capturing and maintaining information of how the IT infrastructure components, i.e. assets, are configured, and what the relationships are between the assets throughout their lifecycle. Configuration management is not interested in the ownership or value of the components or assets, but instead of their configurations and relationships.

For example, if we consider software license management, where the duty of the asset management is to know how many software licenses an organization has purchased, and what the value of those licenses is, the responsibility of configuration management is to report which devices have the licensed software installed, and thus consume a

license. Configuration management is all about giving information and tools for managing the relationships and configurations of IT assets or components.

3.3.1 Configuration Item

Configuration items (CIs) are basically abstractions or management units that are needed to manage the IT or service assets and components in a *configuration management system* (CMS) [OGC11a, pp. 122-123]. In a CMS, there is a separate configuration item for every unique IT component that is desired to be managed. Examples of these include: devices, applications, agreements, and users. The information related to each CI is recorded in a *configuration record*, which is maintained by the ITAM and CM activities throughout the lifecycle of the CI.

Typically, a CI has a certain amount of attributes, which describe and store information about the CI into the configuration record. For example, a software CI would likely have attributes such as software name, software vendor, software version, and information of the installation count of the software (i.e. number of devices which have the software installed). This is of course only an example and subset of the possible attributes.

In operational use, the CIs are like reflections of their "real-life" counterparts, and the actual values of the configuration item attributes are then retrieved, mostly automatically, from the actual IT environment by ITAM and CM sub-processes, such as discovery and inventory procedures. For example, let us say that an organization would have ten different software titles installed to its computers. In that case, the organization would also need ten different software CIs to reflect the applications used in the environment, one for each unique software title. For example, one for a PDF reader program, and another for the word processor application etcetera.

The recorded configuration item attributes may vary a lot between different configuration management systems, or they may be the same with different names, but the aim is always the same – to capture the meaningful information about the configuration items for the use of IT management.

3.3.2 Configuration Management System

A configuration management system is a consolidated information system for collecting, storing, managing, updating, analyzing, and presenting data about CIs, their relationships, and related processes through their entire lifecycle from acquisition to disposal [OGC11a, pp. 123-125 & 335-336]. Usually, CMSs provide automation for most of the configuration management processes, but also support the creation of new relationships between the IT components as well. The set of supported processes and tools, for manipulating the managed configuration items, may vary a lot depending on the CMS vendor.

The objective of a CMS is to enable, unite, and automate the ITAM and CM processes, and support the IT service provisioning by providing accurate, reliable, and up-to-date information and effective tools for the IT users in different roles, such as help desk, IT managers, and information security officers.

3.3.3 Configuration Management Database

Configuration management database (CMDB) is a configuration management system's central database where the configuration items, configuration records, and configuration item relationships are stored [OGC11a, pg. 124]. The CMDB is practically the heart of the entire IT management, as it stores all the information that the asset and configuration management processes capture from the managed IT environment. The more an organization, or IT service provider, can consolidate the information of its IT environment and services into a single CMDB – and thus automate the data processing, the easier the organization can recognize and manage the relationships between the assets and configuration items related to its IT services. Therefore, it is justified to say that consolidation of asset and configuration management data into a single CMDB, instead of having multiple systems with separate databases is beneficial. However, it is common that IT service providers use multiple systems for storing information about the IT and services. For example, IT service providers often have a separate asset management system and service management system running side by side on different databases, which is not optimal.

3.4 Change Management

According to ITIL® glossary [HR11], change management is:

> *"The process responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services."*

According to ITIL Service Transition volume [OGC11a, pg. 77], the meaning of change management process is to ensure that:

- *"Standardized methods and procedures are used for efficient and prompt handling of all changes"*
- *"All changes to service assets and configuration items are recorded in the configuration management system"*
- *"Overall business risk is optimized"*

Earlier we discussed about configuration management and learned that the purpose of the configuration management process is to map the relationships and configurations of the managed IT components. Additionally, it is the responsibility of the configuration management to provide tools for managing the configuration changes, and this is where the process of change management comes in. The change management process is actually a sub-process, or at least very tightly related process with the configuration management process. The purpose of the change management process is to provide a controlled way of making changes to the configuration items, which reflect the actual IT environment, and which are managed by the configuration management process. For example, the change management process describes the required steps that should be taken when a software installation or upgrade is performed to a managed computer. In addition to that, the different policy enforcement settings, such as password policy settings, are also deployed to organization's devices through the configuration and change management processes. Hence, the reliability of the change management process is important in IT management.

3.5 IT Systems Management

IT Systems management is a somewhat vague term that is often used to refer those activities, or a subset of activities, which are considered to be related to the management of organizations IT resources. These may include activities similar to asset and configuration management, change management, and also other activities, which basically makes it a synonym or an interchangeable term with *IT service management (ITSM)*, but perhaps with little more technologist approach to it.

The IT service management term will be discussed in the next chapter, and after that we will prefer that over the IT systems management, because the use of IT systems management term is not really suggested by ITIL. Before that, however, we will take a short look to the term of IT systems management as well.

According to Rich Schiesser, IT Systems management can be defined as follows [Sch12, pg. 2]:

> *"Systems Management is the activity of identifying and integrating various products and processes in order to provide a stable and responsive IT environment."*

In the *IT Systems Management* book [Sch12, pp. 89-107], Schiesser compares the categorization and definitions of *IT infrastructure management (IM)* processes – as suggested in his book, with the ITIL framework, and he notices that there are only minor differences in how these models describe the sub-processes under the IT management. For most parts, the IT systems management concept proposed by Schiesser, is very much alike with ITIL.

In this thesis, we will prefer the ITIL framework because it is a well-established and de facto standard for IT management around the world, and it is not desirable to mix the use of these terms, because there is already so many concepts to handle.

3.6 IT Service Management

Effective management and use of organizations IT resources is a prerequisite for IT service management, which is a higher level management of organization IT. As defined in *Service Transition* volume of ITIL [OGC11a]:

> *"Service management is a set of specialized organizational capabilities for providing value to customers in the form of services."*

The capabilities refer to specialized functions, people, processes, and infrastructure of an organization which are used to manage services through their lifecycle to enable service provisioning. Without these capabilities, the service organization is merely a bundle of resources, which are not able to provide any value for customers. The ability to perform asset and configuration management and change management (i.e. organization's ability to manage its IT infrastructure) is a good example of such capability. So, based on these facts, we might define the IT service management as follows:

> *Information Technology service management means the organizational abilities to provide value to customers through IT services. The activities may include integration and utilization of specialized people, processes, and tools.*

In many organizations there is an internal IT department, which is responsible for the IT services that the organization needs, but there is also great number of third-party *IT service providers (ITSPs)* or *Managed Service Providers (MSPs)*, which offer common IT services, such as IT asset and configuration management, for other organizations seeking for outsourcing. It is also common that the portfolio of IT services varies a lot between the different MSPs, because it is an important way for them to differentiate from each other.

Anyway, the most important goal of the ITSM process is to align the delivery of the IT services with the organization's business needs. It aims to deliver end-to-end operations efficiently, and provide benefits and value, regardless of whether the customers are internal or external to the organization.

3.6.1 The Development of IT Service Management

In Schiesser's *IT Systems Management* book [Sch12, pp. 55-56], it is described how IT evolved into a service industry, since it hasn't always been like that.

According to Schiesser, in the 1970s while the IT industry was still in its infancy, the emphasis of IT departments was mostly on providing the organizations with newer and faster computing systems and machines. At the same time there was only very little alternatives in IT suppliers, and therefore the importance of customer service, or service management was negligible.

However, by the 1980s, it was realized that the quality of IT and the IT services had a positive impact to the organizations' revenue, profits, and image, which significantly increased their importance. At the same time, a greater number of people were exposed to the IT because online applications were starting to replace the legacy information systems, which fueled the demand for high availability and customer support services. As a result, primitive user groups, help desks, and *service level agreements* (SLAs) were established to address the demands. By ITIL glossary [HR11]:

> *SLA is an agreement between the service provider and a customer, which describes and documents the IT service, the service targets, and specifies the responsibilities of the service provider and the customer.*

Again, by the 1990s, PCs and the Internet had become more the rule rather than exception in workplaces and home, and many people were familiar with the use of computers. And as a result of this development, people weren't any more just hoping for a good customer service, but instead, they were expecting for that. The demand for better services often lead to outsourcing of customer IT services, and demand for even higher know-how. Eventually, IT had grown from pure accounting and technical environment into a totally service-oriented entity.

During the last decades we've witnessed a change of paradigm from managing IT and technical environments to managing users and non-technical aspects. It is no more the

ultimate goal of IT to manage the devices, but instead to provide user-oriented IT services, which benefit the user and the surrounding organization.

Since then, it has been common that even the small enterprises and organizations have outsourced the management of their IT to an external third-party service provider, and want to save their own energy and focus on to their core business.

3.6.2 The Levels of IT Service Management

This chapter shortly introduces the different levels of IT service management, according to a three-stage evolutionary model presented in Hewlett Packard's *HP IT Service Management* publication [HP03]. It describes how IT organizations typically evolve from technology providers into strategic business partners, enabling new business opportunities (See Figure 1).

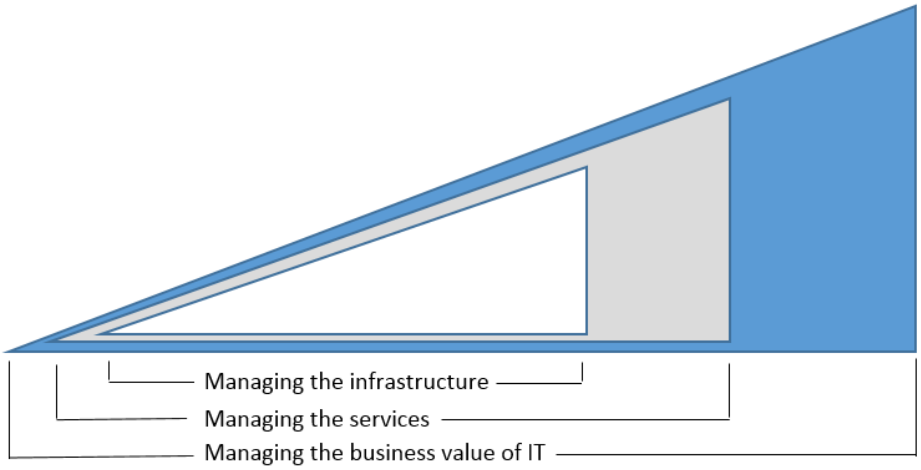

Figure 1: The Evolutionary Stages of IT Organizations (Adapted from [HP03])

In the first stage, the IT organizations are focused on pure IM which means that they are focusing on the management of the organization's IT infrastructure components (e.g. hardware, software, and network). Their aim is to maximize the return on computing assets and take control over the IT by performing effective IM. The desired outcome is to deliver a highly available IT infrastructure and accurate, up-to-date in-

formation on the status of the infrastructure components. At this stage, the comprehensive management and monitoring of the infrastructure are the key processes to the IT organizations.

