jamk.fi

Self-assessment of security in cloud deployment

Pinja Koskinen
Vesa Simola

Master's thesis
April 2019
School of Technology, communication and transport
Master's Degree Programme in Information Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Koskinen, Pinja Simola, Vesa	Master's thesis	April 2019
		Language of publication: English
	Number of pages	Permission for web publication: No

Title of publication
Self-assessment of security in cloud deployment

Master's Degree Program in Information Technology, Cyber Security

Supervisor(s)
Saharinen, Karo
Kokkonen, Tero

Assigned by

Abstract

Increasing number of services running on top of outsourced cloud environments has led to changes in the security landscape. These changes have created a situation where extra care is to be applied in order to ensure that the services continue to run securely. This thesis aims to find the key points organization should take into an account during the lifecycle of service running in the cloud. The result - a self-assessment tool - aims at being an easily manageable checklist which can be used to identify, acknowledge and also to limit the dangers posed by the threats tied especially to the cloud environments.

The self-assessment tool is not meant as a replacement for other audit criterion; its purpose is to define the set of important questions to ask, written especially from the perspective of running services on top of outsourced cloud environments.

Research problem of this thesis is the challenge of identifying the threats closely related to the cloud. The research method used is a literature review; trying to find literature covering the topic either directly or by means of applying what has been written for general security and continuity while adapting it to the context of the cloud. The latter method was required as the amount of literature directly related to auditing cloud deployments was found scarce.

Primary result of this thesis is that seventeen issues were identified as topics for discussion concerning cloud deployment. It is obvious that anyone could add dozens more questions, especially for special needs of different types of businesses and data, but these can be tackled in more detail using specific audit criterion or following the relevant regulation.

Keywords/tags (subjects)
Cloud security, outsourcing, business continuity, self-assessment, audit

Miscellaneous (Confidential information)

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Koskinen, Pinja Simola, Vesa	Opinnäytetyö, ylempi AMK	Huhtikuu 2019
		Julkaisun kieli Englanti
	Sivumäärä	Verkkojulkaisulupa myönnetty: Ei

Työn nimi
Pilviympäristön tietoturvallisuuden itsearviointi

Tutkinto-ohjelma
Master's Degree Programme in Information Technology, Cyber Security

Työn ohjaaja(t)
Saharinen, Karo
Kokkonen, Tero

Assigned by

Tiivistelmä

Yhä yleistyvä Internet-palveluiden tuottaminen pilvipalveluympäristöillä on muuttanut tietoturvanäkökohtia huomattavasti. Pilvipalveluiden luonteen vuoksi palveluiden tietoturvatason ylläpitäminen vaatii uusia näkökulmia ja teknologioita. Opinnäytetyössä pyrittiin löytämään pääasiat, jotka pilvipalveluita käyttävän organisaation tulisi huomioida palvelun elinkaaren aikana. Työn lopputuloksena syntynyt itsearviointilomake tarjoaa hallittavan kokoisen tarkistuslistan asioista, joiden avulla organisaatio voi tunnistaa, käsitellä ja myös hallita tämän uuden kentän tuomia uhkia.

Itsearviointilomake ei ole tarkoitettu varsinaiseksi auditointikriteeristöksi, vaan sen on tarkoitus kysyä kysymyksiä keskeisimmistä pilvipalveluille tyypillisistä piirteistä keskittyen erityisesti operointiin käyttäen julkisia pilvipalveluita.

Opinnäytetyön tutkimusongelma oli löytää erityisesti pilvipalveluita koskevat uhat. Työssä on käytetty tutkimusmenetelmänä kirjallisuuskatsausta sekä pilvipalveluihin liittyvillä hakutermeillä, että yleisillä turvallisuuteen ja jatkuvuuteen liittyvillä termeillä, joiden tulokset on sopeutettu erityisesti pilvipalveluympäristöön. Jälkimmäisen hakusanavalinnan tarpeellisuus korostui pilvipalveluihin liittyvän materiaalin rajallisuuden vuoksi.

Työn varsinainen tulos on itsearviointilomakkeen seitsemäntoista kohtaa, jotka löydettiin tärkeimmiksi pilvipalveluita koskeviksi aiheiksi. Koska pilvipalvelut ovat hyvin heterogeeninen ympäristö erilaisine palveluineen, datoineen ja alustoineen, voisi kysymyspatteristoa laajentaa huomattavasti. Tähän on kuitenkin olemassa esimerkiksi erilaiset tapauskohtaiset kriteeristöt, lainsäädäntö ja ohjeet, joilla tarkistuslistaa voi laajentaa.

Avainsanat (Asiasanat)
Tietoturva pilviympäristössä, ulkoistus, liiketoiminnan jatkuvuus, itsearviointi, auditointi

Muut tiedot (Salassa pidettävät liitteet)

Contents

1 Introduction

1.1 Background of the study

The symbol of a cloud in network and software diagrams has been used for many years to indicate a myriad of details concerning message flows, protocols and communication across a network. This abstraction has since evolved to include computing, storage and applications, both virtual and physical. New flexible cloud capabilities are emerging regularly, better yet at lower costs using pay-per-use models. With these new developments comes the increased security, privacy and IT-governance challenges. (Jamsa 2012)

One of the key aspects in this thesis is the concept of security in cloud context, security being defined as a process of maintaining sufficient level of perceived risk. (Bejtlich 2004.) In their paper ”Cloud computing and security”, Sun, Pan and Bertino give the following definition of cloud computing that gives another insight to the meaning of cloud computing and the inherit security aspects therein: Cloud computing is generally built from hardware and software components residing in one or more data centers within a single organization and used for sharing resources of those data centers among several customers or services. To put it another way, cloud computing is similar to a large pool of resources that are abstracted and virtualized to provide computing, storage, applications and services delivered from the shared pool. Given that the pooling of resources is so concentrated and the architecture to deliver this service is so complex it is a given that there are several matters that need to be investigated from technological and management perspectives when it comes to cloud computing security. Examples of these areas to investigate include security architecture model, data security, cloud computing encryption, privacy protection, access control and authentication, virtualization security and others such as customer isolation and cross-domain service security. (Sun, Pan & Bertino 2018)

There is seemingly some consensus that by placing all customer data and services in a cloud would mean that a successful attacker could gain access to large quantities of confidential information, meaning that the risk of data loss as a result of a security breach is higher in cloud than in traditional enterprise data centers. This idea has its

basis in the thinking that the cloud service provider and its infrastructure are more lucrative targets than a traditional data center. On the other hand, there is a consensus that the cloud can be more secure than a traditional data center, the reasoning being that it is easier to protect larger quantities of services in fewer locations and it would be easier to use the latest technologies of protection in a centralized manner. Furthermore, given that costs tend to increase as more security is implemented, economics of scale, more consistent deployments, centralized log management and such consolidated measures help to reduce the cost of security compared to legacy server farms. (Bond 2018.) To add insult to injury, statements such as ”the cloud is risky” do not deliver any useful security information. Instead, these kinds of statements should include probabilities and measured impacts to give one any value when making decisions. (Pompon 2016.) This controversy of cloud computing is further illustrated by Mather, Kumaraswamy and Latif in their book Cloud security and privacy. They do it using the familiar ”mind the gap” sign seen and heard in the London subway. The principle is that while one constantly hears the choir of ”cloud computing good”, one also gets to hear the ”could security bad” verse. Yet it is apparently not clear what is wrong with the cloud security. (Mather, Kumaraswamy & Latif 2009)

Aforementioned problem landscape is further fuzzed by the fact that each industry has its particular characteristics and risks. This means that the level of tolerance for risks can differ significantly from one field of industry to another, an example of this could be the banking sector that is concerned with the exposure of their records in the cloud. Whereas other industry might decide that the benefits of cloud outweigh the potential risks, which might mean they are more forthcoming towards cloud. This means that the security needs to be viewed as relative to what customer has at the moment and on the other hand, what the cloud service provider can produce. (Ko & Choo 2015)

This thesis tries to find answers to what some of that might mean and what should be considered when evaluating one’s cloud posture.

1.2 Objective of the study: creating criteria-based self-assessment

Criteria-referenced self-assessment is a concept where an individual or organization gathers information about the abilities or progress, compares this data to explicitly defined criteria or standards and then amends or improves their practices and understanding of the topics based on the results. The purpose of the self-assessment is to detect areas where the organization or individual is strong and on the other hand, to find weaknesses to improve on. It is stated that feedback plays a crucial role in learning. The lack of feedback in education environment is largely due to the fact that few teachers have the resources to regularly respond to the work done by students. Luckily, research shows that pupils themselves can be effective origins of feedback via means of self-assessment. (Andrade & Valtcheva 2009)

There is some research suggesting that just by exposing the students to rubric may improve students' insight on the subject matter and to increase the quality of their work. However, even better results can be gained by actively engaging the student to utilize the rubric to self-assess their work. (Andrade & Valtcheva 2009.) Similarly to this, the authors hope that this self-assessment criterion created as a result of this thesis would be usable and approachable enough to be similarly useful. Therefore, the ultimate goal of the study was to create a self-assessment questionnaire for cloud computing security. The motivation for this is that, similarly to the feedback scenario in education, currently there is not all that much regulation to reflect on that addresses the cloud specific issues and risks: likely this will take time for the standards to adjust. (Halpert 2011.) This is also true when it comes to the widely accepted and adopted standards and guidelines currently available for cloud services. (Ko & Choo 2015)

1.3 Methods of the study

By answering a question such as ”what kind of information is this research trying to come up with?”, the authors came up with a reasonable research method (Vilkka 2015). The answer to that question and hence the goal of this thesis is to come up with a self-assessment criterion to evaluate one's cloud posture in terms of security. To this end, the research was done by first conducting qualitative research utilizing

the literature available to the authors from the Finnish Theseus service (Arene ry - the Rectors' Conference of Finnish Universities of Applied Sciences), EPFL library (École polytechnique fédérale de Lausanne, BEAST collection) and the Finna service (free access to material from Finnish museums, libraries and archives). The writers of this thesis and, on the other hand, the topics other researchers had found these materials noteworthy, and the research resulted in reasonable background information to use as a basis for the self-assessment. IETF RFCs were also reviewed, mainly from the standards track in addition to some white papers produced by commercial entities. White papers were mostly select based on completely subjective understanding of the credibility and mostly used as a filling material on topics where not enough literature was found using reasonable effort. Search terms used were: cloud security, change management, network security, log management, data hiding, key management, access management, security standards, life cycle management, privacy management, data governance. In addition to those, authors used search terms such as nuclear power plant security was used to find documentation that was not directly related to cloud security but provided more specific looks to the other fields of security.

The practical part of the research was to actually implement the self-assessment questionnaire that is handled as a separate attachment of this thesis. This assessment is based on the findings of the above literature review.

2 What is cloud

In this chapter, basic concepts of the cloud are explained. In addition, also cloud types and deployment methods are explained. These topics are a must to understand the different technological and security aspects concerning the cloud infrastructure.

2.1 General overview of the cloud

Cloud service is generally understood as a product that consists of services hosted on the Internet. This could include servers, networks, storage systems, software applications and other services. These products could be running anywhere in the world, in

a distributed manner. Cloud allows users to utilize applications without modifications, or access to their locally available files and services can be reachable from any location within the Internet. In addition, in some cases users may share files, data and information between several systems and other users via the cloud infrastructure. (Suikkanen 2013, 8)

To name a few higher level motivators that might push companies towards cloud, the following can be considered (Mather, Kumaraswamy & Latif 2009):

- Initial investment is more manageable than buying a complete set of infrastructures
- Economies of scale provided to the cloud service provider help to keep costs and delivery times down.
- Open standards by open source software are acting as the foundation of the cloud solution.
- Sustainability via means of service provider having already done the major capital investments.

All of the above are beneficial elements of the different categories of different cloud categories. Cloud community uses the following models to categorize their services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). (Ahlgren 2012, 7.) Cloud hosting can be carried out in few different manners: Private cloud, public cloud, hybrid cloud and community cloud (Suikkanen 2013). Aforementioned deployment and hosting models are discussed next.

2.2 Cloud hosting types

As a concept, cloud computing can have multiple hosting types differing from each other that can be seen as ways of delivering the computing service. Some of the different characteristics of these hosting types are described next as they impact their ideal use cases.

2.2.1 Public cloud

Public cloud is hosted in the service provider facilities and all maintenance, modifications and upgrades are carried out by the service provider, meaning that the customer has no control over the hosted infrastructure. One exception to this is the fact that certain service providers give their customers the options of choosing from several geographical locations from which to run their service. (Ahlgren 2012, 12.) The economy of scale can mean that the public cloud can offer efficient storage, compute and connectivity at reasonable price. This can be especially true with the charging models where customers are required to pay only for the service they require and use. (Suikkanen 2013, 11)

2.2.2 Private cloud

Private cloud is understood as a service that is being operated by a service provider as a service to be used by a single customer. Private cloud tends to use the same techniques as public cloud; however, the techniques are configured to help the customer organization be more responsive and efficient in their IT resource usage than with the traditional IT operation model. (Suikkanen 2013, 11)

There are generally two types of private clouds, ones that are hosted on the customer premises and then there are those hosted on a service provider's infrastructure. It should be noted that while cloud infrastructure could be externally hosted, it is still considered a private cloud if the infrastructure is solely used by a single customer organization. (Ahlgren 2012, 10.) Infrastructure on a public cloud on the other hand is shared among the various customers of a service provider (Stamou 2014, 6).

2.2.3 Hybrid cloud

Combinations of the public and private cloud are called hybrid clouds. These clouds can tie the infrastructures of a private and public cloud together and allow the customer to extend their capacity beyond what is available in the private cloud by additionally utilizing the public cloud on time of need. This is called cloud bursting, mean-

ing that the customer uses private cloud under normal circumstances; however, during peak load some or all parts of the service can be transported to public cloud. (Ahlgren 2012, 13)

2.2.4 Community cloud

The fourth and final form of cloud is the community cloud. Community cloud is a multi-tenant cloud setup utilized by several organizations that may share a common interest or computing concerns. Such concern could come in a form of a compliance requirements, audit requirements or that the organizations require high-speed access to common data, for example research organizations working on a common project. (Suikkanen 2013, 12)

2.3 Cloud deployment models

Cloud deployment models have significant strengths and weaknesses across the three different deployment modes. From a commercial standpoint, these models provide greater flexibility and try to make IT more accessible to more consumers. (Winkler 2011.) Following are the rough characteristics of each of the three models.

2.3.1 Infrastructure as a service

Infrastructure as a service (IaaS) is the most basic service in the cloud landscape; it generally means an offering consisting of infrastructure, physical or virtual machines and other related resources like storage of images, networking and security features such as firewalls and load balancers and bundles of software. (Suikkanen 2013, 13.) The benefit of the IaaS cloud for the customer is that certain data center related activities can be abstracted and used from, for example, a web interface or an API. There is no need to manage all levels of the infrastructure anymore and administrative tasks can mostly focus on server side such as operating system management and maintenance as well as third party software maintenance. As in this type of a cloud service only the infrastructure is provided, all software related development and administration responsibilities are left to the customer. (Kavis 2014.) Hence, it is worth to emphasize that while the customer has limited or no control of the underlying ar-

chitecture used to provision the cloud based services, the customer is still responsible for proper use and care of the cloud resources, for example the configuration of an application (Stamou 2014, 5).

2.3.2 Platform as a service

As stated above, IaaS does not address the various scalability issues or automation challenges faced by organizations especially from the perspective of a software. The customer must provide all the parts of the software infrastructure. To ease this task PaaS providers can provide software platforms to a certain level. Typical software platforms can be e.g. databases, logging and payment services which can be used via various APIs (Kavis 2014).

