jamk.fi

Qualitative Study to Explore Obstacles of Public Cloud Adoption

Case Finnish Government Agencies and Public Administration

Mikko Haukkala

Master's thesis
May 2018
Technology, Communication and Transport
Master's Degree in Information Technology, Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Haukkala, Mikko	Master's thesis	May 2018
		Language of publication: English
	Number of pages 46	Permission for web publication: x

Title of publication

Qualitative Study to Explore Obstacles of Public Cloud Adoption

Case Finnish Government Agencies and Public Administration

Degree programme

Master's Degree in Information Technology, Cyber Security

Supervisor(s)

Saharinen, Karo; Saarisilta Juha

Assigned by

Vimana Oy, Maakuntien Tieto- ja Viestintäteknisten Palvelujen Palvelukeskus

Abstract

The benefits of cloud computing are unquestionable to organizations of any size. For public administration and government agencies, the cloud services can cut costs by replacing the internally run data centers and providing more attractive services to their users.

As cloud adoption is faster in the private sector, it is beneficial to investigate the reasons weakening the cloud adoption in the public sector in Finland. An assessment result of an official auditor against public cloud service was examined. This was done to clarify the possible technical security matters affecting the target organizations. The investigation included an interview of relevant persons working closely with related legislation, IT security and administration in the target organizations.

The results indicated that there are no major aberrations in the assessed public cloud service that cannot be mitigated. The results also indicated that some parts of the used criteria cannot be evaluated strictly because of the decentralized nature of the service. The same can be seen from the interview answers when respondents were asked about the weakening matters adopting public cloud services. Another weakening matter was the ambiguousness of the current instructions and regulations.

As a conclusion, the research states that lack of security in public cloud services is not the main reason weakening the cloud adoption. The partly unsuitable current auditing criteria increase the uncertainty in adoption of services.

Keywords/tags (subjects)

Government Agencies, KATAKRI, Public Administration, Public Cloud Service,

Miscellaneous

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Haukkala, Mikko	Opinnäytetyö, ylempi AMK	Toukokuu, 2018
	Sivumäärä 46	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Julkisen pilvipalvelun käytön esteet
valtion- ja julkishallinnon organisaatioissa

Tutkinto-ohjelma
Kyberturvallisuus, Insinööri (YAMK)

Työn ohjaaja(t)
Saharinen, Karo; Saarisilta Juha

Toimeksiantaja(t)
Vimana Oy, Maakuntien Tieto- ja Viestintäteknisten Palvelujen Palvelukeskus

Tiivistelmä

Pilvipalveluiden hyödyt kaiken kokoisissa organisaatioissa ovat kiistämättömät. Julkis- ja valtionhallinnossa pilvipalvelut voivat karsia kuluja korvaamalla sisäisesti hallittuja datakeskuksia mutta myös mahdollistaa houkuttelevampien palveluiden tarjoamista asiakkailleen.

Pilvipalveluiden käyttöönoton ollessa nopeampaa yksityisellä sektorilla on hyödyllistä tutkia mahdollisia syitä, jotka saattavat heikentää pilvipalveluiden käyttöönottoa julkisella sektorilla Suomessa. Tutkimukseen käytettiin virallisen auditoijan tuottamaa raporttia julkisen pilvipalvelun arvioinnista. Näin selvitettiin mahdollisia tekniseen tietoturvaan liittyviä esteitä kohdeorganisaatioille. Tutkimukseen sisältyi haastattelu, jossa julkis- ja valtionhallinnon IT-järjestelmien, hallinnon ja tietoturvaan liittyvien säädösten kanssa työskenteleviä henkilöitä haastateltiin paremman käsityksen saamiseksi hidastavista asioista pilvipalveluiden käyttöönotossa.

Tutkimuksen tulokset osoittavat, ettei julkisessa pilvipalvelussa ole lievennettävissä olevia merkittäviä poikkeamia teknisen tietoturvan näkökulmasta. Tulokset osoittavat, ettei kaikkia kriteerejä voida arvioida sellaisenaan julkisen pilvipalvelun hajautetun luonteen vuoksi. Sama huomio voitiin todeta haastateltavien vastauksista kysyttäessä pilvipalveluiden käyttöönottoa heikentäviä asioita kohdeorganisaatioissa. Toiseksi heikentäväksi asiaksi nähtiin nykyisten ohjeistusten ja säädösten tulkinnanvaraisuus.

Tutkimuksen johtopäätöksenä todettiin, että heikko tietoturva ei ole julkisten pilvipalveluiden käyttöönottoa merkittävästi hidastava pääsyy. Käyttöönottoon vaikuttaa auditointikriteeristön osittainen soveltamattomuus, joka lisää epävarmuutta pilvipalveluiden käyttöä kohtaa.

Avainsanat (asiasanat)
Julkinen Pilvipalvelu, KATAKRI, Julkishallinto, Valtionhallinto

Muut tiedot

Contents

Figures

1 Introduction

The benefits of cloud computing to organizations of any size are unquestionable. European Commission has driven a faster adoption of cloud services in all economic sectors for years to boost productivity, reduce ICT costs and create jobs. For public administration and government agencies, cloud services can e.g. cut costs by successively replacing internally run data centers and ICT departments (European Commission 2012).

1.1 Objectives

The objective of this thesis is to analyse what weakens the adoption of public cloud services in government organizations and public administration in Finland. To investigate the overall objective, the research analyses a set of specific objectives to examine the possible technical and non-technical factors that have an influence on cloud adoption.

To provide better and more precise understanding on what technical factors may affect the cloud adoption, the results from public cloud services assessment were examined and analysed against a national security auditing tool KATAKRI security level 4. The security level 4 is referred as STIV in this document. In addition, the suitability of KATAKRI as an auditing tool for public cloud services was analysed based of the outcome of the assessment results.

To assess the non-technical factors that may affect the cloud adoption, a qualitative survey in a form of an interview was conducted with the targeted people working with related legislation, IT security and administration in government agencies and public administration.

The set of objectives aims to provide better visibility on the technical and non-technical obstacles and issues preventing faster cloud adoption in Finnish government agencies and public administration. The research considers the suitability of current legislation, instructions and regulations for auditing public cloud environments. It also considers the possible ways of mitigating the possible technical

aberrations against KATAKRI STIV classified information as well as identifying the similarities from the answers of the interview about the non-technical issues.

The research is mainly intended to government organizations and public administration aiming to adopt public cloud services and people defining and working with legislation and with ICT.

1.2 Thesis Structure

This research has three parts: the first part examines the assessment of public cloud environment against national security auditing tool KATAKRI (ST IV) implemented by an official auditor. It examines and analyses the results and addresses the main aberrations and possible mitigations found from the assessment.

The second part of the research analyses the results of the conducted interviews made to the chosen employees of government agencies and public administration working closely with administration, IT security and related legislation affecting the decisions to adopt public cloud services.

The third part compares the results between technical and non-technical matters when considering the usage of public cloud services in Finnish government agencies and public administration. It also considers the suitability of the current official guidance affecting the faster adoption of public cloud services in government agencies and public administration in Finland.

The first main chapter (*Cloud Computing*) introduces the concept, benefits and considered risks of cloud computing. It explains the most common service models and deployment models Cloud Service Providers (CSP) offer and the nature of each model. It also explains the responsibilities between CSP and consumers and considers the advantages and disadvantages of the models.

The second chapter (*Security*) introduces the main security principles in cloud computing. It explains the main differences between cloud and traditional IT contracts and considers the problematicalities between the two. It also explains the laws, regulations and official guidance that affects the adoption of cloud services.

The third chapter (*Auditing Cloud Services*) explains the auditing process of cloud services and the auditor's role.

The fourth chapter (*Assessment of Public Cloud*) goes through the scope of the implemented assessment, assessed objectives and used assessment methods.

The fifth chapter (*Interviews*) explains the interview conducted with the employees of public administration and government agencies. It introduces the questions in the interview and the reasons for asking these questions.

The sixth chapter (*Results*) introduces the results and findings of the research. It answers the research questions based on the assessed objectives. It also reflects the results between different objectives and provides a proposal for the problems addressed in this thesis.

The seventh chapter (*Conclusion*) considers the research results and the future acts from the experience of this research. It reflects the outcomes of the examination and predicts the possible future implications of the subject.

1.3 Benefits of Research

As European Commission is driving the cloud adoption in all economy sectors to increase the productivity, growth and generating new jobs, it is beneficial to understand the possible challenges concerning security and legislation to enhance reaching the objective (European Commission 2012).