In order to achieve the capability and maturity required by the first stage, the IT organizations usually implement special solutions, which offer tools for automating and standardizing the key IM processes. These processes include, for example, the discovery, inventory, and monitoring of the IT components. Such technology is often based on distributed clients (a.k.a. *management agents*), which run on the managed devices, and administer the management tasks in collaboration with the management system's central server. The information collected by the management agents is then provided for the IT staff through a single console in order to simplify the infrastructure management. Thus, the success and efficiency of this phase rely heavily on the technology which automates the management processes.

In the second stage, the management focus is on identifying, planning, managing, and delivering the services, which are requested or needed by the customer organization. The IT organizations are likely to have SLAs with the customer organization(s), and the SLAs pretty much set the targets for the costs and quality of the provided services. Therefore, the IT organizations must oversee and measure the provisioning of the agreed set of services to ensure compliance with the SLAs. Thus, in the event of service disruption or quality issue, the IT organizations not only know the devices involved in the case but, more importantly, are aware of the implications that the problem has to the business and organization as a whole. Therefore, the impact of the problem can be anticipated, and required counter-measures started in order to minimize the impact caused by the problem. In other words, the management of the infrastructure components is no more done in isolation from the services, but instead there is a strong relationship between the infrastructure and the services.

In order to achieve the capability and maturity required by this stage, the IT organizations often implement ITSM solutions, which bind the management of people and processes to the IT infrastructure. In that way, they are able to deliver ITSM-based ser-

vices, which enable them to proactively manage the IT infrastructure as part of strategic business services. That wouldn't be possible if the IT organization would purely focus on IM apart from the management of people and processes.

Ultimately, in the third stage, IT organizations have integrated and streamlined the IT processes fully with the organization's business processes. The business-aligned IT processes and services are mature and efficient, and have the reputation of delivering value as promised and supporting cost-reduction initiatives and business goals. At this point, the IT organizations have the know-how and right tools to deliver the services, and they are proven to be capable of delivering the services upon agreed costs and quality targets, so the IT organizations can start selling and billing the same services for other, possibly external, customers as well. Thus, along with the new business opportunities, the IT organization becomes a true strategic business partner.

3.7 ITIL

As we noted earlier, when discussing the IT systems management, there are many ways to conceptualize the IT management, and ITIL is a one set of documented best-practices and guidelines for planning, delivering, measuring, and developing the IT services and their governance to meet organization's business objectives. This chapter is based on [itSMF07] and it provides an introductory overview over the five books, or lifecycle stages which constitute ITIL (see figure 2).

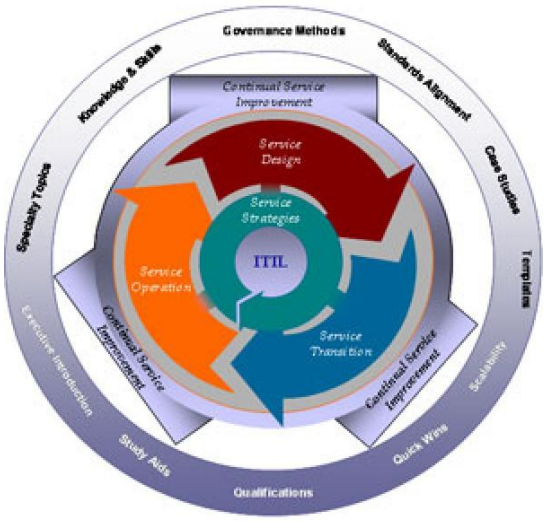

Figure 2: Service lifecycle [itSMF07]

3.7.1 Service Strategy

The service strategy publication is in the core of ITIL, and it helps an organization to establish a solid foundation for the design, development, and implementation of organization's service management capabilities. It provides guidance on service value definition, business-case development, service asset identification, market and competitor analysis, and service measurement and risks analysis.

The intention of the service strategy is to make the reader think *why* something should or shouldn't be done in a certain way. It helps the organization to come up with a service strategy which helps the organization to establish well-defined services, support the provisioned services, and control the costs and risks related to the services. The service strategy, however, doesn't discuss *how* the plans should be implemented.

3.7.2 Service Design

The service design book presents guidelines and best practices for the design and development of the provided services and the related service management processes. It basically instructs *how* an organization can convert its strategic goals into service portfolio in order to meet the organization's business requirements.

Thus, the ambition of the service design is to give best-practice guidance on how organization's strategic objectives can be achieved and maintained on the desired level.

3.7.3 Service Transition

The service transition volume describes, in a practical context the best practices for the development and improvement of organizational capabilities for delivering new and changed services into operational use. It also provides guidance on managing changes in operational services.

The aim of the service transition is to introduce such best practices, which can enable enhancements to organization's services and service management capabilities by enabling well-managed introduction, deployment, transfer, and decommissioning of new or changed services.

3.7.4 Service Operation

The service operation publication contains guidance on all aspects of managing everyday operation of services provisioned by an organization. It focuses on the delivery part of the service lifecycle and introduces the best practices which can help an organization to ensure the delivery of services in accordance to service level agreed with the customer or end-user of the services. It also discusses how provisioned services can be monitored for problems, assessed, and how a balance between service reliability and maintenance costs can be found.

The goal of the service operation is to introduce the practices how both the customer and the service provider can achieve the best possible value through the provisioned services. The service operation is actually the part of service lifecycle where the service is realized and the organization's strategic objectives are either met or not, depending on how everything worked out.

3.7.5 Continual Service Improvement

The continual service improvement (CSI) book focuses on quality management and process development. The main idea of the CSI is not only to make sure that provisioned services will meet the requirements defined in the SLA, but also improve the services further to enable even better services. In order to be able to do this, organizations must employ proper ways of measuring and assessing the level of provisioned services, and for that purpose, the CSI book provides a lot of advices and guidelines. For example, the CSI book introduces a seven-step process for improvement initiatives, which consists of the following seven phases: identification of the strategy for improvement, definition of what should be measured, collection of data, processing the data, analyzing the data, making use of the data, and improvement implementation.

Thus, the intention of the continual service improvement is to help organizations to measure and improve the effectiveness, efficiency, and cost effectiveness of all provisioned services and organization's service management capabilities.

3.7.6 History of ITIL

The first version of ITIL was developed in the 1980s when UK Government's Central Computer and Telecommunications Agency (CCTA) noticed that government agencies were struggling with analogous IT management issues and were developing their own practices from a scratch. The purpose was to share knowledge and guidance of best IT management practices, and so the first version of ITIL was compiled in 1989. The first version consisted of a set of 42 different volumes, which made it quite impractical to use.

In 1991, a user forum for ITIL – named as *Information Technology Service Management Forum (itSMF)* - was formed to act as clearing house and sounding board for discussions and guidance on how to implement and develop ITIL.

In the beginning of next millennium, a second and significantly more consolidated version of ITIL was published to improve the availability and affordability of ITIL. The ITIL version 2 decreased the number of available books to seven, which were: Service Support, Service Delivery, Security Management, Application Management, ICT Infrastructure Management, Planning to Implement Service Management, and The Business Perspective. At those times, CCTA was also merged into Office of Government Commerce (OGC), which then continued the ITIL development.

Third version of ITIL (V3) became available in 2007, and the most significant amendment between the ITIL V2 and ITIL V3 was the introduction of *Service Lifecycle* concept in the ITIL V3. Basically, the ITIL V3 describes the entire service lifecycle with five core publications. Similarly, as was the case with development of the ITIL V2, the itSMF provided a great input and practical suggestions from ITIL users for the development of ITIL V3. Also many organizations, which utilize ITIL, around the world contributed to the development of the ITIL V3.

The latest version, ITIL 2011 edition was released in July 2011, and it provided an update to the ITIL V3, which had been published four years earlier. In addition to correcting errors, the 2011 edition presents additional guidance for the definition of formal processes, and updates to the ITIL vocabulary.

3.7.7 ITIL in Short

Shortly, ITIL is perhaps the most widely known framework and de facto standard for IT service management. Its collection of good practices and guidelines has been proven to benefit organizations in practicing IT service management throughout the entire world regardless of nationality or domain of the organizations.

However, it is good to know that ITIL is not the only conceptual framework for IT service management, but there is also many other frameworks as well. The other interesting IT service management frameworks include, but are not limited to, *Microsoft Operations Framework*, *FITS*, and *Core Practice*, for example.

The reason why only ITIL is discussed in this thesis is because it is a widely recognized de facto standard for ITSM around the world, and the focus of this thesis is not on the ITSM, but instead on the impact that the consumerization of IT has to the IT management and its key concepts.

3.8 Summary

In chapter three, we learned that the members of IT staff are not magicians, but instead they collaborate as a team of educated professionals who have delicately defined responsibilities which are often based on some well-organized management framework (ITIL or some else). The frameworks provide guidance for planning and implementing the different IT processes in a systematical and efficient way – and there is no need to reinvent the wheel, so to speak. In fact, the efficient and almost magic-like ability of IT administrators to manage the IT on different levels is earnings from an organized, and standardized way of working in accordance to well-known best practices. And of course, a big part of the IT management routines can be automated with proper tools, which hugely empowers the efficiency of IT management, and facilitates the everyday work of IT administrators. The tools will be discussed in more detail on the next chapter.

4 IT Management Practices and Tools

In this chapter, we will discuss the automation of different IT processes or functions. We will get familiar with the requirements that would be good to meet before trying to automate any processes, and then we will consider the different types of solutions or tools that are available for automating the IT routines. After that, we will also discuss the different deployment models of IT solutions, and deal with some policies or practices that have been traditionally employed in IT management.

4.1 Before the Automation

According to ITIL [OGC11b, pg. 223], good IT management tools are important assets for the IT-dependent organizations nowadays. Especially the use of IT management suites, which integrate the IT management processes and the IT management toolsets together can be considered as an obligatory requirement for successful management of IT and services in large organizations. However, it should be noted that the tools are not the goal in itself, but instead, a way to reach the goal – which is to provide toolsets and automation for the organization's IT functions and processes. ITIL also includes a statement that the basis for successful service management is created with good people, good process descriptions, good procedures, and with working instructions.

In *IT Systems Management* book [Sch12, pg. 396], Schiesser emphasizes the importance of process design as well. Schiesser reports that the automation of poorly designed processes can do even more harm than if the processes were not automated at all. Wrong technology selections in automation may cause additional problems to the processes and thus harm the process output. In his book [Sch12, pg. 396-398], Schiesser states that any processes should not be attempted to be automated before the following three conditions are met:

1. The process should be well-designed and standardized to the maximum extent achievable. It should be possible to migrate and apply the processes to the other occurrences of the same process without problems.