Several PaaS related technologies also aim at automating the provisioning procedures for the virtual machines and containers that actually run the application. Examples of these services could be, for example, a Kubernetes platform providing an API for containers for automatic scalability. Containers are a relatively new concept in computing but they are used to package the application and its dependencies in to manageable units for distribution and running in cloud platform. (What is a container? Docker documentation 2018). These containers can then be housed in orchestration tools such as the aforementioned Kubernetes or Docker swarm. As a conclusion, PaaS deployment could be considered being one level above the Software as a Service (SaaS) deployment as it eliminates the need for customer owned infrastructure for the deployment of a software application. (Suikkanen 2013, 14)

2.3.3 Software as a service

Software as a service (SaaS) is a method of delivering software application from cloud via Inter- net connectivity with the least amount of manual work from the customer. Using SaaS only requires configuration and user management from the customer, leaving everything else to the service provider. The advantages to the customer are the lack of need to maintain the platform and not needing any personnel to execute the maintenance tasks, which is beneficial especially when talking about services that do not belong to the core functionalities of the customer. Naturally, the SaaS services cannot be used for software that require any heavier tailoring than just

the predefined configuration changes. A real-life example that illustrates the stacking of cloud services and the SaaS could be an email service that has its customer specific front ends running in containers on service provider orchestration tool that utilizes virtual machines housed in service provider facilities and hypervisors somewhere. SaaS services are nowadays very common. (Kavis 2014.) The key point to understand the SaaS model is that the customer has no control of the underlying software deployment or the computing infrastructure in SaaS model (Stamou 2014, 5). This is the essential differentiator between SaaS and PaaS.

3 Security in cloud

As with any environment, the requirement for business continuity planning and disaster recovery planning applies, regardless if the service is run on-premises or in a cloud (Halpert, 2011). Hence, this chapter starts with a description of business continuity plan and disaster recovery plan before diving further into the recognized risks.

3.1 Business continuity and disaster recovery plan

Business continuity plan is a clear plan aiming to ensure that critical functions of a given organization are capable of operating in case of a disaster. Business continuity plan should identify the essential resources such as personnel, systems and infrastructure that are required to run the essential emergency business operation and how to later on re-establish all the business functions. Disaster recovery plan is usually coupled with the business continuity plan, however, it is aimed more towards how to deal with the immediate crisis to safeguard the personnel and also to limit further damage to equipment. (Childs 2008)

3.1.1 RTO - recovery time objective

RTO roughly translates to how quickly the customer needs to recover in case of a disaster taking place. RTO has a direct impact on the budget and resourcing required to recovery operations. As an example, if a customer is to assume RTO of three hours, it is essential to invest a hefty amount of money on a recovery site and make sure that it is operational within the three-hour window. If in turn, a customer is expecting

three weeks RTO service provider could, in some cases, just simply wait for the repairs in data center to take place. (Vora 2017)

3.1.2 RPO - recovery point objective

When RTO is mostly about the time available before operations must continue, RPO is translated into the amount of data that is acceptable to lose in case of a disaster. RPO can give indications as to how robust infrastructure is required to run the service. An example of this would be RPO of five hours, meaning that backups of the service must be taken every five hours. This is to keep the amount of ”in flight” data at bay. (Vora 2017)

3.2 Common cloud security aspects

As cloud is a relatively new approach to computing it is no wonder there is some uncertainty about how security at its various levels can be achieved. This uncertainty has led to decision makers to state that security is their primary concern with cloud computing. (Mather, Kumaraswamy & Latif 2009)

Some general level challenges of cloud computing are identified as follows by Halpert in his book from 2011, Auditing Cloud Computing: A Security and Privacy Guide.

- Availability can be at risk as customers might consume more of the shared resources than expected. This is especially true in public cloud.
- Vast resources of the cloud could be used to launch denial of service attacks.
- Data residency is a factor as different countries and regions have different requirements for information handling.
- Multi tenancy is what allows the economics of scale, it is also a compliance consideration when the same infrastructure is shared among customers.
- Log management of shared infrastructure might present an issue as information from multiple tenants could be visible in the same log files.
- Performance and service levels of the cloud are based on the services purchased, these metrics can be controlled by service level agreements.
- Data evacuation process should be addressed as it sets the boundaries how information is removed from shared infrastructure.

- Supervisory access is of interest as service provider has the highest level of access to the infrastructure.

Some of the more detailed security concerns can be seen as shared among all the deployments while others are more tied to specific deployment models. In their Cloud Security and Privacy book from 2009 Mather, Kumaraswamy and Latif describe the following barriers for cloud implementations that are shared amongst the deployment models.

- Privacy is essential and it may not be obvious if the cloud model meets the current and upcoming requirements to safeguard privacy.
- Connectivity is mandatory to reach the service. Highspeed and reliability are critical for the user experience.
- Reliability requirements are high as enterprise applications are expected to be available 24/7.
- Interoperability with traditional non-cloud software is not given.
- Reliance on the service provider and vendor lock-in are threats that need to be addressed on contract level.
- Economic value can be at risk due to hidden costs that are not obvious. It should be also noted that transitioning to cloud is not free.
- IT governance still has to be taken in to account to make sure that the cloud deployment is in line with the business needs.
- Political and global boundaries can be factors when considering if it is all right to store for example customer data in outsourced data center.
- Changes in IT organization: The organization has to have the skills needed to operate the cloud environment and, on the other hand, the role of the IT organization might change due to a major cloud deployment.

Given the suggested flexibility of the cloud deployments and the vast number of threats shown above, it is only natural that from an IT manager's perspective the very nature of the cloud architecture bypasses and fights against the well-known tools and frameworks of security. This is illustrated by the ease (and contradiction therein) in which services can be migrated, created and deployed in a cloud environment; however, this does not remove the need for compliance and security. (Yeluri & Castro-Leon 2014.) Some of the security concerns of different cloud deployment

models starting from the more general ones towards more deployment model specific ones are discussed next.

3.2.1 Vendor lock-in

Ko and Choo (2015) give the following analogue to vendor lock-in in their book ”The Cloud Security Ecosystem”: The concern of vendor lock-in is often described as the “Hotel-California” syndrome where one can check-in but one can never leave. Essentially this means that a service provider produces the service using their own standards, protocols and policies, leading to a situation where a customer is effectively tied to their current service provider, i.e. the customer cannot take their business elsewhere, or the costs of doing so would become too high. (Ko & Choo 2015, chapter 5.1.)

There could be several reasons why a customer might want to migrate away from a given vendor, e.g. an unacceptable increase in the costs at the time of renewing the contract or when the service provider ceases to operate as a business. In order to avoid vendor lock-in, the customers should review the service level agreement, ask the service provider what their policy is on data moving ,and how this affects the support available if a customer was to migrate to another service provider. Customers should also try to select technologies available on multiple service providers and they could also make sure that they can have the copy of the data on their own premises in an openly available raw format. Customers should also confirm that their application does not need to be written in exotic proprietary language in favor of openly available ones, such as C, Java or Python. (Ko & Choo 2015)

3.2.2 Requirements set by regulation

Combining the relative freshness of cloud as a concept and the fact that there are many service providers to choose from, it is unfortunate that there are not very many rules and guidelines for cloud implementations. It is likely that in the future there will be more regulations for cloud services; however, it is hard to predict what the impact of the regulation will be. On the other hand, this new regulation might make it easier for customers to select their service providers, yet the downside to this is that it could also lead to a situation where the cost benefits of cloud would

shrink as customers would likely have to pay the bill of implementing the requirements defined by regulators. (Halpert 2011)

To understand the regulatory aspects in cloud computing better the meaning of regulation needs to be defined first. The dictionary definition of regulation states that regulation is a rule or directive made and maintained by an authority (Oxford dictionary 2018). In order to broaden the meaning of regulation it could be stated that a regulation is a rule or law with consequences if not followed and that is policing to enforce compliance. The reasoning behind regulation is to protect, i.e. to safeguard resources such as key assets. (Halpert 2011)

Halpert (2011) goes on giving us few international examples of regulation:

- Federal Information Security Management Act is legislation that aims to improve all aspects of system security for federal agencies of the United States.
- Sarbanes-Oxley Law is legislation for publicly traded companies and their reporting systems with the idea of increasing transparency and accountability.
- Privacy Laws are various privacy specific laws on multiple levels, state, and federal and EU.

In Finland there is a security criterion Katakri which essentially is an auditing tool for authorities. Katakri can be used to evaluate the capability of an organization when it comes to security of in- formation classified as e.g. confidential. (Katakri 2015.) Another fine example of regulation that is ratified in Finland is the EU general data protection regulation (short for GDPR). GDPR officially states that stronger rules on data protection mean that people have more control over their personal data and that businesses benefit from a leveled playing field. (Official GPDR website 2019)

Next, the reasons why regulation exists can be discussed. Halpert (2011) states that regulation could be identified as a counter reaction to the failures of security. As an example, he showcases the Sarbanes-Oxley and Enron where authorities determined that Enron had failed at policing itself; in essence, the processes were defined but not implemented, resulting in damage to shareholders. After this incident, the public company accounting oversight board (PCAOB) was formed to create a framework consisting of rules to follow for publicly traded companies. PCAOB went to create the rules based on at that point best-known practices (COSO, Committee of sponsoring

organizations of the Treadway Commission) that were already in place. Using these already defined best practices allowed PCAOB to quickly setup the audit criteria and guidelines. This resulted in Sarbanes-Oxley compliance program. (Halpert 2011)

The content of this chapter could be summarized so that the regulations appear when there is complexity and possibly high risk, and that regulation should be based on known frameworks and standards in order to provide guidance and compliance programs. To put regulation in to cloud context the reason for the need of regulation might surface in order to provide fair playing field and to address problems that could be related to harmonizing regulation across national borders.

3.2.3 Global data residency

Compliance with regulation can be a complex topic in a multinational setting as there can be significant overlap inside legislation and regulation in various countries, sometimes they can even be conflicting. Privacy is one of the most complex and difficult topics within the multinational compliance. Stronger privacy protection takes place in Europe than in the United States and regulation is strict concerning what information is deemed as acceptable to collect, where it must be stored, not to mention where it may be processed. This is illustrated by the EU Council Directive 95/46 that limits the transfer and processing of personal data outside borders of the European union. (EU Council 1995.) It is important that the service provider has a solid strategy and plan to deal with the regulation and legislation related to this topic. To summarize, it is important as customer to understand the jurisdictions where data can be located and the relevant privacy policies of that area. Customer should make sure that proper controls and policies are in place to ensure that the privacy issues are not violated. (Ko & Choo 2015)

3.2.4 Division of responsibility

Based on the security concerns identified above it is essential to understand the concept of division of responsibility. The term division of responsibility means that the responsibility of the service and the data therein is shared between the customer and the cloud service provider as defined by Wan, Lin, Zeng, Li, Xiang, Liao, Huang and Liu (2016) in their conference paper on Security and Privacy in New Computing

Environments (SPNCE) event from 2016. The same paper also clarifies this by stating that this division of work may lead to unexpected consequences and that it may be difficult to clearly define who can be held responsible for what as there are likely multiple factors at play on the same time. Combining the ”many hands working together” problem with the long list of identified security concerns is a factor worth considering.

Another aspect to the division of responsibility is pointed out by Childs (2008) in her book Prepare for the Worst, Plan for the Best: Disaster Preparedness and Recovery for Small Businesses. Service providers likely want to tie their customers to the service provider’s offering as much as they can. The reason for this is that if the customer for whatever reason tries to change their service provider, they might find out that they have been locked-in by relying on certain functionalities offered by the service provider. This means that in the end it might not be enough to just change some portion of a customer’s service but to actually make other far more significant changes. When the disaster strikes, it is not ideal to have one’s hands tied like this. One approach to decreasing this risk is to make sure that the customer has good lines of communications with the candidate service providers and possibly their management as well. This can be accomplished by taking part in information sessions organized by the service provider as these can be a good opportunity to interact with the senior management of the service provider the customer is evaluating. To this end, it is a good idea to tell the service provider that the customer is preparing a contingency plan and that the customer would appreciate the service provider’s recommendations. (Childs 2008)

Assuming there is a pre-existing customer-service provider relationship, there could be a need to request more specific information; in these situations there are at least three options. Maybe the most straightforward one is to send the list of questions to the service provider and give them some deadline for answers. This approach relies solely on the service provider to tell the truth in their answers. One approach to make it tighter is to include formal attestation clause at the end for an executive to sign. The second, a slightly more invasive approach is to request the service provider to include additional documentation alongside the answers. These documents could be screen shots, access control list configurations, outputs of vulnerability scans and

so forth, and they can be used as additional proof that the controls are implemented. The third and the most invasive method is to send a team on-site and conduct a straight review in person. This would need to be planned and executed according to an agenda, including interviews of roles of interest. This is the most resource intensive option, particularly if the business of service provider is very distant of customers business. It is also possible to hire external consultants and auditors for this kind of review. (Pompon 2016)

3.2.5 Segregation of duties

Just like with the customer's own IT environment, the customer should ensure that the service provider is adequately safeguarding itself against issues related to segregation of duties concerning the cloud service offered to customers. The definition of this problem with segregation of duties could be described as a case where single user is able to both initiate and approve an action. Blount and Zanella (2010) give the following example of this in their book "Cloud Security and Governance: Who's on your cloud?": As an example, accounts payable administrator who can both establish a new vendor record, and approve payments to that very same vendor. They also say that issues with segregation of duties can be challenging to identify and to this end very specific policies are required to prevent these issues taking place. Technology can be used to identify and possibly correct these situations as they take place, all in all, a review of the service providers policies, strategy and abilities in this field is important. (Blount & Zanella 2010)

Another approach to segregation of duties could be found from the concept of change management and the risks therein. International atomic energy agency (2001) proposes the following cross-discipline questions to be asked when evaluating the change management process:

- Is there a policy in-place that prioritizes safety, and if that policy is aligned with the values and requirements of the customer?
- Is this change management policy utilized to in systematic and transparent fashion?
- Are all the required resources to make the change available?
- Is proper analysis done that justifies the change, including the risks therein?

- Is there a mechanism in-place that allows management to review the changes regularly?
- Is there a communication plan to keep all the parties informed?
- Is there a criterion to evaluate if the change was successful?