In addition to a broader view of the possible challenges, it is beneficial to receive the experiences of subject matter experts working close to decision-makers, legislation and IT. In order to compare the results from all sources it is possible to gain a wider understanding of possible challenges to help stimulating the active adoption of cloud computing in Finland.

1.4 Research Problem and Research Method

The research problem this thesis attempts to answer is "**Is the lack of security weakening the adoption of public cloud services in Finnish government agencies and public administration?**"

To investigate the research problem, the following research questions were defined:

- How well does public cloud translate to requirements against KATAKRI ST IV?
- What are the biggest challenges in current instructions and guidance to use public cloud services in government agencies and public administration?
- What are the biggest uncertainties of using public cloud from security perspective?
- How well does KATAKRI suit the auditing of public cloud environment?

This research uses empirical research strategy to analyse if the lack of security in public cloud services is slowing down the adoption of these services in public administration and government agencies in Finland. The research uses two main research methods.

The first part of this research is a case-study based on the results of a public cloud service assessment conducted by an official auditor. The assessment and the research are limited to one public cloud service providers' product to keep the scope of the research more limited. The assessment conducted by the official auditor is mainly based on the criteria of KATAKRI auditing tools. This research does not investigate other national criteria in detail due to the limited scope of the research.

The result data of the assessment was reviewed, analysed and interpreted. The case-study methodology was chosen to provide detailed information from the assessed source. The existing auditing results were utilized because of the fact that official auditing against KATAKRI from a wide source such as public cloud is costly and requires plenty of resources. The other reason was that there are only two official organizations capable of executing comparable and reliable assessments of this size. The case-study method has the disadvantage of providing a narrow perspective on a subject; however, in a real-life situation it is known as an effective method to use when carefully planned and crafted (Yin 2003, 19-33). The research contains an exploratory examination to establish the reliability of the findings. The reliability of the conducted assessment used in this research is evaluated according to reliability of the source, objectivity and recentness of the data.

The second part of the research was conducted as a qualitative inquiry to address the questions about non-technical issues on adopting public cloud services in public administration and government organization. The method was chosen to form the relevant personnel's cross-cutting view on the investigated problem. The interviewees were selected by their ability to provide as quality answers as possible.

Even though the basis of survey research is often quantitative in nature, in this research the survey was qualitative, and the material was analysed in a qualitative way. This is due to the limited amount of official authorities in public administration and government agencies. Another reason is that the same legislation and regulations apply to all these organizations.

The inquiry was implemented as a half-structured thematic interview where questions were e-mailed to the people working closely with related legislation, administration and IT systems. The e-mail-based interview was implemented for the logistic reasons when interviewed persons were located across the Finland. E-mail interview is also effortless way for the interviewer and interviewees. Half-structured interview method was chosen because scope of the interview was strictly defined and because there was a need to restrict the scope of the answers. Thematic interview is often used when the aim is to receive information about less known phenomenon (Hirsjärvi & Hurme 2000, 173)

The answers were analysed using thematic analysis method. The thematic analysis was chosen after carefully investigating the KATAKRI criteria and the results from the technical assessment. The thematic analysis is known for its ability to group the provided answers to themes that enables more effective handling and analysing of each topic. It also gives an exposed possibility to the interviewees to provide their insights (Hirsjärvi & Hurme 2000, 173)

The quality of the questions is often considered a disadvantage in a survey research. In addition, the missed answers in questions and misunderstanding of the questions may affect the inaccuracy in the conclusions of survey researches. In this survey, the questions were carefully crafted to ensure the reliability and validity of the answers (Yin 2003, 19-33).

The research also analysed KATAKRI's suitability and ability to act as an auditing tool of a public cloud service based on the results of previous researches. Finally, the results gathered from both main research sources were compared and analysed to form a conclusion of the outcome for the research problem in this research.

2 Cloud Computing

Cloud computing is generally perceived as a computing resource reached via the internet or private networking solutions. The conjunctive factor is that the computing resources do not reside in a single location such as traditionally in users' own data center but are reached through public network from the data centers provided by a Cloud Service Provider (CSP). One of the biggest benefits of cloud computing is that the resources can be reached theoretically from anywhere and with any device. The "cloud" is a combination of data centers distributed to a multiple geo-location creating a connected computing platform. From these data centers the CSP provides e.g. computing, storage and networking services to its customers (Viestintävirasto 2014).

2.1 Cloud Services

Cloud Services can be seen as an extension to traditional Information Technology (IT) services where IT infrastructure resides in an organization's own data center. Cloud services are typically consumed as a "*pay as you go*" model where customers rent an infrastructure, platform or even individual services from Cloud Providers (CP). This enables customers to obtain only the needed amount of computing power and resources.

Even if the cloud services are seen as an extension to traditional IT, there is a growing number of companies aiming primary or even fully at the cloud to strengthen their competitive advantage compared to other competitors. In addition, they take the full

benefits of the highly scalable, agile and almost limitless computing resources to increase their advantages on the market. (Microsoft News Center 2018).

2.2 Cloud Deployment Models

There are different types of deployment models of cloud depending on the resource location, connectivity and management of the infrastructure. The typical options in deployment models are private-, public- and hybrid clouds (Viestintävirasto 2014).

In *private cloud* deployments, the resources are owned and operated by an IT organization. The private cloud is not shared with any other customers and is often referred as a single-tenant cloud (Viestintävirasto 2014).

In *public cloud* deployments, the resources are shared from the same connected platform with other customers. This deployment is referred to as a multi-tenant environment. Even if the resources are shared, the environments are isolated from each other (Salo 2012, 9).

In *hybrid cloud* deployments, the customer keeps some parts of the infrastructure in on-premises servers such as user directories and extends the local environment in to a public cloud to get flexible services with full control of on-premises services. The hybrid deployment can also include a combination of local environment, private cloud and multiple public clouds (Viestintävirasto 2014).

2.2.1 Private Cloud

Private cloud is hosted, managed and maintained by consumers' IT department or external hosting parties. In private cloud deployments, the consumer has full control and responsibility of the environment (Viestintävirasto 2014).

Private clouds are often less scalable and not as distributed as public cloud platforms but provide a full control of the system from networks to applications. Private clouds are often more costly since they invest in hardware, management, operations and side costs such as electricity; however, in some cases the laws and regulations dictate

the possible deployment model options when a private cloud might be the only option in addition to on-premises environment (Salo 2012, 9).

Private cloud is often built with virtualized servers providing some benefits of the cloud services without the drawbacks in specific security, compliance, data location requirements. It also enables wider customization and monitoring options throughout the system (Viestintävirasto 2014).

2.2.2 Public Cloud

Public cloud provides the most scalable, flexible and distributed platform for shared resources. It is a hosted, managed and operated by CSP and services are provided from shared resources to multiple customers. The resources are owned and maintained by CSP, which gives less control of the physical hardware, networking between the data centers and options where the data resides physically. It is usually less costly as the hardware investments, maintenance and physical security of data centres are outsourced to CSP (Viestintävirasto 2014).

Usually, the most regulated organizations with highest service level agreements (SLA), data location and security requirements struggle moving their most business-critical applications and data into public clouds. Lately, the CSPs has brought dedicated data centers to e.g. government parties in the U.S. and in Europe to fulfil the specific needs of highly regulated customers such as government agencies (Zander 2018).

Even some organizations have difficulties in moving completely into a public cloud, the deployment model brings competitive advantages especially to small and middle-sized companies because it is able to deploy resources quickly and without big investments (European Commission 2012).

The biggest public cloud providers at the moment are Amazon, Microsoft and Google (RightScale 2018).

Microsoft Office 365 is a global communication and collaboration platform provided by Microsoft. It is a public cloud service providing Software-as-a-Service model to

consumers that offers Microsoft's well-known Office tools such as Excel, Exchange and Word with their productivity tools such as Teams and SharePoint from the cloud. The services are consumed with a licensing model that dictates the provided services and features to the customer (Alkula 2016).

The services are provided from decentralized locations from Microsoft's data centers to ensure high-availability of services. Today, the services for European customers are provided from Ireland, Netherlands, Finland and Austria. The service is certified against several standards and audited on a regular basis by third-party auditors. The audit reports are publicly available. Today, these audits alone lay around thousand security controls that are verified (Alkula 2016).

The communication to the service and between the data centers is encrypted. The data is also encrypted in rest and in transit. In addition, there are several features to enhance specific security controls depending on the licensing model (Alkula 2016).