2. The process must be streamlined as much as possible. Ensure that all non-value-adding steps are eliminated, and all value-adding steps are included.

3. Discretion should be exercised. Use the tools as they are designed and purposed to be used. Don't try to automate the parts of the process which are not supported by the tool.

Thus, it is important to make sure that the processes are well-designed and streamlined, and also to pay attention to the selection of the tools. The tools should be selected based on how well they match with the organizations needs and requirements.

It may help to assess the importance of the requirements if the requirements are somehow prioritized or weighted. A simple method for prioritizing the requirements is the *MoSCoW technique*, described in a guide published by International Institute of Business Analysis (IIBA) [IIBA09, pg. 102]. In the MoSCoW technique, the requirements are categorized and described approximately as follows:

- M – The selected technology must have this feature.
- S – The selected technology should have this feature if possible.
- C – The selected technology could have this feature, but it's not necessary.
- W – The selected technology won't yet have this feature, but maybe later.

4.2 IT Management Tools and Solutions

Nowadays, there are thousands of different tools, technologies, and solutions which are used to automate one or several part of the IT functions, processes, or services. Some of them are independent point solutions, which solve some specific issue like the discovery of network-connected IP-devices, for example. On the other hand, there are also integrated tool suites, which provide some set of integrated tools for managing the organization's IT resources in a wider perspective. The trend seems to be, according to ITIL [OGC11b, pg. 222], that the ITSM software tools are more often integrated

solutions suites than just point solutions focusing on some specific issue. The integrated IT or ITSM management suites usually provide automation and toolsets, for example, to the following purposes (not a full list, but rather an example):

- Discovery of network devices such as workstations, servers, and printers
- Inventory of configurations (software, hardware, and CI relationships)
- An asset registry and management tools for software and hardware assets
- Change management and release management
- Incident and problem management tools for helpdesk
- Remote support, instant messaging, and communication
- Measuring, reporting, and quality management
- Coordination of process phases and ownerships (workflow management)

Anyway, in addition to the management solution's features and capabilities, it is also important to pay attention to its deployment model and other restrictions, because some solutions are designed to be used in large enterprises and they may not be economic or easy enough to use in midsize or small organizations.

4.3 IT System Deployment Models

This chapter discusses about the different *deployment models* of information systems (IS). Later we will consider their significance to the IT management or ITSM in particular. The IS deployment models, their assessments, and related terminology, presented in this chapter, are for most parts based on the glossary of key information security terms by National Institute of Standards and Technology [NIST11] and the research paper of Parsi & Laharika [PL13].

First however, we aim to recognize the different deployment models and what are the pros and cons of each model. It is important to understand the difference between on-premise and off-premise private cloud deployments, and also the difference of single-tenant private cloud deployment versus multi-tenant public cloud deployment. The terms "cloud" and "cloud computing" are very close to distributed computing, and when some IS is offered from a cloud, it means that the solution doesn't have to be

installed for the users locally, but instead the IS can be remotely used on-demand by multiple users through web technologies. So, in other words, the cloud software or service is mostly ran and maintained elsewhere where it is used from.

It is also good to know that there exist a few different cloud service *delivery models*, which are: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), but in this thesis we will limit ourselves to discuss about the SaaS option only, because that is the way how IT management and IT service management solutions are typically offered. In short, the SaaS means that software is provided for users as a service by a service provider, and the users may use the software or service on-demand via web technologies. The SaaS solutions are often billed according to certain pay-as-you-go rates, which mean that the users only pay for what they use. The service scalability provided by a cost-model like this is also one of the biggest advantages of SaaS services for any type of customers.

4.3.1 On-Premise Private Cloud

In the on-premise private cloud deployment model, an IS is exclusively hosted for the user organization within its own premises. The cloud is *private* because it is operated on a *single-tenant* infrastructure, which means that the system hardware, software, and database are dedicated for the use of particular user organization. This type of IS is usually hosted by the organization itself. This type of deployment is also known as *internal cloud* (see figure 3).

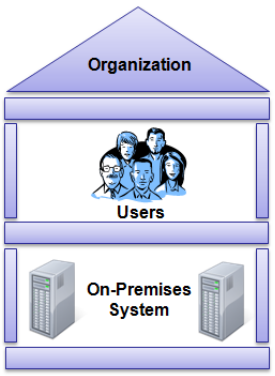

Figure 3: On-Premise Deployment of an Information System

The on-premises model is a traditional approach to use of business software, and it was according to a common opinion also the most commonly used approach until around 2005.

4.3.2 Pros and Cons of the On-Premises Deployment

The benefits of the on-premises deployment and use include, but are not limited to:

- A high control over the systems and business data
- Usually, somewhat customizable and easy to integrate with other systems
- Independency from IT suppliers and services
- Authority to change, update, and restart the solution whenever necessary
- No performance issues due to bottleneck on the Internet connection
- Dedicated resources in private clouds guarantee steady performance
- Full access to systems enable easy development of the systems

On the other hand, the disadvantages of the on-premises deployment and use of IT solutions include:

- Initial costs of setting up systems can be very high due to hardware, software, and license purchases
- The ability to access and utilize on-premise systems is very limited, because the model basically supports in-house use only
- Maintenance can be time-consuming, costly and require a lot of know-how
- Requires space, security, and ventilation from the physical environment
- Not necessarily easy to integrate with open public cloud solutions

Thereby, it seems that the on-premise deployment model is best suitable for organizations which demand high information security and are capable of hosting their own IT i.e. have the required know-how, physical environment, and resources to deploy, run, and maintain their IT solutions. In some cases, when an organization must – due to legal restrictions – know where its data is geographically located, the use of on-premises solution could be a sure way to comply with the requirement.

4.3.3 Off-Premise Private Cloud

In the off-premise private cloud deployment model, an information system is exclusively hosted for the single organization in an off-premise data center, and it is accessible through web-technologies (see figure 4). The user organization doesn't have physical access to the actual servers running the solution, but instead they will be provided an access to the desired solution, which runs as a service — and is usually managed by a third-party IT service provider.

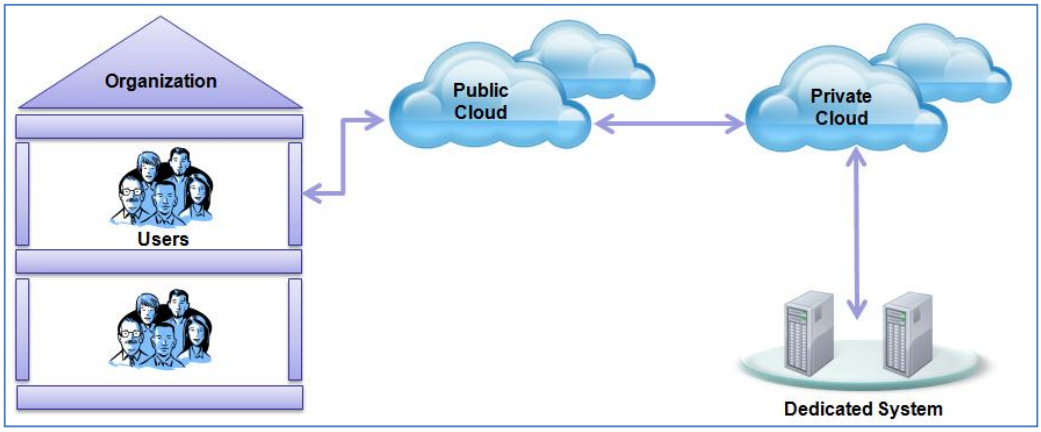

Figure 4: An Off-Premise Private Cloud Usually Runs in a Data Center

IT service providers may also host ISs to multiple customers using a shared infrastructure (not dedicated). That deployment model is known as a *community cloud.* However, due to security reasons the community cloud deployment model hasn't traditionally been used for hosting IT management systems, and therefore we crop it out from this thesis.

4.3.4 Pros and Cons of the Off-Premise Deployment

The benefits of the off-premise deployment and use include, but are not limited to:

- IT users can access the IT solutions even if the organization would be a geographically dispersed one
- Hardware and software costs are usually cheaper when compared with on-premises deployment, because multiple users can use the same cloud-solution
- No major upfront investments are needed in local server hardware or software

- Private cloud-based IT solution(s) are simpler and cheaper to maintain than on-premises systems, because there aren't so many installations of the IT solutions at many different places
- Private cloud deployments have fairly good information security
- Data is located and maintained in one place, which is well-accessible

On the other hand, the disadvantages of the private cloud deployment include:

- Dependency on web-technologies and Internet connectivity
- Information security requires more attention when compared with on-premises IT solutions
- If an external IT service provider hosts the private cloud, the user organization becomes somewhat dependent on the provider
- No total control over the IT solutions or data
- It can be difficult to exit from the private cloud if the user organization wants to change the IT deployment model or the IT service provider

Hence, it seems that the private cloud deployment model provides a viable alternative for the on-premises deployment model, but it also brings some dependency and trust issues with it. However, many external cloud service providers have proven to be able to provide very high availability of services, so in most cases, the IT users' dependency of the Internet connectivity is actually a bigger problem than the organization's dependency on the service provider. Anyway, an internally-hosted private cloud has the potential to provide all the same benefits than an on-premises solution, and besides that, it can address some disadvantages (e.g. accessibility) which are problematic for the on-premises solutions.

4.3.5 Public Cloud

In public cloud deployment, the IT solutions are always provided from off-premise data centers for users over the public Internet as a service, and the IT solutions are not hosted exclusively for the customers (see Figure 5), but instead they are *multi-tenant* by their nature. This means that a public cloud IT solution may process and store data from multiple customers using a shared hardware, operating system, or database. The

access to public cloud services is not limited, and therefore they are usually fairly easy to access when compared to IT solutions running in private clouds. Public cloud service provider is also by definition, external to the consumer or user organizations.