Many organizations are having to deal with the pressure to change. When properly managed, these changes could improve security, reliability and also, the competitive aspects of an organization, all the way from the initial planning stages to the decommissioning phase. (International atomic energy agency 2001)

3.2.6 Importance of incident response

Despite all the implemented controls, righteous plans and ideas for security and availability, the undesired event will eventually happen. This could include various matters such as attempts on attacking the environment, successful attacks on the environment, challenges caused by software issues etc. It is important to make sure that the service provider has a sufficient strategy on incident response to handle these issues. Customers should know the procedures of creating, following and reporting of incidents. Customers should ask questions such as how is the customer notified and what kind of visibility is given to the customers to gain more information on incidents detected by the service provider. Does the service provider have a proper plan to act on a PR disaster, such as loss or leak of credit card information? Possibly the single most important question to ask is to verify whether the service provider and their plans on incident response are consistent with the plans of the customer? (Blount & Zanella 2010)

It is stated that incident response resource should not only be a seen as intrusion detection system to alert on network and host level events, but also computer security incident response team (CSIRT) should be established. Kurtz and Vines (2010) state that CSIRT needs to be able to:

- Analyze notifications of events
- Respond to the event if this is required, based on the analysis
- Escalate the issue as required and by predefined procedures
- Report on identification, resolution and post-incident to proper parties

These capabilities should ideally be present not only on the service provider but also on the customer side. (Krutz & Vines 2010)

NIST Special Publication 800-61, ”Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology” from January 2004 splits the incident life-cycle into four parts:

- Preparation
- Detection and analysis
- Containment, recovery
- Post-incident actions

The above topics highlight few areas that could be worth confirming with the service provider. For example, on the topic of preparation, what kind of mechanics the service provider has in place to prevent attacks from succeeding? Does the service provider implement regular risk analysis, what kind of patch management and host security schemes do they have and what kind of user training and education takes place in matters of security? Detecting a successful attack is usually challenging. To this end, it might be worthwhile to investigate if the service provider does some sort of profiling of the expected system behavior to understand what is normal. What kind of log management and analysis tools are being used and how? How are the detection processes tied to the communication processes with the correct parties? Assuming that the service provider can detect the attack, the customer should then investigate their capabilities to contain the threat. For this purpose, the customer could ask questions such as: What kind of means does the service provider have in order to determine for example the user accounts that might have been compromised, or how will the service provider detect files that might have been changed by the attacker? To gain insight on the post-incident actions of the service provider the customer might ask questions such as how does the service provider report what exactly took place during the attack, or if the service provider has means to learn from the incident that took place? Additionally, what corrective actions could be taken to prevent similar incidents from taking place in the future, and how these improvements would be communicated? (Krutz & Vines 2010)

3.3 Security aspects in public cloud

Based on what has been written above it is likely that it is taken as a given that in a public cloud there are multiple tenants on the same physical infrastructure. Be that as it may, most public clouds offer software based separation and permission control to maintain isolation between customers. Hardware level separation might be an option, however, with likely additional costs involved. It is essential to understand how the platform-of-choice implements the multi-tenancy, for example, if it supports the concept of having multiple directory services, such as Microsoft Active Directory or LDAP, one for each tenant. (Bond 2018)

Responsibility of patching and updating servers in public cloud generally falls to the service provider, but this can also cause unexpected risks to customer systems and applications. Hence, close interaction with the service provider is required to ensure that no new risks are introduced or availability issues surface due to service provider conducting maintenance. It should be also noted that the highest level of access to the infrastructure, e.g. the supervisor level access, is held by the services provider. (Halpert 2011)

3.4 Security aspects in private cloud

Unlike with public cloud, multi tenancy is slightly less of an issue in private cloud, in fact private cloud on its own could be seen as an approach to solve the multi tenancy issue (Bond 2018). Halpert (2011) highlights that usually both the consumer and service provider are internal to the organization which allows more control over the aspects of the cloud service such as quality of service. An example of this is that employees of the customer can more easily impact the way workload is ran based on its criticality to the business. This control comes at the price of customer paying for the whole infrastructure as it is dedicated solely to this customer. (Halpert 2011)

3.5 Security aspects in hybrid cloud

A hybrid cloud as stated above is a mixture of both public and private clouds, and all the aforementioned rules apply to it as well. It should still be noted that while portions of the service may run in a public cloud at times, the same security precautions and metrics should still be met as if the service was running solely in a private cloud.

3.6 Security aspects in infrastructure as a service

It is a key element to understand that the service provider has means to view the activities of any virtual machine running inside an infrastructure as a service cloud (Halpert 2011). Furthermore, the customer is responsible for implementing the required patching inside virtual machines themselves, this is true even if service provider would be patching the hypervisor level.

Another way to describe this illustrated in the Cloud security and privacy book by Mather, Kumaraswamy and Latif (2009) would be to split the security of infrastructure as a service into two pieces:

- Virtualization software security including all the software pieces that implement the virtualization, including hyper visors, paravirtualization etc. This layer is maintained by the service provider.
- Customer guest operating system or a virtual machine running some operating system and software stack. This is maintained by the customer.

The above could also be considered as another way of describing the division of responsibility. This is an essential part on the other service delivery models as well.

3.7 Security aspects in platform as a service

The key differentiation between infrastructure as a service and platform as a service is that the service provider maintains both the hypervisor and the guest operating system patching and configuration. Assuming that the above is met by the service provider it is safe to say that more current system software is being used and there are scalability gains to be attained. In addition, lower administrative overhead can be achieved by moving some of the maintenance burden from in-house staffers to the

service provider. (Jamsa 2012.) Scalability could be seen as a security enhancing feature against certain kinds of attacks, such as denial of service, while lower administrative burden might allow staffers to improve software quality as they may have more time available.

In Cloud Computing Jamsa (2012) highlights the concern of risk of breach by the platform as a service provider. It is stated that if the service provider fails to be compliant with the service levels, performance availability and security of the application running on a platform as a service might be at risk. (Jamsa 2012.) McGrath states in his Understanding PaaS (2012) book that it is not so much about platform as a service being fundamentally different, but customers just do not see all the actions taking place behind the scenes, such as monitoring, tweaking and constant improvements. He also states that while platform as a service might not work for all use cases, it still works well and can be used to improve the security of a significant portion of the computing stack required for applications. (McGrath 2012)

The aforementioned statements are escalated when combined with the statements by Mather, Kumaraswamy and Latif (2009) in their book Cloud security and privacy where it is said that service providers do not in general share the configuration details of their security controls for platform as a service systems. This includes operating systems and the processes that are used to secure the hosts implementing the platform as a service -concept. The reasons for this are that attackers could possibly utilize this information to implement attacks. (Mather, Kumaraswamy & Latif 2009)

Everything mentioned above points to the direction where a customer does not need to implement the host level security but it is good to keep in mind that once again it is still the responsibility of the customer to get the correct level of assurance that the service provider complies with any possible requirements customer may have. (Mather, Kumaraswamy & Latif 2009)

3.8 Security aspects in software as a service

Software as a service typically presents itself as an application hosted and developed by a service provider and delivered over a web browser. This allows the customer to limit their needs of on-site data center based software and applications leading to

smaller amount of administrative burden. Jamsa (2012) also states that as software as a service is likely multi-tenant this may lead to a situation where any customization of software as a service delivery might turn out to be difficult, expensive and in some cases impossible. (Jamsa 2012)

Given that everything from physical hardware, hypervisors and applications is hosted by a service provider it means that the service provider may also have visibility to all information on all customers of their software as a service offerings. (Halpert 2011)

In addition to everything stated above, the last statement concerning platform as a service still holds truth: it is still the responsibility of the customer to get the correct level of assurance that the service provider complies with any possible requirements customers may have. (Mather, Kumaraswamy & Latif 2009)

3.9 Selecting security controls to implement in cloud

In order to operate and use cloud in secure and efficient manner both customer and service provider have to plan in advance when it comes to matters of security. When aiming at a complex environment, it is essential to look ahead and try to consider the methods and procedures required for the operation. While it might be possible to implement a small cloud service without much planning, anything more substantial requires significant planning and design. Failing to do this will usual lead to increased costs or worse. (Winkler 2011)

What is good to point out is that every decision, security related or otherwise, will be a tradeoff between options. Tradeoffs within security are at times not realized in a sense of those tradeoffs having any impact on security. As an example, bulletproof vest protects against gunshots, so why does not everyone put on a bulletproof vest before heading out? After all, likelihood of being shot is greater than zero. The obvious reason is that this likelihood of being shot is vanishingly small, besides, bulletproof vests are cumbersome, uncomfortable and hot, just to name few downsides. Not to mention, they are unfashionable. Therefore, it is decided that the unlikely benefits do not justify the downsides. This same principle applies when choosing controls for cloud deployment, and if one is to transfer some of the responsibilities to cloud service provider. (Halpert 2011)

3.10 Administrative means to improve security and availability in cloud

3.10.1 Description of defense-in-depth

Defense-in-depth is understood as a construct with a multitude of related organizational actions and measures applied in order to minimize incidents and security compromise. If defense-in-depth is successfully utilized, the reliability, resilience and robustness to withstand attacks is also increased. The concept of defense-in-depth could be split into individual components defined as zones that aim at improving the selected aspect of the larger entity, for example identity management and availability management. By splitting the big picture into smaller zones, it is said to be easier to understand the larger requirements and hence to identify appropriate controls to deploy in the environment of a particular organization. (May, Hammerstain, Mattson & Rush 2006)

3.10.2 Service level agreements

Service level agreements (SLAs) are sets of conditions and terms defined in contracts between the customer and the service provider. SLAs can be used to define and agree upon the service levels between the provider and customer, including sanctions if the terms are not met. Conditions and terms in SLAs can include various technical, commercial and business service level objectives (SLOs), combined with mechanics of how to measure that the agreed upon services levels are met. (Stamou 2014.) Another definition to the service level agreements is given by Sun, Pan and Bertino (2018) in their paper ”Cloud Computing and Security” where they define service level agreements as means to assure quality, reliability, security and scalability of the cloud service. (Sun, Pan & Bertino 2018)

To utilize SLA successfully as a way to improve service availability and security, the SLA life cycle could be split into four parts as follows: (Stamou 2014)

- Creation of the SLA including contract
- Implementing the SLA
- Enforcement and monitoring of the SLA
- Termination of the SLA

Generally speaking, the first step consists of service provider predefining a set of various SLA levels for the customer to choose from and to bind the contract upon. These could be considered as templates for the SLA. The customer then reviews these templates, selects one possibly modifying it and sends it back to the service provider for a review. The service provider then accepts, declines or sends a modified version to the customer for a review. (Stamou 2014, 13.) Rest of the SLA life cycle consists of implementation, regular reviews and eventually ending of the SLA as stated above.

What makes the SLA for cloud especially tricky is the fact that currently SLAs for cloud lack standardization. This is not optimal as standardization would lead into more structured content of SLAs. In a perfect world, the SLA should consider the individual risk requirements of the customer but this can lead into highly tailored SLAs. (Stamou 2014, 14.) Nevertheless, ideally it would be appropriate to consider security similarly to other terms of the contract, meaning that customers would be able to be aware of what sort of security systems are implemented to safe guard their data and services. The result of this would be something along the lines of security as a service, delivered under an SLA just like any other part of the complete service. Similarly, to the lack of standards for cloud service level agreements, there currently are not that many models for service level agreements that would focus on security as majority of service level agreements focus on performance and availability. The problem is many folded as there is still the need of specialist knowledge to translate the security requirements into appropriate low-level security controls that can be enforced and monitored so that the service level agreement is met. This monitoring problem is even more difficult to tackle in the cloud environment than traditional IT outsourcing as there are different deployment models - IaaS, PaaS and SaaS - where the underlying responsibility is shared between customers and service providers in varying ways. Traditional SIEM, IDS or vulnerability assessment system might not be sufficient in the cloud. (Casola, De Benedictis & Rak 2015)

Contradicting the whole cloud computing paradigm of on-demand and self-service, currently many of the standard contracts available from cloud service providers are rather one-sided with little room for requirements from the customer, meaning that service providers are trying to avoid any meaningful commitments or assuming any responsibility, which lends itself to standard contracts being very service provider

friendly. This is highlighted by permitting unilateral termination or suspension of the service and they also tend to avoid most of the liability of the service provider. (Casola, De Benedictis & Rak 2015)

3.10.3 Supply chain security and continuity

The oxford dictionary definition of supply chain is the ”sequence of processes involved in the production and distribution of commodity” (Oxford dictionary), and the same source defines management as process of dealing with or controlling things or people. (Oxford dictionary.) While it has been acknowledged that risks and uncertainties exist in the global supply chains, the risk management as such has not played a significant role in the management of supply chain. Risks in the supply chain may come in a variety of forms, such as environmental, ethical or social conduct resulting in a worker strike, or malfunctions in the manufacturing procedure. All of these have a direct impact on the ability to deliver the service or product. (Harilainen 2014)

Information sharing within the supply chain management is an essential component and it is critical in improving the capability and gain competitive advantage; to this end, it is not uncommon for an organization to be reluctant to share their supply chain information. These global supply chains are exposed to various types of risks that stem from the increasing globalization making them vulnerable as they rely in Internet for transport. Based on a statement by U.S Government accountability office from 2012, there are five general threat factors for supply chains:

- Installation of hardware or software with harmful purpose.
- Installation off the hardware or software, built from less than genuine components.
- Failure in the production or distribution of essential products for any reason.
- Relying on a nonqualified or malevolent service provider.
- Vulnerabilities in hardware or software allowing exploitation.

  These risks and threats can be addressed by making sure that:

- Policy protecting against supply chain threats is in place.
- Security controls defined in that policy are implemented and followed.
- Monitoring of the security measures is in place.

Supply chain is a critical element in a modern organization and the success or failure of a business organizations depends on the gains made from the effective supply chain. (Aiguokhian 2013)

To this end, the customer would do wisely to confirm how the cloud service provider implements these policies in their supply chain. The same applies for the internal processes of the customer.

3.10.4 Human factor in security and cycle of deception

There is a complete class of vulnerabilities related to the human factor in the security landscape. The goal of these attacks is to induce the victim to relay information or execute activities they are not supposed to either release or perform. It is stated that the so-called social engineering has significant probability of success. This is highlighted by the protection mechanisms against it being complex, and the success of these defense mechanisms is also difficult to measure. Practical exercises are suggested to train managers and users in addition to the theoretical training; this can include social engineering penetration testing and measuring of success of such tests. The concept of cycle of deception is introduced to explain the different parts of a social engineering attack. The first is the attack cycle which includes the behavior of the intruder and activities taken by the attacker. Just like any other type of attack, a social engineering attack has a purpose, goal and some form of plan how to reach it, this can mean a direct compromise of critical information or gathering knowledge for another attack. These techniques can involve anything from dumpster diving to befriending the victim or someone else with usable knowledge on the victim and then utilizing manipulative methods to make this person hand out information that can be used to attacker's gain, in other words the goal is to scam the victim to trust the attacker. (Nohlberg 2008)

The second cycle in the cycle of deception is the defense cycle, describing the methods available to the defender. Examples of these could be a solid public defense policy or strong reputation of reporting illegal activities to authorities, educating employees and clear guidance on how to act if one detects social engineering attempts. In other words, predefined means how to detect an attack and how to respond. The

goal of these predefined procedures should be to make it easy to report a social engineering attack without any social or professional stigma. This allows the defender to take actions during an ongoing attack. The third and last cycle in the cycle of deception is the victim cycle. Victim cycle is concerned with the actions taken by the target of the attack. It is stated that often too much of the investigative focus is put on the attacker while it might be more efficient to put more focus on the victim in order to understand how the victim might have set himself up for the deception to begin with. This kind of information could be useful to prevent future attacks. One should also note that the victim may evolve from the role of victim to someone who is harder to victimize in the future, while it is also possible that the victim unfortunately regresses to a person who accepts his or her role as a victim who is even easier to exploit in the future. (Nohlberg 2008)

The key takeaway of all this is that training in security related matters is an essential part of the organizational means to maintain acceptable security posture and to avoid accidental loss of data. This training combined with the commitment and attitude from management can create information security culture that develops into security awareness and perception among the employees, influencing their view of matters of information security. (Ndungu & Kandel 2015)

3.10.5 Service life cycle management

Not only has cloud computing transformed the way services can be quickly deployed but it has also altered the way customers may want to implement their service life cycle management. This could be illustrated with the concept of the traditional model where the customer did the implementation and installation in classical data center which has been replaced with a model where the role of the customer is transformed more into a form of an integrator. Whereas the cloud service provider is taking large portion of the responsibilities related to IT infrastructure. Be as it may, also in the core of the cloud service life cycle is the key principle where all services must produce measurable value to enhance the business goals and desired outcomes. (Buyya, Broberg & Goscinski 2011)

The life cycle of a service hosted in a cloud includes several stakeholders, such as service providers and consumers that take role on the delivery of the cloud-based applications and the management of the related services. While the life cycle of a cloud service is still largely in a state of flux, there is general consensus in the literature concerning the individual phases of life cycle and the requirement for service repository in order to support life cycle activities. This service repository consists of two main components. Firstly, a registry for storing and managing the metadata related to the service including attributes such as service name, version, provider and description to name a few. The second component of the service repository is the mechanism that discovers new services. In practice, this repository could take the form of relational database. (Tran & Feuerlicht 2015)

