Jan Lampikari

SECURE CLOUD IMPLEMENTATION IN GOVERNMENTAL ORGANISATIONS

Master's thesis

Master of Engineering

Cybersecurity

2020

South-Eastern Finland
University of Applied Sciences

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree title	Time
Jan Lampikari	Cybersecurity: Master of Engineering	October 2020
Thesis title		
Secure Cloud Implementation in Governmental Organisations		87 pages 0 pages of appendices
Commissioned by		
Intelligent Traffic Management Finland Oy		
Supervisor		
Martti Kettunen, Degree Programme Coordinator, Principal Lecturer		

Abstract

This research studied the basic security-related principles in generalised manner that need evaluating when governmental organisations plan to implement cloud computing as a part of their operations. The main objectives were to find out what are the key elements to focus on in the cloud service provider selection process, and which are the critical areas, and need evaluating and controls from the customer's perspective during and after the cloud implementation.

Information was gathered using qualitative research methods, and the sources used included books, online resources and various standards. The idea was to use as recent sources as possible, but also some earlier materials were used if they were still relevant and provided useful information for the research.

The research indicated that implementing cloud computing in general requires a deep understanding of the concepts behind it and realising how it affects the whole IT ecosystem of an organisation. Due to the extremely broad nature of the subject, this research was not able to discuss all areas related to the topic, nor could it examine any significant technical details behind the presented solutions. However, it was able to identify the key areas the organisations should focus on during the cloud implementation, and it can serve as an introduction to cloud computing for the governmental organisations from a security perspective.

Keywords

cloud computing, cloud security, information technology

CONTENTS

1 INTRODUCTION

The introduction section describes in five chapters how and why the research was done. The background and the motivation for the research are introduced first. They are followed by the research problem and the research questions. The third chapter discusses the chosen research method, and the last two chapters continue to explain how the research was done. The fourth chapter explains the literature review process, and finally the fifth chapter introduces the research structure and process.

1.1 Background and motivation

Cloud computing is a model where machines in large data centres can be dynamically provisioned and configured to deliver services in a scalable manner for various applications. It provides a variety of services to individuals, companies and government organisations. (Ali & Osmanaj 2020, 1-2.) Nearly everyone using the Internet is using the cloud – even if they do not realise it. According to a recent survey, there is a lot of confusion around cloud computing – only 16 % know the purpose of the cloud. 54 % of the respondents claimed they never used the cloud, but in reality, 95 % of them were in fact cloud computing users. (Samani et al. 2015, xvii-1.)

In the current IT industry, cloud computing is growing rapidly, and it is the latest technology in the current era. It works by providing customers on-demand-services, and customers only pay for what they get. Users can store data on the remote servers and can access it anytime and anywhere they prefer. The Cloud Service Providers (CSP) provide users access to this data. (Fatima & Ahmad 2019, 1-2.) The technology of cloud computing virtualisation provides the end users with efficient resources. Cloud computing connects various computing resources, storage resources, and software resources, forming a vast shared virtual resource pool. (Sun 2020, 1.) According to Mthunzi et al. (2019, 1), cloud computing, due to augmented virtualisation, has become the new standard when choosing a computing platform, allowing dynamic, scalable and elastic

reconfiguration of computing resources. The pay-per-use model has made computing a similar utility to electricity, gas, water, etc., giving cloud computing one of its very attractive features. (Mthunzi et al. 2019, 1.) Due to the rapid popularisation of cloud computing, it has made its way into various fields, such as scientific research, production, consumption, entertainment, etc. (Sun 2020, 1).

Organisations have adopted cloud computing because of its scalable and dynamic availability of resources that users can use virtually (Astri 2015, 1). Cloud computing has also the potential to improve the reliability and scalability of organisational systems (Ali & Osmanaj 2020, 1). The ongoing change where applications and infrastructure are moved to the cloud, the massive growth in internet traffic and the shift to mobile-first computing have increased agility in business, and it has also become a major objective for CIOs (Chief Information Officer). This means that organisations have to go through a massive shift in their IT strategies. Following these trends is important for the organisations to empower business users, increase the speed of deployment, create new customer experiences, re-engineer business processes, and discover new growth opportunities. Everything has to be always on, connected and working in today's business. Every user is a power user, and corporate data and applications should be always available regardless of the user's location. (Stiennon 2019, 11-12.)

According to IDC, 87 % of respondents cite security as the greatest worry with regards to cloud computing. (Samani et al. 2015, 19). The problem is that the organisations trying to follow these trends with the traditional security architectures now face several IT challenges. For instance, the growing use of cloud services and the internet create gaps in security coverage, because the traditional corporate network security policies cannot be enforced in a cloud environment. Microsoft Office 365 has moved many of the organisation's most used applications to the cloud, and this strains the existing network capacity. The increasing amount of mobile workforce makes every cloud user a potential source of security vulnerability. (Stiennon 2019, 12-13.) The need to develop

better, faster and more efficient security controls is crucial as we become ever more reliant on cloud computing (Samani et al. 2015, xviii).

Hackers today are sophisticated, and the threats are constantly evolving (Stiennon 2019, 13). A malware that spreads by offering a picture of a female tennis player raised concerns in the past. Nine years later a malware was able to compromise a nuclear plant. (Samani et al. 2015, xviii.) Motivated by financial, criminal and terrorist objectives, the hackers are exploiting the gaps left by existing network approaches. All the organisations now need to adjust their strategies on how to protect and secure their most valuable assets – the employees, customers and partners. (Stiennon 2019, 13-14.)

What was originally designed as an email hosting service has now evolved into a system that hosts applications that are keeping the water clean. Something that was previously built as a movie collection store is now storing sensitive data about each of us. Cloud computing is truly ubiquitous, and the need to secure the cloud has never been more important. (Samani et al. 2015, xvii-xviii.)

1.2 Research problem and questions

The case organisation is at a point where decisions should be made regarding the use of cloud computing. Many service providers that are working with the case organisation are beginning to offer their services from the cloud, and the traditional on-site-solutions are falling behind in terms of service capabilities. The trend is clear; everything is being shifted to the cloud.

The case organisation – Intelligent Traffic Management Finland Oy (further also referred to as ITMF) – is a subsidiary of Traffic Management Finland. Traffic Management Finland Oy operates under the ownership steering of the Ministry of Transport and Communications. The organisation is a special assignment group, and it safeguards the traffic control services that are required by society and the authorities. Ensuring reliability of operations in case of disturbances under both normal and exceptional circumstances on the land, in the air and at sea are the

key roles of the organisation. Intelligent Traffic Management Finland Oy, respectively, is responsible for road traffic control and management. (Traffic Management Finland no date.)

As the case organisation operates in a sector that is vital for a functioning society, security and reliability are the key elements in all of its operations. All the solutions have to be robust and fool-proof. When considering the cloud as the new platform for mission-critical services and systems, cloud security becomes a shared concern for both the cloud service provider (CSP) and the cloud service customer (CSC) – ITMF in this case. The cloud service provider has to provide a secure and safe way for the customer to host its services, and the customer needs to know what to require from the cloud service provider. This was the main reason to begin the research in the first place – to be able to demand the cloud service provider a certain level of service, security and reliability.

With all this in mind, the need for best practices of how to implement and manage cloud services securely is urgent. The cloud is seen as a very important possibility for the whole organisation; it is an environment where to develop and offer entirely new services. Cloud computing is still quite a modern technology, and the case organisation is yet to develop the basic principles of how to deal with security in the cloud. And, as cloud computing is not yet widely adopted in the case organisation, this gave a good opportunity to widen and generalise the research to cover all governmental organisations in general – also giving the possibility to discuss the topic in public, without having to limit the potential audience of this research, as none of the confidential information concerning the case organisation would have to be presented (In the context of this research, a governmental organisation refers to a Finnish governmental organisation explicitly, unless stated otherwise).

The situation described above can be formed into a research question:

How to securely implement cloud computing in governmental organisations?

Then, the question can be further divided into multiple research questions (RQ) to better understand and analyse the problem:

RQ1: *What should governmental organisations take into account when planning to implement cloud computing?*

The first goal is to discover what governmental organisations should take into account as they are planning to implement cloud computing for the first time. How to choose the right cloud service provider, service model and deployment model? What are the most important factors in the planning phase and what to especially focus on before making the decisions?

RQ2: *What are the key elements to focus on in cloud security management and cloud security controls from the customer's perspective?*

The second goal is to find out the key elements regarding cloud security from the cloud service customer's perspective. Do any architectural high-level designs or security controls exist that could be used as a general guideline in the implementation phase? How identity and access management should be addressed? How to deal with the infrastructure?

RQ3: *Is there a way to select and list the best security practices to help securely implement cloud computing in this type of situation?*

The final goal is to find out whether it is possible to list the best security practices for governmental organisations – and also for the case organisation – that could be used to form base-level security requirements for all the new cloud services that are going to be implemented. The target is a compact and informal list of things that are required from the cloud environment to ensure secure implementation of cloud computing.

1.3 Research method

Research methods can be broadly classified into two categories; quantitative and qualitative (Peng et al. 2011, 3). In this research, a mixed research approach was adopted. Combining elements of two research approaches is referred to as a mixed methods research (Johnson et al. 2007, 123). In a mixed-method research, different methods to gather information are intentionally combined (Greene & Caracelli 1997, 7). Compared to a single-method research, mixed-method research is likely to be more useful and generative (Greene & Caracelli 1997, 13). Mixed-method research is also especially useful in research projects where no single approach can fully provide answers to the study (Peng et al. 2011, 6). As the problem is rather complex, a mixed-method research emphasising the methods of qualitative research has the best chances in providing good results.

Various combinations have been derived from qualitative and quantitative research methods, as can be seen below in Figure 1. Many instances have debated over how good or scientific the different methods are – qualitative research has been seen as the only way to conduct proper scientific research, and quantitative research has been thought more as applied research. (Kananen 2015, 54.)

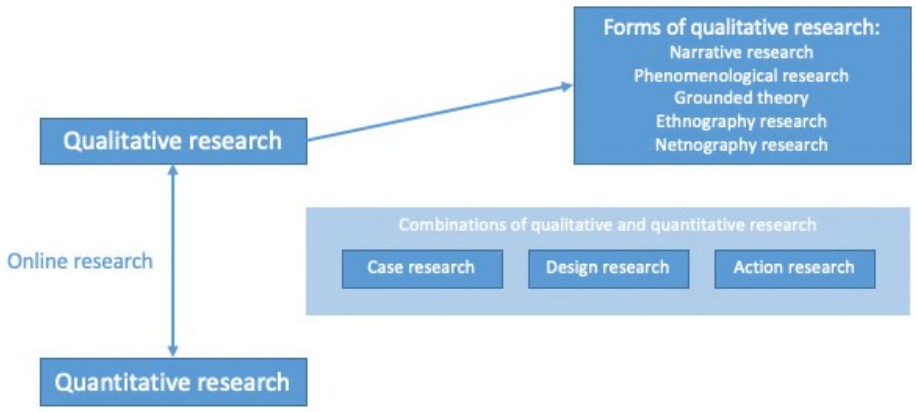


Figure 1. How different research approaches relate to each other. (Kananen 2015, 53.)

The purpose of the research was to gain more understanding, and the research questions were mostly open, a more specific combination – case research -

provided the best approach to the study. The role of the researcher in this study was to act as an external participant, and this matched the case research approach method too. Case research is very close to traditional qualitative research, but does not limit the information gathering methods, and as such should give the researcher certain freedom, and more ways to find solutions to the research problem, and thus justifying the selection of a mixed-method research approach. Figure 2 below explains the various combinations of quantitative and qualitative research approaches in more detail from Kananen's point of view.

	Methods	Relationship of theory and practice	Purpose of research	Role of researcher	Methods of gathering data	Research questions
Methods	Qualitative research	From practice to theory (induction)	Understanding	External participant	Observation, theme interview, interview, documents	Themes, interviews, open questions
	Quantitative research	From theory to practice (deduction)	Generalisation, forecasting	External observer	Surveys	Structured questions
Blended research	Ethnographic research	From practice to theory (induction)	Understanding	External participant	As for qualitative research	Themes, interviews, open questions
Multi strategy approach	Case research	Abduction (also interaction between theory and practice)	Understanding	External participant	Mixture of different research	Mostly open questions
	Design research	Abduction	Change	External participant	Mixture of different research	Mostly open questions
	Action research	Abduction	Change, influence	Active operator	Mostly qualitative research	Mostly open questions

Figure 2. Research approaches and methods classified. (Kananen 2015, 55.)

1.4 Literature review process

The point of the literature review is to provide a high-level overview of the studied subject, and also seek solutions to the presented research problems.

The material for the literature review has been gathered from various sources; Standards and publications written by various authorities and government officials, the XAMK Kaakkuri service, Google Scholar, books acquired from online stores, and also through many online sources. The idea was to use as up-to-date material as possible. The older material was only used as a reference if the information was still relevant and gave value to the research.

The search string "cloud security" did yield a massive amount of case studies and small research articles, but many of the texts revealed to have only a little or no value at all for this research. A fair amount of the previous research on this topic focused more on cloud service providers and the technology behind their

services and did not evaluate the problem from the cloud service customer's point of view, and even less from the governmental perspective. Plenty of actual solutions and best practices could be found through standards and documents written by various authorities and government officials. To help understand the reasons why these specific authors were selected, the most relevant authors must be briefly introduced.

The Cloud Security Alliance (CSA) is dedicated to defining the best practices and helping to secure cloud environments. It is also the world's leading organisation in this sector. The CSA is also responsible for operating the most popular cloud security provider certification program. The program is called the CSA Security, Trust & Assurance Registry (STAR). (Cloud Security Alliance Overview no date.)

ISO and IEC Joint Technical Committee (ISO/IEC JTC1) for information technology is a voluntary international standards group working for the common good. This group has many roles. Some of these include giving recommendations of different baselines and standards that concern safety features, but also adequate quality standards and testing procedures. (ISO/IEC no date.) It is also involved in providing the standards approval environment that can be used when integrating distinct and complicated ICT technologies. (ISO no date).

The national security auditing criteria, Katakri, is an audit tool for government officials to evaluate the ability to protect classified information in an organisation. The Ministry for Foreign Affairs of Finland and the National Security Authority are responsible for the development and administration of Katakri. (Katakri 2015, 2.)

The National Institute of Standards and Technology (NIST) belongs to the U.S. Department of Commerce. As a physical science laboratory, it belongs to the country's oldest lot. A plenty of products and services are dependent – in one way or another – of the technology, standards, and measurements NIST provides. (NIST About NIST 2017.)

The security assessment criteria for cloud services, PiTuKri, is a tool developed by Traficom that can be used to evaluate the security of cloud services. PiTuKri is based on the material provided by various authors, such as BSI (Bundesamt für Sicherheit in der informationstechnik), CSA (Cloud Security Alliance), ISO27001 and ISO27017 standards and Katakri (Traficom 2020, 3.)

The governmental steering committee of digital security, VAHTI, is a group formed by the Ministry of Finance in Finland. VAHTI coordinates and develops the information security standards and best practices for the Finnish governmental organizations. (VAHTI 2012, 7.)

1.5 Research process and structure

A thorough literature review was done to seek for solutions and answers for the presented problems. This research is based almost entirely on the currently available literature as the case organisation is still yet to discover the ways to better start utilising cloud computing in its services, and anything related to the research was not widely in use in the organisation when this research was done. This also gave the opportunity to generalise the research to cover governmental organisations in general, as the research did not yet have to examine any organisation-specific problems.

The first two questions are answered directly through the literature review, and they form the basis of the whole research. The answer to the third and final question is derived from the first two questions, and it gathers together all the information from the research and presents solutions to the existing problem. The structure of the research is presented in figure 3.

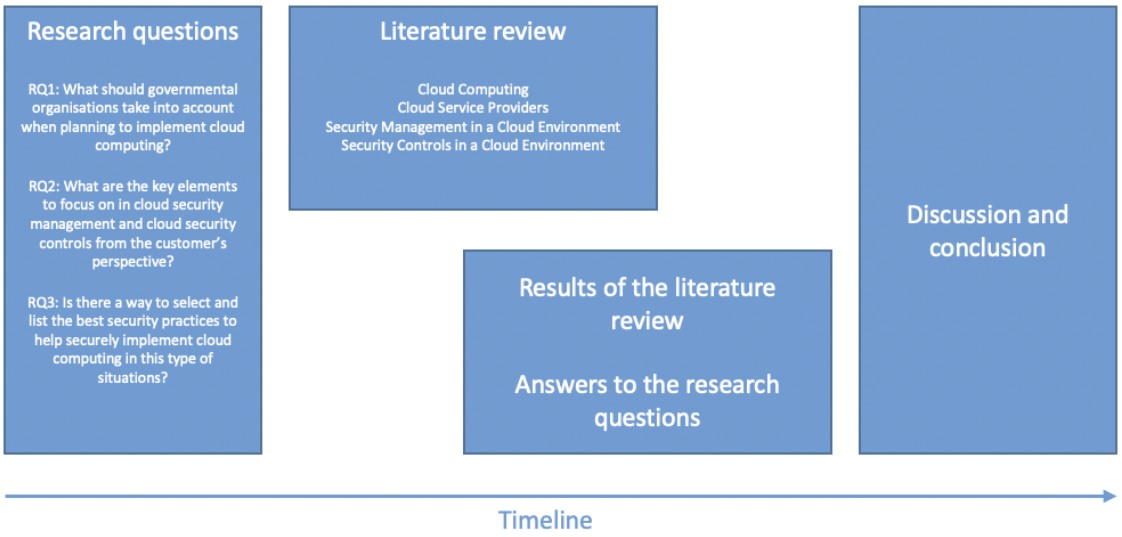


Figure 3. Structure and timeline of the research.