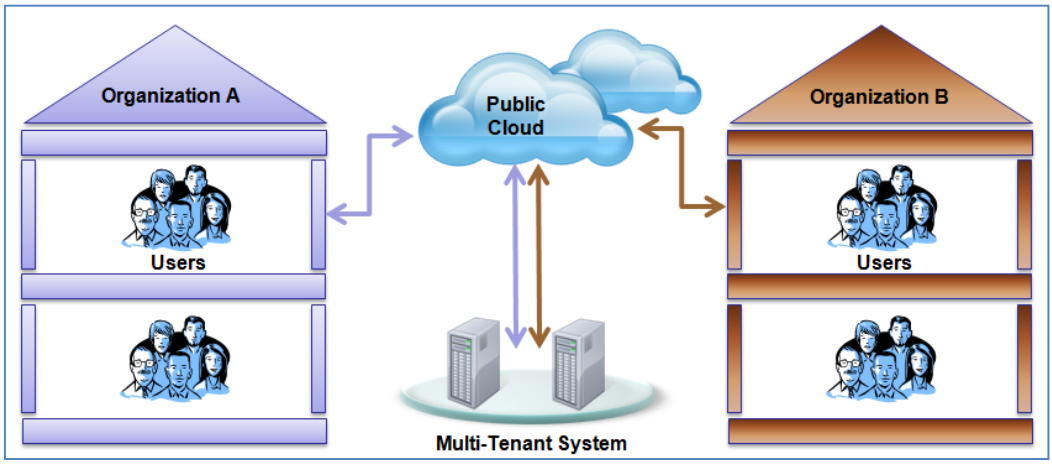

Figure 5: Public Cloud Information Systems Are Available for Public, and They May Use the Same Resources to Process Data of Multiple Customer Organizations

4.3.6 Pros and Cons of the Public Cloud Approach

The benefits of the public cloud deployment and use include, but are not limited to:

- Possibility to use a shared platform for delivering the IT solution for multiple customers usually lowers the solution costs per customer
- The consumer of a public cloud IT solution does not have to pay or worry about the solution maintenance
- Public cloud IT solutions are very well accessible
- Public cloud IT solutions are very well scalable and elastic
- IT staff competence and technology used to support the provisioning of public cloud services are often really good

On the other hand, the disadvantages of the public cloud deployment and use of IT solutions include:

- Security issues: a consumer may not know where its data is processed and stored, or whether it has been encrypted and backed up or not

- There is no guarantees of the reliability and uptime of the public cloud services, although they usually are on a good level
- Consumer is in the hands of the solution vendor, and it may prove difficult to develop the solution or integrate it with other systems
- Because multi-tenant public cloud services are provided using a shared infrastructure, there is no guarantees of such service's performance

Although, public cloud solutions can provide superior cost-efficiency and excellent accessibility of services, the information security concerns often slow down the adoption of public cloud solutions, especially in industries where information security is critical. Financial and healthcare sectors are good examples of industries where the security of information is extremely important. That remark is relevant to this thesis, because IT asset and service management solutions are widely exploited by organizations in different sectors of industry, and it is likely that the interest for public cloud solutions is growing within these two sectors as well.

4.4 IT Management Practices

In this chapter, we will get familiar with the prevalent IT management methods and practices that have been (and still are) utilized in organizations to manage IT resources and services.

4.4.1 Tradition of On-Premise Systems

From the previously presented deployment models, the on-premise deployment model has traditionally been the dominant option when speaking of organization's IT management systems, because many of the IT management systems haven't been even available in other deployment models. Because the organizations' IT assets have been mostly located within the organization walls, it has been a natural choice to use an on-premise system to manage them. At the same time, the management information has remained safe from information security threats lurking online. Additionally, in the

past, the speed of network connections has been slower, and therefore the IT management in a wide scale with online systems wouldn't have been rational as it requires extensive usage of Internet and network connections.

4.4.2 Restrictions for the Personal Use of Organization Assets

For years, the behavior of employees and organization members has been controlled with restrictions or limitation policies, such as workplace policies, that have addressed the personal usage of organization assets. With these policies, organizations have tried to protect their assets from problems like disappearances and breaches caused by the personal use of organization-owned assets. It is understandable that organizations have wanted to protect their investments in IT by prohibiting the personal and possibly risky use of organization's IT assets, because all broken and lost devices have meant financial losses to the organization. At least as important as protecting the investments, has been the motivation to protect the organization's information security, because the personal use of organization's IT assets also might expose the organization's assets to new information security risks.

4.4.3 Standardization

According to Cosgrove & Colville [CC10], *PC standardization* has been the best practice of PC management for over than a decade for now.

> *"In the concept of **PC standardization**, the main idea is to define a manageable number of base configurations, which cover the basic hardware, software, and operating system configurations of a computer, and then promote the use of these configurations in the organization."*

Thus, basically limiting the number of different base configurations has been an essential function in enabling the IM processes. Without standardization, the IM, and other management process, which build on well-managed infrastructure, would have been significantly more complex or even impossible to implement. In its most extreme form, standardization can mean that only one type of computers with a similar set of

hardware, software and operating system are used in the organization, but usually organizations provide at least a few different types of standard PCs for different purposes or different user roles. Anyway, the bottom line is to have a manageable amount of device types in use, which eases the support, minimizes the costs, and reduces the security attack surface area of IT. The actual number of supported device types is likely to vary in accordance with the enterprise size, number of devices and users, and the geographical dispersion of the organization.

4.4.4 Centralization

Traditionally, organizations have reserved the rights to choose the IT assets (hardware, and software) that are purchased for the use the organization. According to Peters [Pet08], this has given the organizations the ability to keep the amount of different devices types manageable, and also to enforce desired control mechanisms to the devices. But in addition to that, it has also provided the organizations a possibility to choose the end-devices in accordance with the restrictions of the management toolsets. For example, if the preferred management tools have been designed for managing Windows-environments, then the organizations have been simply able to choose only Windows-based computers or at least Windows-compatible equipment into the list of accepted IT components.

4.4.5 PC Lockdown Techniques

Without appropriate maintenance and control, the computers, wouldn't stay in the standard-condition very long, because hardware parts and peripheral devices are plugged-in and out every now and then, and IT users might independently install applications without consulting the IT. Therefore, it is a common practice that IT organizations use so called PC *lockdown* techniques to maintain PC standardization. The term of **PC lockdown** is yet missing a singular industry-accepted definition, but Cosgrove & Colville explain it as follows [CC10]:

> *"It describes a control spectrum, which can range from drafting an IT policy enumerating rules about software installation that may not be "enforced" at the*

user's system (more of a trust system), to implementing more controlling measures, such as removing administrative rights and using Windows group policies and other software to control other elements of the PC configuration. IT has a range of options to use that can be combined to address a single user's or groups of users' requirements, while ensuring the appropriate flexibility to do their jobs and remain protected from vulnerabilities."

These lockdown techniques or IT control mechanisms are familiar for many people from workplaces and public organizations where the use of computers, especially shared computers, is typically highly restricted with different types of control measures which are enforced at the system. For example, the user may not be able to change any system settings, install new applications, or visit certain websites, because those actions could possibly endanger the security of the computer, or at least consume its performance. Often, the computers and computer parts like monitors, keyboards, and central units are also physically locked to immovable objects to ensure that they are not detached and stolen. Sometimes, also the plug-in of additional devices is programmatically restricted, because by attaching a malicious USB drive to the system, an attacker could possibly bypass the computer's own operating system by booting the system from the USB drive, or on the other hand, an attacker might also be able install a hardware key logger to the computer, and thus gain information about the use of the computer and user's passwords, for example.

5 Consumerization of IT

This chapter summarizes the literature review results. First, it is explained what is meant with the consumerization of IT, and then we continue to describe the positive and negative consequences which have been identified to link with the consumerization. The main reference for this chapter is the working paper of Niehaves & al. [NKOK12] who analyzed a total of 22 studies in order to find the IS areas which are most affected by the consumerization, and on the other hand to identify the advantages and disadvantages of consumerization that are mentioned most often. They also considered the advantages and disadvantages of IT consumerization from both: the IT organizations' and the IT user's perspective.

Consumerization of IT is a phenomenon or trend which has gained a lot of attention during the past few years. The IT consumerization phenomenon was first recognized in 2004 by Moschella & al. [MNOT04], and since then, especially during the past few years, many analysts and consulting firms have conducted several studies regarding the consumerization of IT. Additionally, according to [NKOK12], Gartner sees the consumerization of IT as one of the five major IS trends, and predicts that what we have seen this far is only the beginning, which makes it a really interesting topic for a thesis as well.

5.1 What is Consumerization of IT

Consumerization of IT is an industry-accepted term introduced by Gartner ® Inc. – an American information technology research and advisory firm [Gar14]:

> *"**Consumerization** is the specific impact that consumer-originated technologies can have on enterprises. It reflects how enterprises will be affected by, and take advantage of, new technologies and models that originate and develop in the consumer space, rather than in the enterprise IT sector. Consumerization is not a strategy or something to be "adopted". Consumerization can be embraced and it must be dealt with, but it cannot be stopped."*

According to Cummings & al., the IT consumerization trend emerged with the emergence of Web 2.0 technologies when these new technologies like blogs, social networking, and wikis were started to be used for improving collaboration and information exchange within the enterprises [CMR09]. Later, Geyer & Felske and Harris & al. have found that the IT consumerization extends to cloud services and mobile devices like smart phones and tablets as well [GF11, HIJ12]. Especially the number of Apple's iPads and iPhones has been rapidly growing when people have acquired new devices to substitute the outdated corporate-provided business equipment. One factor which further fuels the consumerization trend is the so called *Bring Your Own Device (BYOD) policy* which has been adopted by many organizations. With a BYOD policy, the organizations permit and encourage the people to use personally owned IT resources for working and accessing the organization's IT resources.

In different words, the consumerization of IT refers to a phenomenon where the individual IT users use the devices, services, or applications – familiar from a personal life – for working or otherwise organizational purposes (see Figure 6). The use may be based on a voluntary basis, or be led by the employer or the organization where the individual belongs to. Put differently, traditionally the use of IT has been led by the organization's IT departments, according to the principle of centralization, but now the paradigm is changing from the *top-down* to a *bottom-up* approach, where the use of IT is actually being led by the IT users of the organizations.

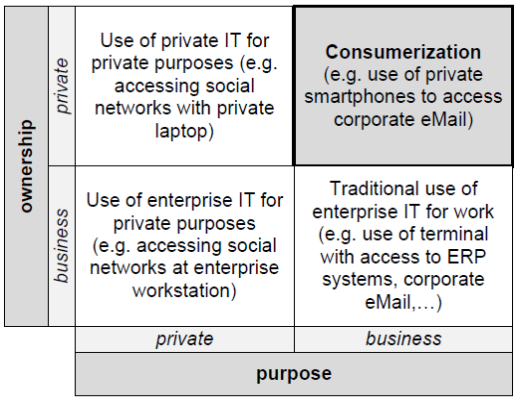

Figure 6: Conceptualizing IT Consumerization [NKOK12]

5.2 What Are the Consequences of IT Consumerization

According to Ortbach & al. [OKBN13], the impact of IT consumerization to IT organizations and individuals has been studied and discussed in the recent years. However, surprisingly little weight has been put to researching the reasons why the consumerization of IT actually affects the IT organizations, IT users, and IT management. This thought is also the cornerstone and motivation for this thesis, and it is good to keep in mind when we discuss about the implications of IT consumerization that have been noticed in the studies this far. Additionally, it has been found that, for multiple reasons, the positive effects of IT consumerization seem to be more difficult to leverage in public sector organizations than private sector organizations [NOK13].