Office 365 integrates partly with Microsoft's other cloud platform Microsoft Azure. Microsoft Azure hosts e.g. the user directory of the services that is a base for Office 365 user management (Alkula 2016).

Microsoft Azure is a Cloud computing platform providing IaaS, PaaS and other services to consumers. As an underlying part of Azure, there are multiple data centers across the world connected to each other to form a physical base with servers, storages and networking (Moisio 2017).

On top of this physical layer, Azure offers IaaS layer of virtualized servers, blocks of storages and logical networking components. It also offers PaaS services to an application software where the infrastructure layer is managed by Microsoft. There are categories from compute, web and mobile, developer services, integration, media, analytics & IoT and data services. There are also hybrid operation services to enable hybrid services between cloud and on-premises data centres and security and management services such as Multi-Factor Authentication (Moisio 2017).

Figure 1 illustrates an overview of the services in Azure.

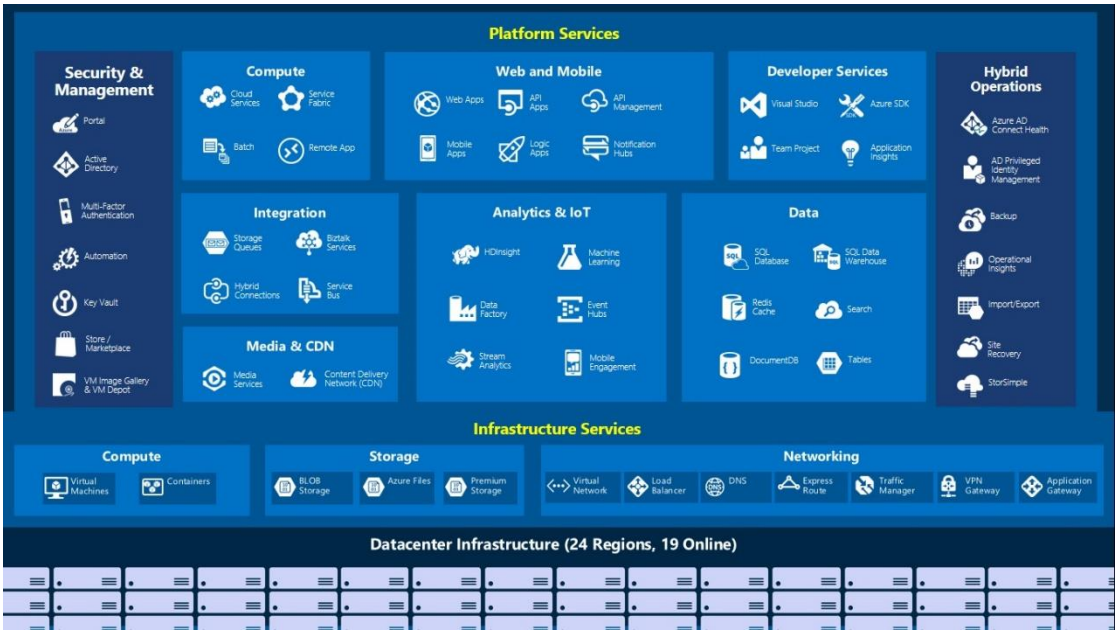

Figure 1. Microsoft Azure Services (Microsoft Azure Webisites)

2.2.3 Hybrid Cloud

Hybrid cloud is considered as an extension of companies' own data centres and network. The deployment model can include a combination of on-premises servers, private cloud deployment and even multiple public cloud platforms. With hybrid setup, an organization can keep some of the critical services and data inside the companies' on-premises and enable flexible and more scalable cloud platforms for some of its workloads. It can outsource parts of the management and operative work to its CSP (Viestintävirasto 2014).

Hybrid cloud model provides best of both worlds as companies can keep some of the most critical and regulated services and data in-house and outsource the rest of the services to a cloud, which often provides savings in costs and less effort for operations and maintenance activities. Some of the drawbacks might be that e.g. all of the monitoring and backup products might not be available in a cloud causing overlapping of products, which may increase the complexity in some areas (Salo 2012, 9).

Hybrid model stays as the most popular deployment model now as it gives organizations the best flexibility in planning the cloud adoption and services run on cloud platforms. (RightScale 2018)

2.3 Cloud Service Models

Comparing to traditional IT service models, cloud computing does not bring only cost savings, it also provides the outsourcing of hardware, maintenance and operations which are often the biggest costs of an IT department (Viestintävirasto 2014).

In addition to cost savings, the cloud computing brings a fundamental change to the way the IT services are consumed. Businesses are more agile and effective to meet the changing business requirements as the capability and ability to implement modern technologies becomes more effortless as upgrading systems and implementing high available, business critical services can be carried out in a more granular way. This way the IT departments can point their limited resources to more productive work (European Commission 2012).

Cloud computing offers three main categories of service models to allow a more granular, on-demand way of consuming services and resources from the cloud. These categories vary in the ways that responsibility of management of the infrastructure, platform and service consumed from the cloud (U.S. Department of Commerce 2011). The categories are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) as illustrated in Figure 2.

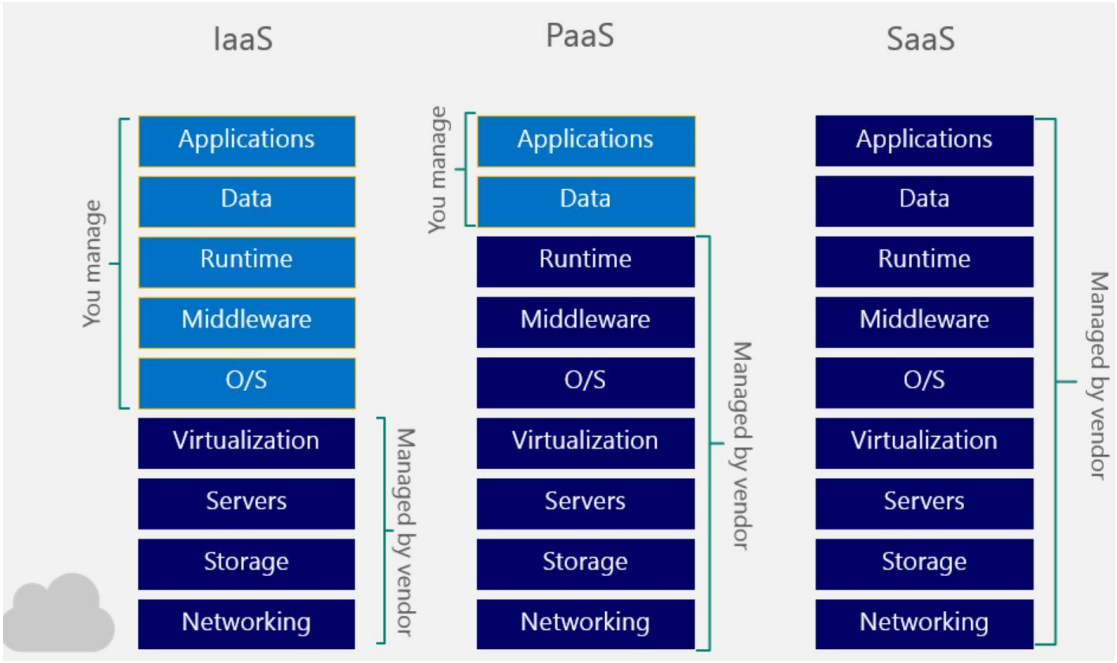

Figure 2. Cloud Service Models (Inspira 2016)

2.3.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service provides most control over the rented resources but also leaves most of the responsibility to a consumer of the three service models. CSP still manages and operates e.g. the physical servers, physical networking, storage services, virtualization platform, electricity, physical security of the data centres. Consumers' responsibilities start from Operating System (OS) level and continue till an application running on a Virtual Machine (Weinhardt et al. 2009, 391-399).

Typically, CSPs offer backup solutions, maintenance services, and high availability solutions which can be managed based on user demand IaaS is the most common way of deploying temporary, highly customisable and experimental workloads. Consumers are also able to scale the resource on demand and the resource is billed only for its usage, which provides a cost-efficient way of consuming resources. (Weinhardt et al. 2009, 391-399)

2.3.2 Platform as a Service (PaaS)

Platform as a Service model provides an infrastructure in the same way as IaaS service; however, with features like development tools, middleware and other support applications to provide development platform for service consumers. Consumers can then build their own applications with security solutions on top of the provided platform. (Viestintävirasto 2014)

PaaS services enable an on-demand, easy to deploy way of building development environments to the cloud. They enable a platform with pre-coded application components and interfaces built into the platform, which can then be enhanced with third-party components that fit for consumers' needs (Salo 2012, 16-23).