The research consists of seven chapters. In the first chapter the background and the motivation for the research is introduced, together with the research problem and the research questions. The first chapter also explains the used research method and the timeline for the research and gives an overview of the literature review process. The literature review provides information on the studied subject, acting as the base of the whole research, and it explains the basics of cloud computing and discusses the security in it from various perspectives. The literature review covers chapters from two to five. Chapter two explains the basics of cloud computing, and chapters three through five focus on security in the cloud in the context of this research. In chapter six the results of the literature review are analysed, and the research questions are answered. Chapter six is also reserved for discussion, and it presents ways to transform the research results into practice, and also provides some future research ideas. The final chapter is reserved for the conclusion, concluding the whole research.

2 CLOUD COMPUTING

2.1 Definition of cloud computing

A direct quote of the definition The National Institute of Standards and Technology (NIST) has determined cloud computing as follows: *"Cloud*

computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (NIST 800-145 2011, 2.) Amazon defines cloud computing briefly as *on-demand delivery of IT resources over the Internet with pay-as-you-go pricing* (Amazon What is cloud computing? no date). Microsoft's definition is similar to the one Amazon uses, and they present cloud computing – directly quoted – as *"the delivery of computing services – including servers, storage, databases, networking, software, analytics, and intelligence – over the Internet to offer faster innovation, flexible resources, and economies of scale"* (Microsoft What is cloud computing? no date). Google, on the other hand, has yet another definition for cloud computing. To better compare it with the others, a direct quote of it is as follows: "*in cloud computing, the capital investment in building and maintaining data centers is replaced by consuming IT resources as an elastic, utility-like service from a cloud "provider" (including storage, computing, networking, data process and analytics, application development, machine learning, and even fully managed services)"* (Google What is cloud computing? no date).

2.2 Cloud computing reference architecture

To better understand the terminology used in this research and to give a perspective where the cloud service customer – i.e. the case organisation – is located in the bigger picture, the concept of cloud computing reference architecture must be also introduced.

A typical reference framework for cloud computing aims to offer the baseline for designing some interoperable cloud services, and also their integration to the existing infrastructure of the Internet and private corporations. These reference cloud architecture models represent abstractions of cloud computing concepts and relationships, which can be used to create standards and guidelines, and also to train organisations. Many vendors like Oracle, Microsoft, Amazon and Google have their own reference models with specific characteristics, but some

of the most important reference architectures in the field are maintained by Cisco, IBM, NIST and VMware. These models are named as follows:

- Reference architecture CISCO – Cisco Cloud Reference Architecture Framework
- Reference architecture IBM – IBM CCRA (Cloud Computing Reference Architecture)
- Reference architecture National Institute of Standards and Technology (NIST)
- Reference architecture VMware – Architecting vCloud

(Petre & Zota 2014, 2-12.)

Between these four architectural models, NIST's reference architecture is the only provider independent model. The NIST reference architecture is also the most comprehensive and has architectural details and concrete case studies of usage. The three other vendor-dependent models follow NIST's reference architecture using their technologies and solutions based on their services and infrastructure. (Petre & Zota 2014, 12.) This is the reason NIST's reference architecture was preferred in this chapter either directly or non-directly through other authors to define and introduce cloud computing.

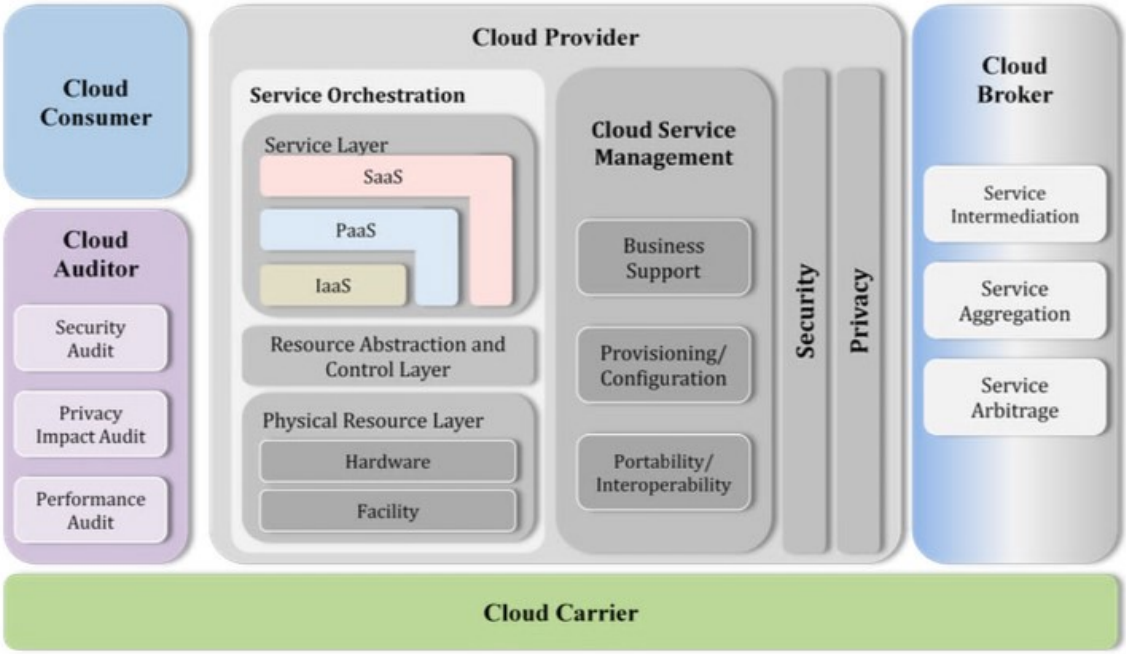


Figure 4. The NIST CCRA. (NIST 500-292 2011, 3.)

Figure 4 represents the NIST CCRA, and it has five main actors; Cloud Consumer, Cloud Auditor, Cloud Provider, Cloud Broker and Cloud Carrier. The actors play important role in the cloud computing process. An actor can be thought of as an entity, and the entity can be either a person or an enterprise. The actor has a role in assisting in the transaction process and has a pre-defined task. (Petre & Zota 2014, 5.)

Figure 5 has the NIST definitions for each of the actors:

Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

Figure 5. NIST's definitions for the five main actors in the NIST CCRA. (NIST 500-292, 4.)

2.3 The essential characteristics of cloud computing

According to NIST, the five essential characteristics, three service models, and four deployment models form a cloud. The purpose of NIST's classification is to characterise important aspects of cloud computing and provide ways to discuss and compare cloud computing, and how to best utilise cloud computing. These service and deployment models are not intended to be used as direct rules in any sort of a deployment or business operation, or when delivering a service. (NIST 800-145 2011, 2-5.) The essential characteristics define cloud computing in general, and the cloud models – service models and deployment models, respectively – classify the cloud service based on the ownership and architecture of the cloud (Samani et al. 2015, 4-5).

The five essential characteristics comprise of the following:

- *On-demand self-service*
- *Broad network access*

- *Resource pooling*
- *Rapid elasticity*
- *Measured service*

(NIST 800-145 2011, 2.)

In addition to these, The Cloud Security Alliance (CSA) has also included multitenancy as one of the essential characteristics of cloud computing (Samani et al. 2015, 4).

The three service models are defined by NIST as the following:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

The deployment models – on the other hand – include these four:

- Public cloud
- Private cloud
- Hybrid cloud
- Community cloud

(NIST 800-145 2011, 2.)

Figure 6 provides a visual representation of these characteristics, service models and deployment models.

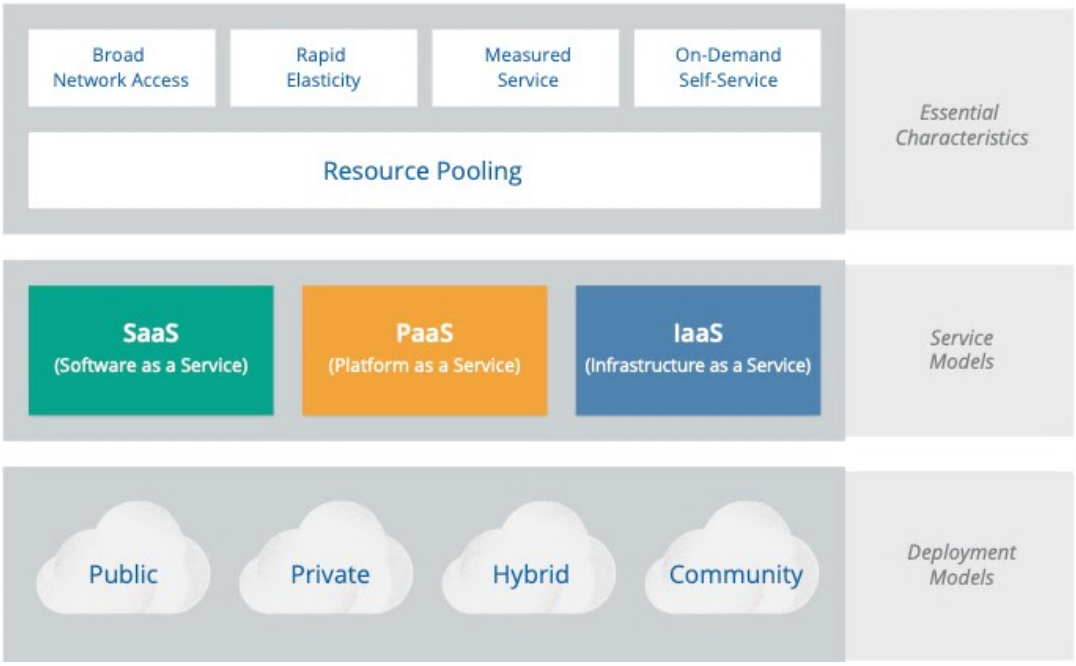


Figure 6. Visual representation of the defining elements of cloud computing. (Cloud Security Alliance 2017, 10.)

On-demand self-service means that it gives the customer the possibility to independently provision computing capacity, such as network-based storage and server time. The provisioning can be done automatically without the need for human interaction with each service provider. (NIST 800-145 2011, 2; Samani et al. 2015, 2.) *Broad network access* represents the availability of capabilities of the network, and the possibility to access them through standard mechanisms – that is – there should be no need for any specific device or software to access the cloud resources. (NIST 800-145 2011, 2; Samani et al. 2015, 3.) In *Resource pooling,* the cloud service provider's computing resources are merged together. This is done in order to serve multiple customers using a multitenancy model, in which an instance of computing resources, such as hardware, operating system, and database are able to serve different customers (tenants), but yet remain isolated from each other (NIST 800-145 2011, 2; Samani et al. 2015, 3-4). *Rapid elasticity* gives the opportunity for the customer to either automatically or manually provision or release computing resources during times of peak demand (NIST 800-145 2011, 2; Samani et al. 2015, 4). *Measured service* guarantees that the resource use is controlled and optimised by cloud systems. It is done by advantaging a metering capability at some level of abstraction, applicable to the type of service. The service can be – for instance – storage, bandwidth, active user accounts, or processing. In other words, the cloud service provider will monitor utilisation to ensure resources are optimally used. (NIST 800-145 2011, 2; Samani et al. 2015, 4).

Within *multitenancy,* an application or resource can be used by other customers of the cloud service provider. It maximises the resources by allowing shared access to resources. The customers can be completely unrelated to each other. (Samani et al. 2015, 4.) Figure 7 below illustrates multitenancy in a simplified manner.

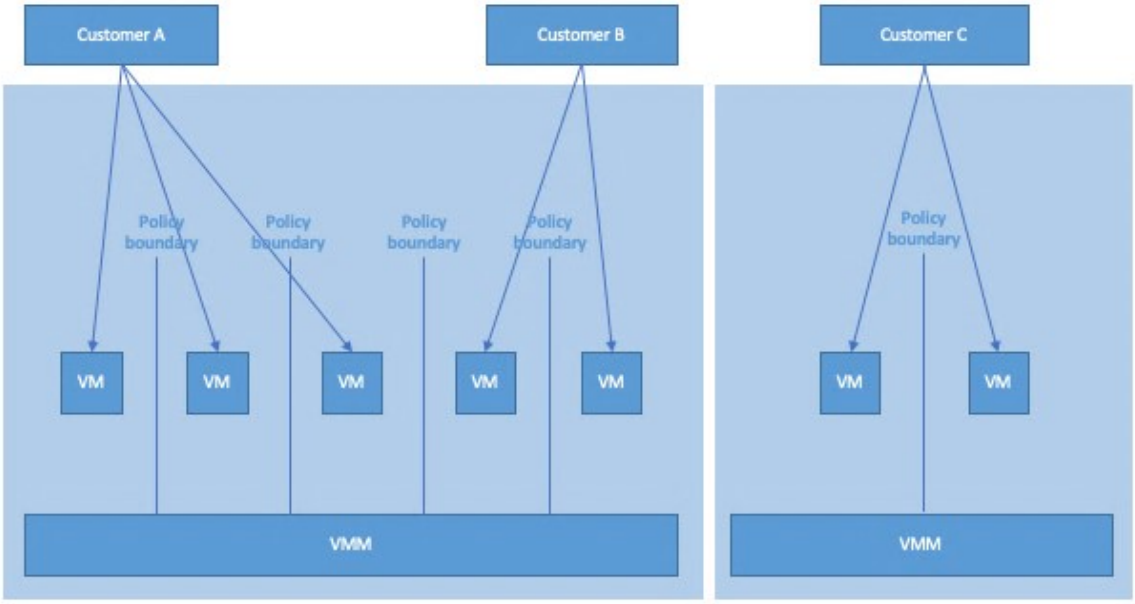


Figure 7. A simplified example of multitenancy. (IBM 2011.)

As can be seen in Figure 5, the different customers are able to access their resources separated by policy boundaries, but the service provider shares the resource base with all the customers.

2.4 Service models in cloud computing

There are many aaS-type services associated with the cloud, and the aaS stands for “as a Service”. These acronyms identify the various cloud-based services, and the architectural design is one of the key points in differentiating the cloud models. (Hastings 2014, 3; Samani et al. 2015, 7). The NIST Cloud Computing Definition has three cloud service categories – or in other words – service models:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

(NIST 500-322 2018). Figure 8 presents these cloud services from the perspective of the NIST Cloud Computing Reference Architecture (CCRA). The reference architecture is discussed later in chapter 2.5.

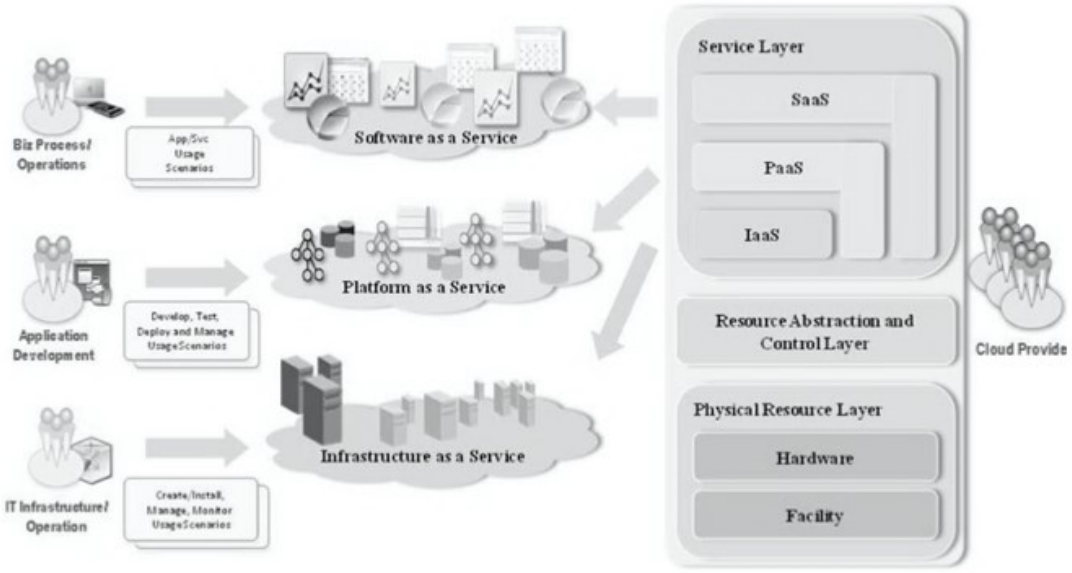


Figure 8. The Service Layer in the NIST CCRA. (Petre & Zota 2014, 8.)

2.4.1 Infrastructure as a Service (IaaS)

All the other service models are built on top of IaaS, and Infrastructure as a Service is the foundation of cloud services (Samani et al. 2015, 7). IaaS is the most basic category of cloud computing types and contains the building blocks for cloud IT (Amazon Types of cloud computing no date; Microsoft Types of Cloud Computing no date). This service model provides the customer the capability to provision networks, storage, processing power, storage, and other traditional resources used in computing. With the help of these resources, the customer is able to deploy and run arbitrary software. This software can include, for instance, operating systems and applications. The customer has the possibility to control storage, operating systems, and also deployed applications. It might also have limited control of select networking components, but it does not manage or control the infrastructure lying underneath in any way. (NIST 800-145 2011, 3.)