Niehaves & al. [NKOK12] researched the impact of IT consumerization to different parts of information systems by analyzing 22 different studies. The analysis was based on IS literature, which identifies hardware, software, data, people, and procedures as the constituting elements of an information system.

Niehaves & al. [NKOK12] found out that the consumerization of IT has a positive impact especially to the people, boosting up the employee morale and enabling a faster knowledge creation. In turn, they also found out that the consumerization of IT has a negative impact to the data, because it arises information security concerns and compatibility issues between information systems. Additionally, the research found out that the consumerization also affects the other elements (hardware, software, and procedures) as well, but the impact to those is not clearly negative or positive, but instead a little of both.

5.3 Advantages and Disadvantages of IT Consumerization

When Niehaves & al. [NKOK12] examined the effects of IT consumerization from the perspective of IT organizations and IT users, they were also able to identify some areas which were clearly positively or negatively impacted by the consumerization of IT.

For an individual the recognized effects are:

- Increased workload, because work hours tend to get longer when same devices are used for private and working purposes
- A greater freedom to choose the tools contributes to the feelings of autonomy and happiness
- Consumer devices are perceived to be more easy to use, and they already might be familiar from the private use, which contributes users' competence

From the IT departments' side, Niehaves & al. identified numerous advantages and disadvantages that are due to the consumerization of IT, but the most significant advantages are the employee satisfaction and availability, and the speed of new technology adoption. In turn, the key downsides are the security, performance, and compatibility concerns, support complexity, and loss of process control.

The advantages of IT consumerization were also considered in the research of Harris & al. [HIJ12] who interviewed executives from different industries, and found out that the benefits from IT consumerization can be put into three categories, which are: Innovation benefits, employee satisfaction benefits, and productivity benefits.

The innovation benefits can mean for example the new ways of working that are enabled by the use of consumer technologies. As an example of this, Harris & al. gave the following hospital nurse's innovation:

"There is always some inefficiency in bandaging wounds. The nurses change the dressing on schedule, but then, perhaps 20 minutes later, the doctor arrives and wants to look at the wound. One day, before taking off a fresh bandage, the nurse asked me to look at pictures of the wound she had taken with her phone moments before. I didn't need her to cut the bandage off. It looked fine; that was all I needed to see."

Also similarly like Niehaves & al., also Harris & al. [HIJ12] found out that IT consumerization was seen as a valuable tool in attracting and retaining the new tech-savvy employees, who are comfortable with the new technologies and expect them to be used in organizations. Part of the people even keep that as an important decision criterion

while they are choosing their next employer. On the other hand, some employees were told to appreciate and value the independence and enjoyment that was results from the ability to choose and use the preferred tools and technologies.

Lastly, as an example of productivity enhancements it was mentioned that the consumerization of IT doesn't only contribute to the competence and productivity of the IT users, but also lowers the IT costs, as IT departments can share the IT purchase or subscription costs with the users.

5.4 How Consumerization Shows in Practice

In the previous sections we established a theoretical understanding of how the IT management is done in the organizations, and what the phenomenon of IT consumerization actually means. But we still haven't concretized what are the practical phenomena under the umbrella of IT consumerization, which actually constitute the consumerization phenomenon.

We will discuss the phenomena and trends included in the consumerization of IT, and which have been identified by IT management research literature. Then, in the next chapter, it is suggested how, and most importantly *why* these trends are likely to affect the IT management in practice.

5.4.1 Cloud Adoption

As we mentioned earlier, the term *cloud* refers to a service or application which is available on demand via web technologies, and the use of a cloud service doesn't usually require any time-consuming installations or whatsoever. Some cloud services may require a registration from the user, but that is mostly a task of few minutes. Examples of widely known cloud (or online) services include, for example: Facebook (a social networking service), Microsoft Office 365 and Google Docs (office software), Dropbox (a file hosting service), and Gmail (an email service).

In September and October 2012, a global security software corporation conducted a research [Sym12] in which they contacted business and IT executives at 3 236 organizations in 29 countries in order to discover the hidden costs of cloud technology adoption. According to the survey, as much as 94 percent of all contacted organizations are at least discussing about clouds or cloud services. So there seems to be great interest and high expectations towards the cloud technology amongst the enterprise IT managers.

What is more concerning is that in three quarters of all organizations, employees had employed so called *rogue clouds*, which means that the employees had started using public cloud applications for working without consulting the organization's IT department. In addition to, some 40 percent of those organizations also reported that they had experienced the exposure of confidential information, and even more than 25 percent of the organizations had also faced account takeover issues, defacement of web properties, or stolen goods or services.

5.4.2 Shadow IT

In September of 2012, a global enterprise storage management company conducted a survey [Nas12] for more than 1 300 corporate IT users to get understanding of employee habits concerning *shadow IT* — the unauthorized use of either hardware or software IT systems and solutions in organizations.

The survey found out that IT users not only used employee-owned computers to access their personal cloud service accounts for working and saving work files, but they also leveraged their personal smart phones and tablets to do so. About 60 percent of all IT users reported using their own device for working, because their employer doesn't provide the tools they need. Additionally, some 25 percent of all respondents also planned to acquire an additional mobile device before the end of the year, and 73% of those people admitted that they will use the device for working.

5.4.3 Mobility and BYOD

In January and February of 2013, *IT professional* - a magazine from the IEEE Computer Society, presented the top 11 pervasive technologies and trends, which they believe to bring both technical and cultural changes for the year 2013 [CP13].

The number one trend, which was believed to have the biggest impact in affecting today's enterprises on the year 2013, was *Mobility and BYOD.* According to the article, consumers and employees are starting to introduce their personal devices to enterprises similarly like people started to adopt Internet back in the early 90's. Anyway, an entire army of new different sorts of non-corporate consumer devices is flooding into the enterprises, and people are mixing their personal and work tasks on the same devices. At the same time this means that people are rapidly expanding the array of network-capable devices that are frequently used to access corporate network and the resources within.

In addition to that, United Nations reported in March 2013 [UN13] that nowadays more people have a mobile phone than have access to a flush toilet. That is really stunning information, and it concretizes well how real the mobility trend actually is. Additionally, according to Disterer & Kleiner [DK13], mobile device adoption is expected to explode, and in the year 2016 there might already be even 1 billion smartphone users. Disterer & Kleiner also state that in the year 2016 that around 350 million users would be using their smartphones for work related tasks. Thus, it seems clear that the boundaries between personal and work life are rapidly disappearing.

The difference between the earlier mentioned shadow IT and Bring Your Own Device (BYOD) thinking is that in the first mentioned, the IT users have started using consumer devices and applications for working by themselves without consulting the organization's IT department, and in the latter the IT users are actually permitted, supported, and even advised to use their own devices or applications for working. Hence, in the case of BYOD, the organization is at least aware of what is happening, although the situation might otherwise be similar to the shadow IT.

6 Why the Consumerization Affects IT Management

In this chapter, we will consider the traditional IT management practices against the IT trends brought by the consumerization of IT, and we try to identify why the phenomena introduced by the consumerization of IT are likely to have an impact to IT management.

6.1 Non-Corporate Owned Devices

Let's imagine a scenario where an IT user decides to pursue for better usability and efficiency and therefore transfers his/her corporate-tasks to a personal device, which isn't any of the standard hardware types approved by the organization's IT department. For example, let's say that the user would synchronize his/her email and calendar to a personal smart phone or tablet. How, in that case, could the company data or service be protected? How would it be possible to make sure that the device is in compliance with the organization's security policy? Or how could the IT organization make sure whether the user has installed malicious applications to the device which he/she uses to access the company data? What if the device gets stolen, with the company data and e-mail access residing with it? The answer is: it's not possible to do much with the conventional management practices, which have traditionally focused on managing a standardized set of devices, with very little variation.

Of course the IT department could employ MAC-address filtering or some other control mechanism to the enterprise network and educate the users from not using their personal devices, but that would mean a lot of extra work for the IT department in form of planning the education and maintaining the rules for MAC-filtering – not the desired outcome. Most importantly, it would no more be possible to trust in the good, old management processes, but instead it would be necessary to create, test, and introduce a totally new management processes to handle the situation.

In small scale, issues like described above are easy enough to handle and make exceptions to the rules, but not in the scale of large organizations when the entire organizational culture changes. In that case, the costs and security risks of IT management would rapidly increase along with the users, because that would basically ruin the concept and benefits of device standardization. According to Cosgrove & Colville [CC10], the lowest-cost approach for IT departments would be to divide all IT users into groups based on their needs, and then lock down a subset of the users, rather than everyone, because some users (e.g. software developers) are likely to have legitimate needs to modify the configurations of their device (see Figure 7).

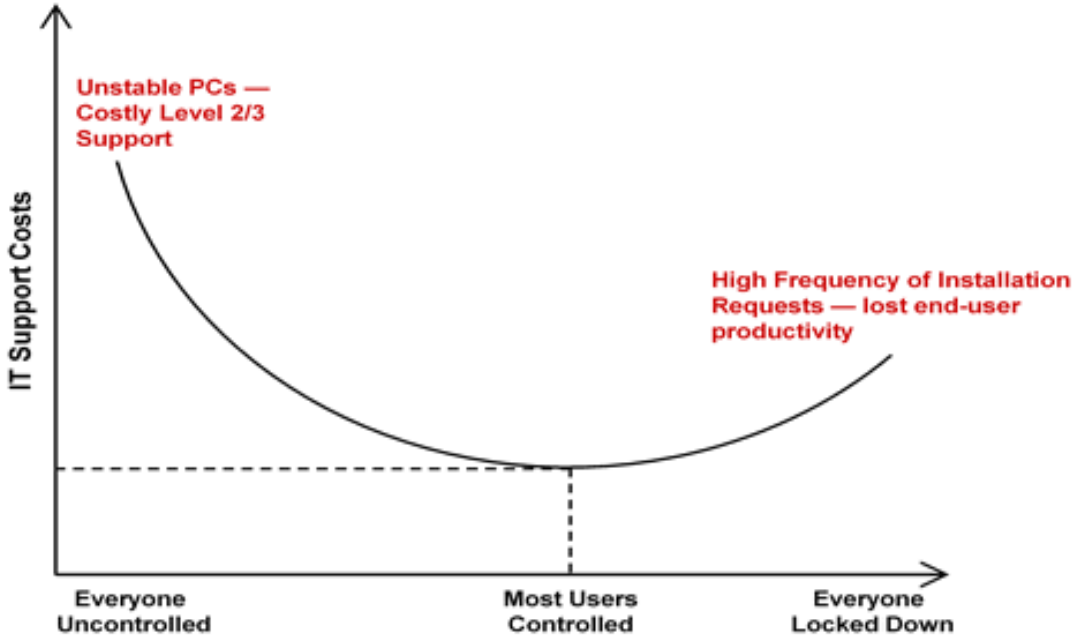

Figure 7: The relationship between the IT support costs and PC lockdown [CC10]

Anyway, there is also a fundamental problem with the legislation and ownership of the device. If the device has been purchased by an individual for personal use, and he/she then starts to use it for working as well, what is the amount of control that the employer or organization can have over the device? That may be even dependent to the local legislation, but even without that, it's not a simple question. According to Richard Walters [Wal13], some BYOD pioneers have even removed the option for employees to use their own devices due to the legal challenges. Additionally, as the

device is purchased by the user, it also means that the organizations loses control over the decision power when it comes to the selection of device type and platform.