Some of the key benefits of building applications on PaaS are quick deployment of wide variety of development platforms, e.g. mobile applications, pay-as-you-go model on development tools, support of all phases in application development from building to updating. In addition, development teams in different geo-locations can easily access the platform via the internet (Viestintävirasto 2014). This enables agility, cost-efficiency and a wide variety of tools for all companies of all sizes. (Salo 2012, 16-23).

2.3.3 Software as a Service (SaaS)

Software as a Service is a service model offering the least amount of control and responsibility to consumer. In SaaS model, the consumer rents software or combination of software from CSP that the consumer then uses via public or private network. The most typical services consumed as SaaS services are web-based office and collaboration software and storage applications. (Viestintävirasto 2014)

SaaS services are often billed with licence models where consumer pays a licence and receives a combination of software to use. The licences are paid on a monthly basis, which enables an agile way of consuming.

SaaS services release consumers from the need of upgrading software and minimize the need of management and updating of the software (Salo 2012, 17-22).

In SaaS model, the IT organization acts as a service broker to provide and enable the needed services to its end-users without having to spend time on migrations, updating nor upgrading of the software or the platform the software is running on. Even if the service is “plug and go” type of service, the consumer organization is often responsible for authentication and access to the service when the access solution is typically implemented in a way that users use their existing organizational accounts. (Azodolmolky, Wieder & Yahyapour 2013, 54-62)

3 Security

According to Statistics Finland, Cloud Services were used in 66% of the Finnish companies in year 2017, which is one of the top margins in European countries. The most cloud services are used in Information and communication industry with 87% of the companies. Administrative and support services use cloud services in 75% of the companies where the usage of public cloud services is 61%. (Statistics Finland 2017) The security concerns of cloud, data privacy, compliance requirements and lack of knowledge have been the biggest issues when companies and organizations are considering moving their services to a cloud. (Statistics Finland 2017)

3.1 Responsibilities

In cloud services, the security is a combination of CSPs’ security responsibilities with customer’s own security measures and processes. It can be seen as a shared responsibility of the service provider and the customer. Like in traditional IT systems, also in cloud-based systems the security topics concerning authentication, authorization, availability, confidentiality identity management, integrity, audit, security monitoring, incident response and security policy management need to be considered (U.S. Department of Commerce 2011). There are also topics that are mostly customers’ responsibility regardless of the service model the customer is using. Customers’ security responsibilities are often considered to cover at least data governance, endpoints, user access management and identity infrastructure in cases

the customer is not using cloud-based identities but has its own identities synced or federated to be used in the cloud. Security responsibilities such as application, network controls and OS security depend on the used cloud service model (U.S. Department of Commerce 2011).

3.2 Privacy

One of the main concerns for cloud consumers has been privacy (Statistics, U.S. Department of Commerce 2011). The CSPs' ability to protect personal information and to provide visibility where personal information is moved and how it is processed is one of the main imperatives for public administration and government agencies when considering cloud services (Statistics, U.S. Department of Commerce 2011). The standardized framework of the EU on handling the personal information of EU citizens was applied in May 2018 with General Data Protection Regulation. It gives a unified set of rules for the organizations doing business in Europe to handle data protection with personal information (European Commission 2018).

3.3 Data in Cloud

As cloud computing continues to grow, the amount of data stored in the cloud grows along. As users do not have complete control of their data when storing data in the cloud, the data security is still one of the main concerns for organizations (Statistics Finland 2017). As data is shared with a third-party and accessed via the internet, the consumers want to be assured of confidentiality, integrity and availability of the data. The protection of private information such as credit card numbers and medical records plays a critical role in data security in cloud. Also, as the cloud services are accessed over the internet, the availability of the data relies not only on the service itself but on the connection as well, which has its own security concerns (Viestintävirasto 2014).

Another matter that worries organizations is the data location. As public cloud services are distributed and often the data resides in another country, it is a valid concern for the organizations having business critical information that needs to be accessible all the time even if the network connection is not available across the borders.

On the other hand, the distribution of the data and data replication between geo locations gives better security against data losses when data is not in a single location. In case of damage in data center or even natural disaster in one of the data center locations the data is not deleted since the data can be distributed between geographical locations and even between different continents. Also, the connection to the service itself can be secured further with technology provided by CSPs to use private and dedicated network to access the services (Microsoft Trust Center 2018).

The physical security of the servers and the data disks has many security controls e.g. video monitoring, secured server racks, security personnel and access controls. Also, the data disks are striped on a way that the data is distributed between physical devices and encrypted disks complicating the targeted theft of the physical data (Microsoft Trust Center 2018).

The security of data is also a combination of CSPs security measures, processes and policies with the security measures provided by consumers. To provide data security from the perspective of confidentiality, integrity and availability as well as data in rest, transit and in use end-to-end security measures to provide the best possible solution need to be planned and implemented well (Microsoft Trust Center 2018).

3.4 Contracts

A consumer and CSP accept a certain base contract between each other when cloud service is deployed. The consumer agrees not to use the service for any illegal or immoral activities whereas the CSP agrees to provide services on a certain level, confidentiality and provide the agreed platform services (e.g. network, servers, electricity, physical security). Consumer and CSP can agree on more detailed agreements depending on criticality, availability and location where the service is

provided. These more detailed agreements can also be based on a classification of the data, restricting legislation and other threats and restrictions that need to be considered when providing the service. Agreements can also include specific information about the permissions to manage the data. The need for the specific agreements is defined during the risk analysis of the service and the data handled in the service. This way the consumer can prepare more carefully to exceptions in the service (Viestintävirasto 2014).

In traditional IT outsourcing, the contracts were negotiated more related to data storage, processing facilities and more specifically related to an exact service whereas in cloud computing the contracts are defined as a framework to provide access to flexible and scalable computing resources. The different nature between these two computing models and the complexity and uncertainty of the legal framework towards CSPs results in more complex contracts and SLAs with extensive disclaimers, which reduces the certainty of consumer to adopt cloud services. For that reason, the development of model terms for cloud computing is important as the SLAs between CSP and professional users determine the basis of trust between cloud users and CSP (European Commission 2012).

3.5 Legislation and Regulatory

In Finland, the main determinant borders for information security are enacted in legislation. The Finnish Constitution, the Personal Data Act and the Act of the Openness of Government Activities are examples defining the ground rules of information security and how to handle data in public administration, government agencies and in general (Ministry of Finance 2016). The laws are complemented with specifications, instructions and regulations leaving some room for interpretations. Some regulations are laid in the European Union like General Data Protection Regulation (GDPR) that defines how the personal data of European citizens can be handled.

On European Union level, the minimum standards and basic principles of information security are laid in Security Rules for protecting EU Classified Information (Ministry of

Defence 2015). For Finnish central government handling classified information, the Government Decree in Information Security in Central Government is the most important legislation. The instruction to implement the decree is instructed in VAHTI, a set of instructions for government information security (Ministry of Defence 2015). To audit organizations handling classified information, the information security auditing tool KATAKRI is used.

The key statutes related to information security are listed in Appendix 1: *Key statutes relating to information security* and Appendix 2: *Valid VAHTI publications*.

3.5.1 KATAKRI

The information security auditing tool KATAKRI is an official auditing tool for authorities in Finland. KATAKRI is used to assess a target organization's ability to protect classified information, its facilities as well as its ability to secure its information systems with technical elements, policies and processes. It can also be used to develop the security of companies and organizations in mentioned fields (Ministry of Defence 2015).

KATAKRI ensures that the target organization has appropriate security arrangements in preventing unauthorized access to its or its customers' data and to the environments where the data is stored (Ministry of Defence 2015).

KATAKRI is a collection of requirements from national and international legislation of information security; however, it does not set any mandatory requirements for organizations from information security perspective. When an organization is assessed against the criteria in KATAKRI, the results of the audit and assessment are reported to the target organization.

KATAKRI has three subdivisions of criteria: Security Management, Physical Security and Information Security. The Information Security is further divided into three subdivisions reflecting the protection level of the information. These levels are marked as *IV*, *III* and *II* which are equal with internationally used classification levels: *Restricted*, *Confidential* and *Secret*. Each classification level has its requirements with an example implementation scenario. The additional examples and information can

be found in other related guidelines and policies such as VAHTI instructions (Ministry of Defence 2015).

3.5.2 VAHTI

VAHTI is a Government Information Security Management Board. Its main function is guiding, developing and steering the government information security to support the quality, efficiency and productivity of government services (Ministry of Finance 2016).