2.4.2 Platform as a Service (PaaS)

PaaS is built upon IaaS, and the considerable flexibility present in IaaS is not available in PaaS (Samani et al. 2015, 8). PaaS allows the customer to deploy consumer-created or acquired applications onto the cloud, but the provider must

support the programming languages, libraries, tools and services that are going to be used (NIST 800-145 2011, 2). On the contrary, Platform as a Service makes the organisations free of managing the underlying infrastructure, also making it easier to concentrate on the application deployment and management (Amazon Types of cloud computing no date). According to NIST, in this model, the customer cannot control or manage the infrastructure that is related to storage, servers, network, or operating systems. However, it has control over the deployed applications and also configuration settings for the environment where the applications are hosted (NIST 800-145 2011, 2-3).

2.4.3 Software as a Service (SaaS)

When comparing Software as a Service with IaaS and PaaS, SaaS has very limited flexibility, but provides the customer a finalised product that is entirely under the responsibility of the service provider (Amazon Types of cloud computing no date; Samani et al 2015, 8). Software as a Service makes it possible for the customer to use the applications provided by the cloud service provider. These applications are running in the cloud, and the applications are accessible from various client devices having a web browser or a program interface. The customer has no control over the underlying infrastructure, with the only possible exception of limited user-specific application configuration settings. (NIST 800-145 2011, 2.) A typical example of SaaS application is a web-based email, in which the user can operate the email service, but leaves it free of having to manage the email product itself, or the infrastructure the service is running on. (Amazon Types of cloud computing no date).

2.5 Deployment models in cloud computing

The deployment models in cloud computing consist of Private cloud, Community cloud, Public cloud and Hybrid cloud. These models classify cloud computing based on the ownership and sharing models of the cloud. (Samani et al. 2015, 5.) Figure 9 below reviews the characteristics of the deployment models and how

they compare with each other, and the next four chapters explain each of the models in details.

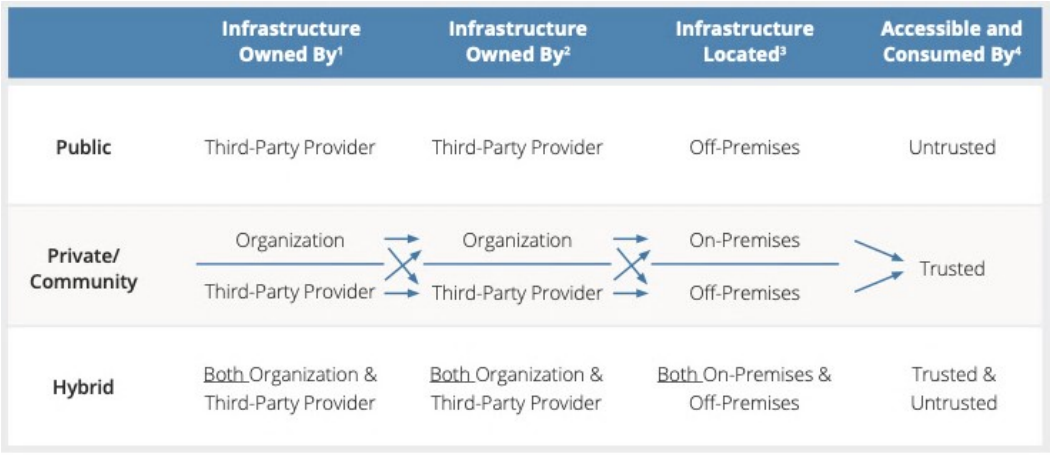


Figure 9. Deployment models in cloud computing. (Cloud Security Alliance 2017, 12.)

2.5.1 Public cloud

The most well-known and popular cloud services used are deployed using the public cloud model (Samani et al. 2015, 5). The cloud infrastructure exists on the premises of the cloud service provider, and it is provisioned for open use by the general public. This infrastructure may have various owners and managers. These can be, for instance, businesses, government organisations, academic organisations, or combinations of these. (NIST 800-145 2011, 3.) Typical examples of public cloud would be e-mail services, such as Hotmail, or storage services, such as Dropbox. In this model, all the customers are untrusted, and they are not necessarily even a part of an organisation – and furthermore – usually completely unaware of other cloud customers. A public cloud is available to use for any customer. (Samani et al. 2015, 6.)

2.5.2 Private cloud

A private cloud is the opposite of a public cloud, and the cloud infrastructure is reserved for a single customer, instead of multiple customers, and the customer is a single organisation comprising of multiple consumers. Private cloud may exist either on or off premises, and the infrastructure, platform, software, etc. may be owned, managed, and operated by the end customer, the cloud service provider, or some combination of them. (NIST 800-145 2011, 3; Samani et al. 2015, 6.) Customers using the private cloud are trusted, or at least known, and the organisation using the cloud can define the access levels for the users. The customer also has control over the geographic location of the infrastructure, making it a preferred model for hosting data that is regulated, and has regulations on where the data can be hosted. (Samani et al. 2015, 6.)

2.5.3 Community cloud

A community cloud is an extension of the private cloud. The cloud infrastructure is provisioned for the use of multiple customers that have something in common. The are many possibilities for connecting factors; security requirements, a similar mission, policies, or compliance considerations. It may exist on or off premises, and the ownership, management and operation of the cloud infrastructure may belong to practically anyone in the community, but also to a third party, or possibly some combination of these. (NIST 800-145 2011, 3; Samani et al. 2015, 6.) A typical example of a community cloud would be a situation in which there is a collaboration between the organisations with a common interest. To maintain the security, only trusted parties are provided access to the data after an authorisation process has been initiated. Samani et al. 2015, 6).

2.5.4 Hybrid cloud

A hybrid cloud is located between the private cloud and the public cloud (Samani et al. 2015, 6). The cloud infrastructure combines the characteristics of private, community and public cloud infrastructures. These infrastructures remain as entities of their own, but standardised technology ties the infrastructure together.

This can enable data and application portability, and load balancing between clouds can occur. This is also referred to as cloud bursting. (NIST 800-145 2011, 3.) An example of a hybrid cloud implementation would be an intention to utilise a single cloud platform – creating a central platform – from which to deliver public services for both citizens and public departments. The resources for the citizens would be available through the internet, while the resources for the public departments would be not. (Samani et al. 2015, 6-7.)

3 CLOUD SERVICE PROVIDERS

This third chapter aims to introduce and discuss the challenges organisations may face when choosing between the cloud service providers. The selection process is difficult, and simple solutions or answers to the problem do not exist. According to ZDNet, the current market leaders are Amazon, Microsoft, and Google, but also companies like IBM, Dell Technologies, and Hewlett-Packard Enterprise are willing to get their share of the market among many other companies. (ZDNet 2020.)

3.1 Selecting a cloud service provider – a security perspective

The requirements and evaluation criteria for selecting the cloud service provider are unique in every organisation (Cloud Industry Forum no date). There is no specific formula regarding the level of due diligence that should be followed either. Only certain frameworks for regulated data may either be advisable or required. The selection process and the factors guiding it are completely subjective, and these factors should be tailored according to the corresponding business. (Samani et al. 2015, 25.) There are – however – still some common areas that can be focused on when assessing the service providers and these factors can provide guidance in the selection process (Cloud Industry Forum no date; Samani et al. 2015, 25).

When evaluating the possibility to engage with a cloud service provider, it is important to look beyond the benefits; a thorough due diligence and risk assessments of the related elements should be performed beforehand. Three

different lists are presented to compare the key points the different authors make about the selection. Samani et al. recommend to at least look into these elements when choosing between the service providers:

- Solid reputation
- Best of breed technology partnerships
- Financial stability and growth
- Enterprise-grade data centres and state-of-the-art equipment
- Compliance, availability, and performance

(Samani et al. 2015, 24.)

Microsoft – on the other hand – has listed these as the most important factors when choosing the cloud service provider:

- Business health and processes
- Administration support
- Technical capabilities and processes
- Security practices

(Microsoft How to choose a cloud service provider no date.)

For comparison, the Cloud Industry Forum (CIF) has eight criteria to ensure the success of a cloud service provider selection process:

- Certifications and standards
- Technologies and Service Roadmap
- Data Security, Data Governance and Business policies
- Service Dependencies and Partnerships
- Contracts, Commercials and SLAs
- Reliability and Performance
- Migration Support, Vendor Lock in and Exit Planning
- Business health and Company profile

(Cloud Industry Forum no date.)

As can be seen, all the presented lists have similar elements. All of these are definitely important in the selection process, however, as this research focuses on the security of the cloud, it is not relevant to go through all of the criteria in more detail – instead, the focus is on the security-related elements. These three lists were collected in order to highlight the quite vast amount of details that should be considered in addition to the security aspects when planning the move to the cloud.

3.1.1 Certifications and standards

Certification is a process in which an organisation's processes and services are evaluated against a predefined set of criteria. This evaluation – or an audit – is conducted by a third party, which formally acknowledges that the criteria set by the standard are met. Certifications – and in this case cloud service certifications – signal the service quality and allow the decision makers to assess the service beforehand. They also increase market transparency and ultimately support in making better decisions in adopting the services. (Lansing et al. 2019, 2-5.) Cloud service providers complying with the recongnised standards and different quality frameworks mean they are also committed to following the best practices and standards present in the industry. These standards may not necessarily automatically determine the best choice, but they can provide help in shortlisting the potential candidates. (Cloud Industry Forum no date.)

From the security perspective, suppliers with accredited certifications like CSA STAR, General Services Administration FedRAMP, ISO 27001 and ISO 27017 should be considered. When looking at the privacy aspect, TRUSTed Cloud Data Privacy Certification and the European Privacy Seal are the certifications to look for. (Cloud Industry Forum no date; Lansing et al. 2019, 5.)

As an example, Dropbox – a cloud service for storing and exchanging documents – had to convince the users that the service is secure, it has ~~a~~ good privacy, and the availability to the data is continuous. To mitigate this uncertainty among the users, Dropbox obtained ISO 27017 and CSA STAR certifications as an assurance of the security of the service. It also obtained ISO 27018 to cover the privacy aspect, and ISO 22301 to address business continuity and availability. EuroCloud, for a comparison, chose to combine security, privacy and availability assurances in one certification. (Lansing et al. 2019, 2.)

3.1.2 Data governance and security

The organisation should be at least aware of the cloud service provider's regulatory or data privacy rules concerning personal data. Things such as the location of the stored data and the laws the organisation needs to follow might be important in the selection process. Cloud service providers should be transparent of where their data centres are located, and providers that give the possibility to control where and how the data is stored, processed, and managed should be considered in case the customer's environment sets any specific requirements for the service. Also, the provider's data loss and breach notification processes are important to understand, and they should support the risk strategy and legal or regulatory obligations of the customer organisation. (Cloud Industry Forum no date.)

The cloud service provider's maturity in security operations and security governance processes should also be assessed. All the information security controls the provider has should clearly support the policies the customer has in place. User access and user activity should always be auditable, and security roles and responsibilities should be carried out as demonstrated in the documentation containing the policies. Also, the validity of the certifications and standards should be checked. Incident reports, internal security audit reports, and the correcting actions taken to react to the problems can also provide useful information. (Cloud Industry Forum no date.)

3.1.3 CSA STAR Registry

In 2011, the Cloud Security Alliance launched the Security, Trust and Assurance Repository (STAR) to help the customers determine the security controls the cloud service providers have implemented. One of the greatest challenges regarding cloud computing is the lack of transparency in the level of these controls. STAR provides a central repository for the potential customers, and the customers have the possibility to browse this registry and compare the cloud service providers. (Samani et al. 2015, 25.)

The CSA STAR Registry is based on three layers:

1. Self-assessment
2. Third-party assessment-based certification
3. Continuous monitoring-based certification

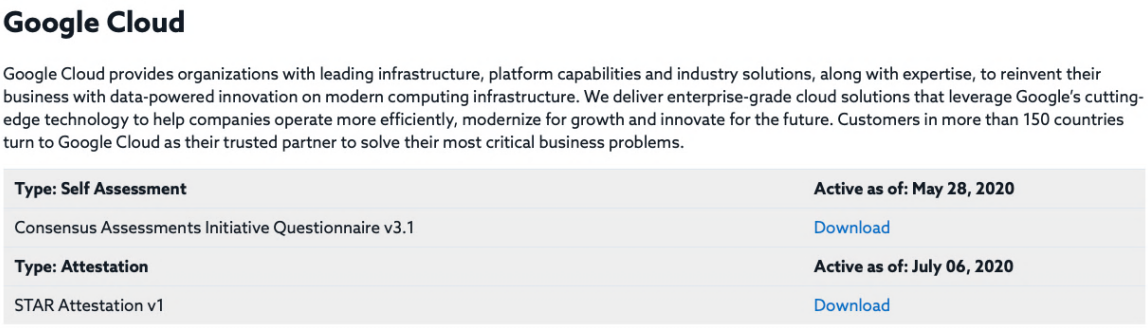
(Samani et al. 2015, 25-26.)

The first layer – self-assessment – provides information given by the service provider itself, as the name suggests. It publishes results of the Consensus Assessment Initiative Questionnaire (CAIQ) and / or the Cloud Controls Matrix (CCM). This layer provides less assurance and transparency than the subsequent layers. (Samani et al. 2015, 25-26.)

The second layer, namely the Third-party assessment-based certification, publishes results of an assessment done by a third party on the cloud service provider against the CCM and International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27001. Results in this layer provide more assurance as they are verified by a third party. (Samani et al. 2015, 26.)

The third layer called Continuous monitoring-based certification works by continuously publishing new results of the target organisation. Instead of relying on the audit and certification cycle, continuous monitoring leverages the Cloud Trust Protocol (CTP) to update the results constantly. The CTP is a tool for cloud service customers, and they can leverage it to find out security related information about the cloud service providers. This gives customers the greatest transparency and assurance regarding the security maturity of the provider. (Cloud Security Alliance no date; Samani et al. 2015, 26.)

At the time of writing this thesis, the CSA STAR Registry could be accessed at https://cloudsecurityalliance.org/star/registry/. Figure 10 provides an example of the registry entries concerning Google Cloud on 15th of July 2020:



Google Cloud

Google Cloud provides organizations with leading infrastructure, platform capabilities and industry solutions, along with expertise, to reinvent their business with data-powered innovation on modern computing infrastructure. We deliver enterprise-grade cloud solutions that leverage Google's cutting-edge technology to help companies operate more efficiently, modernize for growth and innovate for the future. Customers in more than 150 countries turn to Google Cloud as their trusted partner to solve their most critical business problems.

Type: Self Assessment	**Active as of: May 28, 2020**
Consensus Assessments Initiative Questionnaire v3.1	Download
Type: Attestation	**Active as of: July 06, 2020**
STAR Attestation v1	Download

Figure 10. Google Cloud's entries in the CSA STAR Registry. (Cloud Security Alliance STAR Registry no date.)

As can be seen, Google Cloud has the layer 1 (Self Assessment) and layer 2 (Attestation) entries in the registry. The potential customer could use this information as one evaluation criteria when selecting the cloud service provider. However, the level of due diligence should be in line with the risk level an organisation is willing to tolerate (Samani et al. 2015, 26).

4 SECURITY MANAGEMENT IN A CLOUD ENVIRONMENT

The fourth and fifth chapters discuss the security and security risks in cloud computing, the best security practices, and secure architectural solutions from a general point of view, but also from the perspective of a governmental organisation. The focus is more on the areas the cloud service customer can control itself, and it lists the most important security-related recommendations for the different areas of cloud computing from authors such as CSA, CSCC, VAHTI, PiTuKri, Katakri, NIST, ISO/IEC, etc., and briefly discusses the currently present threats in cloud computing. The security is looked more from a high-level, technical point of view, and areas like governance and risk management are are covered briefly.

As many well written publications and standards already exist, it is not necessary to re-write them in this thesis – the idea is to look for elements that affect the security and secure use of cloud services the most, but also to examine the limitations cloud services may set to a governmental organisation operating regularly with classified information. Attention will be paid to VAHTI, PiTuKri and Katakri requirements throughout the chapters, as governmental organisations –

and the case organisation as well – need to follow these requirements in order to be able to comply with Finnish laws, and furthermore, to be allowed to process classified information.

4.1 Classified information

As VAHTI bases its recommendations using the different levels of classified information, the concept behind these classifications must be introduced too. According to VAHTI, the most important goal of information security is to support the organisation's operation by ensuring the confidentiality, integrity and availability of the data (VAHTI 2012, 25). A direct quote of the definition of classified information by Encylopedia tells that "*Classified information is any data or material that belong to the federal government and relate to sensitive topics such as military plans or the vulnerabilities of security systems"* (Encyclopedia 2020). In Finland, the law defines how the government officials need to handle and classify the documents belonging to the government (Criminal Sanctions Agency 2020). Non-public information can be classified using either the security classification marking "Turvallisuusluokintamerkintä" (I - IV) or the another security classification marking "Suojaustasomerkintä" (ST I - ST IV) depending on the information it contains and the possible damage it would cause should the information be revealed to the public. Although, the security classification marking "Turvallisuusluokintamerkintä" is only allowed to be used in situations where the information – if revealed – would have the potential to damage Finland's international relations. (VAHTI 2012, 25-26.)

The classifying of the documents with the security classification marking "Turvallisuusluokintamerkintä" is following (Corresponding international classifications can be seen in brackets):

- I "ERITTÄIN SALAINEN" ("TOP SECRET")
- II "SALAINEN" ("SECRET")
- III "LUOTTAMUKSELLINEN" ("CONFIDENTIAL")
- IV "KÄYTTÖ RAJOITETTU" ("RESTRICTED")

(Finlex no date.)