It is said that the life cycle of a cloud service consists of five phases: specification of requirements, discovery, negotiation, composition and consumption. In the requirement specification phase, both functional and non-functional requirements for the service are described, i.e. the requirement the given service needs to fulfill is defined. While there are differences in the specification depending on the type of the service, normally the specification will include technical details, such as service interface (for example WSDL); however, it may also include technological details such as hardware specifications or programming languages used. The non-functional requirements include attributes such as availability, performance and security. Service identification is based on both the functional and non-functional requirements specified in the requirements specification phase. The service identification phase utilizes service category hierarchy and the attributes identified in the service requirements stage. These attributes are then stored in to a web-based service repository that allows consumers to search services based on their various attributes. This leads to consumers trying to search for services that are already registered and available in the repository, meaning that they are certified for use. After the appropriate service is found and selected, testing and approval phases follow. Service approval is defined as an internal certification procedure, deciding if the cloud service is certified for use. This can be very time consuming as the selection of services is wide. (Tran & Feuerlicht 2015.) These internal certifications can take advantage of rigorous frameworks that are used to evaluate the service capability and risks involved prior to the new

service being deployed or old service is being modified. This can include things such as approved service release package, updated service package or bundle, updates in the service portfolio, updates in contracts and new documentation. (Buyya, Broberg & Goscinski 2011)

In the service integration phase, the cloud service is integrated into the customer's enterprise environment and processes. At this stage the service is taken into production, i.e. business processes are executed on the cloud environment. The effectiveness of the operation relies on the ability to detect any deviations or defects from the normal operation. (Buyya, Broberg & Goscinski 2011.) To this end, the monitoring state of the life cycle is defined. As the name states, monitoring takes place during the runtime of the application or service. It is common that both the customer and the service provider implement their own monitoring independently, which is natural as both parties share the responsibility of the availability of the service. The service repository is used to store runtime performance and availability of the service, including e.g. response time and error messages. Maintaining accurate statistics enables the customer to compare the seen performance to what was stated in the service level agreement. In addition to monitoring, also service optimization shall take place when the service is in the running phase, including software upgrades and possibly changing of the service provider, for example PayPal could be replaced by SecurePay. The optimization phase can also include aspects of optimization of processes internal to the customer organization. (Tran & Feuerlicht 2015.) Both monitoring and optimization contribute to the continuous service improvement where the object is to ensure that the cloud service is still a feasible option to meet the business requirements. (Buyya, Broberg & Goscinski 2011)

For comparison with the above statements specific to cloud computing one can look into the life cycle management process of a nuclear power plant. Similarly, to cloud service life cycle, nuclear power plant starts its life cycle with a design phase followed by construction and commissioning that eventually should lead to the start of operation. Just like in cloud service life cycle, a nuclear plant has safety management that aims to improve the safety of the organization by enforcing planning, control and supervision to activities concerning safety. The safety management also supports the safety culture with education. As with cloud service, nuclear plants have a preventive

maintenance that is performed to detect and mitigate degradation. Properly executed preventative maintenance is seen as an essential part of life cycle management. In addition to preventative maintenance, nuclear plants have predictive maintenance that that is performed continuously or at given set of intervals, similarly to the periodic safety reviews. Safety reviews assess e.g. the symptoms of ageing, compare the original design safety stance to current situation, and identify achievable improvements. (International Atomic Energy Agency 2002)

Nuclear plant life cycle management has one phase not mentioned in any of the above cloud service life cycles: Decommissioning phase. According to the nuclear plant life cycle, the planning for decommissioning is an integral concept already in the running phase since it allows time to prepare for the actual decommissioning process and the final decommissioning of the facility in a controlled manner with positive outcomes. It is stated that detailed decommissioning planning should start already five years before the planned transition to the actual decommissioning. Planning for decom- missioning should be seen as a part of design and building phases. (International Atomic Energy Agency 2002)

This planning for decommission is something that should be addressed in cloud service life cycle as well. In fact, BMC software states on their ”Cloud lifecycle management: managing cloud services from request to retirement” that cloud service might be seen as out-of-sight and out-of-mind, so unless a cloud service is not actively placed in the termination queue it will easily linger indefinitely. This is especially true as the goal of the cloud is to improve the usage of resource, which makes service decommissioning important function that actually completes the life cycle. (BMC Software 2010)

3.11 Securing data

3.11.1 Encrypt static data and in-flight data whenever possible

As stated earlier, the very nature of cloud computing relies in the resource pooling, which on own poses the question if cloud storage service is suitable as several customers usually utilize the same storage system. To lessen the risk of data leakage within the cloud, a customer should implement encryption to protect static data. For infrastructure as a service environment that could mean using encryption methods provided by the service provider or encrypting the data using a third party system. When using encryption, it is essential to use appropriate encryption algorithms, at the time of writing this includes for example AES. The customer should select the encryption algorithm based on actual need and so that it is compliant with regulations. Encryption highlights the importance of managing the encryption keys in an efficient manner and customer should implement a standardized method of user key management and distribution method so that they can utilize the encryption and manage data in a secure fashion. (Sun, Pan & Bertino 2018) In their paper on ”A Formal Security Analysis of the Signal Messaging Protocol” from 2017 Cohn-Gordon, Cremers, Dowling, Garratt and Stebila illustrate the use case for end-to-end encryption of communications. They state that in the past there have been attempts to improve security by encrypting the messaging between the customer and service provider; while this provided some security, it still allowed the service provider to access the messaging in plain text. To overcome this, there has been a push for mechanisms authenticating the customer’s end nodes using either public keys or pre-shared secret to obtain end-to-end confidentiality and integrity. While these attempts at end-to-end encryption have been novel, there is apparently some track record of problems related to key management, example being Apple’s iMessage where users have no means of manually verifying the keys of their contacts, and there have apparently been flaws in the key management that undermine the security. (Cohn-Gordon, Cremers, Dowling, Garratt & Stebila 2017)

As a result, it is obvious that key management is of extreme importance and customers should pay special attention to this if they embark on encrypting their communications and data. This is especially true as regulatory requirements such as PCI-DSS

and ISO 11568 state that key management must be implemented. Proper key management should cover the whole lifecycle of the keys and that different application requirements do not contradict the key management process, which lead to vulnerabilities. (Andreasen, Norgaard, Mot, Snowman, Buecker, Frehr, Peen & Johnston 2014)

Winkler (2011) gives us a list of the most common mistakes when dealing with encryption in his book Securing the Cloud:

- Not using encryption when it would be a viable option.
- Failing to use encryption with protocols that have encrypted counterparts. For example FTP, telnet or HTTP
- Grand (false) ideas of being a cryptographer and implementing his or her own algorithm.
- Reinventing a wheel by trying to implement a known algorithm instead of using a proven implementation
- Including password inside a binary, configuration file etc.
- Storing keys together with data being encrypted
- Failing the bus test: What happens if the few critical individuals with the keys suffer a disaster while sitting in the same bus?
- Distributing sensitive data via unencrypted email

Winkler (2011) also reminds readers that development of cryptographic algorithms is a highly specialized and challenging problem, and correctly implementing cryptography in software is an almost equally difficult task. Even commercially available products utilize encryption in a flawed manner and even a single flap in cryptography may undermine the security of the entire chain of trust. Cryptography is also an area where products have been shown not to work as expected, and there is a long history of products that are flawed or that use algorithms that have not been subjected to peer review or test of time. It is especially essential to steer clear of products that rely on secret cryptographic algorithms; instead, the customer would do wisely to select products that implement an open and recognized algorithm that has passed the test of time and been peer reviewed. (Winkler 2011)

3.11.2 Encryption key management

According to Smith (2013), the management of encryption keys has been a long-standing challenge. Military and intelligence offices have spent better part of the 20th century in their attempts at trying to understand the strengths and weaknesses of different approaches on doing key management. The problem is twofold:

- Make sure that the right people have the correct crypto keys.
- Ensure that the wrong people cannot gain access to any keys.

The real problem is that it is difficult to keep those two in a reasonable balance. In attempt to solve this, key management systems have been developed to ensure that the keys are changed regularly as this will lessen the likelihood of crypto analysis via means of making it more difficult to gain enough cipher-text to break that specific key. In addition, beneficial side effect is that this also limits the damage caused if the key was to be leaked. Another approach is to change the key when the entity holding the key no longer should have it. (Smith 2015)

3.11.3 Information hiding

In addition to traditional encryption, the customer might consider another approach known as information hiding. This is a radically different concept towards the same goal as encryption: instead of openly trying to secure the given piece of information, this approach aims to hide the data inside junk data or split the data so that an attacker needs to have multiple pieces of data in order to gain any information of value. This concept is apparently actively used in systems such as nuclear weapons where at least two different persons are required to turn two separate keys at the same time to activate something. The underlying principle is that the attacker can only control the asset (in the previous example, a nuclear weapon), data or message if they can find it. Examples of this could be sound files or images that can be shared openly over the Internet. They could provide possibilities to hide even large messages in the noise of those images or audio files, and it might be unlikely that anyone can expect to find the information. It is stated that roughly one eighth of an image file could be utilized to store information without significantly impacting the quality of the original image file. Adding that to the concept of splitting the information into

number of parts stored in different locations, one might have a reasonably good way to make information disappear. This approach can also be utilized to create redundancy, for example 3-bit error correcting codes can be used to recover the secret if one of the three parts is changed. (Wayner 2009)

One reason why information hiding might be especially interesting in the cloud scope is that a cloud can provide relatively low-cost and location independent environment to store data. Additionally, given the underlying idea of cloud being available from anywhere at any time (Yang & Jia 2013), the cloud might provide interesting opportunities for information splitting, especially when data is being split into parts stored at different cloud service providers.

3.11.4 Searchable encryption

To preserve confidentiality of data, it should be strongly encrypted whenever it is not within the secure boundaries (Katakri 2015). Thus, it is a natural conclusion that the data should be encrypted during the data transfer to and from a cloud as well as while the data is at rest, if the cloud provider cannot be considered fully secure. The problem with this kind of setup is that not much processing can be done without breaking the encryption.

To search for documents stored encrypted in cloud, a searchable encryption system could be applied. In a system taking advantage of this technology, the data is originally stored encrypted in the server. Several searchable encryption systems exist which can make it possible to make for example a keyword search against a document database. In addition, this search query is encrypted by the user with a specific key. Thus, if the encryption system is applied correctly, any clear text data should not be available for unauthorized users at any point of storing, searching or document retrieval. (Pham, Woodworth & Salehi 2018)

3.12 Technological means to improve security and availability in cloud

3.12.1 Data redundancy

Had the cloud storage been an option some decades ago, it would have been quite unlikely that there would have been the same backup processes and mechanics that

are actively in use today. Be as it may, the fact is that cloud did not exist and enterprise IT departments had to make do with what was available to protect their data against various threats; this includes everything from natural disasters and computer viruses to human errors. This led to best practices of taking backup copies and storing those into off-site locations from which the data could be restored if needed. (Farley 2013.) There are at least three methods providing data redundancy: replication, backup and encoding redundancy. Cloud service provider may replicate virtual machines to several locations and so-called availability zones for implementing policy or service level agreement to increase availability and disaster recovery capability. (Yeluri, Castro-Leon 2014)

Surely enough, cloud computing may provide protection against certain disasters in addition to replication by delivering online data copies to another, alternate location. This may save significant amount of money in a form of not requiring purchase of redundant hardware and software, while still allowing cloud user to recover in case of a harmful event takes place. (Krutz, Vines 2010)

As the same principles apply to cloud backup as to normal backup, it is reasonable to review the traditional meaning of data backup. Backups are understood as snapshots duplicates of the data taken at a certain point in time, stored in some usable format for a given period of time defined by their usefulness in case of need for a restore. There are few different types of backups that can be created, full backup being the representation of the complete dataset and full backups are used as a baseline for other kinds of backups. Differential backup captures data that has changed since the last full backup while incremental backup captures data that has changed since any kind of backup regardless if it has been a full backup or a differential one. Given the definitions of the different backup types it is easy to assume that incremental backup is the best choice. However, it has a downside when it comes to restoring: it might require several backup images to restore a given set of data depending on the times when different files of that data set have changed. (Nelson 2011.) One notable exception to this rule is the synthetic full backup that by definition means that multiple partial (incremental or differential) backups are aggregated in the background to create a backup set that represents a view of the data if a full backup was taken instead

of partial one. (Farley 2013.) Synthetic full backup might make restoration far simpler than from partial backup, depending on the software.

More cloud-like definition of data redundancy is defined as both copy and encoding redundancy. To explain these further, coding redundancy is used during the data access process if data is damaged while copy redundancy can be utilized when data is damaged or lost after once it has been stored. One common approach of encoding redundancy is the erasure coding that relies on the principle of: n file block data is generated as $n + m$ coded data blocks with the erasure code data redundancy is k, where $k = m/n$. Finally store the $n + m$ redundant coded data to multiple cloud storage facilities, the result being that any n blocks can recover the original data. It should be stated that there are multiple erasure encoding methods and many algorithms as erasure codes are an open platform. (Sun, Pan & Bertino 2018)

It should be noted that while replication and backups give the service provider the ability to comply with service level agreements, they also include a risk of e.g. dispersed copies of data and credentials floating in the cloud. In addition to ensuring that the aforementioned does not take place, the customer should make sure that if they decide to change service provider, the backup copies and replicas are destroyed according to the agreement. This can be difficult to achieve as there are no standard means of proving that certain dataset is actually properly destroyed. (Yeluri & Castro-Leon 2014.) One problem worth highlighting is the issue of medium and technology obsolescence. This refers to new backup media being developed and customers having to make sure that the backups stored to old mediums are still readable when required. This is especially problematic with long term data storage or archiving; however, it is worth noting nonetheless. (Farley 2013)

In cloud medium, obsolescence could take place in a form of a storage protocol or proprietary format disappearing from the service offering. This can happen when utilizing proprietary deduplication mechanisms in order to save money. The processes of deduplication aims at reducing redundancies that can be created in many ways, such as user copying a file and then making small changes to the copy and sharing these files with multiple persons within the client environment. To save capacity, backup (or production, for that matter) software can store only unique data, be it a

complete file or a chunk of a file, and replace redundancies with indices, pointing to the actual data. (Sejun & Choi 2017)

3.12.2 Authentication

In the book Cloud security: A comprehensive guide to secure cloud computing by Kurtz and Vines (2010) it is stated that as usual, authentication and identification play major roles in most access control systems. To better understand what this is about, both of those terms are given as a set of definitions and what to look for in relations to cloud environment. Identification could be understood as user giving the system something to establish accountability on, which is usually understood as username or logon ID to the given environment. Username or logon ID should not consist of user's real name, job title or function, which is to limit the information available to potential attacker if they ever gain the knowledge of usernames. Authentication, on the other hand, is the means of making sure that the identity given is the correct one, which is commonly implemented by using a password. Authentication should be constructed using the three types listed below (Kurtz & Dean 2010):

- Something the user knows, for example a password or a PIN code
- Something the user has, for example a smart card or a token
- Something that is unique to each user, for example physical fingerprint or a retina scan

It is also possible to combine some of the above authentications mechanics and come up with some- thing called two factor authentication. An example of this would be an ATM requiring both the card and the PIN codes. (Krutz & Dean 2010)