VAHTI instruction is a compilation of Finnish government instructions on secure handling of information (KATAKRI). The instructions are a comprehensive set of guidance on how to implement information security regulations targeted mainly to public administration and government agencies. The instructions gather together a wide area of topics related to information security, classified information and environment handling this kind of data (VAHTI). Where the Government Decree in Information Security in Central Government lays down the legislation in information security for central government, VAHTI instructions give guidance and examples how to implement and meet the legislation (Ministry of Finance 2016).

3.5.3 General Data Protection Regulation (GDPR)

The European Union's General Data Protection regulation, or GDPR, advances privacy rights of European citizens. It is a privacy law ensuring and strengthening the data rights of EU citizens and it harmonizes data protection and privacy regulation in all member states of the EU. It also lays down a unified regulative over European companies as well as foreign companies doing business in the EU area who are handling and managing information on EU citizens (European Commission 2018).

The main objectives are to specify how organizations can collect user data and how the data can be used and handled. It sets technical regulations on how the user data must be handled in a secure manner and obligates organizations to report data breaches and violations to persons that the violations concern as well as official

authorities. If these regulations are violated by an organization, it may result up to 20 million euros in fines or fines up to 4% of the organizations' annual revenue (European Commission 2018).

4 Auditing Cloud Services

"The Cloud" is a combination of physical data centers connected with each other; however, there is still a physical IT infrastructure on the background. The distributed, virtualized and multi-tenancy nature of clouds makes it still different and more complex than traditional IT infrastructure (Doelitzscher 2014).

Auditing cloud services has still the same principles as in auditing traditional data centers even though the nature of the services is different. The audit aims to validate and investigate the physical and technical security of the service as well as examine that the policies and processes are appropriate (Doelitzscher 2014).

Where traditional IT architecture renews more in phases, cloud services are evolving constantly, which may create development needs to legislation, instructions and regulations as well as to traditional IT auditing criteria to be renewed. (Doelitzscher 2014).

4.1 Auditing

Auditing is a process of examining and evaluating an organization, its IT system, policies and processes to find out if they are accurate and meet the laws, regulations and standards related to the audited field and objects. Auditing ensures that appropriate controls and processes work according to the regulations and legislation the auditing is executed against. Auditing is executed by an external authorized auditor that has proven authorization and competence to audit targets against the specific legislation, regulations and standards. The auditor may grant a certification or diploma after successful auditing result to prove that the audited objects meet the requirements of against certain criteria. (U.S. Department of Commerce 2011)

4.2 Auditors

An auditor is an independent party that can conduct an assessment to examine cloud services. In addition to the information system operations of cloud services, performance and security of cloud services are audited. The audited security controls are the safeguards of organizations' information systems that ensure the confidentiality, integrity and availability of a system (U.S. Department of Commerce 2011). The controls include technical, managerial and operational aspects that combine the security of the system.

Security auditing verifies that the security controls are correctly implemented to provide the required outcome. The audit often includes a verification of the used policies and processes to verify that the correct policies are implemented to ensure the regulatory compliance (U.S. Department of Commerce 2011).

In Finland to become an official institute in auditing IT security for public authorities, the company must meet the criteria in assessment of the institution instructions (*Ohje tietoturvallisuuden arviointilaitoksille*) and become accredited by FINAS accreditation service. The institute will be accepted by Finnish Communications Regulatory Authority (Viestintävirasto 2016).

5 Assessment of Public Cloud Environment

The assessed environment was Microsoft's Office 365 public cloud service platform which was assessed against KATAKRI ST IV environment reference framework. The assessment was not an official audit where the audited environment should be a working production environment when parts of the environment were implemented to be a target for the assessment made by an official auditing institute in Finland. The assessment was implemented as far as possible in accordance with the evaluation provisioned down by FICORA (KPMG 2017).

5.1 Assessment scope and used methods

The scope of the assessment included administrative requirements and technical verifications. The assessment also describes the methods used at the assessment. (KPMG 2017).

The assessment was implemented using existing documentation of the cloud service and comparing existing audit and assessment reports to KATAKRI of ST IV requirements. The assessment included interviews with Microsoft's subject matter experts and product area experts to reflect the answers to the requirements of KATAKRI. The results and outcomes were verified from two sources as far it was possible as described in the FICORA assessment guidelines (Confidential offer). The inspections were carried out in Microsoft's data centers, which also provide production environments to consumers. The design, maintenance and implementation of the environments were inspected physically and by the people corresponding to the matters. Because of the nature of distributed cloud services and the nature of some criteria in assessment of the institution instruction, some areas could not be assessed against the criteria (KPMG 2017).

5.2 Administrative requirement

The inspection in administrative requirements included sub-requirements in safety management and the environmental assessment of business information systems. Safety management focuses on how security and its management are implemented throughout the organization and in specific inspected subjects. The inspection aims to examine if the target organization of an inspection has sufficient administrative and physical security controls to manage the security risks. It also validates the procedures to manage and develop the security of its employees (Confidential offer). The assessment of the Business information systems environment examines the data processing environment particularly focusing on parts dealing with classified and confidential items. The assessment was implemented to the entire life-cycle of the data from the creation to deletion (KPMG 2017).

5.3 Technical Verification

The assessment also included a variety of technical verification measures against the organization and environment.

Physical security assessment examines the physical safety of the environment where privileged information is stored. It investigates that the security controls to store confidentiality of information are met and that the target and related areas related to production environments are protected against unauthorized access, processing and listening. Physical security assessment examines the ability of a target organization to prevent, block and detect unauthorized access to areas where production or management systems are located. It also investigates the access control and permission management to confidential areas and information (KPMG 2017).

The assessment also includes testing the access of target environment and areas depending on the target (KPMG 2017).

5.4 The methods used at work

The assessment was carried out following the criteria of certification manual of Finnish Communications Regulatory Authority. It defines the methods, processing of the material and processes related to used equipment and the data received during the assessment (KPMG 2017).

The assessment was implemented using dedicated equipment with a dedicated base image installed including the needed application to carry the assessment phase. The equipment was cleared and reinstalled with the clear base image after each assessment phase (KPMG 2017).

The classified data received during the assessment was processed only in a dedicated space with access controls and managed permissions. Where appropriate, the data was processes only in customer premises (KPMG 2017).

All confidential communication was communicated between the persons defined in advance and by using secure communication methods. Confidential data were not transferred. (KPMG 2017).

6 Interviews

This thesis investigates the possible reasons for weakening the adoption of public cloud services in government organization and public administration in Finland. To investigate especially the non-technical factors that may affect to the adoption of public cloud services, a half-structured thematic interview was conducted to get more clarification from the human perspective of the objective. The interview included questions targeted to people working on related legislation, IT security and administration in government agencies and public administration. The addressed themes were chosen based on the orientation of the topic and the nature of the research problem. The research topic and the research questions were formed to an exploratory form. The questions were targeted to answer a certain topic; however, they leave space for a personal opinion of an interviewee. The interviewees were selected based on their role in an organization in order to aim at maximizing the quality of the answers.

The questions in the interview were:

1. *How do KATAKRI and VAHTI instructions suit the auditing of public cloud services?*
    a. *In what parts does it?*
    b. *In what parts does it not?*

2. *What are the biggest factors weakening the adoption of public cloud services in government agencies and public administration?*

3. *What are the biggest factors to be renewed in decrees and instructions related to public cloud services?*

4. *What are the biggest benefits and weaknesses of public cloud services from the security perspective?*

These questions aim to clarify the human perspective of the factors in public cloud adoption. The questions aim to clarify the objectives about the biggest technical and non-technical matters affecting to the adoption. They also examine how KATAKRI and current legislation, instructions and regulations are experienced to fit in assessing public cloud services.

The first question was asked to get a general view about pros and cons of KATAKRI and VAHTI instructions as an auditing criterion. It was also asked to gain material that can be compared to the technical assessment conducted to a public cloud service against KATAKRI criteria. This way the comparison can be done and analysed if the technical assessment report provides equal feedback with the feedback provided by the people working closely with the regulations and instructions.

The second question was asked to get persons' own opinions about the matters weakening the public cloud adoption in the target organizations. It is noteworthy that this question does not define if the factors need to be technical or non-technical. This way it is possible to clarify if the experienced factors are technical or something else. The question is also asked to get more information on the main research problem: *Is a lack of security weakening the adoption of public cloud services in Finnish government agencies and public administration?*

The third question is targeted to getting information about the topics in the current legislation, instruction and regulations that need the most renewing. In this question it is noteworthy that the question does not specify if the environment is in cloud or in on-premises even if the previous questions might drag the answers towards cloud services. Depending on the answer, it still has an underlining effect for the previous questions.