If the documents are classified using the security classification marking "Suojaustasomerkintä", then the corresponding levels are as follows (Translations are also included in brackets):

- ST I: suojaustaso I (protection level I)
- ST II: suojaustaso II (protection level II)
- ST III: suojaustaso III (protection level III)
- ST IV: suojaustaso IV (protection level IV)

(VAHTI 2012, 26.)

4.2 Threat landscape in the cloud

It is important for the scope of this research to understand the underlying threats that concern cloud computing. According to ENISA, directly quoting, threat relates to *"Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service."* (ENISA Glossary no date). Outsourcing a service to a third party will introduce risk. Whether the risk will increase or decrease depends on the service provider and the security the internally provisioned service has. And while the service can be outsourced, risk rarely can – there will always be an element of risk in both externally and internally provisioned services. Organisations benefit from cloud services, but these benefits come with a number of threats; some of these threats are already well-known, but others are completely unique to the cloud environment. (Samani et al. 2015, 35.)

Cloud Security Alliance's (CSA) Top Threat Working Group surveyed 241 industry experts on cloud security issues to create their latest 2019 Top Threats report. These experts acknowledged 11 salient threats, risks and vulnerabilities in their cloud environments, and these threats were named as the Egregious Eleven by the Top Threat Working Group. In this latest report, the 11 threats were ranked in order of significance per survey results with applicable previous rankings as follows (The number inside the brackets indicate the previous ranking):

1. Data Breaches (1)
2. Misconfiguration and Inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy

4. Insufficient Identity, Credential, Access and Key Management
5. Account Hijacking (5)
6. Insider Threat (6)
7. Insecure Interfaces and APIs (3)
8. Weak Control Plane
9. Metastructure and Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Use of Cloud Services (10)

(Cloud Security Alliance 2020, 6.)

What can be learned from the list is that data breaches have clearly stayed as the top threat in cloud computing. Insecure interfaces and APIs (Application Programming Interface) have moved down on the list but are yet present. According to CSA, the report raises awareness of critical security issues such as data breaches, misconfiguration and identity and access management. Also, limited cloud usage visibility and weak control plane are highlighted, and the users may be experiencing a lack of control in these areas with CSPs. The report also points out the concerning fact that there are still significant challenges in securing interfaces and APIs, as these are the modern ways to consume services. The cloud in its complexity is a perfect place to hide for an attacker and can act as an ideal launchpad for attacks. (Cloud Security Alliance 2020, 41.)

4.3 Cloud security scope and the shared responsibility model

In a cloud computing environment, the structural characteristics are the main causes of security problems. The nodes involved in cloud computing are diverse, and difficult to control effectively. The cloud service provider has the risk of compromising privacy when transmitting, processing and storing the data. (Sun 2020, 3.) As applications and databases are moved to large data centres where management of the data and services are not trustworthy, a great deal of new security challenges has emerged, and these security challenges vary between the cloud deployment models. The complexity of these risks in a complete cloud environment is presented in Figure 11 (Subashini & Kavitha 2010, 2.):

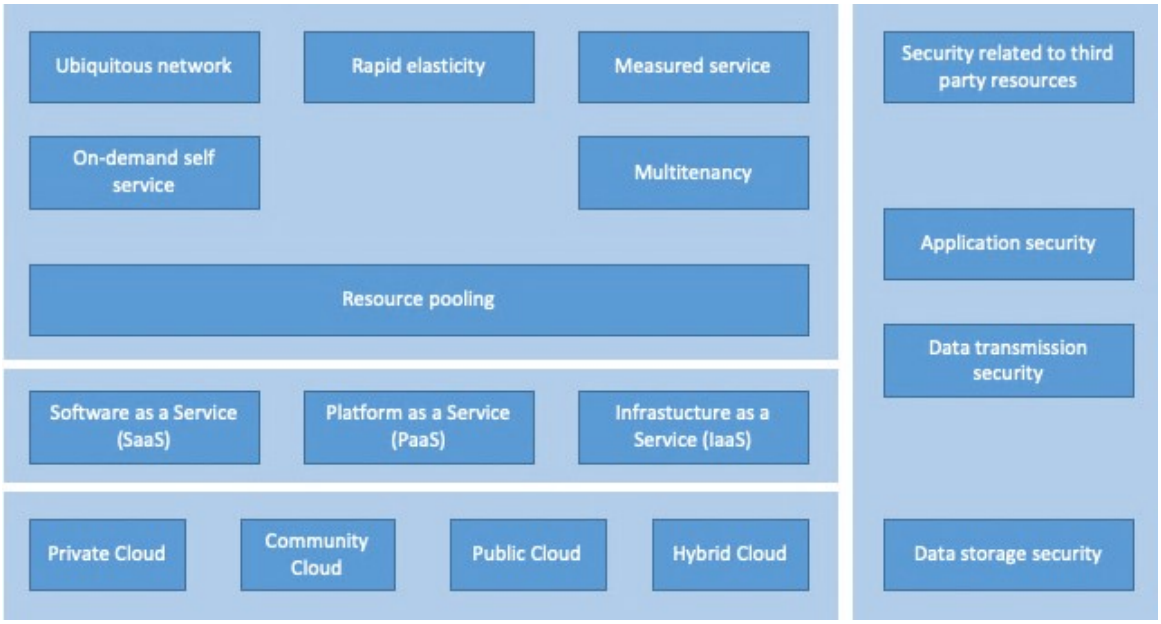


Figure 11. Security risks in a cloud computing environment. (Subashini & Kavitha 2010, 2.)

Cloud Security Alliance states that cloud computing can be thought as a model of shared technology. In this model, the organisations are responsible for implementing and managing different parts of the technology stack. This leads to a situation where responsibilities are distributed across this stack. Furthermore, the responsibilities are also distributed across all the organisations that are involved. This described situation is commonly known as the *shared responsibility model*. This model can be seen as a responsibility matrix that depends on the particular cloud service provider and the chosen product, the service model, and also the deployment model. (Cloud Security Alliance 2017, 20.)

In a high-level design, security responsibilities correspond to the degree of control any given actor has over the architecture stack (Cloud Security Alliance 2017, 21). Figure 12 illustrates the responsibility shift between the service models:

Figure 12. Security responsibilities between the service models. (Microsoft Shared responsibility in the cloud 2019.)

The security responsibilities gradually shift from the customer to the provider; in an on-premises solution, the customer is responsible for everything, and on the contrary, in a SaaS solution, the provider is responsible for nearly all security in the service (Cloud Security Alliance 2017, 21; Microsoft Shared responsibility in the cloud 2019).

In any cloud project, knowing exactly who is responsible and of what has the greatest impact on the security overall. As an example, Microsoft states that regardless of the type of deployment, the customer is always responsible for the data, endpoints, account and access management in the service. Comparing specific security controls between the service providers may be less important, as long as the functionality of the current security controls are known. The customer can fill the security gaps by implementing own security controls, or ultimately change the service provider, if it is not possible to close the gap in the security controls. (Cloud Security Alliance 2017, 21; Microsoft Shared responsibility in the cloud 2019).

To deal with the challenges the shared responsibility model may create, Cloud Security Alliance has two recommendations:

- Cloud service providers should have a clear documentation available for the customers of their internal security controls and customer security features.
- Cloud service customers should create a responsibilities matrix in order to document everyone's responsibilities of different controls. This matrix should also align with any compliance standards necessary for the project.

The Consensus Assessments Initiative Questionnaire (CAIQ) and the Cloud Controls Matrix (CCM) are available to help meet these requirements and can provide a comprehensive starting template to ensure that requirements for compliance are met.
(Cloud Security Alliance 2017, 21.)

4.3.1 Cloud security models

According to the Cloud Security Alliance, the security decisions can be made easier by using cloud security models. These models often overlap, and may be difficult to distinguish from each other, and they depend directly on the goals set by the developer of the model. But, as the terms are used often interchangeably, it makes sense to group them for clarity's sake. These groups include:

- Conceptual models or frameworks
- Controls models or frameworks
- Reference architectures
- Design patterns

Conceptual models or frameworks use different visualisations and also descriptions in order to explain various cloud security concepts and principles. Controls models or frameworks are used to categorise and give details to specific cloud security controls. Reference architectures – on the other hand – work as templates for implementing cloud security, and they are typically generalised in style. Design patterns provide reusable solutions to particular problems in security. (Cloud Security Alliance 2017, 22.)

The Cloud Security Alliance recommends the following models:

- The CSA Enterprise Architecture
- The CSA Cloud Controls Matrix

- The NIST draft Cloud Computing Security Reference Architecture (NIST Special Publication 500-299)
- ISO/IEC FDIS 27017 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

(Cloud Security Alliance 2017, 22.)

Even though many of the factors, such as the details of implementation, controls, processes, and reference architecture together with design models vary among the environment, the Cloud Security Alliance has introduced a relatively straight-forward high-level process for managing cloud security (Cloud Security Alliance 2017, 23):

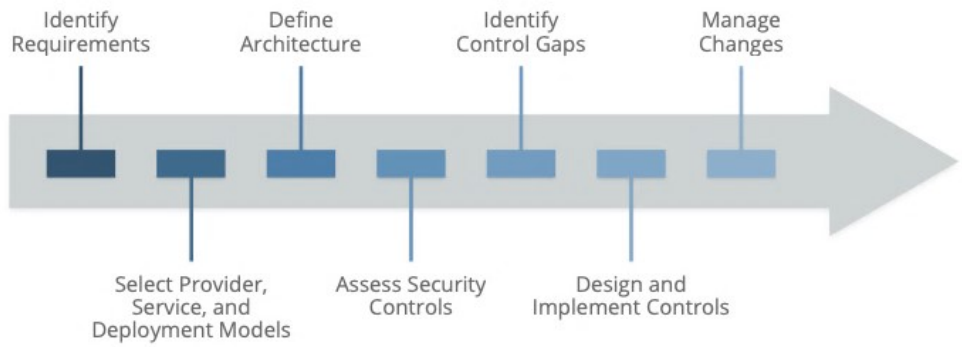


Figure 13. Process for managing cloud security. (Cloud Security Alliance 2017, 23.)

4.4 Governance and risk management

As topics, governance and risk management are very broad, and as such out of the scope of this thesis. For this reason, these topics are only briefly covered with the cloud security perspective in mind.

According to the CSA, cloud computing has an impact on four different areas of governance and risk management, and these areas are as follows:

- Governance
- Enterprise risk management
- Information risk management
- Information security

(Cloud Security Alliance 2017, 27.)

In general, effective governance must be in place to guide the different management processes, but also to help decision making to deliver IT services according to what the organisation in fact needs. Standards supporting the governance of IT are used commonly around the globe, but these governance standards are not specific to cloud computing. However, the standards are still sufficiently general and can be applied to the governance of cloud computing. Some general governance standards include:

- ISO/IEC 38500 – IT Governance
- COBIT
- ITIL
- ISO/IEC 20000
- SSAE 16
- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
- Cloud Security Alliance (CSA) Cloud Controls Matrix

(CSCC 2016, 6-7.)

Standards and frameworks that operate at country or regional levels also exist. These standards and frameworks can also apply to some specific data or industries. Furthermore, also standards that deal specifically with governance and management of information security exist. The ISO/IEC 27000 series of standards is very likely to be the most used set of standards that is designed to secure ICT systems. It is recommended that the cloud service customers look for cloud service providers that have proven to be able to conform to the ISO/IEC 27001 and 27002 standards, but also providers with the ISO/IEC 27017 certification. (CSCC 2016, 7-10.)

Contracts define the relationship between the cloud service providers and the cloud service customers and are also the primary tool of governance in public and private cloud deployments. Contracts act also as the only guarantee of any level of service or commitment. Risk management relies on contracts too, as the contracts define the roles and responsibilities for risk management between the cloud service provider and the cloud service customer. For risk management, there are standards for the cloud service customers to look for, too, such as the

ISO 31000:2009, ISO/IEC 31010:2009 and NIST SP 800-37 Revision 1. (Cloud Security Alliance 2017, 29-30.)

It is important to identify the shared responsibilities of security and risk management; The Cloud Security Alliance recommends the customer to understand how contracts with the cloud service providers affect the governance framework, and to develop a process for cloud provider assessments. A specific risk management and risk acceptance and risk mitigation methodology should also be put in place to assess the risks the solutions might possess. Industry best practices, global standards, and regulations should be used to develop a cloud governance framework. (Cloud Security Alliance 2017, 35.)

4.5 Compliance and audit management

One of the challenges organisations face in migrating from traditional data centres to the cloud is delivering, measuring and communicating compliance with different regulations across multiple jurisdictions. Significant adjustments are needed to approach based on physical instantiations of information and processes because of the distributed and virtualised nature of cloud computing. Cloud Security Alliance recommends that compliance, audit and assurance should be continuous. In cloud computing, the environment changes all the time. The cloud service is often audited by a third-party, as direct audits can be problematic. Especially this is a problem in public cloud deployments, where the environment is shared with a large number of customers, and this is also something the cloud service customers should check; the cloud service providers must be open for third-party audits. It is also important for the customer to select auditors with experience in cloud computing. In addition, the cloud service customer should also understand their full compliance obligations before implementing cloud computing. (CSCC 2016, 10-11; Cloud Security Alliance 2017, 54-59.)

4.6 Information governance

The cloud-based architecture has challenged the traditional methods in securing the data. New architectures – both physical and logical – and also abstracted controls, now require new strategies to secure data as users might transfer data to external – or even public – environments in completely new ways. Cloud Security Alliance has given information governance the following definition, directly quoted: "*Ensuring the use of data and information complies with organizational policies, standards and strategy — including regulatory, contractual, and business objectives."* Before planning a transition to a cloud, it is important to determine the governance requirements for information. This includes also any legal and regulatory requirements, and also corporate policies. Also, it must be ensured that the contracts and security controls enforce information governance policies and practices to extend to the cloud too. (Cloud Security Alliance 2017, 60-66.)

4.7 Contracts and legal issues

Moving data to the cloud might create legal issues. To address the specific issues, the organisation should consult with legal counsel in the jurisdiction in which the organisation operates and / or in which the organisation's customers reside. Cloud customers need to understand the relevant legal and regulatory frameworks, and also the requirements and restrictions set by the contracts that direct how the data in their custody should be handled. Also, it is important to understand the legal implications of using particular cloud providers, as they operate and store data physically in varying locations. A comprehensive evaluation of a proposed cloud service provider should be conducted before signing a contract with the service provider. (Cloud Security Alliance 2017, 36-53.)

4.8 Incident response

All information security programs should include incident response. And while many organisations have incident response plans to investigate attacks, the

cloud environment sets some new challenges in both access to forensic data and governance – meaning that organisations will have to re-evaluate their incident response processes. (Cloud Security Alliance 2017, 101-102.) NIST 800-61 rev2 document defines the incident response lifecycle as follows:

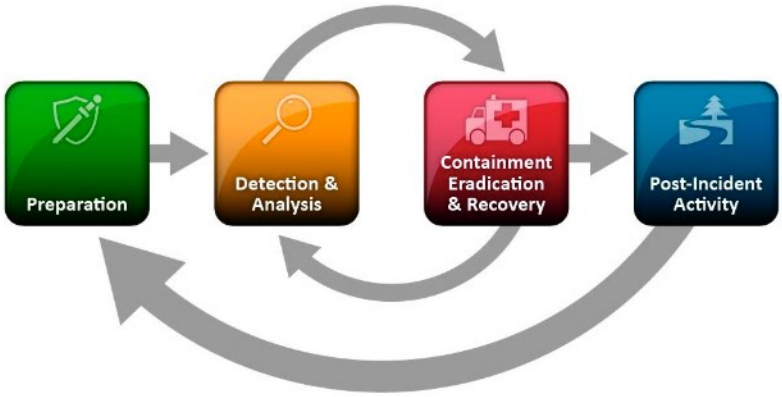


Figure 14. NIST's incident response lifecycle. (NIST SP 800-61r2 2012, 21.)

Cloud deployment affects each of the phases described in the lifecycle. Some are similar to any incident response, and outsourced environments will require a third party to coordinate with. SLAs form the most important part of incident response for cloud-based resources. Also, knowing the responsibilities between the customer and the provider is crucial, and this is related to the preparation phase. The customer must know the content and also the format of the data the provider is about to deliver to the customer for analysis purposes. To detect potential issues earlier, incorporating continuous and serverless monitoring is also advised for cloud-based resources. To enhance the response rate, containment, and recovery, cloud-based applications should also leverage automation and orchestration. No matter the service provider, the SLA must guarantee the support for the required incident handling to effectively execute the enterprise incident response plan. (Cloud Security Alliance 2017, 103-107.)

4.9 The effects of service models and deployment models on security

Service models and deployment models also affect the ability to manage governance and risk. Cloud Security Alliance recommends to recognise the fact that the chosen cloud deployment and service models affect the shared

responsibilities of security and risk management. Developing a cloud governance framework using the relevant industry best practices is highly recommended. This can include the following:

- CSA CCM
- COBIT 5
- EU GDPR
- HIPAA
- ISO/IEC 27017
- NIST RMF
- PCI DSS

(Cloud Security Alliance 2017, 31-35.)

4.9.1 Service models

In a cloud environment, IaaS is closest to the traditional data centre. In this implementation, a majority of the existing governance and risk management activities organisations have already in place can be transferred directly to this environment (Cloud Security Alliance 2017, 32). As with every service that resides outside the organisation's own network, acquiring new data connections to the service is a challenge. Also maintaining the confidentiality of the information, conducting audits, performing security clearances on the service provider's personnel, and handling the log files securely might cause problems – and especially when the cloud environment is shared with multiple customers. (VAHTI 2010, 53.)