3.12.3 Reliance to connectivity

Once an application is running in the remote location, it is obvious that connectivity is of paramount importance, in essence, having no connectivity in the campus means having no application, which can mean having no business. While many organizations have Internet connectivity, these days it is still surprisingly uncommon for organizations to have backup connectivity if the unthinkable disruption happens. Fiber cuts are not all that uncommon. (Hayford-Acquah & Ben Asante 2017.) To reduce the impact of a last mile failure it is a common practice to have two physically separate

lines from a service provider, terminated to two separate customer premises' routers in two separate equipment rooms. (Bøe, Faltinsen & Lillebrygfjeld 2011.) Two routers using VRRP protocol act in active-passive manner to provide so-called first-hop redundancy (RFC 5798 2010). This approach, combined with physically separate lines provides protection from fiber cuts on the last mile and also protects from power supply failures in the customer premises router and also acts as a backup connection during router software upgrades and some configuration changes. However, this method does not protect against catastrophic failures in the service provider network. To accomplish this, it is required to have similarly separated lines and routers from two separate service providers. Assuming that the customer has some IP block(s) to announce over BGP and that the service providers accept the customer IP block(s) for transit, it is possible to create fully redundant last mile connectivity. All these relatively complex and expensive requirements are likely the reason why organizations will not purchase redundant connectivity but instead accept the risk of significant business impact and downtime. (Packetworks 2016)

Similarly, if a cloud application is running in a ”stretched” network infrastructure, for example data center interconnect, it is essential that the interconnect is built in a redundant fashion. While redundancy is all-good it can also cause failures of a different kind, however, with equal potential for catastrophe (Pepelnjak 2011). This problem with location redundancy could be solved by making the application layer not so reliant on the underlying IP layer. This could be done for example by de- coupling the service IP address that end users connect to - and advertising it to data center routers via BGP over only locally significant subnet. Even while there are tools for this sort of decoupling (RIPE 2010), this kind of approach has apparently been deemed as a non-trivial and time-consuming task; hence, currently it would appear that the accepted solution is to introduce more complexity outside the application to hide the underlying already existing complexity of IP transport. One such method is overlay networking, such as VXLAN, that builds up a stretched OSI layer 2 domain over routed network (RFC7348). While there are quite a few methods of implementing encryption in net- work, it should be questioned if it is a sustainable choice to outsource application security to the network layer. Implementing encryption using IPSEC (RFC4301) commonly indicates that OSI layer 3 routing should be implemented

between data centers, while doing routing is a healthy choice for data center interconnect in terms of limiting failure domains. It also means that an overlay net- working is likely required if OSI layer 2 transparency is insisted upon. To implement both OSI layer 2 transparency and encryption one could choose to do encryption on OSI layer 2 via MACSEC (Juniper 2018), VXLAN over IPSEC or by utilizing encryption in DWDM (Arista 2018) level. It should be noted that both MACSEC and IPSEC have an impact in the capacity of performance in terms of payload transferred versus the capacity utilized. Running VXLAN over IPSEC may have an impact in the net payload as well, or at least MTU should be carefully considered. Many public cloud providers such as Amazon (Amazon 2018), Google (Google 2018) and Microsoft (Microsoft 2018) support IPSEC tunnels to tenant specific virtual routing and forwarding instances that are logically separated from one another. Still, it is worth mentioning that even if the data center interconnect from customer data center to cloud provider is encrypted, this does not mean that the internal data center traffic inside the service provider facility is encrypted in any fashion. This is one reason why it might be a good idea not to rely on the network level to implement the encryption but instead utilize sufficient encryption in the application level, just to be sure.

3.12.4 Network as part of defensive arsenal

Network is said to be the first layer of defense in the defense in depth mindset. This is also true for cloud services as the network is still the first contact point for the attacker towards the cloud environment. (Vora 2017.) Network can also provide ideal visibility to the traffic, depending on where the security appliances are placed. In a perfect world, there would be a security device in every ingress and egress point into and onto the network; this would include such as Internet upstream, possible peerings, MPLS links, and encrypted VPN links. Placement of the security device should also take into consideration the possible private IP addresses being used, as it is useful to be able to easily identify which internal IP address is part of the possible alert or packet-filtering rule. (Sanders & Smith 2013)

Generally, security on network layer is built using firewalls, intrusion detection (and prevention) systems, virtual private network (VPN) gateways utilizing encryption, and segmentation to demilitarized zones just to name a few. Next, the basic principles of

few of the aforementioned technologies are discussed and where they might fit in the larger security landscape, starting with the firewall. Firewall is a device that sits between the client and server, and whenever a client is requesting something from the server, the request is first seen by the firewall. Firewalls rely on rules to define what kind of requests are allowed. These rules are based on ports, protocol names (and numbers), IP addresses and flags. (Vora 2017)

There are approximately two different kinds of firewalls: stateful and stateless, the difference being that the stateful firewall keeps track of the connection status so that it knows about the three-way-handshake of TCP, while stateless firewall relies on matching rules against each individual packet. Firewall, in its classical meaning, does not understand the upper layer protocols; this is where IDS or IPS comes in. These techniques usually rely on signatures to identify packets belonging to known attacks and they can then make decisions if a particular packet is to be allowed or denied or if an alarm needs to be raised. IDS can be a complementing feature on a firewall as well. In the cloud context, IDS can be implemented by using cloud service provider's traffic mirroring features, which means that cloud instance would replicate all the traffic it receives and send it to a central IDS for analysis. This has a known drawback of leading to large volume of traffic at peak times. (Vora 2017)

Even higher in the stack after IDS, IPS and the TCP headers is the web application firewall (WAF). WAF can be used when something is required between the client application and the servers, and network layer and transport layer are required to be left open. This is the case with any typical web application that is supposed to be accessible from everywhere in the Internet. WAF is supposed to understand HTTP protocol, SQL, XML and cookies, all parts of the application server or even the application itself. To implement WAF efficiently in-depth knowledge of the application being protected is required. (Vora 2017)

Virtual private network is a completely separate concept of the two mentioned above. VPN is a transport mechanism that creates an encrypted tunnel across the Internet, idea being that plain text packets can be transported over the Internet in a secure fashion. In cloud context the virtual private network could be used for example to migrate virtual machines between security domains. (Xu, Di, Zhang, Cheng & Wang 2011)

3.12.5 Virtual machine image management

To discuss the security aspects of virtual machine disk images, it first needs to be established what is meant by virtual machine disk image. Base images of virtual machines run inside a cloud environment come in two basic form factors: disk images and container images. Disk image represents the underlying hard disk of the virtual machine and there are quite a few different formats to this. (Yeluri & Castro-Leon 2014.)

- RAW is a non-structured image format
- QCOW2 is the format-of-choice of the QEMU system, this supports dynamic expansion and copy- on-write
- VHD is a format accepted by various proprietary systems and KVM amongst others
- ARI is the amazon kernel image

There are others as well, such as VMDK and VDI. Container format on the other hand contains also required metadata about the virtual machine itself in addition to the disk image thus it is not just the backing hard drive. (Yeluri & Castro-Leon 2014)

The images may be provided to the customer by the cloud service provider as pre-configured virtual machine images or the customer may provide their own or even download the images from somewhere on the Internet. Customers should not assume that the pre-configured container images or virtual machines are secure or compliant with the customer requirements, regardless if the cloud service provider provides them, or especially if downloaded from the Internet. In addition to this, it is left to the customer to deal with the patch management of these images as the service provider only takes care of the underlying infrastructure. This has to be seen as a continuous effort, not just as something that takes place only during the initial roll out. (Vacca 2016)

3.12.6 Vulnerability and patch management

As stated above the responsibility of the security posture of virtual machines provisioned in Infrastructure as a service cloud deployment is on the customer. (Vacca 2016.) Be as it may, customer should still make sure that the service provider has a

policy to upgrade and patch their own systems in a timely and safe manner in order to limit exposure. (Winkler 2011)

It is regarded as a best practice to regularly run vulnerability scans. Generally speaking, there are two different types of scans. Firstly, one can initiate scans that are initiated outside of a machine, over the network. These scans can target any device that is reachable and they do not assume access to the target system. Secondly, more thorough scan requires access to the target system in order to create a complete inventory of what the target system has in store, these authenticated scans may take significant amount of time. Ideally, these scans should include everything from cloud management platforms, servers and possible network devices. The idea of the scan is to identify new or left-over vulnerabilities so that the relevant risks might be mitigated. These scans can also be utilized to crosscheck the found devices against the catalog of known devices, if unknown devices are found then more thorough investigation is required. Scans can also help to identify missing patches if the service is reachable over the network. (Winkler 2011)

3.12.7 Log management

First, a definition is given to what is meant by log management. Services, operating systems and applications usually have some means to provide information on errors, warnings and events related to security, for example users logging in and out of a system. These events are stored as log entries, which in turn are the main contents of a log file. The reason behind logging is to use those log files to analyze, debug and optimize systems and services; however, in addition to that they can be used to detect security compromise or attempts at it.

The problem with the logging systems is that quite often they are not configured ideally, meaning that essential messages may go unnoticed in the large stream of messages caused by events of low importance or even those completely irrelevant. Another problem is that users of these logging systems might not even know where to begin their search for specific logs, or how to configure the logging mechanics to begin with. Luckily enough, there are tools that support users in their task of trying to keep track of log files as some tools can even analyze the log files on their own to some extent. These tools are essential since it is of particular importance to filter the

logs for both reasons: to summarize the events and to identify suspicious or even dangerous activity. The usability of these tools can be improved further by configuring automated alarms or in some cases, automated counter measures when there is sufficient evidence about likely malicious actions happening. (Basin, Challer & Schläpfer 2011)

In addition to technical reasons, organizations often try to configure their logging to meet certain audit criteria, for example PCI DSS, an industry standard followed by anyone who handles credit and debit cards. PCI DSS requires that an organization keeps track of all access to resources and cardholder data. Another example could be HIPAA (Health Insurance Portability and Accountability Act from 1996) with rules regarding the system logging. It does not end there, as many of the criteria expect not only logging but also monitoring of the logs. (Smith 2015)

Given the nature of the log files and their purpose, it is essential to safeguard these log files them- selves against compromise as attackers may try to modify log entries in order to cover their tracks. There are several approaches to increase the security of the logs. One approach to improve log file security is to set the log files in append only mode, meaning that log files can be on modified from the end of the file, making it impossible to modify or delete the log entries. In addition, it is advised that log files are readable only by the system administrator as this makes it more difficult for the attacker to construct an idea of normal traffic, hence making it more difficult to hide their activities in a flood of regular activity. The two previous security improvements are based on the idea that the attacker has not compromised the system storing the logs. One approach is to use a separate logging server(s). This can be efficient as it decouples the logs from the server or application that produces the service. As an example, email, DNS and HTTP daemon logs could be copied to a central log server. The result is that the attacker would have to compromise both the service and log server, which allows log server to implement additional security controls.

To harden the remote logging approach, it is feasible to store the log server hostname and IP address in the /etc/hosts file, just in case the attacker manages to disturb DNS leading to difficulties in sending the logs to the remote host. It is also recommended to utilize encryption when sending the logs whenever possible, which can be accomplished using covert channels such as tunneling the log messages. To

further improve the security of log files, one could consider storing the logs to write-once medium, such as CD-ROM. Nevertheless, performance of these mediums is noticeably different especially if considering doing this real-time. A better approach might be to flush the logs to CD-ROM regularly, for example once a day or when a given criterion such as size of a log file is met. (Lantz, Hall & Couraud 2006)

In addition to securing the log servers, much effort has taken place to come up with such cryptographic mechanisms that could same time resist attackers that have gained full control of the logging system that holds the secret key and, on the other hand, still continues to function in order to help exposing the illicit log modifications that might have taken place before to the attacker managed to their hands on the secret key. The main idea of all this is that it would not be possible to modify the logs without being noticed. Since this is seen as impossible using regular means there is a proposal for forward-secure schemes. These take the assumption that time shall be divided into intervals, known as epochs, and different secret keys are used for each epoch. For the sake of efficiency, the secret key for an epoch is calculated using the secret key of the previous epoch t - 1, in addition to that there is one verification key. To make the scheme secure, secret keys are to be securely erased when they expire, this ensures that the attacker cannot reconstruct the signatures of the previous epochs. (Hartung, Kaidel, Koch, Koch & Hartmann 2017)

Given all the above, a customer would do wisely to discuss the approach the cloud service provider has taken concerning the above log management aspects and that it complies with the regulation and criteria expected. On the other hand, customer implements his/her own logging and log management for the application being delivered inside cloud, these also need to be aligned with the requirements.

4 Self-assessment

4.1 Self-assessment of cloud security posture

Before going further, the concept of criteria-based self-assessment and how one might approach the whole concept of self-assessment is discussed. As an example, in educational environment, students can utilize the self-assessment as a means to take

greater responsibility of their own studies as they get to evaluate their own work. This gives a student an opportunity to themselves to detect the areas where they need to improve upon. Via this, they can gain the opportunity to improve their studies independently and in a responsible way as well to monitor the evolution of those studies. (Kokkonen 2012)

Just by reading the above statement and by replacing the words ”student” with ”cloud user”, ”education” with ”IT” and ”study” with ”application” one can see that regular self-assessment works fine with the idea of continuous improvement and when preparing for audits. Self-assessment should not be seen as an exercise in weakness finding that just consumes resources, Kokkonen points out; instead, students should concentrate on the benefits of self-assessment. Similarly, an internal audit or self-assessment run by the organization itself could be seen as means to improve the constantly developing security policy, using the finest controls to the currently known risks that the organization may afford. The attitude of self-assessment, be it for studies or IT, could also be illustrated by as follows: Negative culture pushes persons and organizations towards avoiding getting blamed for mistakes and managing just up to the letter of the law, not any further. Culture of safety, on the other hand, is all about preventing the undesired event from occurring including preventative measures such as transparency and continuous improvement. In addition, in a safety culture, everyone acts as some sort of internal auditor, e.g. spotting flaws and areas of improvement in order to promote safety. Mistakes and findings are not to be used as means to blame someone, but instead they are to be learned from. (Pompon 2016)

4.2 Difference between self-assessment and audit

As stated, self-assessment means observation and evaluation of oneself or activities, viewpoints and performance of one’s capability, performance or ability at a given task in relation to on objective standard. The important issue here is that self-assessment is done by oneself, not by an external party (Oxford dictionary 2018). This is a key differentiation to audit and compliance, as described next.

Prior to going deeper into self-assessment of cloud security posture we need to define what is meant by compliance and audit, and how they differ from self-assessment. The classical definition of compliance is to meet a requirement, yet in the context of security, compliance is a security blueprint for certain type of data. An organization that owns the data defines the minimum level of security. Audit, on the other hand, is the process that measures how the organization is aligned with the given compliance requirement at a given point in time. (Priyam 2018.) Another definition of the term auditing refers to the accounting of user activity on data. This can mean read and write operations, who did them and when. Cloud offers a multitude of options to provide security; yet it largely depends on the requirements and talent available to implement those security features in practice.

It is a key point to understand that the implementation of security in cloud is slightly different from what it is with on-premise or traditional deployments. (Priyam 2018) Oxford dictionary definition of audit states that the audit is an official inspection of entity's accounts by an independent auditor (Oxford dictionary 2018). Another definition of audit is given by Halpert (2011) in his book "Auditing Cloud Computing: A Security and Privacy Guide" as follows: Audit is a method of assuring that certain standard or practice is implemented and this is done by the auditor systematically examining the evidence for the compliance against given criteria. The authors believe that the aforementioned statements highlight the difference of audit and self-assessment.