The fourth question is asked to clarify the considered security weaknesses of a public cloud services. It also aims to get clarification on the main research problem of the thesis even though all questions and answers have some clarifying aspect on it.

The interview was conducted by e-mail and the answers were analysed confidentially. The aim of the analysis was to spot similarities in the answers and group the similar answers into themes. The similar answers were grouped together and the topics that stood for each theme are introduced in Chapter *7, Results*.

7 Results

The results provided in this chapter are presented in a logical order to be able to come up with a conclusion for the main research problem of this thesis.

The research began with the analysis of the technical assessment results of Microsoft Office 365 service. As the assessment did not show any unmitigable and clear aberrations, the research was continued to get more insight to be able to conclude the main research question.

The research continued with the interviews and analysis of the answers. The recurring answers were grouped into themes. The themes are addressed in Chapter *7.2 Findings from Interviews*.

The final part of *Results* chapter analyses and compares the results from the technical assessment with the answers of the interviews concerning KATAKRI's suitability and its ability to translate to an auditing tool of a public cloud service. It aims to reflect the two sources of information on the same topic.

7.1 Technical Security Assessment of Microsoft Office 365

To start examining the research problem *Is a lack of security weakening the adoption of public cloud services in Finnish government agencies and public administration?* and to get more information to support the conclusion, the research was started with an analysis of the results of a technical assessment that was conducted by an official auditor KPMG against KATAKRI ST IV criteria. KPMG, an official auditor is an external, third-party actor not linked to the subscriber of the assessment, which may increase the reliability of the results. The results examined in this research are based on the recent assessment of the public cloud environment in Finland, which also may increase the reliability of the results.

The analysis was based on the case study results gathered from the assessment. The research was conducted based on the methods used and explained in the beginning of this thesis.

The technical assessment was conducted by KPMG to Microsoft's Office 365. Even though Microsoft Azure was not within the scope of the assessment, some parts of the assessed security controls are managed in Microsoft Azure because of the nature of the services and the reason that the platforms are partly integrated. The main functionalities of the Office 365 service were assessed against the KATAKRI ST IV criteria in a way the criteria allow. The results are reflected from the essential observations of the assessment mainly because of the confidentiality of the detailed assessment (KPMG 2017).

The technical assessment indicates that the security controls assessed against KATAKRIs' security management are appropriate in Office 365 and that the practices are mainly in-line between the locations. It was noteworthy that even though the information is classified differently comparing to Finnish officials, the baselines are the same that separate customer data, personal data and special protected data from each other (KPMG 2017).

The essential observations indicate that all the security controls in Office 365 cannot be assessed precisely against the criteria used in the assessment because of the nature and structure of the service; however, these controls can be agreed upon with a contract. An example case is the difficultness of verifying customer data deletion, which is difficult to verify in centralized systems where the data can be stored in a many location and can also be in transit at the same time. Even though Microsoft is committed to remove the data within a scheduled timetable, the customer can affect the availability of the data by e.g. implementing Bring Your Own Key (BYOK) feature to manage their own encryption keys in the service. In this way when a customer removes the key from the service, the data will be unavailable within hours (KPMG 2017).

Office 365 is a multi-tenant environment where the tenant is separated mainly in logical ways based on Application Programming Interface (API), network structure or encryption. As in Finland the national encryption requirements are more demanding and are based on the defined protection time of 25 years, the service's encryption methods do not meet these requirements. The essential observation notes that these requirements can be compensated e.g. also with Bring Your Own Key (BYOK)

feature by renewing the encryption keys more regularly to meet the Finnish requirements (KPMG 2017).

Office 365 maintenance is carried out globally. If customer data is moved outside Europe, the European Unions' model clause and the Privacy Shield contract between United States (US) and Europe stands. Some user data is collected and moved from Azure AD to US for billing purposes and an analysis of performance. The customer can still control what data from the objects is copied from local Active Directory to Azure AD. The essential observation notes that the telemetry data is collected from the services and servers. The data is sanitized but not always completely and the telemetry data is also removed manually. The observation highlights that the telemetry data is also collected by Windows workstations, Google and Apple, which might be used to consume this service (KPMG 2017).

As a closing, the essential observation states that Microsoft executes comprehensive internal and external security auditing to its services. As an example, the observation mentioned internal Red Teaming activity, public Bug Bounty program and acknowledgement to Microsoft's customers to test its services. In addition, separate third-party auditions are ordered. The results are not as detailed as the KATAKRI criteria requires; however, Microsoft's regular auditions are comprehensive and provide a good overall picture about the security of the service. In addition, the results steer the continuous planning, implementing, auditing and reacting of the security of Microsoft's services (KPMG 2017).

7.2 Findings from Interviews

The research included a qualitative inquiry to examine the possible matters affecting the adoption of public cloud services in public administration and government organizations. The inquiry was targeted at relevant personnel working closely with related legislation and regulations, government and public administration and on the IT systems of these organizations. The answers of the people participating in the interviews were analysed to find the similarities from the answers. The questions are presented in Chapter 6, *Interview.*

The dominant themes chosen to this inquiry were:

1. *Suitability of current criteria as an auditing tool against Public Cloud*
2. *Weakening factors in Public Cloud adoption*
3. *Biggest factors to be renewed in current legislation and instructions related to Public Cloud environments*
4. *The security benefits and weaknesses of Public Cloud*

The answers were examined open-mindedly. The themes formed from the answers of the interviews followed the defined themes chosen to this inquiry. There were no unexpected themes raised from the answers of the interview. The themes were formed with the help of coding and quantifying the received answers. From each interview, the similar answers were grouped and sorted under each theme. The results are based on confidential interviews that cannot be published here.

From the first theme, the unified view from the persons answering to the interview was that the current auditing tools suit partly to the auditing of a public cloud environment (Appendix 3-7). The part that was considered the most suitable was the Security Management in KATAKRI (Appendix 5,6). The answers that clearly stood up about the unsuitability were that the criteria do not fit well for auditing a multi-tenant environment (Appendix 4,5,6). In addition, the administration of decentralized systems was discussed in the answers (Appendix 5,6,7). The other issue that was mentioned was that the criteria do not include cloud specific security controls (Appendix 4,5,7).

From the second theme, the most significant factor reducing the adoption of public cloud services in the target organizations was considered to be the lack of cloud specific criteria when auditing the cloud environments against the requirements of classified information (Appendix 5,7). Because not all the criteria can be met or verified because the criteria do not completely suit to the auditing of a public cloud, the organizations do not dare to use the services. Another issue that clearly stood out in the answers was that the information is classified too easily because of the ambiguousness of the instructions, which leads again to the situation that the organizations do not dare put the information into cloud environment (Appendix 3-7). Another matter that was mentioned was the uncertainty of the location of the

data, the lack of general knowledge as well as the knowledge about the security controls available in a cloud, fear of losing reputation, old-fashioned attitudes against cloud services and the fact that there are no common principles across the organizations (Appendix 3,4).

From the third theme, a single factor that needs to be renewed from the current decrees and instructions according to persons answering the interview was almost unanimous: information protection levels, since information protection levels of information were considered too ambiguous (Appendix 3,4,5,7). The other specific answer that stood up from all the answers was the lack of unified policies, which increases the uncertainty in using public cloud services in government agencies and in public administration (Appendix 3,4,5).

From the fourth theme, the biggest advantages of public cloud services in security perspective were considered the security controls of the services (Appendix 4,5,6,7). The respondents thought that the security controls in cloud will bring cost savings compared to traditional IT security controls (Appendix 3,5,7). Also, high level of availability and recovery from service interruptions stood up from the answers (Appendix 4,5,6,7).

The disadvantages in public cloud service were considered to be in getting the data back from the service to local data centers in case of major conflicts and incidents (Appendix 4,5). This was the answer that clearly stood up from the rest. The others that were mentioned most were the clearance of the laws that apply in case of conflict situations, and that the contracts between the Cloud Service Providers are usually one-sided (Appendix 3,4,5,6).

The effective matters that may affect reliability of the conducted inquiry are e.g. sampling, low response rate, presence of an interviewer, quality of the questions and the examination of answers (Yin 2003, 19-33). The sampling of the inquiry included ten persons from where five persons provided an answer. The material gathering using interviews was stopped once the similar answers started to stand from the received answers. The interviewed persons were carefully chosen to maximize the quality of answers.