In a PaaS environment, the provider might give some control to the customer to build applications on top of the platform, but any security below the application level – such as host and network intrusion prevention systems – is managed by the provider. It is more extensible than SaaS, but on the contrary, lacks the customer-ready features, which extends to security features and capabilities as well. The built-in capabilities are less complete, but PaaS provides more flexibility to layer on additional security. (Subashini 2010, 8.)

SaaS forces the customer to depend on the provider for proper security measures (Subashini 2010, 3). It has also the most critical need for a negotiated

contract (Cloud Security Alliance 2017, 31). In this model, the customer usually gets a bulk product according to the service agreement, and the service provider can build the service using the technology it prefers, as long as it fulfills the agreement between the customer and the provider. In case the service is completely a bulk product, the customer must ensure the service agreement includes proper security controls. Many of the SaaS services are built in a way that the customer has no other way but to comply with the given service agreement, and it is not possible to customise even the security aspects in the service. (VAHTI 2010, 55.) The way how a SaaS application works is not visible to the customer – instead – all the customer is able to see is entirely limited to the user interface the cloud service provider has developed. (Cloud Security Alliance 2017, 31).

4.9.2 Deployment models

Deployment models have an effect too; for instance, in public cloud, the customers have a limited ability to govern the operations and to negotiate contracts, and this has an impact on how they can extend their governance model into the cloud. This limitation might also force the customer to re-evaluate the available service providers for better contracts. This problem occurs in private cloud too. If an organisation allows a third party to manage the private cloud, it will also mean shared responsibilities with obligations. All these are also defined in the contract. However, private cloud may give the customer more control over the contractual terms. There is a slight difference in terms of the contract as well, when compared to public cloud. Public cloud will perform as agreed in the contract, and there is no need for the customer to analyse the service any further. In an outsourced private cloud, the service will only cover exactly what has been written in the contract, and everything else comes with an extra price. A self-hosted private cloud is different; the focus of cloud governance is on the internal service level agreements that concern the cloud users. (Cloud Security Alliance 2017, 32.)

In a hybrid cloud environment, the cloud user is connecting either two cloud environments together, or a cloud environment and a traditional data centre. In both cases, the minimum set of controls that consist of the customer's internal governance agreements and the cloud service provider's contract, must be considered in the governance strategy. Community clouds are not public, but a shared platform with multiple organisations. The governance extends to cover the members of the community in this situation. The approach can be thought as of a mix of governance between a public cloud and a hosted private cloud. (Cloud Security Alliance 2017, 33.)

4.10 Outsourced services in governmental organisations

As discussed earlier, cloud deployment models and cloud service models affect the security in the cloud. The affect these models might have need further evaluation from the perspective of governmental organisations.

VAHTI recognises nine different deployment models to outsource ICT services. When using services with shared capacity or services hosted in a cloud environment, the organisation loses the control over the governance of the service, and the responsibility of the service moves towards the service provider. The more control the service provider has, the more important are the processes, controls and reports the customer can use to monitor that the data is processed securely and according to the service agreements. (VAHTI 2012, 57.) PiTuKri has pre-requirements for using cloud services too; it insists that the proposed cloud service must have detailed system description in place that can be used to evaluate the applicability of the service to the customer. (Traficom 2020, 14.)

In the figure below, these nine deployment models are displayed together with the possible use cases. The figure includes the corresponding data classification levels in relation to the proposed deployment models and environments. PiTuKri has a similar form too that can be used to evaluate the services and the service provider against the different types of classified information, and what to require as a customer in the different scenarios (Traficom 2020, 16).

Deployment model	Example of level of classified information that can be handled in the proposed model
1) Dedicated environment - service hosted by the organisation	ST I ("TOP SECRET")
2) Dedicated environment - service hosted by the government service centre (Valtionhallon palvelukeskus)	ST I ("TOP SECRET")
3) Dedicated environment - service hosted by a third party - the service is hosted in Finland	ST I ("TOP SECRET")
4) Dedicated envionment - service hosted by a third party - personnel has security clearances	ST I ("TOP SECRET")
5) Service hosted by the government service centre (Valtionhallion palvelukeskus) - service is hosted in Finland	ST II ("SECRET")
6) Service hosted by a third party with shared capacity to several government-based organisations - service is hosted in Finland	ST III ("CONFIDENTIAL")
7) Service hosted by a third party with shared capacity to several unknown customers - service is hosted in Finland	ST III level risk analysis ("CONFIDENTIAL") / ST IV ("RESTRICTED")
8) Service hosted by a third party with shared capacity to several unknown customers - security clearances can be done on the personnel	ST III level risk analysis ("CONFIDENTIAL") / ST IV ("RESTRICTED")
9) Service hosted by a third party with shared capacity to several unknown customers - service can be hosted anywhere - it is not possible to name the personnel hosting the service - it is not possible to audit the service	Public information

Figure 15. The deployment models and possible use cases in governmental organisations. (VAHTI 2012, 58.)

In addition to this, deployment models 3 and 9 have specific conditions that must be fulfilled in order to be able to process the classified data according to the level presented in the figure. In model 3, the provider must have a separated network and the technical solutions it requires – if these requirements are not met, the highest level of classified information that can be handled in the system is ST II (“SECRET”). Also, attention must be paid to the availability of the service in model 9, in which the customer’s only option is to agree the service agreement of the provider. Services that fall into this category are – for example – social media services Facebook and Twitter, and the packages offered by Microsoft, Google and Apple that include email, calendar and cloud storage services. Organisations also run hybrid environments which are combinations of these nine models. (VAHTI 2012, 58-65.)

As can be seen, the models VAHTI has listed are different implementations of the previously introduced cloud service and cloud deployment models. This also highlights the fact that there are numerous ways to consume cloud services, and the cloud environment can be set up in many different ways. To help the governmental organisations decide how to start implementing cloud computing, VAHTI provides clear instructions which to follow – assuming the organisation has already classified its assets and data accordingly. PiTuKri can be used together with VAHTI to even better evaluate the services and service providers.

5 SECURITY CONTROLS IN A CLOUD ENVIRONMENT

5.1 Management plane security

The management plane can be thought as the single most significant security difference between the traditional infrastructure and cloud computing. The cloud sort of centralises and abstracts the administrative management of resources, but nevertheless, it is still always present within the various tools and user interfaces that are used to manage the infrastructure, the different platforms and all the applications. Boxes and wires have changed to API calls and web consoles as the ways of controlling the configuration. Gaining access to the management plane is comparable to gaining a non-restricted access to a traditional data centre, making it inevitable to have security controls implemented to restrict the management plane access. (Cloud Security Alliance 2017, 67.)

In more details, the management plane is referred to as the interface from which the cloud assets can be managed. Deploying and configuring virtual machines is done through the management plane, for instance. In SaaS environment, the management plane can be thought as the administrator tab in the user interface. This tab allows configuring things like users and settings for the organisations. In addition, it has a major role in enforcing – and also enabling – isolation and separation in multitenancy. To segregate customers and different users within a single tenant, limiting the availability of APIs is also important. (Cloud Security Alliance 2017, 69.)

The management plane is delivered through APIs and web consoles. Web consoles are managed by the service provider and they can be organisation-specific. A variety of authentication mechanisms exist, but the most common ones used are HTTP request signing and OAuth. In these, cryptographic techniques are used in order to validate authentication requests. It is also important to notice that in private cloud deployment the organisation is

responsible for building and maintaining the management plane itself. When the organisation is only a consumer the responsibilities extend only to the parts of the management plane the provider exposes. When securing the management plane, there are five important areas to focus on:

- Perimeter security
- Customer authentication
- Internal authentication and credential passing
- Authorisation and entitlements
- Logging, monitoring and alerting

(Cloud Security Alliance 2017, 70-72.)

Perimeter security is crucial with API gateways and web consoles, and MFA (Multi Factor Authentication) should always be used in the authentication processes. (Cloud Security Alliance 2017, 72.) Securing the management plane requires good security practices with identity and access management (IAM) too, which is discussed in the next chapter in more detail.

5.2 Identity, entitlement, and access management

Identity and Access Management (IAM) is probably the most important set of security controls. In breaches that involve web applications, lost or stolen credentials have been the attackers' most used tool for several years (Dotson 2019, 49.) By managing people, roles and identities it is possible to ensure a controlled access to data and applications in a cloud computing environment (CSCC 2016, 12).

IAM consists of identification, authentication and authorisations (including access management). In other words, IAM is used to determine who can do what within a cloud platform, and this affects directly the management plane security as well. (Cloud Security Alliance 2017, 70.) What needs to be noted is that the term IAM is not universal. IAM is also often referred to as Identity Management, or IdM. (Cloud Security Alliance 2017, 131). There is also overlap and confusion between the terms entitlement, authorisation and access control. Depending on the context, they are all always defined differently. (Cloud Security Alliance 2017,

137). IAM comes in many different specific options and configurations, and these vary between the cloud service providers and platforms, each having their own implementations. Even the terms might not be interchangeable for things such as groups and roles. (Cloud Security Alliance 2017, 70.) Cloud computing has a great impact on IAM in both public and private cloud implementations, as IAM must be managed by two parties without compromising security. IAM is different in cloud computing compared to internal systems – the issues are probably not new, but they are bigger. (Cloud Security Alliance 2017, 129.)

The relationship between the cloud provider and the cloud customer is the key difference, as managing IAM is not possible alone. Managing IAM requires many things, such as trust, responsibility designation, and also technical processes to enable them. The core infrastructure administration is vulnerable to network attacks, as cloud tends to change fast, it is distributed in nature, and has a complex management plane that relies on broad network communications. (Cloud Security Alliance 2017, 129.)

5.2.1 Identification and authentication

PiTuKri states that all the users from both the provider and customer must be identified and authenticated before allowing access to classified information (Traficom 2020, 36). Several IAM security standards with support for cloud computing exist. Important for the cloud service customers is to look for IAM systems that have support for federated IDs, and also for single sign-on and privileged identity management (CSCC 2016, 13).

Many standards and technologies are available that can be used in cloud computing, and which support federated IDs and single sign-on (CSCC 2016, 13; Cloud Security Alliance 2017, 132). Despite this, the service providers have settled with only a selected group of standards, and the following are the most commonly supported by the widest range of service providers:

- Security Assertion Markup Language (SAML)
  SAML is an OASIS standard. It is designed for federated identity management and it supports both authentication and authorisation. XML is used to make

assertions between the relaying party and the identity provider. SAML has a very wide support in both enterprise tools and cloud providers but configuring it might turn out to be somewhat difficult.

- OAuth
  OAuth is an IETF standard, built for authorisation, and is widely used among web services. OAuth is designed in a way that it works over HTTP and is most often used for delegating access control and authorisations between services.
- OpenID
  OpenID is a standard for federated authentication, and it is commonly supported between web services. OpenID bases on HTTP and uses URLs to identify the user and the identity provider. It is very popular in consumer services.

(Cloud Security Alliance 2017, 132.)

In addition to these, also these standards can be used:

- LDAP (Lightweight Directory Access Protocol)
- WS-Federation
- SCIM (System for Cross-domain Identity Management)
- Active Directory Federated Services (ADSF2)

(CSCC 2016, 13-14.)

Federated identity is a concept instead of a specific technology. The user may have identities on two different systems which are linked together so that the user has no need for separate accounts for the systems. (Dotson 2019, 61.) Figure 16 displays the concept of federated identity management:

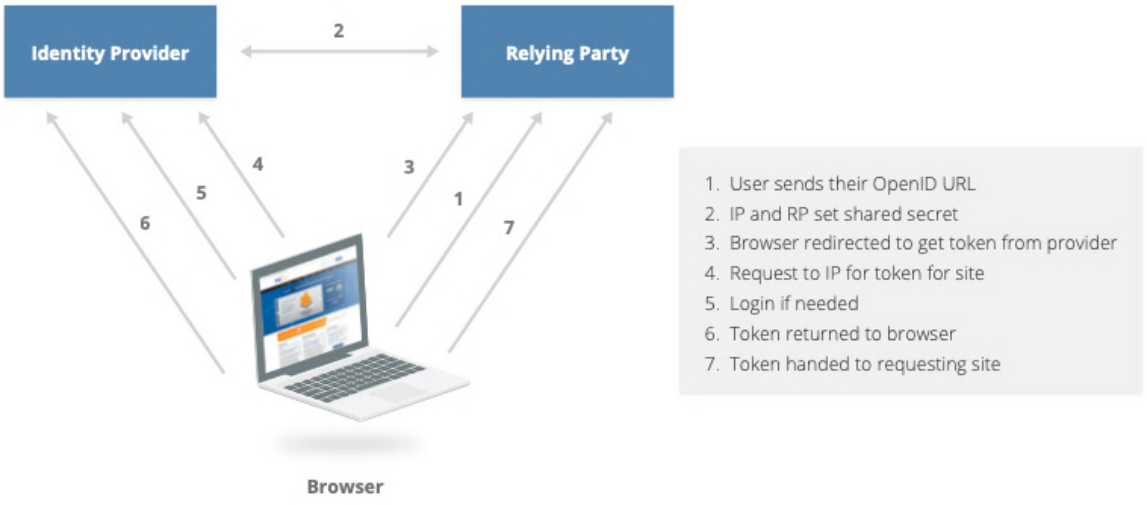


Figure 16. How federated identity management works using OpenID URL. (Cloud Security Alliance 2017, 133.)

PiTuKri lists five key elements of a reliable identification and authentication process:

1) The authentication method must be protected from man-in-the-middle attacks
2) In the log-in process before the authentication phase no unnecessary information should be revealed
3) The credentials used in the authentication process must always be encrypted
4) The authentication method must be protected against replay attacks
5) The authentication method must be protected against brute force attacks

(Traficom 2020, 36.)

In situations where federated identity management is used to authenticate to a cloud service, attention must be paid to the reliability between the identity provider (IdP) and the relying party. When classified information is involved, only identity providers that offer identity based on strong authentication can be used together with a secure relying party. Organisation-centric identity management is usually more suitable than the user-centric model when operating with classified information. (Traficom 2020, 36.) Between the authentication options, multifactor authentication (MFA) is one of the strongest alternatives, and there are multiple ways to implement MFA:

- Hard tokens
  Physical devices generating one-time passwords – the best option when aiming for the highest level of security
- Soft tokens
  Soft tokens are like hard tokens, but on the contrary, are software applications running either on a phone or computer
- Out-of-band Passwords
  Some sorts of typically text-based messages sent to the phone of the user
- Biometrics
  A new and growing option as biometrics readers have become available on mobile phones

(Cloud Security Alliance 2017, 137.)

There are – of course – other techniques and standards too that are used in cloud computing for identity, authentication, and authorisation. The example above could be applied to a SaaS environment – but for instance – IaaS providers have their own internal IAM systems and might not use any of these

mentioned standards. As a general recommendation, the identity protocols must be analysed in the context of a use case, as no protocol solves all identity and access control related problems. (Cloud Security Alliance 2017, 134.) CSCC suggests that from the cloud customer's perspective the most important consideration for IAMs is the support of different versions of technologies and standards. (CSCC 2016, 15).

5.2.2 User and identity management

Many of the cloud service providers offer IAM services for free to use in accessing their cloud services. These systems have one central location to manage the identities of cloud administrators in the customer organisation. (Dotson 2019, 53.) In identity management, the identity part focuses on the processes and technologies related to managing the identities. To begin the management, a fundamental decision needs to be made on how to manage identities; knowing where to manage their identities is very important information for the cloud users.
Also, the architectural models and technologies they are willing to support when integrating with cloud providers must be known by the cloud users. When using federation – like most organisations do due to its scalability – the authoritative source that holds the unique identities, and the architecture behind it, must be determined by the cloud user. This is usually an internal directory server. In general, two models exist; Free Form (direct connection to cloud providers) and Hub & Spoke (communication via a central broker to cloud providers). (Cloud Security Alliance 2017, 134.)

Dotson (2019) has listed some of the common IAM systems the service providers offer to authenticate the customer's cloud administrators with the services in the cloud:

Provider	Cloud identity system
Amazon Web Services	Amazon IAM
Microsoft Azure	Azure Active Directory B2C
Google Compute Cloud	Cloud Identity system
IBM Cloud	Cloud IAM

Figure 17. Cloud identity systems. (Dotson 2019, 56.)

When the organisation also needs to manage end-users – be it external customers or the organisation's own employees – there are also several IDaaS (Identity-as-a-Service) solutions available, which can again be integrated to the organisation's own information registry of employees (Dotson 2019, 56.):

Provider	Cloud identity system
Amazon Web Services	Amazon Cognito
Microsoft Azure	Azure Active Directory B2C
Google Compute Cloud	Firebase
IBM Cloud	Cloud Identity system
Auth0	Customer Identity Management
Ping	Customer Identity and Access Management
Okta	Customer Identity Management
Oracle	Oracle Identity Cloud Service

Figure 18. Cloud identity management systems for end-users. (Dotson 2019, 56.)