6.2 Device Heterogeneity

Grouping users in the way Cosgrove & Colville [CC10] suggested would certainly help, but it doesn't solve the problem related to rapidly expanding array of device platforms and applications that users would introduce to the company if they were allowed to freely use their personal devices for working.

That, in turn, complicates the management of IT services in a very fundamental level, because for technological reasons, the management tools (e.g. management agent) cannot be directly utilized to manage many different device platforms. As a result, for example, the restrictions that prevent a Windows-user from installing new applications to his or her PC cannot be directly applied to Macintosh computers running Apple OS, or smart phones running on Windows Phone platform. Thereby, all these management policies should be created, tested, and distributed again for each platform separately when somebody introduces a new type of device to the organization, which of course would multiply the efforts required from an IT organization to achieve the same level of control than it used to be with the standard set of devices running on selected platforms. In order to solve this problem, Walters [Wal13] has suggested that the management of user actions should perhaps be based on managing the web browsers instead of devices.

Put shortly, the increasing device heterogeneity disrupts the asset and configuration management and change management processes, which all are needed in order to perform the infrastructure management. And as we know, the higher-level IT management activities like IT service management build on the infrastructure management, so therefore the increasing device heterogeneity can cause very fundamental problems to the IT management.

6.3 Mobility

As IT organizations have traditionally focused on managing stationary computers and locally installed software applications, the trend is that mobile devices, including smart phones, tablets, laptops etc. and the use of cloud-provided services is on growth. As a result of this development, the practices which once used to be best practices, are no more the optimal way to manage the organization's IT resources. Instead, the management of the cloud-based services and mobile devices may even prove totally impossible with the traditional tools and working practices.

6.4 Disintegrated Point Solutions

Another essential problem caused by the consumerization of IT is the increasing number of disintegrated point systems and tools that are used for working and management. When the IT users have the power to employ whatever cloud services and applications that they'd like to, it is likely that the compatibility between the systems and tools suffers.

Additionally, when the heterogeneity and number of disintegrated technologies and systems arise amongst the IT users, it is also highly possible that even the IT departments try to employ new systems and tools, which would enable them to have better control over the new consumer devices and technologies. This may help the IT departments to get some control, but also usually leads to a more disintegrated and dispersed jungle of management systems, which then complicates the support provisioning and increases the IT related compatibility issues.

6.5 Use of Rogue Clouds

The earlier introduced lockdown methods are not likely to be able to prevent the users from employing the rogue cloud services or applications, because the lockdown methods are designed to prevent users from installing applications to their computers – not from using them via web browsers.

In fact, there are only few well-known methods or tools for managing the use of cloud services or web applications. According to Walters [Wal13], some vendors are offering proxy-based tools for controlling the use of cloud services and web applications, but the problem is that those tools are quite clumsy, because they are not applicable to managing all types of web applications equally, and on the other hand, they provide only little flexibility in terms of management. Basically, the problem is that they only provide the possibility to deny the use of cloud services and web applications by filtering them by their URL address, and that is not very dynamic or efficient. Another problem related to the use of proxy-based control methods is that new cloud services are born every day, and the IT departments can't keep pace with the new cloud offerings, which makes this approach insufficient and almost impossible to implement.

In addition to not being able to prevent the use of the cloud services, most of the IT management solutions nowadays also lack the ability to perform asset and configuration management for the cloud services. This means, for example, that the solutions cannot provide any inventory information about the use of such services, which is of course a prerequisite for managing and controlling their use. It is simply impossible to manage what cannot be seen. This is also due to the fact that prevalent management solutions have been designed for a whole different purpose – for performing ITAM and CM for locally installed software.

According to Walters [Wal13], one possible solution to this problem would be to build a role-based access control framework delivered and enforced within a web browser, which would allow the IT staff to control the functions within a web application on a more granular level regardless of the computing device that is used to access the service or application. By integrating such framework to enterprise directories like Microsoft Active Directory, it would be possible to manage individual user's privileges on different features and functions in web applications, including control over export, download, share, send, and file attach functions.

6.6 Growing Complexity Requires More Competency

On the higher level, one of the most obvious and quickly growing problems is that the IT infrastructure and the IT management as functions are both changing into more complicated over time. Earlier when people mostly used the IT resources with company-provided standard PCs (mostly Windows-based), it was enough if it was possible to perform the basic IM for those computers, but the quicker the people adopt new devices, the faster the complexity of IT and IT management grows. In order to reach the same level of visibility and control over the devices, it is now necessary to perform these management processes to Linux and Macintosh computer platforms, and mobile platforms like Android, iOS, RIM, Symbian, and Windows Phone as well. So, instead of implementing a management framework just for the Windows platform, it must be implemented for multiple other device platforms as well. The focus has shifted from pure Windows-PC management towards the management of heterogeneous devices, which often are mobile and employee-owned as well.

As a result of this development, it is clear that the IT staff is continuously required to maintain and develop their competencies and skills related to new technologies and services.

6.7 Management System Deployment Models

One thing which could easily go unnoticed is that the IT management solutions have also become to support deployment models from cloud. There is already device management systems which are available instantly from a public or community cloud, such as Miradore Online, and also such management systems which are available from an offsite private cloud in matter of minutes or hours. This type of management systems can provide IT organizations and IT service providers huge cost and time savings, and enhance the reachability of the management systems, but at the same time, they naturally introduce a whole bunch of new information security risks to the IT management systems, which doesn’t necessarily apply to the traditional IT management systems hosted on-premises.

Anyway, there is a huge potential in these new deployment models, because they address some of the most irritating downsides of the traditional IT management systems, such as their slow and costly deployment, and at the same time enable a totally new business opportunities for the IT service providers.

6.8 Information Security Concerns

According to Disterer & Kleiner [DK13] and Morabito [Mor14], especially the growing use of privately owned mobile devices is threatening the information security in organizations. Disterer & Kleiner say that: "*A lack of separation between private and business spheres yields significant risks for companies*", meaning that there should be a way to isolate the business use and the private use of mobile devices from each other. They also state that: "*The level of complexity of the information security technology to be mastered increases when a distinction has to be made between private and business use on a large number of devices channels".* These statements also support the points that were made in chapters 6.3 and 6.6 in this thesis.

Anyway, information security and the other qualitative measures of the IT management are very likely to be strongly affected by the consumerization and growing complexity of IT.

It is obvious that the management of the information security requires more skills, efforts, and special tools while the number of device platforms and ways to deliver applications increase. Additionally, if the device, which is used for working, is actually owned by an employee – not by the organization like it usually was before – then it is not so clear whose responsibility it really is to make sure that the device is compliant with the organization's information security policies.

And yet another thing to ponder is what control measures the organization's IT staff is allowed to perform in the device without stepping on the toes of the device-owning end-user. In some countries it may be even illegal to track the location of employees' mobile devices. Still, however, many organizations want to track the location of their own mobile devices.

In the following subchapters, we will consider some concrete examples of why the consumerization of IT is likely to affect the information security of IT management. These examples will be discussed in subchapters through different elements of information security.

6.8.1 Accountability

In the context of IT management, the assurance of information security element of *Accountability*, introduced by the International Organization for Standardization [ISO12], can be interpreted to mean that all actions or events must be unambiguously traceable and logged with sufficient accuracy to establish an *audit trail* of the sequence of the activities or events which have happened. It should be possible to track down who did what and when.

> *"**Audit trail** is a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result."*
>
> – *Definition by National Institute of Standard and Technology* [NIST11].

Earlier, this was based on the automation of IT asset and configuration management tools, which were capable of tracking the organization-owned devices with reasonably standardized configurations.

Now, however, people have started to use their consumer-devices and applications for working, which means that the organization IT staff is no more able to utilize the formerly used automation tools to establish a full audit trail of actions and events that have happened in the organization's IT systems. In order to be able to do that, the IT staff would not only need to implement technological support for various new device platforms. In addition to that, they also would need to agree about the control measures with the device-owning users as well. Anyway, the bottom line is that, accountability is lost because the audit-trail-type of information is likely to scatter or even disappear.

6.8.2 Authenticity

In the context of IT management, the assurance of information security element of *Authenticity*, discussed by Bosworth and Kabay [BK02], can be interpreted to mean that it must be possible to validate the genuineness of data or the parties involved in communication – whether they are users, devices, or applications.

Authenticity can be validated on many different levels and ways, but one example would be the device recognition in the organization's local wireless network. Earlier, the IT staff was able to recognize devices using MAC-address identification or by installing an authentication certificate in the device. However, if the devices are purchased by employees, the IT staff doesn't even necessarily know the devices' MAC addresses, or neither are they able to install certificates to them. Therefore, the IT staff must develop new ways to do the same things which earlier were routine tasks. This development may require building support for new technologies and possibly involving the end-user into the security processes somehow. Additionally, Disterer & Kleiner have stated [DK13] that "*Authenticity is threatened when devices are used to trigger business transactions that cannot be traced clear without ambiguity".*

6.8.3 Availability

In the context of IT management, the assurance of information security element of *Availability*, discussed by Andress [And11], can be interpreted to mean the ability to reach the organization's data, services, or whatever IT resources in timely manner as expected.

Earlier when most of the organization's IT resources were residing within the physical walls of the organization, and standard workstations were all manageable and accessible similarly, the availability of the IT resources was quite easy to ensure even with a reasonable set of automation tools.

Now, however, when the physical distribution of devices is booming, and the devices are more mobile and heterogenic than ever, the IT staff needs more advanced tools and competence to manage and support the devices. Without proper tools, it may even

prove impossible to perform the very basic infrastructure or asset management for the brand-new device models, which pretty much prevents the IT staff from managing the devices and services. Thus, it is undeniable that IT consumerization has made it more difficult to ensure the availability of the IT resources.

6.8.4 Confidentiality

In the context of IT management, the assurance of information security element of *Confidentiality*, discussed by Andress [And11], can be interpreted to mean the ability to protect data from being viewed or used by unauthorized parties.

One great example of this are the device screen lock policy settings, which can be easily enforced for Windows workstations that are attached to organization's domain. It is, for example, possible to configure the workstations so that users must always login with their credentials when they start up their workstation. On the other hand, the workstations can be configured to automatically lock-up if the computer is not used in *x* minutes. With this type of control mechanisms the organizations have earlier been able to protect the confidentiality of information systems like e-mail etc.