4.3 Risk analysis: Selecting targets for assessment

In general, decisions related to compliance and security would ideally be backed by risks. To this end, it is important to have accurate understanding of the risks one is ascertaining, as this will make the organization's security policy more effective. For this to happen it is essential to understand the concept of risk. Risk could be defined as a possibility of suffering harm for a particular asset, the asset being anything of value. The value of asset could be interpreted as time and resources required to rebuild or restore the asset to its former state. Vulnerability on the other hand is a

known weakness in that particular asset that could lead to the exploitation of the asset in question. All of this can be put into a form of an equation: r*isk = threat x vulnerability + asset value*. (Bejtlich 2004)

In practice this means that one should identify the key assets, how to handle them and what risks they may pose before spending any money on security. This is called risk analysis and it can be used to identify where the organization should put their focus on in terms of security. Risk analysis will likely not be perfect given the apparent fuzziness of measuring a risk, yet it will probably be better than any guesswork, especially when adapted to each organization and repeated at regular intervals so that it matches the reasonably current situation. Valuable risk analysis could be defined as realistic, actionable and reproducible. (Pompon 2016)

Unfortunately, cloud also presents an extra challenge when conducting risk assessments compared to traditional IT. This represents itself in a form of cloud service providers generally keeping the locations, architectures and other security details of their environment confidential from cloud consumers, which makes it difficult for customers to assess the threats, risks and vulnerabilities of those environments. In addition to this, service providers also have to prioritize the problems they solve first as risks are realized, and these prioritizations might not be openly communicated. This leads to a situation where the customer has to rely and trust on the service provider when carrying out their own risk assessments. The net result of this should be that the accountability and trust are mandatory factors to consider before customer should go forward with a cloud approach. (Cayirci 2015)

Another way to look at the extra challenge of risk management with cloud is to say that cloud service providers design and implement their architectures and services to fit the requirements of a large pool of potential cloud customers in a way that requires the smallest possible amount of per customer customization. Ideally, the responsibility of cloud service providers and privacy controls therein are on the service providers' side and based on applicable laws, directives and standards while being considered for their effectiveness. Service providers do not know the specific requirements and expectations and therefore these controls provided by service providers should be seen as a generic core set of controls available. (Vacca 2016)

Problems aside, according to Pompon (2016), there are essentially two kinds of risk analysis: qualitative and quantitative. Qualitative method is based on specialists doing ratings on the factors against a scale. This scale could consist of levels, such as low, medium and high, or colors and so forth. Pompon also points out that due to the somewhat subjective nature of qualitative method it may need some clarifying for the ratings used. One could utilize a table with meanings, such as the following for likelihood:

- Frequent: Assumed to take place more than 10 times per year
- Occasional: Assumed to take place between 1 and 10 times per year
- Remote: Assumed to take place between 1 time per year and once every 5years
- Very Unlikely: Assumed to take place less than once every 5 years

Pompon (2016) also proposes three impact ratings: minor, major and critical. All three of these can also be split into three sub categories: confidentiality impact, integrity impact and availability impact.

To elaborate on the impact ratings, an example of confidentiality of minor scale could be under 10 database records of confidential nature being exposed internally without any proof of exploitation, while the major impact of the same thing would entail that several internal employees with no authorization having accessed these records. Critical rating would be under ten data records being exposed externally or more than ten records exposed internally. Integrity impact follows the same guidelines but it essentially replaces the exposure of data with data being altered without authorization and whether the alteration can be detected and corrected. Availability impact is a slightly different concept; minor being several users having no access for from one to five days, or customer facing service down up to an hour. Major availability impact could be characterized as a customer facing service being down for more than an hour but less than a day; critical represents a situation where a customer facing service is down for more than a business day. (Pompon 2016)

Quantitative risk analysis utilizes real statistics and data instead of subjective specialist opinions. These statistics can be collected from asset analysis and monitoring systems. Similarly, as with qualitative analysis, an organization shall match its assets

against attack surface, known weaknesses and implemented controls. For example, if a company hosts ten websites (assets) it might know that on average it is missing two security patches on each (weakness) and the control against this weakness could be a firewall (control). Another example that follows the same lines would be: 350 (attack surface) users (asset) are subject to social engineering (weakness) but only 4 % failed the last phishing test training (control). While the above gives a reference point it is likely that in the end something like security steering committee will make subjective calls; however, at least they will have best possible data to base their decisions on. With risk and asset information at hand, it is easier to select the aspects to self-assess.

4.4 Controls to assess

According to Chris Jackson's book Network Security Auditing (2010) There are three main categories of controls:

- Administrative controls are made up of policies, training and processes.
- Technical controls include technologies such as firewalls and IDS to name but a few, which are used to implement access control.
- Physical controls are used to control the physical access to resources, for example locks and fences fall into this category.

These same categories can also be found from the Katakri tool (Katakri 2015), similarly these primary control groups can be further split into more granular controls:

- Preventative controls such as firewalls, login banners and policies are used to enforce confidentiality.
- Detective controls are in essence alarming mechanisms to indicate that bad things are happening.
- Corrective controls can be used to double check that security controls are in place and take actions if needed.
- Recovery controls come into play if the bad thing happens. Examples are backup, redundant power supplies and spare parts.

Interleaved nature of the various controls described above provides a way to investigate whether service provider, customer of application being assessed has met and implemented its controls to sufficient level. (Jackson 2010)

5 Self-assessment

This self-assessment is based on key points that were found the most important from the literature and covered throughout this thesis. In some areas ideas behind Katakri 2015 are followed; yet, as the target audience of these criteria is not officials but instead common businesses, organizations and individuals, several topics from Katakri are out of scope. Yet, as these criteria are based on common topics, this applies to official data as well.

Similarly to Katakri, this self-assessment is divided into three sections: administrative, physical and information technology sections. In this thesis, each of the criteria within the sections is described in relation to this thesis. In addition, a spreadsheet for self-assessment purposes is distributed as an attachment.

5.1 Administrative topics

5.1.1 Documentation

When it comes to transferring data and services to cloud, it is important that the customer understands the type of the cloud used and its features, possibilities and threats, which are described in sections two and three in this document. To succeed in these matters, several documents should exist to write down the needs and restrictions and to show that the cloud's distinctive features are understood. The following documents are an example of written acknowledgement of fulfilling this:

- BCP - Business continuity plan.
- DRP - Disaster recovery plan.
- RTO - Recovery time objective.
- RPO - Recovery point objective.
- Risk analysis.
- Infrastructure and service documentation.

As described in section 3.1, business continuity plan aims at ensuring the organization's ability to function in case of a disaster. It also describes certain important roles among the personnel and notify different systems and infrastructure that is needed

both in the normal operations and during a disaster. Disaster recovery plan provides further details to ensure the safety of business and personnel.

The RTO and RPO requirements describe in sections 3.1.1 and 3.1.2 can have much value in a cloud environment, especially as cloud services are usually meant to be online and accessible around the clock. In addition, as the cloud provider is usually a different entity, these documents can aid in choosing a suitable service provider and guide the organization in making the contract with the provider. Written RTO and RPO can also help in monitoring the service later on, especially after an incident requiring a realization of recovery needs. Similarly, written RTO and RPO can be tied to the possible service level agreement as parts of the criteria.

As cloud creates new risks with the new possibilities, a sufficient risk analysis documentation can help recognizing what measures are needed to protect the service and data, this is discussed in detail in section 4.3. A comprehensive risk analysis should also recognize the distinctive features of the chosen cloud deployment method described in 2.3 and hosting type described in 2.2. A wide variety of issues to consider in their security are described through sections from 3.3 to 3.8. Although private cloud can greatly resemble a traditional self-hosted environment, especially public cloud brings new risks the analysis should be aware of:

- Multi-tenancy, as different customers may have access to the same infrastructure, including for example APIs and hypervisors.
- Certain responsibilities now falling to the service provider's field, including patching and updating servers.
- Geographical location may vary, as described in 3.2.2 and 3.2.3.
- A malicious actor has many of the same advantages as the customer.

Nevertheless, as the private cloud does not necessarily impose the aforementioned risks, it may not provide the expandability the public cloud offers, which often might be one of the key reasons to choose using a cloud service in the first place. A thing to consider with the chosen deployment method from the risk perspective could be for example the responsibilities and capabilities. A variety of tasks is now on the service provider, yet the ability for the customer to modify the services might be limited although possibly less demanding.

In addition to administrative documentation, it is vital to have a decent description of the service and data. This documentation is needed throughout this self-assessment to verify that the needs are met. In this documentation, the customer can for example spot the data locations, connections and possible data replication.

5.1.2 SLA

Existence of a service level agreement contract can help to ensure the service level offered by the cloud provider meets the needs of the service. The customer should have a clearly stated requirements from their side, matching the provider's promise. Even if the contract itself is important, it is equally as important to get it implemented and monitored to ensure that the goals are met, as described in chapter 3.10.2.

5.1.3 Transferability

As cloud is meant to be agile, it is important to ensure that data and services can be easily transferred. Thus, as it is a basic feature of a cloud that the capacity can be increased and decreased if needed, it is important that this is ensured in contracts and chosen technologies. It is also important to be able to transfer a service elsewhere, if for example a service provider ceases to exist or does not meet the requirements, to name a few examples. Transferability can especially help fighting a possible vendor lock-in situation. Some key points can be picked from chapter 3.2.1 Vendor lock-in:

- Ensure common standards are used
- Ensure common protocols are used
- Ensure policies will not prevent data transfer

The ability to transfer services from a provider to another is not only about using certain formats and standards, but also the many functionalities and features below this. As described in 3.2.4, division of responsibility plays a major role in preparation for disasters and for ensuring recovery, which can also be about moving the service around. As the responsibilities of data and service are shared between the customer and service provider, there should be a clear understanding on duties that fall into either one's field. Furthermore, the customer should have some means in place to

realistically be able to transfer the service to another provider's infrastructure in case of need.

5.1.4 Regulations

Especially as cloud can be often hosted in distinctive geographical locations as stated in 3.2.2, reviewing possible legislative and regulatory limitations is essential, as described in 3.2.2 and 3.2.3. To succeed in reviewing the requirements, it is self-evident and mandatory that the data, customers and other possible factors are recognized to successfully recognize the relevant regulation. As described in 3.2.3, the data residency has a major role as laws and regulations can greatly vary in different countries. As a result of this, the country's regulations must be studied to ensure compliance the local limitations. As an example of this in Finland, the customer must especially recognize the possible use of personal data, where GDPR will have major consequences. Other examples are certain types of data and customers, which have to follow criterion or recommendations such as Katakri or VAHTI.

The customer should note that regulations may also change as they knowingly do, and additionally they might impact the requirements through the entire lifecycle of the service and data (Katakri 2015). Thus, a frequent review process of these should be in place to fully ensure meeting the requirements through all the lifetime of the service and data.

5.1.5 Personnel

As this self-assessment does not focus on any kind of classified data, possible background checks are not covered here. It is left to the organization to decide whether they are needed in some roles or not.

To protect against human related factors, the organization should firstly recognize the key roles. Some, e.g. managers, are also mentioned in chapter 3.10.4 covering human factors in certain types of attacks. The customer should train their personnel frequently to recognize and defend against human related attacks, as these can be easy to execute successfully. As important as it is to train the customer's personnel, the customer should have means to ensure that the service provider is committing itself to the same level of training at least, unless stated otherwise in contracts. To

successfully train all employees, the management should be strongly involved to get the necessary resources and time, and to maintain a grasp of who is trained on what and at what point of time. To this end, a log of taken trainings should be kept.

5.1.6 Incident response

Having a proper process, personnel and technologies to handle incidents is a relatively big task that should apply at least to the topics described below:

- Ensure that the responsibilities are defined between the customer and provider.
- Ensure the service provider and the customer have sufficient strategy for incidents.
- Ensure the service provider and the customer have the ability to properly handle incidents.
- Ensure that proper technology to identify potential attacks exist and operate properly, these can be for example intrusion detection or prevention systems and proper logging infrastructure.
- Ensure that dedicated personnel exists to handle the incidents, the incident response team should have the ability to analyze, respond, escalate and to report any incidents.

As described in section 3.2.6, incidents do happen despite of different preventive actions. In a customer-provider relationship it is advised to have a tested incident response process that is agreed upon by the parties, thus the roles described in the previous chapter might greatly vary depending on the case. To further highlight the importance of incident response, the incident response is not just about taking action in times of trouble, but also having the ability to recognize and contain them is just as important. For the future, it is also essential to be able to improve the systems and processes according to post incident analyzing.

5.2 Physical security and continuity

5.2.1 Physical security and continuity of cloud infrastructure

Physical security in cloud environments is a complex topic to tackle, especially as the customer does not necessarily have any chance of studying this matter towards the provider. This is especially true with public clouds, where the customer does not necessarily have any control over the infrastructure whatsoever, as described in 2.1. If a private cloud is used, the customer can more freely apply methods of necessity to ensure meeting the needs covered under aforementioned topics such as the risk analysis.

As stated before, there might be very little the customer can do for the physical security. Nevertheless, from generic topics like SLA several issues can be derived:

- Verify the cloud provider's documentation about physical security.
- Verify that the physical security meets the needs of generic requirements for the customer.

5.2.2 Supply chain security and continuity

Supply chain is a commonly known risk factor, as depicted in chapter 3.10.3. In addition to keeping the new hardware, software and installations secure, it is also as important to keep them available with a decent delivery time in all possible situations to ensure availability of the service. It is worth noting that this can also be an important factor in disaster recovery. A customer should ensure that the following threats are under control, with methods such as contracts, controls, policies and monitoring:

- Software or hardware installation with malicious purposes
- Fake software or hardware installation
- Distribution or production failures
- Non-satisfactory service provider
- Vulnerabilities in software or hardware

5.3 Information Technology

5.3.1 Defence in depth

Defense in depth is a common concept in information technology and it involves zoning of the architecture into smaller parts, as described in chapter 3.10.1. Creating multiple layers of security can help during the incident when protecting more sensitive parts of the infrastructure or operations via creating more capabilities to withstand attacks. Based on Katakri 2015, components such as network could be divided into different zones applying the same defense-in-depth method to this concrete design to protect more sensitive data.

A way to validate defense in depth is in use, could be to verify if there is for example some isolation between different segments, such as demilitarized zone and internal zone, via firewalls and VPNs to name a few as described in chapter 3.12.4. On the other hand, also the existence of several different methods of protection could be taken as a visible proof of such actions, these could be for example including user policy, firewalls, intrusion detection system and virus detection to protect a single machine.

5.3.2 Segregation of duties

The chapter 3.2.5 explains the basics of the need of segregation different duties in different environments. The customer should ensure that the same person cannot for example initiate and accept the same transaction, in addition all changes should be trackable. The requirement of segregating duties applies to both customer and service provider and this should be ensured to minimize any potentially malicious actions. Good examples in the cloud concept could be for example ensuring that:

- A single person cannot access all steps of for example a log transfer.
- The provider’s policies, ability and strategy are satisfactory.
- Changes done by all parties are tracked.

5.3.3 Encryption and key management

As in cloud the data practically never resides in the customer's isolated protected zone, the data should be encrypted whenever possible, as described in chapter 3.11.1 and 3.11.4. To ensure this is done, there should be a decent documentation displaying all data locations and data flows. It should be also ensured that the encryption algorithms used in all locations and connections are decent ones, for example AES, but should always be according to regulations and recommendations. The software used to do the encryption should be of good reputation and according to regulations, and if possible accepted by national authorities, as encryption software is known to often have problems.

To ensure proper security, key management is a vital part of proper encryption. Firstly, the keys used should be of acceptable length, for example following regulations or current recommendations. The same applies to the frequency of key renewals. The keys should always be kept very secure and there should be minimal risk of their exposure to unauthorized actors, as described in 3.11.2. Additional focus should be targeted also at the service providers, as they might have open access to for example devices and network.

In addition to key management and encryption as such, it should be ensured that no encryption keys are sent or visible by mistake. This might require ensuring for example the behavior of software, configuration, key locations and network access. In addition, it should be ensured that no sensitive data is transferred via unencrypted channels like email. In addition to adding more reliance to network, properly planning the network can add to security, as described in chapter 3.12.2 In many cases encryption of connections can be applied in network devices in the means of for example MACSEC or IPSEC, although this cannot necessarily be applied to data transfers inside the data centers.