5.2.3 User account policy and access control

According to PiTuKri, the main goal of user access management is to ensure that only the authorised personnel have access to the information systems and the classified information it holds (Traficom 2020, 35). An account owner with super-admin privileges always exists, no matter the platform or service provider. It is recommended that this account is enterprise-owned, tightly locked down, and almost never used. Super-admin accounts for individual administrative use can usually be created separate from the account-owner, and these privileges should be used sparingly. For daily use, lower-level administrative accounts should be

used, should the provider support them. These accounts can also be referred to as service administrators or day to day administrators and prevent the entire deployment from exposing when compromised. Multiple lower-level administrative accounts can be used to compartmentalise individual sessions, and it allows the administrators to log in with an account having only the privileges they need for the task in hand. This way there is no need to expose the higher-level account. Figure 19 presents an example of a baseline of cloud management plane user accounts. Also accounts for super-admins and service-admins are included (Cloud Security Alliance 2017, 71.):

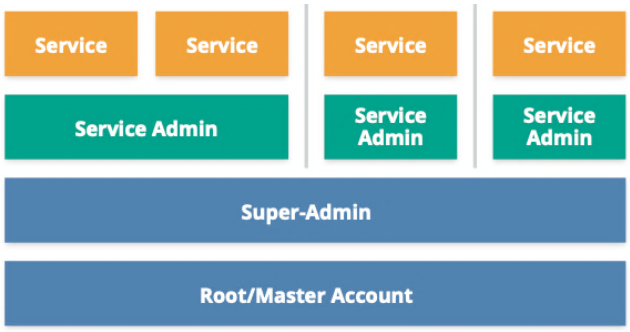


Figure 19. Example of baseline cloud management plane user accounts. (Cloud Security Alliance 2017, 71.)

A good practice for both providers and customers is to follow the policy of least privilege. This applies to the management plane use, the users, and also the applications. Also, all the privileged user accounts should use multi-factor authentication (MFA) – this is considered as one of the most effective security controls in defending from a vast range of attacks. (Cloud Security Alliance 2017, 71.) PiTuKri has a similar target in managing the user accounts and user rights. Managing the user rights should be done according to the principle of least privilege: The user accounts have been granted only for the personnel that require them based on their current task or role. User rights have been limited to cover only the functionalities, applications, devices and networks that are necessary for the task. The need for the user rights has to be evaluated according to a schedule, and a process must be in place for situations where the employee's contract changes or ends. Also, the shared responsibility between the service provider and the customer must be noted when evaluating these

criteria. (Traficom 2020, 35.) As PiTuKri is based on the ISO 27000 series of standards, the same recommendations can be found in the corresponding standards. ISO/IEC 27002:2013, for instance, introduces the same principles as PiTuKri to user and access management (ISO/IEC 27002 2013, 21-24). The controls also follow the same base line in NIST's corresponding publication SP 800-53 (NIST SP 800-53 2013, 164-165).

Figure 19 represents a real-world example in cloud environment of how the access is and can be controlled between the users. In this scenario, the cloud service provider uses an API to launch new virtual machines and this API has a corresponding authorisation to allow launching new virtual machines. Cloud Security Alliance refers to this as an entitlement matrix. It is a written policy that is used in the cloud service provider's system for enforcing the rules. (Cloud Security Alliance 2017, 138.)

Entitlement	Super-Admin	Service-1 Admin	Service-2 Admin	Dev	Security-Audit	Security-Admin
Service 1 List	X	X		X	X	X
Service 2 List	X		X	X	X	X
Service 1 Modify Network	X	X		X		X
Service 2 Modify Security Rule	X	X				X
Read Audit Logs	X				X	X

Figure 20. Example of an entitlement matrix. (Cloud Security Alliance 2017, 138.)

In general, the cloud provider is responsible for enforcing the policies regarding authorisations and access controls, and the cloud user is responsible for defining the entitlements and also properly configuring them in the cloud platform. XACML (eXtensible Access Control Markup Language) can be used for access control and security policy decisions. Usually, for IAM, cloud platforms have better support for the Attribute-Based Access Control (ABAC). ABAC also offers greater flexibility and security than the Role-Based Access Control (RBAC) model. The ABAC model is also preferred in cloud-based access management. (CSCC 2016, 14; Cloud Security Alliance 2017, 138.)

5.3 Infrastructure and network security

According to Cloud Security Alliance, infrastructure security is the foundation that ensures secure operation in the cloud; networks and computers act as the base layer, and everything is built on top of them. Infrastructure security forms the lowest layers of security, and it stretches all the way from physical facilities to the consumer's configuration and implementation of infrastructure. In a complete security assessment, the security of physical infrastructure and facilities is also included. However, the facilities and the physical infrastructure is usually owned by the cloud service provider, and it is up to the cloud service customer to ensure appropriate security controls are in place. With this in mind, cloud service customers are recommended to seek providers that have proven the ability to comply to the ISO/IEC 27002 standard for physical and environmental security, and even though this particular standard is not specific to cloud computing, the same principles can be applied to cloud environments too. (CSCC 2016, 23; Cloud Security Alliance 2017, 77.)

Cloud Security Alliance has divided the infrastructure into two separate macro layers. The first is the physical and logical compute, networks, and storage. The cloud's pool of resources is built of these assets. The security of the networking hardware and also software are included in this layer that is used – for instance – when creating the network resource pool. The layer can be thought as the set of resources that are needed to create a cloud. The second layer is the virtual and abstracted infrastructure managed by a cloud user. From the first introduced resource pools, the users can utilise compute, network and storage assets on this second layer. An example use-case of the second layer would be a cloud user managing the security of the virtual network. (Cloud Security Alliance 2017, 77.)

The idea of this chapter is not to discuss infrastructure and network security in general – only the cloud-related and most relevant areas are introduced. PiTuKri has two separate sections for physical and network security, and the

requirements in PiTuKri should be evaluated in case classified information is involved. PiTuKri, for instance, goes into great detail in listing the physical perimeter security controls for the sites where the classified data is handled (Traficom 2020, 27-34). Listing the controls in full is not necessary in this context – more important is to point out that these controls exist, and they should be examined closely when needed. The goal is to understand the actions the cloud customer can take to enhance the security related to this area, and which areas can be only evaluated through auditing processes. Also, the areas of responsibility are not fixed; the deployment and service models affect this, as is described, for instance, in the Microsoft's shared responsibility model (Microsoft Shared responsibility in the cloud 2019). As an example, in an IaaS environment the service provider is unable to affect the safety of the configuration used in software firewalls that are managed by the customer. On the contrary, neither can the customer affect the security controls the service provider has implemented into the IaaS environment. (Traficom 2020, 33.)

5.3.1 Network security

Cloud service providers must attempt to secure the network traffic, but the service providers might not necessarily know what sort of traffic the customers might generate. However, cloud service customers should still expect their cloud service providers to segregate the external and internal network segments at some level. The traditional network security controls that are perimeter-based might turn out to be not very effective in cloud environments. Also, corporate firewalls may lead to a false sense of security, as many ways exist which can be used to get inside the corporate perimeter; services traditionally located behind corporate firewalls are now directly accessible from the Internet. In addition to the ISO/IEC 27001 and 27002 standards, also the ISO/IEC 27033 standards provide detailed guidance on how to implement the network security controls. (CSCC 2016, 21-22.) There are currently several network security features available directly from the cloud service providers, and Dotson (2019) has listed some of these features:

Provider	Features
Amazon Web Services IaaS	VPC and network ACLs, security groups, virtual appliances available in the marketplace
Microsoft Azure IaaS	Virtual networks, network security groups (NSGs), network virtual appliances
Google Compute Platform IaaS	VPC and firewall rules
IBM Cloud IaaS	VPC with network ACLs, gateway appliances, security groups
Kubernetes (overlay on an IaaS)	Network policies

Figure 21. Segretation features offered by the cloud service providers. (Dotson 2019, 122.)

From a cloud provider's perspective – but also in situations when managing a private cloud – segregating the networks physically is important for both operational and security reasons (Cloud Security Alliance 2017, 78). The goal is to ensure that the classified information can be handled in a completely controlled environment, and PiTuKri lists the segregation of data processing environments as one of the most important controls when securing classified information (Traficom 2020, 33). Katakri has the same requirement when processing classified information (the corresponding cloud environment must be segregated from other environments), and it extends all the way from the top to the lowest level of classified information (ST IV "RESTRICTED") (Katakri 2015, 30). According to Cloud Security Alliance, there are usually three separate networks that are isolated onto dedicated hardware, as there is no functional or traffic overlap:

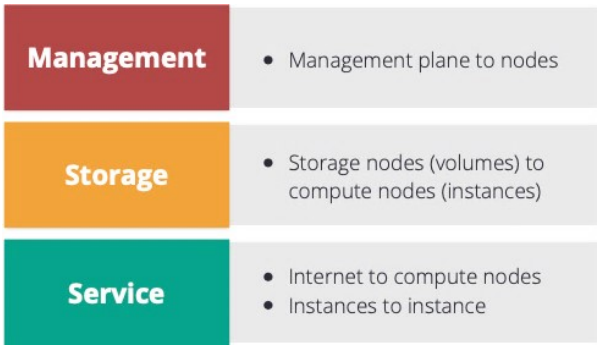


Figure 22. Separated network segments in IaaS deployment. (Cloud Security Alliance 2017, 78.)

The management network is used for management and API traffic. The storage network connects virtual storage to virtual machines, and the service network

communicates between virtual machines and the Internet. The service network is the previously mentioned resource pool for the cloud users. This presented architecture represents only one way to create a private cloud network, but as such it is also a commonly used baseline. (Cloud Security Alliance 2017, 78.)

Virtual networking in cloud environments is used to form a network resource pool. In a typical situation, the cloud user can provision the networking resources from this pool, and the configuration can be done within the limits the used virtualisation technique sets. Some cloud platforms may only support allocating IP addresses from pre-defined subnets, while others may allow provisioning entire class B virtual networks with the possibility to completely design the subnet architecture. Some commonly used network virtualisation techniques used in cloud computing are Virtual Local Area Networks (VLANs) and Software Defined Networking (SDN). VLANs can leverage the existing technology present in most network hardware, but they are not designed for cloud-scale virtualisation or security and should not be considered as the only security control for isolating networks. It is also not possible to substitute physical segregation with VLANs. SDN, on the contrary, is a layer built on top of networking hardware, and provides a more complete layer of abstraction as it removes the limitations of a traditional LAN. Several implementations exist, and SDN is able to offer higher flexibility and isolation, and for this reason, is also recommended to use, when available. (Cloud Security Alliance 2017, 78-90.)

5.3.2 Perimeter security

The perimeter security that protects the cloud environment is also important in a private cloud implementation, and it is an area the cloud service provider is responsible as well. In a multitenant environment, it is critical to maintain segregation and isolation. The cloud service providers need to make the security controls available for the cloud users, giving them a possibility to properly configure and manage their network security. (Cloud Security Alliance 2017, 83.) PiTuKri requires that the traffic is monitored and restricted in a way that only the traffic necessary for the current environment is allowed between the outer

perimeter and internal zones of the cloud service environment (default-deny policy). To segregate the outer perimeter and the data processing environment a properly configured firewall or similar device must be used, and the device must be protected from unauthorised use. (Traficom 2020, 33.) Distributed Denial of Service Protection (DDoS) and baseline IPS can be used to filter out hostile traffic. Cloud firewalls should be applied to workloads instead of networks. Scrubbing any potentially sensitive information is vital in situations where a virtual instance is discharged and given back to the hypervisor to avoid a situation where another customer could read the information when the drive space is provisioned again. (Cloud Security Alliance 2017, 83-89).

5.3.3 Security in hybrid implementations

Hybrid clouds work in a way that a private cloud or data centre is connected to a public cloud provider. This is usually done through a dedicated connection – like WAN (Wide Area Network) link or VPN, for example. If the private network lacks security controls, the hybrid connection may compromise the overall security of the cloud network. Typically, it is preferable to minimise hybrid connections for management and security reasons. Different tools should be used in maintaining separation. These tools can include routing, access controls, firewalls, or some other network security tools. Connecting together numerous distinct networks is complicated and may potentially increase routing complexity. In addition, the possibility to run multiple cloud networks that have overlapping IP address pools might be also reduced. (Cloud Security Alliance 2017, 83.)

Virtual transit network is one possible architectural level solution to this problem (Cloud Security Alliance 2018, 83). There are different implementations of this, and Dotson (2019) refers to these as bastion hosts or jump hosts (Dotson 2019, 127). In this scenario, a single hybrid connection is used to connect multiple cloud networks to one single data centre. The hybrid connection is built using a dedicated virtual transit network, and all the connections to the other networks are made in the virtual transit network. As the second-level networks are connected to the data centre through the transit network, and are not able to see

each other, segregation is maintained. To further protect the traffic in the transit network, tools like firewall rulesets and access control lists can also be implemented. (Cloud Security Alliance 2017, 83.)

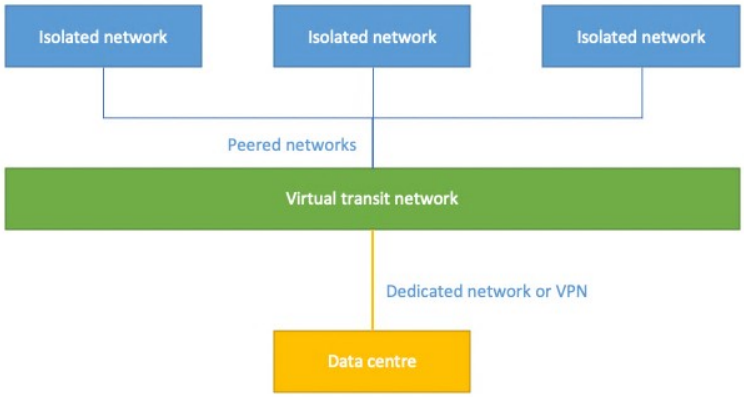


Figure 23. A possible architectural solution to hybrid environments. (Cloud Security Alliance 2017, 83.)

5.3.4 Remote connections

According to PiTuKri, remote connections must be protected to ensure it is not possible to leverage them in gaining unauthorised access to the customer database or the cloud service. Using remote connections is usually the most common way of managing the cloud services. Also, the web consoles and portals offered to the end user are typically classified as remote connections. The remote access in a cloud environment should go through monitored devices, such as jump hosts, management portals, etc. The remote access should leverage at least two-way multifactor authentication (password + token, for instance) to identify the users, and the management traffic must be encrypted properly. The access points that allow remote access should also be isolated from each other between the end users and the service provider itself. (Traficom 2020, 37.) VAHTI instructions also point out that when accessing information systems and data that has security classification (Turvallisuusluokintamerkintä), the remote use of such systems is usually only possible when the data is classified as IV (“RESTRICTED”). Level III (“CONFIDENTIAL”) classified data would require a working area approved by the government officials. Although, when operating with national level information, it is possible to remotely use the systems

containing ST III level information from physically safe locations, such as the person's home. VAHTI has also determined the criteria for the remote locations that must be met before the classified information can be accessed remotely. (VAHTI 2012, 51-52.)

5.3.5 Zones and microsegmentation

PiTuKri requires that behind the outer perimeter the cloud environment must be divided into separate zones, using techniques like segmenting or microsegmenting (Traficom 2020, 33). Microsegmentation is also sometimes referred to as hypersegregation, and it leverages virtual network topologies in running smaller and isolated networks without costing any additional hardware as it is based on software. Creating own dedicated virtual networks for applications and connecting the networks together only on-a-need-basis is a common example of this capability. The leads to a smaller blast radius should an attacker compromise an individual system, and the attacker can no longer use this foothold to move and expand across the entire data centre. SDN capabilities – when available – can and should be used to achieve this. (Cloud Security Alliance 2017, 82-89.)

5.3.6 Workload and computing security

A workload refers to a processing unit. This unit can exist inside a virtual machine or a container, or also inside an abstraction of some other sort. All workloads have one thing in common; they always run on a processor and consume memory. Workloads can have a great deal of different processing tasks, ranging from applications to GPU- or FPGA-based specialised tasks, and nearly all of the possible tasks are supported in cloud computing. Every cloud workload has its own hardware stack that it is run on. Maintaining the integrity of this described hardware is a very important task for the cloud service providers. To achieve this, the cloud service providers use different techniques. These can include, for example, secure execution environments, hardware-based supervision, process monitoring, and encryption and key management solutions. Selecting the proper

hardware might yield great gains in overall security, but customers rarely get the opportunity to control where their workloads are physically run, regardless of the deployment model. (Cloud Security Alliance 2017, 84-86.)

Multiple compute abstraction types exist: Virtual machines, containers, platform-based workloads and serverless computing. Each one of these have different levels of segregation and isolation. Auto-scaling and containers work best when instances are launched dynamically based on an image; only the underlying image is updated when reconfiguration for the instance is needed. No changes or patching is done on the running workload, and the new instances are enabled by switching the images underneath. Virtual machines that are managed this way are called immutable by the Cloud Security Alliance. These immutable virtual machines can enhance the workload security significantly, and it is recommended to use them, when possible. When used, remote logins to running workloads should be disabled to prevent inconsistent changes across the stack. Most of the security testing should be done along with the image creation process, and the possible security agents should be cloud-aware by nature. (Cloud Security Alliance 2017, 85-90.)

5.4 Virtualisation security

Virtualisation security in cloud computing also follows the shared responsibility model and understanding the impact it has is mandatory for properly architecting and implementing security in the cloud. Virtualisation adds two new layers that need security controls: Security of the virtualisation technology itself, and security controls for the virtual assets. Compute, network and storage are all major virtualisation categories relevant to cloud computing. Compute typically refers to virtual machines. Networks can be virtual in multiple ways, from basic VLANs to full Software-Defined Networks (SDNs). Some of the most common forms of storage virtualisation include Storage Area Networks (SAN) and also Network-Attached Storages (NAS). (Cloud Security Alliance 2017, 91-98.)