7.3 KATAKRI as auditing tool against public cloud

The results of the technical security assessment of Microsoft's Office 365 against the KATAKRI STIV criteria indicate that KATAKRI suits partly for the auditing of public cloud services (KPMG 2017). The results of the interview indicated the same as interviewees felt that the criteria partly suit the assessment of public cloud (Appendix 3-7). The one common thing that raised from both sources was KATAKRI's security management's suitability to fit as auditing criteria against public cloud.

The essential observation noted that because of the decentralized nature of Microsoft Office 365 service, some criteria could not be evaluated as they are mentioned in KATAKRI. The assessment pointed out that differentiating customer network traffic from each other e.g. for auditing purposes is difficult since the data is moved partly on the same network. The assessment also produced aberrations on the physical security part as criteria related to personnel security cannot be fully evaluated since the maintenance and administration of the service is done globally (KPMG 2017). These same problems were noted also on the interviews as the interviewees mentioned that differentiating network traffic from other customers' traffic might be difficult since the traffic is logically separated (Appendix 5,6). It seems that the auditing tool is mainly designed for traditional, internally managed, IT environments and systems with more centralized way of administration. This is understandable since some parts of the criteria have been defined before cloud computing became more general. This creates a reason to question about the suitability of current auditing criteria and their ability to keep up with the continuous development of cloud services.

The matter that differentiates the assessment results from the interview results was the suggested mitigation possibilities raised on the assessment. Where most of the interviewees did not come up with any mitigatable actions to fulfill the evaluated criteria, the assessment came up with several mitigations to address the points that could not be evaluated against the criteria or did not fulfill the requirements laid down by KATAKRI or Finnish legislation. An example of the requirement that the cloud service did not completely fulfill against the criteria was the Finnish national encryption requirements. However, it was possible to compensate this requirement

with customer managed encryption key and its possibility to be renewed more often (KPMG 2017).

The possible reason why the interviewees did not come up with the compensating actions might be that there was no specific question about possible mitigations in the interview, and the interviewees did not take the freedom to present overcoming possibilities. This can also address the lack of knowledge or unwillingness to overcome the aberration. The auditors had the advantage to be able to interview Microsoft's experts about the additional security controls provided on the service.

In the results of the interview, privacy was mentioned as being one of the main concerns, for example, the concern of some personal information being transferred outside of Europe (Appendix 4,5,6,7). The same matter came up in the technical auditing; however, the technical assessment noted that privacy needs to be considered on a wider perspective, as the users' end devices used to consume the services with can collect and transfer the privacy data as well (KPMG 2017). The privacy is still one of the key topics that cloud service providers need to invest in to enhance the trust between customers and cloud service providers.

The essential observation indicated that the aberrations found in the assessment can be mitigated with additional processes and security controls. The result of the assessment also indicated that the criteria cannot be used strictly as some parts, such as KATAKRI Security Management suit almost directly for assessing public cloud as the specific criteria of the topic did not point any criteria that could not be assessed (KPMG 2017).

8 Conclusion

The aim of this research was to investigate the possible reasons weakening the adoption of public cloud services in public administration and in government agencies in Finland. The possible reasons were investigated by means of technical assessment results and results received from interviews. The technical assessment of Microsoft's Office 365 indicates that there are no major security risks in Office 365

against KATAKRI STIV criteria. The aberrations raised from the assessment were mainly due to the criteria not fitting completely for the assessed environment and most of the aberrations that did not meet the auditing criteria or national requirements were mitigatable with additional security controls and processes. The interviews indicated that security controls in public cloud are seen more as a positive matter and as an entity which may even increase the security and reduce the costs compared to traditional IT systems used in public administration and government agencies. The uncertainties from a security perspective that were mentioned are privacy concerns and availability of the data in major conflicts and incidents. When asked about the main weakening factors in adopting public cloud in target organizations, the significant majority answered that the lack of cloud specific criteria in current auditing tools increases the uncertainty in adopting the public cloud services. Another significant result was related to the data classifications where data is perceived to be classified too strictly and it was also noted that the instructions are ambiguous to interpretation, which leads to uncertainty as to where the data can be stored. According to technical assessment results, the auditing criteria are capable of assessing public cloud service in adaptive way; however, they cannot be used exactly as they is used against traditional IT systems.

According to the technical assessment of results and interviews, there is a clear need for more cloud specific criteria and a unified framework, which provides a more suitable tool when auditing decentralized public cloud environments. According to some of the answers in an interview, there is also a need for a more centralized way of consuming services in public administration and government agencies. The instructions on classifying information are clearly considered to be too ambiguous for end users, which increases the uncertainty of how the information can be managed. Now every organization needs to interpret the information security instructions and guidance by themselves without having a centralized approach on cloud services and their usage.

Even though KATAKRI can be partly used as an auditing tool for public cloud, the unsuitable criteria for cloud services are getting much weight without observing the meaning of the assessed criteria and the vulnerability it is tested against. According to technical assessment, there are possibilities of mitigating possible vulnerabilities

that would help fulfilling the current gaps between the criteria and the cloud services. It would be interesting to further investigate how actively the possible aberrations resulted from the unsuitable criteria are examined and which methods are used.

As cloud services are constantly evolving, how are more static criteria keeping up with the development of the modern services? European Commission has stated in its confidence-building steps plan in 2012 that the clear and protective framework for public sector and appropriate set of standards would help to increase the trust towards cloud providers. It would help public sector to ensure to be compliant with the obligations (European Commission 2012). This might be the desirable way also in Finland.

The research provided a wider insight into the weakening matters affecting the adoption of public cloud services. In addition to technical matters, the research was able to clarify challenges in the current information security legislation, instructions and regulations. It also took into account the human perspective of the weakening matters.

The research was able to answer all the defined research questions on a high level as well as the main research problem as there are other issues than security concerns that are weakening the cloud adoption in target organizations. The research gives a direction about the weakening matters; however, it does not indicate the activities that would effectively solve the matters. To understand the nature of the weakening matters more closely, an additional research should be designed and implemented. The results of this research can still be used as a base for other researches about the topic as well as considering the issues in current legislations, instructions and regulations.

The risk in analysing qualitative material is that the researcher might try to point out positive or negative results above others. To avoid this, I tried to carefully analyse the answers of the interviews as well as take a neutral approach when analysing the technical assessment results. I have tried to avoid the technical assessment results from effecting how to approach the interview results and vice versa, to keep an exploratory attitude during the research. The sampling in interview was large enough

to provide similar answers to the questions. The reason why people did not answer was the lack of time or they considered not to have enough knowledge about the matter. Those people would have had different opinions about some of the questions than the interviewees that participated. That might have affected the results of the interview.

The benefits of cloud services are clearly being noticed in public administration and government agencies. The main aim of these organizations is to be compliant with the legislation and protect the citizens of the country, acting by laws and being certain about the interpretation of public policies.

References

Alkula, J. 2016. Office 365 -palvelun käyttöönotto IT-palvelutalon asiakkaille. Bachelor's Thesis, Metropolia University of Applied Sciences, Computer Networks, Accessed on 21.5.2018. Retrieved from http://urn.fi/URN:NBN:fi:amk-201605046256

Azodolmolky, Wieder & Yahyapour. 2013. Cloud Computing networking: challenges and opportunities for innovations. Communications Magazine, IEEE

Doelitzscher, F H-U. 2014. Security Audit Compliance for Cloud Computing. Doctoral thesis, Plymouth University, Communication & Electronics. Accessed on 27.5.2018. Retrieved from https://pearl.plymouth.ac.uk/bitstream/handle/10026.1/3005/2014Doelitzscher10322206PhD.pdf?sequence=1&isAllowed=y

European Commission 2012. Unleashing the Potential of Cloud Computing in Europe. Accessed on 15.5.2018. Retrieved from https://eur-lex.europa.eu

European Commission. 2018. 2018 reform of EU data protection rules. European Commission website. Accessed on 14.5.2018. Retrieved from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#abouttheregulationanddataprotection

Hirsjärvi, S. and Hurme, H. 2000. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino. 173.