In some cases, other means than encryption could also work, such as information hiding described in 3.113. Cloud and technology in general will evolve and there might be other decent methods to secure data, which could be sufficient to some cases, for example the information of critical nature could be hidden inside larger set of public data.

5.3.4 Backups

Although the cloud has brought in many new features, the challenge of backing up data still persists, as cloud providers do not necessarily provide any features like this. Cloud may provide many possibilities in addition to the old-fashioned backups as described in chapter 3.12.1, nevertheless, it must be ensured that the chosen mean is usable and reliable in any thinkable scenario. To ensure recovery of data, the customer should ensure if for example one of these methods is in use:

- Backup to a geographically separate location using for example traditional backup systems.
- Replicating a necessary part of the service and data to a separate location or different availability zones.

It should also be ensured that in case of a complete data loss the recovery can be done, this means that the data is in such a format that it is usable in different platforms and that the data can be transferred from the backup system to the new production environment. To ensure this, a frequent recovery test can act as a decent proof that the backup system meets the needs.

5.3.5 Authentication

As described in chapter 3.12.2, proper authentication and identification should be in place. The authentication should be verified throughout the service, as a result of which the customer should ensure that the services provided by the cloud service provider also comply with the necessary authentication and identification requirements. Two-factor authentication is a preferred method when applicable. As a conclusion, at least the following should be ensured:

- Logon ID does not consist of person's name, title or similar easily accessible data.
- Authentication should be constructed using at least one of the following: something the user knows, the user has or is unique to each user.
- Authentication data is protected as sensitive data (Katakri2015).
- Authentication is needed to identify the user in all necessary actions (Katakri 2015).

Even more requirements can be added if for example applicable regulations pose requirements of this nature.

5.3.6 Lifecycle management

Even though the implementation of a service is a very important concept, the maintenance and decommissioning play equally as important role, as described in chapter 3.10.5. The organization should ensure that it has an up to date registry of all the services and systems properly set up and maintained. To succeed in setting up a new service according to business needs the service specifications should be properly described, this can also help later during the lifetime.

During production state the lifecycle management should ensure that business processes are properly executed on the service. During runtime the service should be monitored, both from the business perspective and operational state, which can also add to security. Proper data can also help the customer recognizing that contracts - such as SLA - are respected.

The decommissioning phase is the final step in the service lifecycle. The customer should ensure that the outdated service is properly removed, the data disposed of or transferred securely. The lifecycle management process should ensure that no services are just forgotten, as this may pose an unnecessary business and security related risk.

5.3.7 Hardening

Often in cloud environment, the service provider might be providing the disk images as described in chapter 3.12.5. The customer should not forget that also in SaaS deployments, not only in IaaS and PaaS, the virtual machine still runs an operating system. To verify that the virtual machine images can be trusted, the following details at least should be checked:

- Processes, contracts or similar methods exist to define secure sources for images.
- The images used in virtual machines are according to customer requirements.

For example, the images might be required to be hardened or patched in a certain manner or frequency, which should be also monitored.

5.3.8 Vulnerability and patch management

The customer should ensure that proper management of patches and updates are applied by both the customer itself and also the service provider, the details vary greatly depending on the chosen deployment. As described in chapter 3.12.6 also the underlying infrastructure should be patched in a timely manner, not alone the services running on top of them. This should be in the service provider policies.

To help with the vulnerability and patch management automated security scans should be used. These could be done in an agreed and timely manner over the entire network and independent servers. A proper scan should include all, including the management platforms, servers and possible network devices, not forgetting the customer's services built on them.

5.3.9 Log management

Logs can play an important part in all service monitoring and security. The customer should ensure that the logging infrastructure is decent to provide logging for example service optimization, debugging and about events of security compromises, as described in 3.12.7.

As the size of logs are easily enormous, the customer might have a need to have proper systems to also analyze the log files. The logs should also be properly configured to provide the necessary information throughout the system. Log files must be safeguarded against tampering to ensure authenticity of the logged actions. In a cloud environment many of the log files can be out of the customer's reach directly, in this case there should be policies for the service provider to provide the necessary information without possible exposing data from other tenants sharing the infrastructure.

As usual, the log files may contain sensitive information. Thus, any transfer or storage of log files should be properly protected from unauthorized access throughout the entire lifetime. In addition, the log servers should be heavily protected so that for

example the proof of a security breach cannot be easily wiped out by the malicious actor. There might also be some regulation that is found in Katakri 2015 which regulates the storing time of logs.

6 Conclusions

Even though the cloud as a technology has been existing for several years, there are still surprisingly little material available in terms of audit criterion, this became a reality when authors started to gather material for this thesis. Especially the security in cloud seems to be investigated quite little, even though there is definitely need for this. However, as there was rather limited material to use for this cloud security survey, especially given the confidential nature of the questionnaire, the shortcomings were seen more like a challenge and something that we took as a sign of need for the thesis. The shortage of material was not the only challenge as the material we found was often written from different standpoint. As this thesis was made by two technically oriented professionals, the lack of real-life experience of many writers was quite disturbing. Nonetheless, from the material a few real treasures were found, such as Halpert's book of cloud security and privacy, also there are some academic material that discusses cloud in particularly from descriptive stand point, such as the master's thesis of Saara Suikkanen that provides clear descriptions and definitions for basic concepts of the cloud. While not maybe 100uating if a solution proposed by service provider is compliant with the standards. Also, as our focus was strongly from the audit perspective, many of the sources seemed quite shallow and eve n naive.

Although the aging criteria in Katakri 2015 was a big motivator on this, it was clear that it wouldn't fully benefit the target audience as such, as many of the criterion in it are too complex, controversial or just simply too tight for trivial business use-cases. Nevertheless, during the writing process of this thesis, there was an ongoing debate with a cloud criterion going on in Traficom, which we provided some feedback to. Another motivator was the Cloud Alliance's Cloud control matrix. We went through it with much detail, although this work didn't find its way to this thesis. Nevertheless, many of the core topics can be found in here. The biggest challenge with the Cloud Alliance's Cloud control matrix is the mere size of it: dozens and dozens of criterions makes it purely exhausting. One of the key aspects to this work was to avoid coming up with too technical audit criterion, this was deemed as especially important in order to avoid non-technical parties being ”scared” with audit text. Authors tried to

compensate on this with more detailed introduction to cryptography and the availability aspects within networking. In the end, we are quite happy with some of the criterion, but there are some flaws also. We managed to keep the criteria in a manageable amount, yet in our material some obvious details were neglected, similar to network time protocol or precision time protocols, as it is important particularly in logs. In addition to missing network time protocol, also and protecting administration connections, which is one of the top three things to secure, is neglected, yet a knowledgeable person would most likely include this into defense-in-depth. Although we would have wanted to add several details here and there, we left them out because of the fact that these were not mentioned in the source material, yet a skilled technician can understand that at least these two examples are a part of logging and encryption with defense in depth.

During the time of writing, Traficom's cloud criteria was worked upon. As one can guess from Katakri, certain administrative issues are covered there in more detail as well as personnel related issues, as these requirements often come strongly from legislation e.g. the ”need to know” principle. For the same reason data classification and separation is emphasized. These difference s are very natural and are to be expected. Yet, topics like secure development conventions missing in this thesis is a bit annoying fact, though it is natural when judging the source material - secure development conventions aren't seen as a cloud related topic but instead, a software development related topic. A major flaw in all criterion and assessments is their long update procedure - they do now react to new emerging threats very fast. It is a hard topic to figure out how to expect or even demand something that is during the publication time completely vague. Maybe these could be derived from awareness, roles and training, but this would still be quite superficial.

In a cloud environment, as well as actually any environment that is not very simple and thus self- evident, it is not possible to achieve perfect security. The correct way of thinking might be to mix both technical and contractual details to gain sufficient level of trust, this viewpoint can be in our opinion derived from lot of the cloud material available, as this thesis has pinpointed several issues related to that, and also from the fact that e.g. the cloud alliance cloud criteria and Traficom's work address legislative and contractual details quite strongly. As new technologies emerge in

huge speed and there is often a lot of pressure to adapt these to different environments, one should probably try to think modern IT systems from the business point of view, not just from technological viewpoint. In this possibilities, contracts and different actors playing together can create a secure and prudent environment.

References

Ahlgren, J. 2012. *Reasons to Think About Cloud Computing*. Bachelor's thesis. Metropolia. Accessed 10 November 2018. Retrieved from http://urn.fi/URN:NBN:fi:amk-201303243590.

Aiguokhian, E. 2013. *Supply Chain Security Using RSA Algorithm*. Master's The- sis. Savonia University of Applied Sciences. Accessed 28 January 2019. Retrieved from http://urn.fi/URN:NBN:fi:amk-201302052078.

Aikaterini, S. 2014. *Systematic Service Level Agreement SLA data management*. Doctoral the- sis. University of Geneva. Accessed 10 November 2018. Retrieved from https://archive-ouverte.unige.ch/u- nige:40738.

http://www.tandfonline.com/loi/htip20 Andrade, H., Valtcheva, A. 2009. *Promoting Learning and Achievement Through Self-Assessment*. Routledge, Taylor & Francis Group https://doi.org/10.1080/00405840802577544.

Andreasen, M., Norgaard, T., Mot, A,. Snowman, P., Buecker, A., Frehr, C., Peen, S., Johnston, W.C. *Key management deployment guide : using the IBM Enterprise key management foundation*. 2014. IBM Redbooks. Accessed 10 January 2019. Retrieved from http://www.redbooks.ibm.com/redbook- s/pdfs/sg248181.pdf.

AWS Whitepaper. 2019. *AWS Managed VPN Connections Amazon*. Accessed 28 March 2019. Retrieved from https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity- options/aws-managed-vpn-network-to-amazon.html

Basin, B., Schaller, P., Schläpfer, M. 2011. *Applied Information Security: A Hands- on Approach*. Springer-Verlag Berlin Heidelberg. Accessed 18 January 2019. Retrieved from https://doi.org/10.1007/978-3-642-24474-2.

Bejtlich, R. 2004. *The Tao of Network Security Monitoring Beyond Intrusion Detection*. Addison- Wesley Professional. https://isbnsearch.org/isbn/9780321246776.

Blount, S., Zanella, R. 2010. *Cloud Security and Governance: Who's on your cloud?*. IT Governance Publishing. https://isbnsearch.org/isbn/9780321246776.

Bond, J. 2018. *Cloud security*. O'reilly media, inc. https://www.oreilly.com/library/view/cloud- security/9781492033790/.

Buyya, R., Broberg, J., Goscinski, A. 2011. *Cloud Computing: Principles and Paradigms.* John Wiley & Sons. https://isbnsearch.org/isbn/9780470887998.

Casola, V., De Benedictis, A., Rak, M. 2014. *Accountability and security in the cloud. First Summer School, Cloud Accountability Project*, A4Cloud, Malaga, Spain. https://isbnsearch.org/isbn/9783319171982.

Cayirci, E. 2014. *Models for Cloud Risk Assessment: A Tutorial. First Summer School, Cloud Accountability Project*, A4Cloud, Malaga, Spain. https://isbnsearch.org/isbn/9783319171982.

Childs, D.R. 2008. *Prepare for the Worst, Plan for the Best: Disaster Preparedness and Recovery for Small Businesses*. John Wiley & Sons. https://isbnsearch.org/isbn/9780470170915.

Cohn-Gordon, K., Cremers, C., Dowling, B,. Garratt, L., Stebila, D. 2017. *A Formal Security Analysis of the Signal Messaging Protocol.* University of Oxford, UK, McMaster University, Canada, Royal Holloway, University of London, UK. Accessed 10 January 2019. Retrieved from https://eprint.iacr.org/2016/1013.pdf.

European Commission. 1995. *Directive 95/46/EC* Accessed 9.1.2019. Retrieved from https://ec.eu- ropa.eu/eip/ageing/standards/ict-and-communication/data/directive-9546ec_en.

European commission. *Official GDPR website*. Accessed 7.1.2019. Retrieved from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

Farley, M. 2013. R*ethinking Enterprise Storage: A Hybrid Cloud Model.* Microsoft Press. https://isbnsearch.org/isbn/9780735679603.

Google cloud documentation. 2019. *Cloud VPN Overview*. Accessed 28 March 2019. Retrieved from https://- cloud.google.com/vpn/docs/concepts/overview.

Halpert, B. 2011. *Auditing Cloud Computing: A Security and Privacy Guide*. John Wiley & Sons. https://isbnsearch.org/isbn/9780470874745.

Harilainen, H-R. 2014. *Managing Supplier Sustainability Risk*. Doctoral thesis. Hanken School of Economics. Accessed 28 January 2019. Retrieved from https://helda.helsinki.fi/handle/10138/44842.

Hartung, G., Kaidel, B., Koch, A., Koch, J., Hartmann, D. 2017. *Practical and Robust Secure Logging from Fault-Tolerant Sequential Aggregate Signatures*. Springer. Accessed 18 January 2019. Retrieved from https://eprint.iacr.org/2017/949.pdf.

International Atomic Energy Agency. 2002. *Safe and effective nuclear power plant life cycle management towards decommissioning*. International Atomic Energy Agency. Accessed 21 January 2019 from. Retrieved https://www-pub.iaea.org/MTCD/Publications/PDF/te_1305_web.pdf.

International Atomic Energy Agency. 2001. *Managing change in nuclear utilities.* International Atomic Energy Agency. Accessed 27 March 2019. Retrieved from https://www-pub.iaea.org/MTCD/Publications/PDF/te_1226_prn.pdf

Jackson, C. 2010. *Network Security Auditing*. Cisco Press. https://isbnsearch.org/isbn/9781587053528.

Jamsa, K. 2012. *Cloud Computing*. Jones & Bartlett Learning. https://isbnsearch.org/isbn/1449647391.

John, R. V. 2016. *Cloud Computing Security*. CRC Press. https://doi.org/10.1201/9781315372112.

Kavis, M. 2014. *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)*. John Wiley & Sons. Accessed 25.9.2018. Retrieved from http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=62597.

Kim, D., Sejun, S., Choi, S-B. 2017. *Data Deduplication for Data Optimization for Storage and Network Systems*. Springer. Accessed 11 January 2019 from. Retrieved https://doi.org/10.1007/978-3-319-42280-0.

Kizza, M. J. 2012. *Guide to Computer Network Security*. Springer. Accessed 15.1.2019. Retrieved from https://doi.org/10.1007/978-1-4471-6654-2.

Ko, R., Choo, R. 2015. *The Cloud Security Ecosystem*. Syngress. https://isbnsearch.org/isbn/9780128015957.

Kokkonen, T. 2012. *The experiences with and opinions on self-assessment among students and their teachers*. Master's Thesis. University of Jyväskylä. Accessed 10 January 2019. Retrieved from http://urn.fi/URN:NBN:fi:jyu-201205241727.

Krutz, RL., Dean Vines, RD. 2010. *Cloud security: A comprehensive guide to secure cloud computing*. John Wiley & Sons. https://isbnsearch.org/isbn/9780470589878.

Lantz, B., Hall, R., Couraud, J. 2006. *Locking down log files: enhancing network security by protecting log files*. Utah State University. Accessed 18 January 2019. Retrieved from http://iacis.org/iis/2006/Lantz_Hall_Couraud.pdf.

Loske, A. 2015. *IT Security Risk Management in the Context of Cloud Computing*. Springer Fachmedien Wiesbaden. Accessed 7 January 2019. Retrieved from https://doi.org/10.1007/978-3-658-11340-7.