For cloud service providers, there are some recommendations to ensure virtualisation security:

- Any underlying physical infrastructure that is used for virtualisation should be inherently secured
- Security isolation between tenants is very important
- The physical infrastructure and virtualisation platforms should be well defended from attacks or internal compromises
- All customer-managed virtualisation features should be offered with a secure-by-default configuration
- Customers should be offered sufficient security capabilities at the virtualisation layer to allow the customers properly secure their assets

(Cloud Security Alliance 2017, 99.)

Cloud users, on the contrary, should ensure at least the following concerning virtualisation:

- Virtualisation services must be configured properly according to the industry best practices and also to the guidance given by the cloud service provider
- For repository management and containers role-based access controls (RBAC) and strong authentication are both recommended
- Understand the capabilities the cloud service provider offers, and where the security gaps lie

(Cloud Security Alliance 2017, 100.)

5.5 Container security

Containers are portable environments where code can be executed providing an isolated user space that uses a shared kernel. These containers can be run on virtual machines or built directly on top of physical servers. Container security consists of several key areas, and the technology platform does not affect these areas that include:

- Assuring the physical infrastructure underneath is secure
- Assuring the management plane is secure
- Securing the image repository
- Building security into the tasks that are run inside the container

As a general guideline, the container management products used should have, at minimum, the support for strong authentication and role-based access controls. Also, the possibility for secure configurations that include isolated file systems,

processes and network access, should be also available. The security isolation capabilities must be clear for the involved parties. These capabilities must be studied before applying any configuration, and they are related to the container platform and also to the operating system underneath. Physical or virtual machines should be used in order to provide container isolation, and containers with the same security context should be grouped on the same physical or virtual hosts. To understand container security, one must have a tremendous amount of knowledge of operating system internals like memory, network port mapping, storage access and namespaces. (Cloud Security Alliance 2017, 97-100.)

5.6 Data security and encryption

Data can be in three different states; in motion (being transmitted over the network), in use (being processed somewhere) or at rest (being on persistent storage), and security considerations apply to all these three states, but mostly to the data in motion and at rest (CSCC 2016, 14; Dotson 2019, 20). Data security is related to information and data governance and is a key tool to enforcing these areas (Cloud Security Alliance 2017, 119). Especially, when public networks or similar weakly protected networks are used, encryption is often the only way to ensure the confidentiality and integrity of classified information. As it is extremely difficult to substitute encryption with any other controls, it is crucial to evaluate the encryption methods and use cases thoroughly. In cloud services, encryption is also often used to separate the customers' data from each other in situations where the physical platform is shared between the customers, and it also ensures the reliability when data is being destroyed. (Traficom 2020, 43.) The ISO/IEC 27000 series standards have some common approaches regarding the security of data. The standards NIST SP 800-57 and ANSI X9.69 and X9.73 are good tools for helping establish good security with encryption and key management (CSCC 2016, 15; Cloud Security Alliance 2017, 125).

According to Cloud Security Alliance, data security controls in the cloud tend to fall into three different categories:

- Controlling what data goes where

- Protecting and managing the data
- Information lifecycle management security

The data in the cloud is most commonly stored using some of these storage technologies; object storage, volume storage, database, application or platform. Object storage is similar to a filesystem and volume storage is a virtual hard drive for virtual machines. Databases are usually supported in many forms, and both commercial and open source databases can be used. An example of an application or a platform storage would be a content delivery network (CDN), or files stored in SaaS. (Cloud Security Alliance 2017, 119-120.)

5.6.1 Securing the data in motion

The first step before transferring any data to the cloud should be defining the policies that control what data is allowed to be transferred and where, and these policies should comply with the organisation's baseline security requirements. The next step is to identify and start monitoring the key data respositories to detect all sorts of breaches and misuse scenarios. There are several utilities available to monitor the actual data transfers, such as Cloud Access and Security Brokers (CASB), URL filters and web gateways, and Data Loss Prevention (DLP) tools. To ensure the data is safely transferred to the cloud, in-transit encryption methods should be used, and this can be achieved, for example, using client-side encryption or network encryption (TLS / SFTP etc.). Transport Layer Security (TLS) is widely supported by the service provider APIs. HTTPS provides security for the regular connections from cloud service customers using the cloud services over the Internet, and VPNs with IPSec or SSL should be preferred among the customer's employees when connecting to the cloud service. (CSCC 2016, 16; Cloud Security Alliance 2017, 121-122.) When protecting data that has security classification, it is extremely important to implement encryption methods that have been reliably proved as secure. In addition to this, the threat level of the use environment must be evaluated. As an example, when accessing data over the Internet, the level of threat is considerably higher than in a situation where encryption is used to secure the data transfer between two physically protected and safe locations, or safe zones. (Traficom 2020, 43.)

The Internet, MPLS networks provided by the internet service providers, and the dark fibre connections (connections leased fibre optic cable (5G.co.uk no date)) are considered as public networks. Using radio frequency communications, such as WLAN or 4G, is seen as leaving the physically protected safe-zone and can therefore be compared to using a public network. In these situations, the classified information must be transferred properly encrypted and using the methods suitable for the situation, and the recipient must be identified in a secure way before allowing access to the transmitted data. When classified information is transferred inside the physically protected safe-zone and inside the correspondingly classified network, lower level encryption or unencrypted file transfer can be used, if the needed level of protection can be achieved using physical safety controls. (Traficom 2020, 44.)

5.6.2 Securing the data at rest

The core of data security controls consists of access controls and encryption. Within a cloud service, the data at rest and sensitive in nature should be encrypted. For encryption in cloud computing, multiple architectural approaches exist. These approaches incorporate encryption at some of these levels:

- Storage device level
- Agent based
- File system based
- Application level

To control the access to the data, Cloud Security Alliance recommends, that access controls should be implemented at minimum on three layers:

- Management plane
- Public and internal sharing controls
- Application level controls

An entitlement matrix should be created to document who can access what resources. The actual access control functions will vary based on the cloud service model and the service provider. (CSCC 2016, 16; Cloud Security Alliance 2017, 123.)

Available encryption methods are too fully dependent of the service provider, selected service model and application and deployment details. Two separate technologies exist; encryption and tokenisation. Encryption works by applying a mathematical algorithm that scrambles the data, and the data can then be only recovered through a decryption process with a corresponding key. Tokenisation works by replacing data with random values. Both the original version and the randomised version is then stored securely in a database and can be later recovered. Tokenisation works well in situations where the format of the data is important. (Cloud Security Alliance 2017, 123.)

An encryption system consists of three main components – data, key management and the encryption engine. As the name suggests, an encryption engine encrypts the data, and the key manager handles the keys needed in the encryption. IaaS, PaaS and SaaS environments all have their own encryption methods. In IaaS, volume storages and object and file storage can be encrypted. PaaS allows application layer encryption, database encryption, and other provider-managed layers in the application. SaaS, in the other hand, can incorporate any of the options present in IaaS and PaaS. SaaS specific options include provider-managed encryption and proxy encryption. In general – across all the service models – it is recommended to use provider-managed encryption and storage options. In addition, CASB should be also considered in SaaS deployments to monitor the data flows. (Cloud Security Alliance 2017, 123-128.)

5.6.3 Key management

For handling key management, four potential options exist:

- Hardware security module (HSM) or appliance
- Virtual appliance or software
- Cloud provider service
- Hybrid solution

Hardware security module uses a traditional hardware security module, or alternatively, an appliance-based key manager. A dedicated connection is used to deliver the keys to the cloud. Other options exist too – a software-based key manager in the cloud or a virtual appliance works as well. There is also yet

another option to use a key management service from the cloud service provider, but the SLAs and security model must be evaluated before selecting this option. Hybrid solution could be, for instance, a situation where a hardware security module is used to provide the root of trust for the keys. Application-specific keys could then be delivered to a virtual appliance residing in the cloud, dedicated to managing keys for its particular context. (Cloud Service Alliance 2017, 125.)

The increased security that can be achieved through encryption might be lost in situations where vulnerabilities in the key management can be used. PiTuKri requires that the governing processes for key management must be planned, implemented and documented. It should be also noted that the cloud service provider has always access to the data that is stored in its systems, in case the data is in readable format. Solutions such as BYOK (Bring Your Own Keys) or HSMs installed in the cloud service provider's data centre typically only limit – not prevent – the access to the data. (Traficom 2020, 44.) Nevertheless, using customer-managed keys is still recommended as it moves control over to the customer, despite the fact that the encrypted data can still be revealed with governmental orders. Dotson (2019) has listed some of the key management options the major cloud providers currently offer:

Provider	Dedicated HSM option	Key management service
Amazon Web Services	CloudHSM	Amazon KMS
Microsoft Azure	-	Key Vault (software keys)
Google Compute Platform	-	Cloud KMS
IBM Cloud	CloudHSM	Key Protect

Figure 24. Key management options. (Dotson 2019, 21.)

5.7 Example set of requirements for user identification – classified data involved

This last chapter of literature review aims to point out the amount of details that need evaluating when the used cloud service contains classified information. This case is not tied to any organisation in particular, but it assumes that the

organisation is governmental, and it regularly operates with some level of classified information. It assesses how the user identification to a cloud service should be set up in general. The evaluation was done using PiTuKri and Katakri. These requirements can be applied to networking equipment, servers, information systems, workstations and other terminal devices (Traficom 2020, 36):

1. All the users and administrators (both the service provider's and the customer's) must be identified and authenticated before they are allowed access to the classified information.
    1.1. Personal user accounts must be in use.
    1.2. All users must be identified and authenticated.
    1.3. A safe, well-known and reliable process must be in use for the identification and authentication.
    1.4. The user accounts will lock up in situations where too many failed consecutive identification attempts occur.
    1.5. The administrative credentials for the systems and applications are personal. In case it is not technically possible to achieve this, the shared credentials require pre-defined and documented controls that allow identifying the individual users.
    1.6. Strong authentication must be used that is based at least on two factors, for instance, password + token. The connection is encrypted appropriately using valid and standardised encryption methods and protocols.
        1.6.1. In case the authentication is done inside a physically protected safe zone, the authentication can be done using only a password. *In such situations, the users must have been instructed about the good security practices regarding passwords and the application monitoring system use must have minimum requirements for the password and force to change the password on a pre-defined basis.*
2. In situations where a connection is made outside the physically protected safe zone (for instance, between the cloud service provider's data centre and the customer's terminal device), the data and the traffic must be encrypted using methods the government officials have approved.
3. The terminal devices and systems (both the service provider's and the customer's) that are involved in offering the cloud service must be identified reliably before they are allowed to access to the classified information.

(Traficom 2020, 36.)

Controls presented in section 1 are needed when the processed information contains personal data, or it is classified as "Salassa pidettävä", TL IV & KV-R (KV-R means "RESTRICTED" on international level), or TL III. Controls in sections 2-3 are needed when the processed information is classified as TL IV & KV-R or TL III. (Traficom 2020, 36.)

According to Katakri, the controls in section 1 are sufficient when operating with information classified as ST IV. The only difference is that Katakri does not require strong authentication; a password is a minimum authentication requirement. More controls are required when the level of classified information involved is higher (ST II or ST III). (Katakri 2015, 40.) These further controls include:

4. The user authentication must be based on at least two factors.
5. The terminal devices must be identified in technical manner (device identification, 802.1X, or similar process) before allowing access to the network or the service, unless physical security controls are used to limit the area where the network or service is accessed. These physical controls can be, for instance, locating the server inside a locked device cabinet inside a technically protected safe zone that is approved by the government officials.

(Katakri 2015, 40.)

Overall, the controls are practically identical – the only difference is that the controls are presented slightly differently in both of the documents, and they apply to different sorts of classified information. However, securing an ST IV environment with controls in full presented in PiTuKri, for instance, is no security risk – on the contrary, the system would be even more secure. As PiTuKri states, using the criteria will always involve adapting the requirements to the corresponding use cases. Also, Katakari 2015 framework can be used to evaluate the areas belonging to the cloud customer. (Traficom 2020, 4.) With this in mind, using both sets of criteria in applicable situations when evaluating a cloud service will ensure good baseline security that allows processing classified information. Other frameworks and certifications can be also used with certain limitations to assure requirements set in PiTuKri are met (Traficom 2020, 5).

6 DISCUSSION

This chapter presents answers to the research questions and discusses the subject in general. In chapters through 6.1 to 6.3, the research questions are answered. Chapter 6.4 discusses briefly the reliability of this research, and chapter 6.5 focuses on the future, and which areas need further research.

6.1 What should governmental organisations take into account when planning to implement cloud computing?

The first goal of this research was to find out what governmental organisations should take into account when it is planning to implement cloud computing in general. It turned out that many of the steps that should be taken before engaging with a cloud service provider are universal – the same principles apply to both governmental and non-governmental organisations and can be also applied as such to the case organisation.

Cloud computing becomes more popular every day and there are many potential cloud service providers available. The current market leaders seem to be Amazon, Google and Microsoft with their cloud products, but also other companies like IBM, Dell Technologies and Hewlett-Packard are willing to take part in the competition. All three of these market leaders offer tremendous amount of capabilities and services that are built into the cloud – it is only up to the customer to decide which one to engage with. The cloud service providers itself offer some basic information about their services, and other public sources, such as the CSA STAR Registry, offer useful data about the providers and can work as an easy way for the customers to find information about the quality and security of the providers. No special formula exists that could be used to pick the most convenient provider for an organisation. The selection should be tailored according to the business, and a thorough due diligence and risk assessments are required. Certifications and standards provide a good starting point to start evaluating the candidates, and from the security perspective, the customers should look for cloud service providers with accredited certifications – for instance – from the ISO 27000 standards series. Solid reputation, state-of-the-art equipment and reliability are all important factors too. Further in the selection process things such as negotiating the contracts, SLAs, etc. will become important. Also, to avoid vendor lock-ins, exit planning is vital and must be done before signing a contract.

An important thing already in the planning phase – but especially after the contract with the service provider has been made – is for the cloud service customer to understand the effects of the shared responsibility model before progressing further with the implementation process. The responsibilities between the cloud service provider and the cloud service customer vary between the service models and deployment models, and variation occur also between the cloud service providers and the services they offer. The most important security consideration in all cloud projects is to know exactly everyone's responsibilities and the Cloud Security Alliance's Cloud Controls Matrix (CCM) provides a good starting point to begin evaluating requirements and compliance. For governmental organisations it is especially important to know precisely the responsibility boundaries, as classified information sets new requirements for the cloud environment that must be met. Also, things like where the data is stored and processed, and how personal data is handled, are key elements to consider for the governmental organisations to be able to comply with the requirements. VAHTI instructions, PiTuKri and Katakri should be used already before the implementation phase to evaluate the potential candidates, and to help in planning an appropriate cloud implementation. It is crucial to ensure the requirements set by classified information are met. All these findings can be applied to the case organisation too, and by using the principles presented in this research it is possible to start evaluating the cloud service providers, and eventually implementing cloud computing in a secure way.

6.2 What are the key elements to focus on in cloud security management and cloud security controls from the customer's perspective?

The second goal was to find out the key elements regarding cloud security management and controls. Managing and controlling the security in a cloud is different compared to a traditional data centre and requires new approaches from the organisations. At this point, differences emerge between governmental organisation and non-governmental organisations – and especially in situations, where classified information is involved. As the security in a cloud is an incredibly broad topic, this research focused more on the relevant high-level technical areas

from the customer's perspective, but also governance and compliance were briefly studied.

Managing the security in a cloud is also based on understanding the shared responsibilities – in other words – who is exactly responsible and of what. Outsourcing services to a third party will always introduce risk, and currently the top threats in cloud computing are data breaches, misconfiguration and inadequate change control. When selecting the service and deployment models, it is extremely important to completely understand how they affect the responsibilities, governance, risk management and information security, as all these areas have direct impact on the overall security of the cloud. In IaaS model, a plenty is on the responsibility of the customer, and on the contrary, in SaaS, the service provider in responsible for almost everything. In addition, knowing full compliance obligations is also necessary for the cloud service customers before further implementing cloud computing. Auditing and incident response processes should be in place, and the cloud service customers should be aware of any legal issues moving the data to the cloud might create. Ensuring that all the policies the organisation has extends to the cloud, too, might not always be easy, but for maintaining good security, it is mandatory.

Using controls to ensure the security in a cloud involves both parties, the cloud service provider and the cloud service customer, to do their part in areas they are responsible for. From the cloud service customer's perspective, there are several key areas to focus on:

- Management plane security
- Identity and access management
- Infrastructure and network security
- Data security and encryption

Again, the responsibilities vary along the service and deployment models. In IaaS and private cloud deployments, all these need actions from the cloud service customer, but in public SaaS deployments, only a few areas are left to the cloud service customer to handle. Identity and access management relies on the principle of least privilege, and standards such as SAML, OAuth and OpenID are significant factors in that area. Federated identity is an important concept, and as

a single security feature, multi-factor authentication (MFA) is one of the most effective features. In network security, the traditional perimeter-based network security controls might be ineffective. Segmenting the networks in one way or another – most preferably physically – is vital in cloud environment. Also cloud firewalls should be applied on a per-workload basis. To ensure the security of the data, encryption is an absolutely mandatory tool for that purpose. Encryption provides ways to secure the data in many situations, be it securing a remote connection to a cloud service, or securing data residing at the cloud service. TLS, HTTPS, and VPNs with IPSec or SSL are common methods of protecting the data in motion, and different forms of encryption or tokenisation can be used to secure the data at rest. The last important factor in data security is the key management; poorly designed key management can compromise the security gained through encryption at once. In key management, solutions like hardware security modules (HSMs), virtual appliance or software, cloud provider service, or a hybrid solution can be used.