Inspira. 2016. What is Cloud Computing? Blog post. Accessed on 21.5.2018. Retrieved from http://inspira.co.in/blog/benefits-iaas-vs-paas-vs-saas/

KPMG. 2017. Microsoft – O365 & Azure -KATAKRI STIV -arviointi. Confidential assessment report

Microsoft Azure websites. Website. Accessed on 23.5.2018. Retrieved from https://azure.microsoft.com/en-us/resources/infographics/azure/

Microsoft News Center 2018. Saxo Bank and Microsoft partner to shape the future of cloud services in the financial industry. Accessed on 10.5.2018. Retrieved from https://news.microsoft.com/2018/04/24/saxo-bank-and-microsoft-partner-to-shape-the-future-of-cloud-services-in-the-financial-industry/

Microsoft Trust Center. 2018. Data management at Microsoft. Security Center websites. Accessed on 29.5.2018. Retrieved from https://www.microsoft.com/en-us/trustcenter/privacy/you-own-your-data

Ministry of Defence. 2015. Information security audit tool for authorities – 2015, Finland. Accessed on 1.5.2018. Retrieved from https://www.defmin.fi/files/3417/Katakri_2015_Information_security_audit_tool_for_authorities_Finland.pdf

Ministry of Finance. 2016. Vahti instructions. Website. Accessed on 24.5.2018. Retrieved from https://www.vahtiohje.fi/web/guest/vm-vahti-ja-tietoturvallisuus

Moisio, Mika. 2017. Microsoft Azure: Virtuaalikoneet. Bachelor's Thesis, Tampere University of Applied Sciences, Network Services. Accessed on 26.5.2018. Retrieved from http://urn.fi/URN:NBN:fi:amk-201705127966

Pauly, M. 2011. T-Systems Cloud-Based Solutions for Business Applications. Cloud Computing: Principles and Paradigms. John Wiley & Sons, Inc., Hoboken. 461-503.

RightScale 2018. State of the Cloud Report. Research report. Accessed on 25.5.2018. Retrieved from https://www.rightscale.com/lp/state-of-the-cloud?campaign=7010g0000016JiA

Robert K, Yin 2003. Case Study Research. Design and Method. Sage Publications. 19-33.

Salo, I. 2012. Hyötyä pilvipalveluista. Jyväskylä: Docendo. 9-23.

Statistics Finland. 2017. Tietotekniikan käyttö yrityksissä. Statistics. Accessed on 28.5.2018. Retrieved from https://www.stat.fi/til/icte/2017/icte_2017_2017-11-30_kat_003_fi.html

U.S. Department of Commerce 2011. NIST Cloud Computing Reference Architecture. Accessed on 25.5.2018. Retrieved from https://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf

Viestintävirasto. 2016. Ohje tietoturvallisuuden arviointilaitoksille. Instruction. Accessed on 30.5.2018. Retrieved from https://www.viestintavirasto.fi/attachments/Ohje_tietoturvallisuuden_arviointilaitoksille.pdf

Viestintävirasto 2014. Pilvipalveluiden turvallisuus. Accessed on 18.5.2018. Retrieved from https://www.viestintavirasto.fi/

Weinhardt, C., Anandasivam, D. I. W. A., Blau, B., Borissov, D. I. N., Meinl, D. M. T., Michalk, D. I. W. W. 2009. Cloud computing – a classification, business models, ans research directions. Busniess & Information Systems Engineering.

Zander, J. 2018. Microsoft expands cloud services in Europe and into Middle East to meet growing customer demand. Blog announcement. Accessed on 30.3.2018. Retrieved from https://blogs.microsoft.com/blog/2018/03/14/microsoft-expands-cloud-services-in-europe-and-into-middle-east-to-meet-growing-customer-demand/

Appendices

Appendix 1: Key statutes relating to information security

- The Finnish Constitution (731/1999), Chapter 2 Section 10: Protection of privacy and secrecy of confidential correspondence
- The Finnish Constitution (731/1999), Chapter 2 Section 12: Public accessibility of documents and records in the possession of authorities
- The Act on the Openness of Government Activities (621/1999)
- The Decree on the Openness of Government Activities and on Good Practice in Information (1030/1999)
- The State Civil Servants Act (750/1994), Section 17: Statute on the state public service relationship
- The Act on Municipal Civil Servants (304/2003)
- The Employment Contracts Act (55/2001)
- The Government resolution on state administration information security (VM0024:00/02/99/1998)
- The Archives Act (831/1994): Drafting, storage and use of documents
- The Act on International Security Obligations (588/2004): Sensitive international documents
- The Personal Data Act (523/1999): General principles relating to the processing of personal data
- The Act on Background Checks (177/2002)
- The Act on the Protection of Privacy in Working Life (759/2004): Processing of personal data on employees
- The Act on Electronic Services and Communication in the Public Sector (13/2003) Information security in electronic services and transfer of information between authorities
- The Act on Electronic Signatures (14/2003)
- The Act on the Protection of Privacy in Electronic Communications (516/2004) Confidentiality of electronic communications and protection of privacy
- The Penal Code (39/1889) Chapter 34 Section 9a: Causing harm to data processing
- The Penal Code (39/1889) Chapter 38 Section 8: Data trespass, hacking
- The Penal Code (39/1889) Chapter 38 Section 9 Paragraph 1: Personal data offence
- The Personal Data Act (523/1999) Section 48: Personal data file violation

- The Tort Liability Act (41/1974)

Appendix 2: Valid VAHTI publications

- VAHTI 4/2009 Information Security Instructions for Personnel
- VAHTI 3/2009 Logging instructions *
- VAHTI 2/2009 General instructions on ICT contingency planning *
- VAHTI 1/2009 VAHTI annual report 2008 *
- VAHTI 9/2008 General instructions on information security in projects *
- VAHTI 8/2008 Information security terms *
- VAHTI 7/2008 Informationssäkerhetsanvisningar för personalen **
- VAHTI 6/2008 Report by IS training in the central government *
- VAHTI 5/2008 24/7 information security services in the central government *
- VAHTI 4/2008 General instructions on information security auditing in the central government *
- VAHTI 3/2008 Encryption technologies in the central government *
- VAHTI 2/2008 Personnel security as a part of information security *
- VAHTI 1/2008 VAHTI annual report 2007 *
- VAHTI 3/2007 Summary of general instructions on information security management *
- VAHTI 2/2007 Information security in modern mobile phones *
- VAHTI 1/2007 Challenges in international information security work *
- VAHTI 12/2006 Electronic identification in the central government services *
- VAHTI 11/2006 Instructions for information security trainers *VAHTI 10/2006 Security instructions for the personnel *
- VAHTI 9/2006 Best practises in access control and management *
- VAHTI 8/2006 Assessment of information security in the central government *
- VAHTI 7/2006 Change and information security, from regionalisation to outsourcing – a-controlled process *
- VAHTI 6/2006 Setting and measuring information security targets *
- VAHTI 5/2006 Records management information security instructions *
- VAHTI 4/2006 Review of the arrangement of round-the-clock information security in the central government *

- VAHTI 3/2006 Review of the distribution of central government informa- tion security resources *
- VAHTI 2/2006 Electronic-Mail Handling Instruction for State Government
- VAHTI 1/2006 VAHTI annual report 2005 *
- VAHTI 3/2005 Management of information security anomalies *
- VAHTI 2/2005 Electronic mail handling instructions for central government *
- VAHTI 1/2005 Information Security and Management by Results
- VAHTI 5/2004 Securing the state administration's key information systems *
- VAHTI 4/2004 Datasäkerhet och resultatstyrning **
- VAHTI 3/2004 General instructions on protection against malware *
- VAHTI 2/2004 Information Security and Management by Results
- VAHTI 1/2004 Government Information Security Development Program 2004-2006
- VAHTI 7/2003 Risk assessment instruction to promote government information security *
- VAHTI 3/2003 Assessment of information security management systems *
- VAHTI 2/2003 Secure remote access from insecure networks *
- VAHTI 1/2003 Secure use of the Internet *
- VAHTI 4/2002 Instructions for processing sensitive international data *
- VAHTI 3/2002 Information security instructions for telework *
- VAHTI 1/2002 Information security recommendation for ICT rooms *
- VAHTI 6/2001 Information security checklist for ICT procurement *
- VAHTI 4/2001 General instructions on the information security of elec- tronic services *
- VAHTI 2/2001 Information security recommendation on government local area networks *
- VAHTI 3/2000 General recommendation on information system development *
- VAHTI 2/2000 Information security instructions for processing government data material (revised) *

* (only available in Finnish)

** (Swedish publication)

Appendix 3: Interview answers – interview 1 (confidential)

Appendix 4: Interview answers – interview 2 (confidential)

Appendix 5: Interview answers – interview 3 (confidential)

Appendix 6: Interview answers – interview 4 (confidential)

Appendix 7: Interview answers – interview 5 (confidential)