However, as the mobility and heterogeneity of devices increase, the management and enforcement of the policy settings becomes significantly more challenging and difficult to monitor. According to Disterer & Kleiner [DK13], unauthorized parties might be able to obtain access to sensitive private information or confidential company information by manipulating insufficiently protected mobile devices, and that is a clear threat to the confidentiality. In addition to that, nowadays people very often synchronize, for example, their work emails to their personal smart phones, which still fuels the problem further. It should be possible to protect the confidentiality of the IT resources regardless of the device platform, their physical location, or device owner.

6.8.5 Integrity

In the context of IT management, the assurance of information security element of *Integrity*, presented by Andress [And11], can be interpreted to mean that there must

be a way to make sure that the management information is complete, and that it has not been altered by unauthorized parties.

In IT management systems and information systems in general, the integrity of information is often verified when data is transferred between two or more parties. This can be done using integrity checks which basically calculate a checksum of the received information block and compare it with the checksum which was calculated before the information block was transferred. This way it is possible to detect whether the information was altered while its transfer.

Actually from the perspective of integrity, the consumerization of IT doesn't really require anything new or major changes to the traditional IT management practices, but naturally it increases the number of integrity check implementations that must be built for the IT management components that are needed to manage mobile and heterogenic IT environments. The more there are different types of devices using different types of communication interfaces, the more there are possibilities for integrity issues.

6.8.6 Non-Repudiation

In the context of IT management, the assurance of information security element of *Non-Repudiation*, presented by the International Organization for Standardization [ISO12], can be interpreted to mean the ability to complement the accountability perspective. This can be done by focusing on giving undeniable guarantees that the audit trail or security log can be trusted and is not to be argued.

In the concept of IT management there must be a way to prove that a certain kind of audit trail can only emerge as a result of certain sequence of actions or events in a specific order, and no other way. In practice, this could perhaps mean that all events, which are logged to audit trail must be logged with their accurate timestamps, in the order they took place, and unambiguously so that it can be always undeniably said what in-practice events or actions each of the log entries reflect.

Anyway, in my opinion, non-repudiation is not greatly affected by the consumerization of IT as it merely concerns the way how logging is done. But of course if multiple

separate point solutions are used to manage the heterogenic fleet of devices, then it also becomes more difficult to ensure the non-repudiation security aspect.

6.8.7 Possession

In the context of IT management, the assurance of information security element of *Possession*, introduced by Bosworth & Kabay, can be interpreted to mean the physical disposition of IT resources, like mobile devices or the data within those devices.

The possession perspective is greatly affected by the consumerization of IT, because along with the consumerization the physical distribution of devices is extremely likely to increase and therefore organizations don't so often have physical control over their devices. Earlier, when the computers were mostly within the walls of the organization, they were easier to protect against thefts or damaging attempts. Due to the increased distribution of devices, some level of physical control will be totally lost for good, but the organizations are still able to at least build new type of control measures which may help to locate the stolen property or at least erase the information contents from the stolen physical device. This, however, requires new type of tools and approach for the IT management from the IT staff. Good examples of such tools are the management systems which provide, for example, the possibility to remotely lock and wipe, or map the location of a device.

6.8.8 Reliability

In the context of IT management, the assurance of information security element of *Reliability*, presented by Andress [And11], can be interpreted to mean the ability to deliver IT services and functions consistently as expected or stated in the service level agreement. Fault tolerance is one way to measure reliability.

When the heterogeneity of organizations' IT resources, such as devices and applications increase, the assurance of reliability becomes more difficult. The more there are different types of IT resources and unique processes supporting the operation of those resources, the more there is to maintain and manage, which means that IT management

becomes more complex and requires more know-how. So, it is obvious that the reliability in the concept of IT management is strongly influenced by the consumerization of IT.

6.8.9 Utility

In the context of IT management, the assurance of information security element of *Utility*, discussed by Bosworth & Kabay [BK02], can be interpreted to mean the ability to maintain utility or usability of data and IT resources.

In the context of IT management, the utility aspect becomes important when assessing the pros and cons between disintegrated point solutions versus comprehensive, all-in-one management suites. For example, we may have an access to a lot of good data in a few separate systems, but we cannot "see the big picture", because we fail to appropriately (or automatically) combine the data from different sources. For example, we might have one systems which stores all asset management data, including inventory information from managed devices, and then another systems which is used for configuration management. Because these systems are separate, we cannot easily see which version of some application some specific device already has installed, and therefore we might do unnecessary work or even mistakes in the application deployment.

The consumerization of IT seems to have a considerable effect to the utility in IT management, but it is also dependent on the strategic decisions that an organization makes while setting up the automation for IT management systems and control.

7 Management Strategies for IT Consumerization

A research from Harris & al. [HIJ12] surveyed the different management strategies that organizations have adopted in order to be able to leverage the benefits of IT consumerization. They were able to recognize so called "laissez-faire" strategy, which is a very permissive and tolerant strategy, and on the other hand, an authoritarian strategy, which is pretty much the opposite for the laissez-faire strategy. In addition to these two, they also identified four "middle-ground" strategies, which position themselves in between of those two first mentioned, and which are not exclusive for other strategies (see Figure 8). These strategies will be shortly introduced next.

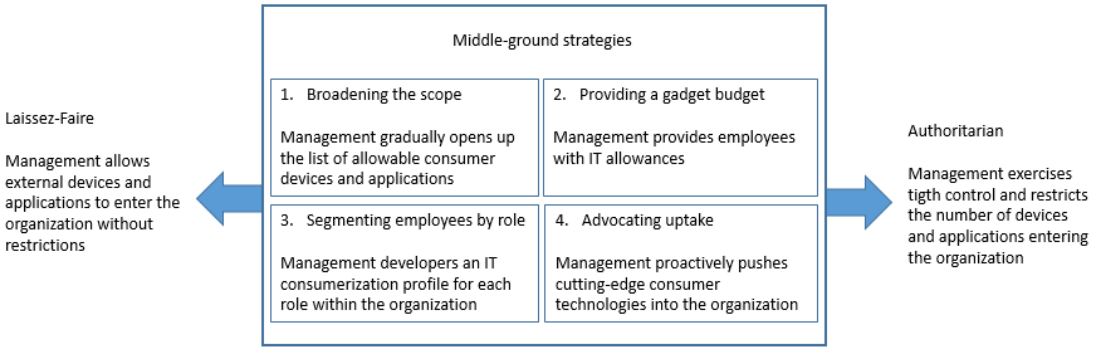

Figure 8: Management strategies (drawn based on [HIJ12])

7.1 Permissive Strategy

According to Harris & al. [HIJ12] about one third of surveyed executives told that their organizations has not addressed the consumerization of IT at all. In some organizations this has been a conscious decision, but some organizations just have failed to address the IT consumerization. Anyway, this strategy is also called "Laissez-faire" strategy, and it is characterized by boundless tolerance of allowing people to use whatever IT they like. This strategy was found to be surprisingly appealing since as much as 43 percent of all respondents (employees) were told to be comfortable with making the decision of which hardware of software they use for working. It was said that this

strategy might reduce the costs of IT for the organization, and promote entrepreneurship, but at the same time, the information security concerns and increased compatibility issues are the downsides of this strategy.

7.2 Authoritarian Strategy

As opposite to the laissez-faire strategy, Harris & al. [HIJ12] identified the authoritarian strategy, which had been adopted by another third of the surveyed organizations. These organizations are basically holding on for the principles of standardization and centralization, since they define a short list of allowed devices, and then only allow the use of those devices within the organization, and the use of all other devices types is forbidden. The motivation for this strategy is the assumption that maintaining security controls and providing support is easier and more cost-effective when the number of hardware and software options is smaller. This strategy is often used by industries which are strictly regulated or where the information security is top priority.

7.3 Middle-Ground Strategies

The first of the "middle-ground" strategies identified in the survey was named as "broadening the scope". The main idea in this strategy is not to specify an accurate list of devices and models which are allowed to be used or not, but instead to define some sort of boundary conditions for the devices. For example, one may use the device for working in our organization if the device supports data encryption, screen locking, and remote wipe. It is obvious that this type of list is easier to maintain and control than a list of specific devices. And what's best, the same strategy can be similarly applied to the use of applications as well.

The second of the middle-ground strategies is to provide IT allowances i.e. gadget budgets to the IT users. The users are given a fixed amount of money, and they can use it to purchase the IT they need for the next two or three years. Usually, but not necessarily, the allowance has some constraints which limit the options to a manageable amount. But most importantly, the user still has the right and freedom to choose

his or her IT, even though the list of allowed IT would contain all options from markets.

The third middle-ground strategy is actually almost alike with the strategy that we already mentioned in the chapter 6.1, and which was suggested by Cosgrove & Colville [CC10]. It is the strategy of segmenting the IT users by their role or IT needs. In many organizations it is very obvious that the IT needs of the different groups of people may vary a lot, and therefore it is rational to apply a more liberal strategy to one group, and then a more authoritarian strategy to another group of users.

The last of the four middle-ground strategies is to advocate uptake, meaning that the IT organizations should actively encourage the IT users to adopt the use of new devices and applications. This strategy is perhaps best appropriate for such organizations that wish to drive innovation and build an image of a tech-savvy organization.

And as it was stated earlier, these middle-ground strategies are not exclusive, but instead they can be adopted as such, or together with some other strategy.

Anyway, whatever the strategy will be, it is important to understand that the organization is not just creating a social media strategy or BYOD (bring your own device) strategy, but instead, addressing the underlying cause, the consumerization of IT, which comes with many faces and in many different forms including the use of cloud services, mobile devices, and social medias – it's all about the consumerization of IT.

8 Discussion and Conclusions

In the chapter three, we aimed to answer the RQ1 by getting acquainted with the essential IT management concepts including IT asset management, configuration management, change management, IT systems management, and IT service management. We also got familiar with ITIL, the de facto standard of IT and IT service management, and also noted that, in addition to the ITIL, there also exists many other IT management frameworks, which provide proven best practices for the different IT management functions.

In the chapter four, we explored the RQ2 and learned that the IT and IT service management ranges all the way from the management of technological IT infrastructures to the management of high-level business-aligned IT people, processes, and services. We also learned that the IT management as a whole is a well-established, multi-level function, and that the management of larger entities, such as IT processes or services requires mature and successful management of smaller, lower-level entities, such as IT infrastructure components. The management of high-level IT services or processes wouldn't be possible without successful low-level management activities. Therefore, highly automated and reliable asset management, configuration, and change management processes are important cornerstones of IT management. From the literature, we learned that IT organizations have traditionally trusted in IT standardization, IT centralization, restriction policies, and several lockdown methods to ascertain their ability to perform the low-level IT management in an efficient way.