All these previously presented factors are relevant to both governmental and non-governmental organisations. When the governmental perspective is introduced, differences start to show up, and a slightly different approach is needed. To begin managing and controlling the cloud security in governmental environment, the most important questions to begin with are:

- Have the systems and applications been evaluated and classified appropriately that are going to be used in a cloud?
- Is classified information involved – and if yes – which sort?

The answers of these questions will form the base level of security requirements that must be at least met in the cloud environment. All the guidance and requirements rely on this information, as the Finnish laws direct how certain types of information must be handled. By using VAHTI instructions, PiTuKri, Katakri and possibly other relevant standards and industry best practices – which these documents also offer as an option – the cloud environment can be designed and operated accordingly and securely. These mentioned documents are based on the international standards but are designed in a way that they can be used in securing governmental ICT systems to comply with the Finnish laws. The

baseline of managing and controlling the security in governmental cloud environment is to look for what sort of systems, applications, and classified information are involved, and then plan and implement the cloud services according to and by the instructions of the previously mentioned documents and standards.

6.3 Is there a way to select and list the best security practices to help securely implement cloud computing in this type of situation?

The third and final goal of this research was to find out whether there is a way to collect a list of best practices that could be used in securing a cloud implementation in this type of situation. Industry best practices do exist – and in great numbers. These best practices are extremely useful, but they must be used accordingly; organisations and cloud environments are all different, and therefore require evaluating which set of best practices and implementation guidance to follow. Neither there is any reference architecture that would fit every organisation. Therefore, it is not possible to list the best practices that would apply everywhere, or they would have to be very generalised in manner, and as such would not be very useful. When the scope is narrowed down from all governmental organisations in general to the case organisation only, listing the best practices would become possible, but nevertheless relevant. A more convenient way would be to list the sets of best practices to follow, instead of listing the best practices; it would make no sense to re-write the well-written instructions all over again. The key is to know which ones to follow. For all governmental organisations in general – and for the case organisation, too – the previously mentioned VAHTI instructions, PiTuKri and Katakri provide excellent security guidance for implementing cloud computing, but they also contain links to other industry best practices too that can help to analyse the situation even better.

As a generalisation, the ISO 27000 series sets of standards and NIST's security-related publications provide a great amount of detailed information about securing the cloud environment, and practically any organisation can refer to

these in their implementations. In governmental organisations, these same sets of standards and publications work, but a more practical way is to use the guidance written by Finnish authors, as they comply with the Finnish laws, and the scenarios used as examples in these documents represent better the environments a typical governmental organisation might have. This makes it also a lot easier for the governmental organisations to follow the instructions and build their systems as required by these documents and the Finnish laws. Should no solution to some specific problem exist in these documents, the ISO 27000 series and NIST's publications can always be used as a reference.

6.4 Reliability analysis

If it is possible to reproduce the results of a study using similar methodology, then the research is considered reliable. As a term, 'reliability' is generally used for testing and evaluating a quantitative research, but the idea is very often used in all kinds of research. Reliability and validity are two factors that should be used when analysing the results and judging the quality of the study. (Golafshani 2003, 4-7.) At the beginning of this research it was not entirely clear how all the necessary information would have to be gathered, and which sorts of methods it would require, and mixed methods research (case research, to be more specific) offered the possibility to start the research without ruling out any options, as there were doubts that the limitations could have potentially affected the quality of this research. Later on, it turned out that a traditional qualitative research would have actually fitted better this research. However, the researcher thought that the reliability of this research would not be compromised even by staying with the selected research method, as the methods used in this research were practically identical to a traditional qualitative research, and case research is relatively close to this.

In chapter 1.4, the literature review process is described. The material used in this research included books, online sources and various standards. For cloud computing in general – and for cloud security in general – material was available in many forms, but research material and studies concerning cloud

implementations in governmental organisations was not widely available, even in international context. This meant that the research had to be based almost entirely on different recommendations and standards, and it was up to the researcher to decide which areas to focus on in more detail. It is highly possible that a different researcher would pick and highlight different details in the same situation, but it does not necessarily make this research unreliable – the bigger picture would still remain the same, as the standards and recommendations would have to be used to answer the research questions. In addition, using such material has positive impact on the validity of the research. However, as many of the areas concerning cloud security had to be discussed using only high-level terms and generalisations – due to the incredibly wide topic – there is a chance that the terms overlap and get mixed up. As a cause of this, the reliability and overall quality of this research might be affected. Nevertheless, a research with this perspective is unique, and as such should provide some useful information for governmental organisations with plans to implement cloud computing.

6.5 Future research

Cloud computing is evolving at an incredible rate, and new solutions and ways to implement cloud computing are introduced continuously. The governmental organisations need to follow this trend, too, due to the many benefits the cloud offer, but at the same time maintain the high security standards in their systems.

This research was very generalised in nature and looked for high-level solutions to the security issues governmental organisations may face – going into more specific details would not simply have been possible within the scope of this research.

In the future, it would be important to start to investigate the various cloud service providers in more detail. Which of the current cloud service provider would be the most competent to answer the security and compliance requirements of governmental organisations, or are there several? In addition – either after, or combined with this research, another important problem to be studied: How to

securely implement an X-as-a-Service environment in governmental organisations using the most suitable cloud service provider? The latter research could be also tied to a specific organisation, instead of organisations in general, and in that context have a more detailed approach.

7 CONCLUSION

The ultimate goal of this research was to find out how to securely begin implementing cloud computing in governmental organisations. In Finland, a similar research from this particular perspective has not been done, or it is not available for the public. A recent interview given by Finnish Brigadier General Mikko Heiskanen supports the latter opinion, as he stated that the Finnish Defence Forces have recently begun re-evaluating the possibility of using cloud services to support their operations (Kuka puolustaa Suomea? 2020). On international level, there are several researches that evaluate somewhat similar problems, but in slightly different context. Many of the cloud security related research addressed more specific and detailed problems and they are not related to the governmental organisations in any way. Reasons for this remain unclear, but it is possible, that this sort of research is not meant for the public to see – especially the researches that go into more detail and as such have the potential to cause damage to the governments when exposed to audience with illegal intentions.

The research relied entirely on the currently available literature, standards, and regulations, and it was very generalised in nature, as cloud computing – even in this context – is a colossal topic to be studied. Topics discussed in this paper were cloud computing and cloud service providers in general, the current threats and risks in cloud computing, and managing and controlling the security in a cloud. All these topics were discussed in general, and the perspective of the governmental organisations was introduced usually after what was more an overall perspective to the discussed topic.

Understanding that the cloud environment always includes shared responsibilities that shifts as the service models and deployment models are altered, and also acknowledging where the responsibility boundaries lie, are key elements in managing the security of a cloud. Also, controls concerning user and access management, and data security and encryption, form the basis of technical security controls in a cloud. Knowing the classifications of the systems and processed data is the fundamental idea for the governmental organisations before cloud computing can be implemented.

For governmental organisations, cloud computing introduces many new possibilities, but also security challenges. The importance of following the rapidly growing trend of cloud computing cannot be argued, but as the methods and techniques behind data breaches become more and more sophisticated, it is absolutely vital – especially for the governmental organisations – to completely understand what is exactly about to be moved to the cloud, and recognising where the greatest security risks lie. However, Brigadier General Mikko Heiskanen is certain that even the Finnish Defence Forces will inevitably implement cloud computing in the future that will allow them to process data with security classification (Turvallisuusluokintamerkintä) in the cloud, and mentions, that countries similar to Finland have already accomplished this. (Kuka puolustaa Suomea? 2020).

As the area of research was extremely broad, this research was not able to discuss all areas related to the subject, nor could it analyse the technical solutions in greater detail. However, it succeeded in finding out the key areas the governmental organisations should focus on when they are planning to implement cloud computing, and it has also the potential to be used as an introduction to cloud computing for the governmental organisations from a security perspective.

REFERENCES

5G.co.uk. No date. What is dark fibre and why is it essential to 5G? WWW document. Available at: https://5g.co.uk/guides/what-is-dark-fibre/ [Accessed 10 August 2020].

Ali, O., Osmanaj, V. 2020. The role of government regulations in the adoption of cloud computing: A case study of local government, Computer Law & Security Review: The International Journal of Technology Law and Practice. Research article. Available at: https://doi.org/10.1016/j.clsr.2020.105396 [Accessed 26 June 2020].

Amazon. No date. Types of Cloud Computing. WWW document. Available at: https://aws.amazon.com/types-of-cloud-computing/ [Accessed 2 July 2020].

Amazon. No date. What is cloud computing? WWW document. Available at: https://aws.amazon.com/what-is-cloud-computing/ [Accessed 29 June 2020].

Astri, L. 2015. A Study Literature of Critical Success Factors of Cloud Computing in Organizations. Research article. Available at: https://doi.org/10.1016/j.procs.2015.07.548 [Accessed 26 June 2020].

Cloud Industry Forum. No date. 8 criteria to ensure you select the right cloud service provider. WWW document. Available at: https://www.cloudindustryforum.org/content/8-criteria-ensure-you-select-right-cloud-service-provider [Accessed 10 July 2020].

Cloud Security Alliance. 2017. Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. WWW document. Available at: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/ [Accessed 15 July 2020].

Cloud Security Alliance. 2020. Top Threats to Cloud Computing: Egregious Eleven. WWW document. Available at: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven [Accessed 15 July 2020].

Cloud Security Alliance. No date. CloudTrust Protocol Data Model and API. WWW document. Available at: https://cloudsecurityalliance.org/artifacts/cloudtrust-protocol-data-model-and-api/ [Accessed 15 July 2020].

Cloud Security Alliance. No date. CSA STAR Registry. WWW document. Available at: https://cloudsecurityalliance.org/star/registry/ [Accessed 15 July 2020].

Cloud Security Alliance. No date. Overview. WWW document. Available at: https://cloudsecurityalliance.org/about/ [Accessed 22 July 2020].

Cloud Standards Customer Council. 2016. Cloud Security Standards: What to Expect & What to Negotiate Version 2.0. WWW document. Available at: https://www.omg.org/cloud/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf [Accessed 11 August 2020].

Criminal Sanctions Agency. 2020. Turvaluokiteltujen ja muiden salassa pidettävien asiakirjojen käsittelyohje rikosseuraamusalalla (9/004/2010). WWW document. Available at: https://www.rikosseuraamus.fi/fi/index/seuraamukset/saannokset/maarayksetjaohjeet/turvaluokiteltujenjamuidensalassapidettavienasiakirjojenkasittelyohjerikosseuraamusalalla90042010.html [Accessed 23 July 2020].

Dotson, C. 2019. Practical Cloud Security. Sebastopol, CA 95472: O'Reilly Media, Inc.

Encyclopedia.com. 2020. Classified Information. WWW document. Available at: https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/classified-information [Accessed 23 July 2020].

ENISA. No date. Glossary. WWW document. Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary [Accessed 14 July 2020].

Fatima, S., Ahmad, S. 2019. An Exhaustive Review on Security Issues in Cloud Computing. Research article. Available at: http://doi.org/10.3837/tiis.2019.06.025 [Accessed 26 June 2020].

Finlex. No date. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa. WWW document. Available at: https://www.finlex.fi/fi/laki/alkup/2010/20100681 [Accessed 23 July 2020].

Golafshani, N. 2003. Understanding Reliability and Validity in Qualitative Research. Research article. Available at: http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf [Accessed 17 August 2020].

Google. No date. What is cloud computing? WWW document. Available at: https://cloud.google.com/what-is-cloud-computing [Accessed 29 June 2020].

Greene, J., Caracelli, V. 1997. Defining and Describing the Paradigm Issue in Mixed-Method Evaluation. Research article. Available at: https://doi.org/10.1002/ev.1068 [Accessed 8 June 2020].

Hastings, R. 2014. Making the most of the cloud: how to choose and implement the best services for your library. Maryland: Scarecrow Press, Inc.

Herrasmieshakkerit. 2020. Kuka puolustaa Suomea? Vieraana prikaatinkenraali Mikko Heiskanen | 0x08. Interview. Available at: https://www.f-

secure.com/fi/business/podcasts/herrasmieshakkerit [Accessed 1 September 2020].

IBM. 2011. Multi-customer, multi-tenancy considerations. WWW document. Available at: https://www.ibm.com/blogs/cloud-computing/2011/07/29/multi-customer-multi-tenancy-considerations/ [Accessed 2 July 2020].

ISO. No date. ISO/IEC JTC1 INFORMATION TECHNOLOGY. WWW document. Available at: https://www.iso.org/isoiec-jtc-1.html [Accessed 5 August 2020].

ISO/IEC 27002. Second edition 2013-10-01. Information technology – Security techniques – Code of practice for information security controls.

ISO/IEC. No date. About. WWW document. Available at: https://jtc1info.org/about/ [Accessed 5 August 2020].

Johnson, R., Onwuegbuzie A., Turner, L. 2007. Toward a Definition of Mixed Method Research. Research article. Available at: https://journals.sagepub.com/doi/10.1177/1558689806298224 [Accessed 8 June 2020].

Kananen, J., Makkonen, T. 2015. A guide for conducting qualitative and quantitative research online. Publications of JAMK University of Applied Sciences -series. Jyväskylä: JAMK University of Applied Sciences.

Katakri. 2015. Tietoturvallisuuden auditointityökalu viranomaisille. WWW document. Available at: https://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille [Accessed 5 August 2020].

Lansling, J. Siegfried, N., Sunyaev, A., Benlian, A. 2019. Strategic signalling through cloud service certifications: Comparing the relative importance of

certifications' assurances to companies and consumers. Research article. Available at: https://doi.org/10.1016/j.jsis.2019.101579 [Accessed 11 July 2020].

Microsoft. 2019. Shared responsibility in the cloud. WWW document. Available at: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility [Accessed 17 July 2020].

Microsoft. No date. How to choose a cloud service provider? WWW document. Available at: https://azure.microsoft.com/en-us/overview/choosing-a-cloud-service-provider/ [Accessed 10 July 2020].

Microsoft. No date. What are the different types of cloud computing services? WWW document. Available at: https://azure.microsoft.com/en-us/overview/types-of-cloud-computing/ [Accessed 2 July 2020].

Microsoft. No date. What is cloud computing? WWW document. Available at: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/ [Accessed 29 June 2020].

Mthunzi, S., Benkhelifa, E., Bosakowski, T. et al. 2019. Cloud computing security taxonomy: From an atomistic to a holistic view, Future Generation Computer Systems. Research article. Available at: https://doi.org/10.1016/j.future.2019.11.013 [Accessed 26 June 2020].

NIST. 2017. About NIST. WWW document. Available at: https://www.nist.gov/about-nist [Accessed 22 July 2020].

NIST Special Publication 500-292. 2011. NIST Cloud Computing Reference Architecture. WWW document. Available at: https://www.nist.gov/publications/nist-cloud-computing-reference-architecture [Accessed 2 July 2020].

NIST Special Publication 500-322. 2018. Evaluation of Cloud Computing Services Based on NIST SP 800-145. WWW document. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf [Accessed 2 July 2020].

NIST Special Publication 800-61 Revision 2. 2012. Computer Security Incident Handling Guide. WWW Document. Available at: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final [Accessed 11 August 2020].

NIST Special Publication 800-144. 2011. Guidelines on Security and Privacy in Public Cloud Computing. WWW document. Available at: https://www.nist.gov/publications/guidelines-security-and-privacy-public-cloud-computing [Accessed 10 July 2020].

NIST Special Publication 800-145. 2011. The NIST Definition of Cloud Computing. WWW document. Available at: https://csrc.nist.gov/publications/detail/sp/800-145/final [Accessed 29 June 2020].

Peng, G.C., Nunes, J.M.B., Annansingh, F. 2011. Investigating information systems with mixed-methods research. Research article. Available at: http://eprints.whiterose.ac.uk/74737/ [Accessed 26 June 2020].

Petre, I.A., Zota, R. 2014. An Overview of the Most Important Reference Architectures for Cloud Computing. Research article. Available at: https://www.researchgate.net/publication/279234234_An_Overview_of_the_Most_Important_Reference_Architectures_for_Cloud_Computing [Accessed 7 July 2020].

Samani, R., Honan, B., Reavis, J., Jirasek, V. 2015. CSA Guide to Cloud Computing. Implementing Cloud Privacy and Security. Waltham: Elsevier Inc.

Stiennon, R. 2019. Secure Cloud Transformation: The CIO's Journey. Birmingham (Michigan): IT-Harvest Press.

Subashini, S., Kavitha, V. 2010. A survey on security issues in service delivery models of cloud computing. Research article. Available at: https://doi.org/10.1016/j.jnca.2010.07.006 [Accessed 15 July 2020].

Sun, P. 2020. Security and privacy protection in cloud computing: Discussions and challenges, Journal of Network and Computer Applications (2020). Research article. Available at: https://doi.org/10.1016/j.jnca.2020.102642 [Accessed 26 June 2020].

Traffic Management Finland. No date. Traffic Management Finland in brief. WWW document. Available at: https://tmfg.fi/en/tmfg/traffc-management-finland-brief [Accessed 26 June 2020].

Traficom. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). 2020. WWW document. Available at: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf [Accessed 31 July 2020].

VAHTI. 2012. Teknisen ICT-ympäristön tietoturvataso-ohje. WWW document. Available at: https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-32012-teknisen-ympariston-tietoturvataso-ohje [Accessed 22 July 2020].

ZDNet. 2020. Top cloud providers in 2020: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players. WWW document. Available at: https://www.zdnet.com/article/the-top-cloud-providers-of-2020-aws-microsoft-azure-google-cloud-hybrid-saas/ [Accessed 14 July 2020].