In the chapter five, we familiarized ourselves with the concept of consumerization, which was the goal of RQ3. We learned from the research literature that several different IT trends, including the adoption of cloud services and the use consumer-originated devices and technologies for working, are booming and being noticed by IT professionals around the globe. These trends, collectively called the consumerization of IT, encapsulate at the same time a huge potential and great risks for the IT organizations when it comes to the IT management.

Earlier, for example Niehaves & al. [NKOK12] and Harris & al. [HIJ12] had researched how the consumerization of IT impacts to the IT management. In other words, they had researched what are the consequences of consumerization of IT to the IT management. Those studies indicated that IT consumerization has a positive impact to the employee satisfaction, availability, productivity, and the speed of new technology adoption that seemed to bring innovation benefits as well.

However, it was noticed that the research literature was missing the perspective *why* the consumerization of IT affects to the IT management, and what are the factors included in the consumerization that are changing the way how IT management is done in organizations. Therefore, this thesis intended to confirm that gap in the research literature and identify those factors.

8.1 Findings

In order to answer the RQ4, a literature review was conducted as part of this thesis, and it seems that the researchers' focus has been on analyzing how consumerization of IT affects to organizations, but no research has been dedicated for researching the factors why consumerization changes IT management. However, these factors are casually discussed in some researches which focus on some other areas of research. Therefore, based on the observations from the research literature, and the author's personal experience from the development of IT management tools, it is suggested that the consumerization of IT affects to IT management through, at least, seven different factors, which are:

1. **Ownership of IT resources**

   It will become more common that devices and web applications, which are used for working, will be purchased and owned by their users (e.g. organization members and employees), but not by the organization. This, in turn, breaks the practice of centralization which has traditionally been employed by IT organizations.

2. **Heterogeneity of devices**

   As devices are more often selected by their users, not by the governing organizations, the device base is likely to become more heterogeneous, which in turn, breaks the practice of standardization and hampers the use of traditional management toolsets and processes.

3. **Mobility of devices**

   Traditionally IT organizations have been able to focus on the management of stationary workstations, servers, and network-attached devices. However, the consumerization of IT and the rapidly developing wireless communication technologies are boosting the mobility of devices, which creates new limitations and interests for the IT management. For example, the ability to remotely protect the mobile devices by locking, tracking, or wiping are features which are very useful if a mobile device is lost or stolen.

4. **Use of cloud services and web applications**

   The increasing use of cloud-based services and web applications is problematic to traditional IT management practices, because the traditional tools are designed for managing locally installed applications, and the tools for managing the online use of applications and services is still immature.

5. **Disintegrity of IT resources**

   The more heterogeneous device-base, together with the adoption of cloud applications and services for working and management of IT, leads to an increased use of point-solutions in organizations. As a result, the compatibility issues are likely to increase, and the IT management and support are likely to become more complex, and therefore inefficient.

6. **Deployment model of information system(s)**

   Also the IT management systems, or toolsets, are now more often available as offsite private or public cloud services, which offer time and cost saving possibilities for IT organizations, and also may enable totally new business opportunities, as well. However, the downside of new IT management system delivery models is that they expose the IT management solutions to a totally new kind of information security risks if compared against the traditional IT management systems, which were hosted and operated on-premises.

7. **Complexity of information security management**

   The consumerization of IT will most likely also have a great influence to the information security of IT management by making the IT management, in a technical sense clearly more complicated thing to do. What makes it even more complicated, is that when the devices and web applications are owned by the IT users, it is necessary to separate between business and private use of those resources, or otherwise the IT users' privacy may get endangered. Therefore, it seems clear that the preservation of information security on an accustomed level requires great development of the IT management systems, processes, and competence.

Although, these conclusions were attempted to be based on research literature and author's experience from the development of IT management tools, they are still, for big part, based on the author's own discretion and judgment, and they should be therefore assessed and taken critically.

8.2 Future work

As a future work, it would be valuable to do more research on the automation possibilities of IT and IT infrastructure management processes in consumerized IT environments. For instance, the role-based framework for managing the use of cloud services and web applications, suggested by Richard Walters [Wal13], would certainly be an interesting topic to research and develop further. It might have potential to solve many

challenges that are related to the use and management of web applications and shadow IT.

Secondly, it would be necessary to do more research on the reason why consumerization of IT impacts to the IT management practices and methods by closer analyzing the seven factors suggested in this thesis, and also by researching if it is possible to identify more factors though which the consumerization of IT might have an impact to the IT management.

Thirdly, as many of the traditional IT management solutions are based on the use of platform-specific management agents, it would be interesting to do more research on platform independent management methods. As Walters stated in his article [Wal13], the browser is the new endpoint, and it should be possible to manage the browser-based activities in the same way that we are able to manage the traditional fixed and mobile endpoints. Would it be somehow possible to perform IT management on a satisfactory level without platform-specific management agents, or would it be possible to develop management agents that compatible with multiple platforms? For example, would it be possible to gather inventory information and perform other management activities, like change management, if the management method would be a cloud-based application, or a framework embedded in a web browser.

Lastly, one obvious area which still needs more attention and efforts from the IT management practitioners and researchers, is the development and use of key IT management terminology, especially when it comes to the solutions and toolsets, which are in actual use in IT organizations. The management toolsets and solutions are extremely difficult to assess against theoretical IT management frameworks such as ITIL, or compare head-to-head against each other, because the naming and scope of the toolsets and their features vary a lot between different solution vendors. In many solutions, same feature names are used to mean different things, and on the other hand, one feature can have multiple different names, which eventually all mean the same thing. This problem might be also partly caused by the fact that the IT management frameworks, such as ITIL, put the focus mostly on the theoretical management of people and processes, but not on the tools, which are used to implement those processes. Therefore

the theory (documented best practices) and practice (the tools for implementing the practices) have started to drift apart from each other.

References

[And11] Andress J. (Elsevier, 2011, USA) *The Basics of Information Security*, Chapter 1: What is Information Security?

[BK02] Bosworth S., Kabay M. E. (John Wiley & Sons Inc., 2002, USA) *Computer Security Handbook,* Fourth Edition, Chapter 5: Toward a New Framework for Information Security by Donn B. Parker.

[CC10] Cosgrove T., Colville R. J. (Gartner, 2010) *Organizations Are Increasing PC Lockdown*.

[CP13] Costello T., Prohaska B. (IEEE Computer Society, 2013) 2013 Trends and Strategies, *IT Professional*, pp. 61-63

[CMR09] Cummings J., Massey A. P., Ramesh V. (2009), *Web 2.0 Proclivity:* Understanding How Personal Use Influences Organizational Adoption, Operations and Decision Technologies Department, Indiana University

[DK13] Disterer G., Kleiner C. (University of Applied Sciences and Arts, Hannover, Germany, 2013) BYOD Bring Your Own Device, *CENTERIS 2013 - Conference on ENTERprise Information Systems / ProjMAN 2013 - International Conference on Project MANagement / HCIST 2013 - International Conference on Health and Social Care Information Systems and Technologies*

[Gar14] Gartner, *IT Glossary,* Consumerization, Available at: http://www.gartner.com/it-glossary/consumerization (accessed 15th April 2014)

[GF11] Geyer M., Felske F. (ACM, 2011) Consumer toy or corporate tool: the iPad enters the workplace. *Interactions*, Volume 18, Issue 4, pp. 45-49

[HR11] Hanna A., Rance S. (AXELOS Limited, 2011) *ITIL® glossary and abbreviations, English.*

[HIJ12] Harris J., Ives B., Junglas I. (2012) IT Consumerization: When Gadgets Turn Into Enterprise IT Tools. *MIS Quarterly Executive*, Volume 11, Issue 3, pp. 99-112

[HP03] Hewlett Packard (2003) *HP IT Service Management (ITSM).*

[IIBA09] International Institute of Business Analysis (2009) *A Guide to the Business Analysis Body of Knowledge® (BABOK® Guide),* Version 2.0

[ISO12] The International Organization for Standardization and the International Electrotechnical Commission (2012) *Information Technology – Security techniques – Information security management systems – Overview and vocabulary,* International Standard, Second Edition

[itSMF07] The IT Service Management Forum (2007) *An Introductory Overview of ITIL® V3*, Version 1.0

[MNOT04] Moschella D., Neal D., Opperman P., Taylor J. (El Segundo 2004), *The "Consumerization" of Information Technology,* CSC research white paper.

[Mor14] Morabito V. (Springer International Publishing Switzerland 2014), *Trends and Challenges in Digital Business Innovation,* Chapter 5, pp. 89-109.

[Nas12] Nasuni Corporation (2012), *Shadow IT in the Enterprise,* White Paper

[NIST11] National Institute of Standards and Technology (U.S Department of Commerce, 2011) *Glossary of Key Information Security Terms.*

[NKOK12] Niehaves B., Köffer S., Ortbach K., Katschewitz S. (European Research Center for Information Systems 2012) *Towards an IT Consumerization Theory – A Theory and Practice Review*, Working Paper No. 13

[NOK13] Niehaves B., Ortbach K., Köffer S. (ACM 2013) IT consumerization under more difficult conditions – Insights from German local governments, *The Proceedings of the 14th Annual International Conference on Digital Government Research*, pp. 205-213

[OKBN13] Ortbach K., Koeffer S., Bode M., Niehaves B. (Milan, 2013) Individualization of information systems – analyzing antecedents of IT consumerization behavior, *Thirty Fourth International Conference on Information Systems*, Completed research paper

[OGC11a] Office of Government Commerce (2011) *ITIL Version 3 Service Transition*

[OGC11b] Office of Government Commerce (2011) *ITIL Version 3 Servicer Improvement*

[PL13] Parsi K., Laharika M. (2013) A Comparative Study of Different Deployment Models in a Cloud, *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 5, pp. 512-515

[Pet08] Peters C. (Techsoup, 2008) *Tips for Standardizing Your IT Infrastructure.* Available at: https://www.techsoup.se/node/810 (accessed 15th April 2014)

[Sch12] Schiesser R. (Prentice Hall, 2012) *IT Systems Management*, Second Edition

[Sym12] Symantec (2012), *Avoiding the Hidden Costs of the Cloud*, Available at: http://www.symantec.com/content/en/us/about/media/pdfs/b-state-of-cloud-global-results-2013.en-us.pdf (accessed 15th April 2014)

[UN13] United Nations (2013), *Deputy UN chief calls for urgent action to tackle global sanitation crisis*, Available at:

http://www.un.org/apps/news/story.asp?NewsID=44452&Cr=sanitation&Crl=#UZHvFcrkx96 (accessed 15th April 2014)

[Wal13] Walters R. (SaaSID 2013), Bringing IT out of the shadows, *Network Security*, Volume 2013, Issue 4, pp. 1-20

[Web14] Webopedia, *Computer systems administrator*, Available at: *http://www.webopedia.com/TERM/C/computer_systems_administrator.html (accessed 15th April 2014)*