Mather, T., Kumaraswamy, S., Latif, S. 2009. *Cloud Security and Privacy*. O'Reilly Media, Inc. https://isbnsearch.org/isbn/9780596802769.

May, C J., Hammerstein, J., Mattson, J., Rush, K. 2006. *Defense in Depth: Foundations for Secure and Resilient IT Enterprises.* Carnegie Mellon University. Accessed 22 January 2019. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?rep=rep1&type=pdf&doi=10.1.1.208.737.

McGrath, M. P. 2012. *Understanding PaaS*. O'Reilly Media, Inc. https://isbnsearch.org/isbn/9781449323424.

Mehan, J. 2014. CyberWar, *CyberTerror, CyberCrime and CyberActivism*. IT Governance Publishing. https://isbnsearch.org/isbn/9781849285711.

Microsoft Azure. 2019. *Azure VPN Gateway Documentation*. Accessed 28.3.2019. Retrieved from https://docs.microsoft.com/en-us/azure/vpn-gateway/.

Ndungu, M,. Kandel, S. 2015. *Information security management in organizations*. Bachelor's thesis. Centria university of applied sciences. Accessed 28 January 2019. Retrieved from http://urn.fi/URN:NBN:fi:amk-2015061613437.

Nelson, S. 2011. *Pro data backup and recovery*. Apress. Accessed 9 January 2019. Retrieved from https://www.apress.com/us/book/9781430226628.

Nohlberg, M. 2008. *Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks*. Doctoral thesis. Stockholm University, University of Skövde. Accessed 28 January 2019. Retrieved from http://www.diva-portal.org/smash/get/- diva2:200190/FULLTEXT01.pdf.

Packetworks. *The risks of not having business internet redundancy*. Accessed 3 April 2018. Retrieved from http://www.packetworks.net/blog/the-risks-of-not-having-business-internet-redundancy.htm.

Pepelnjak, I. *Distributed firewalls: how badly do you want to fail?* Accessed 3.4.2018. Retrieved from https://blog.ipspace.net/2011/04/distributed-firewalls-how-badly-do-you.html.

Pham, H., Woodworth, J., Salehi, M. A. 2018. *Survey on Secure Search Over Encrypted Data on the Cloud*. University of Louisiana at Lafayette, LA, USA. Accessed 11 January 2019. Retrieved from https://arxiv.org/pdf/1811.09767.pdf.

Pompon, R. 2016. *IT Security Risk Control Management: An Audit Preparation Plan*. Apress. https://doi.org/10.1007/978-1-4842-2140-2.

Sanders, C., Smith, J. 2013. *Applied Network Security Monitoring*. Syngress. https://isbnsearch.org/isbn/9780124172081.

Smith, R. E. 2015. *Elementary Information Security, 2nd Edition*. Jones & Bartlett Learning. https://isbnsearch.org/isbn/9781284055931.

Stevenson, A. 2018. *Oxford dictionary of English*. Oxford University Press.

Suikkanen, S. 2013. *Cloud computing, Tieto cloud server model*. Master The- sis. Saimaa University of Applied Sciences. Accessed 10 November 2018. Retrieved from http://urn.fi/URN:NBN:fi:amk-2013060613360.

Sun, X., Pan, Z., Bertino, E. 2018. *Cloud computing and security : First International Conference, ICCCS 2015, Nanjing, China, August 13-15, 2015, Revised selected papers.* Springer. Accessed 9 January 2019. Retrieved from https://link.springer.com/book/10.1007/978-3-319-48671-0.

Thai Tran, H., Feuerlicht, G. 2015. *Service Repository for Cloud Service Consumer Life Cycle Management.* Faculty of Engineering and Information Technology, University of Technology, Sydney. Accessed 21 January 2019. Retrieved from https://link.springer.com/con- tent/pdf/10.1007%2F978-3-319-24072-5_12.pdf.

Vilkka, H. 2015. *Tutki ja kehitä*. PS-Kustannus.

Vora, Z. 2017. *Enterprise Cloud Security and Governance*. Packt Publishing. https://isb- nsearch.org/isbn/9781788299558.

Wan, J., Lin, K., Zeng, D., Li, J., Xiang, Y., Liao, X., Huang, J,. Liu, Z. 2016. *Cloud Computing, Security, Privacy in New Computing Environments,2016. Conference, SP- NCE 2016, Guangzhou, China*. Accessed 3 January 2019. Retrieved from https://link.springer.com/content/pdf/10.1007%2F978-3-319-69605-8.pdf.

Wayner, P. 2009*. Disappearing Cryptography, 3rd Edition*. Morgan Kaufmann. https://isbnsearch.org/isbn/9780123744791.

Winkler, V. 2011. *Securing the Cloud*. Syngress. https://isbnse- arch.org/isbn/9781597495929.

Xu, Z., Di, S., Zhang, W., Cheng, L., Wang, C. 2011. *WAVNet: Wide-Area Network Virtualization Tech- nique for Virtual Private Cloud. IEEE*. Accessed 15 January 2019. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6047197.

Yang, K., Jia, X. 2013. *Security for Cloud Storage systems*. Springer. Accessed 11 January 2019. Retrieved from https://doi.org/10.1007/978-1-4614-7873-7.

Yeluri, R., Castro-Leon, E. 2014. *Building the infrastructure for cloud security: a solutions view.* Apress Accessed 3 December 2018. Retrieved from https://doi.org/10.1007/978-1-4302-6146-9.

Appendices

Appendix 1. Self-assessment sheet

Self-assessment for Organization Y

Instructions

Read through the requirement and examples. Fill in to the empty column by answering these questions:

1. How is this requirement currently fulfilled?
2. What is currently missing in order to meet this requirement? Make notes of the findings:

- Is there an administrative issue keeping the organization from meeting the criteria?
- Are there resourcing issues that prevent the organization from meeting the criteria?
- Maybe there is an acknowledged residual risk that makes the criteria obsolete?
- Are there technical reasons or measures that full fill the criteria via other means?

Administrative requirements

1.1	Documentation	Notes
Existence of necessary documents	• Business continuity plan exists • Disaster recovery plan exists and includes this service • Recovery time objective is defined for this service • Recovery point objective is defined for this services • Risk analysis exists and is regularly updated • Infrastructure and service documentation is written and has a process for frequent updates	
Reference	2.2, 2.3, 3.1, 3.1.1, 3.1, 3.2.2, 3.2.3, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 4.3	

Examples	• Business continuity and disaster recovery plans are written and updated as needed, and they include this service.
	• Recovery time objective is defined for this service. A defined RTO aims at ensuring that the service level is met by the provider and ensures the service quality can be monitored.
	• Recover point objective is defined for this service. A defined RPO aims at ensuring that the service level is met by the provider and ensures the service quality can be monitored.
	• A comprehensive risk analysis is written and it includes threats for this service. A comprehensive risk analysis should take into account for example:
	  ○ The chosen cloud type and deployment model are recognized and the threats they imply are verified.
	  ○ Possible threats derived from e.g. multi-tenancy,	

	responsibilities and geographical location are recognized and analyzed. • There exists for documents that for example describe the service's architecture, data locations, data flows and interfaces. This documentation is up-to-date. • The necessary documentation is up-to-date and there exists a process to continuously update these. Also, the documentation should also include the cloud provider's aspect.	

1.2	**SLA**	**Notes**
Service level agreement documents	• SLA contracts exist with some or all service providers • SLA meets the needs of the service or services	
Reference	3.10.2	
Examples	• SLA contracts are done with all necessary cloud providers. • The documents are signed by all involved parties. • The SLA requirement follows the needs specified in the service descriptions. • The SLA documents ensure quality, reliability, security and scalability of the service.	

1.3	Transferability	Notes
Technologies and contracts enable fast transfer of the service and data	• The service uses common standards • The service uses common protocols • The policies do not prevent data transfer	
Reference	3.2.4	
Examples	• The programming languages and data formats to name a few are common and not e.g. proprietary. • The protocols used in the service and related services are common and not e.g. proprietary. • There exists e.g. another service provider to whose infrastructure the service could be transferred. • There are no contractual limitation to transfer the service or the limitations are recognized and there is a plan to overcome them.	

1.4	Regulative requirements	Notes
Requirements set by regulations	• Necessary documents exist to depict the regulations each party and service has to commit into • Procedures exist to audit and update the documentation and procedures regularly	
Reference	3.2.2, 3.2.3	
Examples	• The implemented regulations by the service are documented. • Procedures exist to audit the compliance regularly. • Procedures exist to follow changes in the regulations.	

1.5	Personnel	Notes
Personnel: roles and training	• Key roles are recognized • The personnel is trained to recognize and act upon any attacks	
Reference	3.10.4	
Examples	• Key roles, like manager roles, are recognized and named. • All personnel is trained to recognize malicious deeds. • All personnel is trained to follow defined procedures upon a malicious deed. • There is a document verifying training. • There is a documented procedure to to keep the training up-to-date.	

1.6	Incident response	Notes
Incident response and definitions of responsibilities	• Ensure that the responsibilities are defined between the customer and provider • Ensure the service provider and the customer have sufficient strategy for incidents • Ensure the service provider and the customer have the ability to properly handle incidents • Ensure that proper technology to identify potential attacks exist and operate properly, these can be for example intrusion detection or prevention systems and proper logging infrastructure • Ensure that dedicated personnel exists to handle the incidents, the incident response team should have the ability to analyze, respond, escalate and to report any incidents	
Reference	3.2.6	

Examples	• The customer and provider both have a detailed and documented incident handling workflow. • There is an up-to-date incident response team in all parties and shared communication channels during incident escalation. • Technologies exist to recognize incidents, for example: SIEM, IDS, detailed information about the normal state including protocols, devices and IPs to name a few. • Incident handling process is tested frequently and the personnel are trained.	

Physical requirements

2.1	**Physical security and continuity**	**Notes**
Physical security and continuity: physical security fulfilling the requirements	• Verify the cloud provider's documentation about physical security • Verify that physical security fulfills the requirements	
Reference	2.1	
Examples	• Documentation exists about the cloud provider's physical security. • The documentation is up-to-date and the provider applies the procedures with e.g. interviewing the provider or using 3rd party audit reports. • There is internal documentation about physical security requirements for this service or the company in general. • Compare the provider's document against company's internal requirements.	

2.2	Supply chain security and continuity	Notes
Supply chain security and continuity	• Verify there are contracts, controls, policies and monitoring which ensure availability and security of new hardware, software and installation	
Reference	3.10.3	
Examples	• Verify that support contracts secure and fast enough delivery of replacement hardware, software and installation. • Verify that proper hardware and software updates are taken care of by the contract. • Ensure that the delivery chain is trustworthy. • Ensure that there are written procedures to verify that the deliveries are received in proper state, e.g. seals are untouched, installations are done by designated persons.	

Technical requirements

3.1	Defense-in-depth	Notes
Defense-in-depth: segmentation	• There are multiple layers of defenses • Segments requiring more security are separated from those requiring less security • There are protective measures between different segments • The connectivity towards cloud is robust and redundant from both ends	
Reference	3.12.4	
Examples	• Based on architecture diagrams there are different segments	

	separated from others, when required security measures differ between devices and services. • The built system follows the aforementioned documentation. • There are technologies like firewalls, VPNs and intrusion detection systems between segments. • Individual systems are protected with additional measures like host IDS, host firewalls and malware detection software. • Dual homed connectivity via different Internet Service Providers.	

3.2	**Segregation of duties**	**Notes**
Segregation of duties: avoiding dangerous work combinations and tracking changes	• Segregation of duties is done by both the provider and customer • It is ensured that a single person can not execute a full path of actions • Changes are tracked	
Reference	3.2.5	
Examples	• Critical processes that require multiple actors are defined. • All parties' policies, abilities and strategy are ensuring segregation of duties. • There are technical and process oriented measures to ensure segregation. • There is sufficient tracking for all critical actions. • A single person can not modify tracking logs.	

3.3	**Encryption and key management**	**Notes**
Encryption: securing data and keys	• Data stores and flows are documented • Data is encrypted during storage and transfer when required • The encryption algorithms used are sufficient and fulfill legislative requirements • The encryption keys are sufficient and stored so that their secrecy and availability are ensured • Backups to cloud are encrypted	
Reference	3.11.1, 3.11.4	
Examples	• All data locations whether moving or in rest are documented. • The data is encrypted or protected with other acceptable methods like hiding all the time. • The encryption algorithms satisfy the requirements of legislation, policies and current recommendations. • The encryption devices, software and configuration are according to legislation, policies and recommendations. • The encryption keys are of required length and complexity, the keys are changed on required intervals. • The keys are stored securely and separated from data, the keys are stored so that they can not be lost. • Process exist to verify that the encryption and keys are updated as needed. • Process exist to audit that data and communication are encrypted when needed. • Backups are encrypted using keys not shared with the service provider.	

3.4	**Backups**	**Notes**
Backups and restoration	• Regular backups are taken of all the relevant data • Backups are stored regularly to an offsite location(s) • Full backup (if applicable) is taken regularly enough for restore time to meet the RTO • Backup mediums are being refreshed so that when new backup systems become available, old backups are still readable for restores • Expired backup mediums are destroyed according to standard or overwritten by new backups • Restore functionality is tested regularly	
Reference	3.12.1	
Examples	• All relevant data is identified and backups are configured. • Tape/disk library in a separate location. • Full backup (if applicable) is taken regularly enough for restores to be fluent. • Backup mediums are refreshed as new medium generations are being introduced. • Mediums are destroyed using a standard compliant mechanism once they are at the end of their life cycle. • Restore functionality is tested regularly by using scripts and status is being monitored.	

3.5	**Authentication**	**Notes**
Secure authentication throughout the infrastructure	• Users, devices and services are authenticated throughout the service • Authentication methods follow recommendations • Authentication data is protected	
Reference	5.3.5	
Examples	• All data and process access requires authentication and authorization. • When possible, two-factor authentication is used. • Authentication is constructed using at least one of the following: something the user knows, has or is unique to each user. • Logon ID does not consist of e.g. person's name or other easily accessible data. • Authentication data is properly protected. • The authentication requirements are fulfilled all over the service, including also the platform and other dependencies.	

3.6	**Life cycle management**	**Notes**
Managing services throughout their lifetime	• Different stages of service life cycle are identified and record of services is kept • There is a regular procedure to update the service catalog • There is a clearly defined de-commissioning procedure for services	
Reference	3.10.5	
Examples	• Specs, discovery, negotiation, composition, consumption and decommissioning are identified. • Automated mechanism in-place to detect new hosts and ser-vices. • Decommissioning planning is part of the initial specification.	

3.7	**Hardening**	**Notes**
Minimized installations	• Used disk images are hardened to contain the desired settings and patches	
Reference	5.3.7	
Examples	• The disk images used in services are acquired from a defined source. • The images are minimized to contain only the needed soft-ware and correct configuration. • The images are updated fre-quently. • The image installation and up-date processes are monitored. • Other requirements by the cus-tomer concerning the operating system and dependencies are fulfilled.	

3.8	**Vulnerability and patch management**	**Notes**
Vulnerability and patch management: keeping software up-to-date	• Updating and patching of devices and services are applied in a managed manner by both the customer and provider • Security scans are used to ensure proper update and patch procedures	
Reference	5.3.8, 3.12.6	
Examples	• Both the customer and provider have a process to recognize and analyze any vulnerabilities in the systems. • Updates and patches are applied frequently in a controlled manner. • Vulnerability scans or equivalent methods are used to verify that all devices and services are up-to-date. • Patching, updating and scanning are applied to different parts of the infrastructure.	

3.9	**Log management**	**Notes**
Log management: securing and gathering logs for tracing and alarms	• Logging is configured • There is a log filtering and alarming configured • There is a mechanism in-place to detect and prevent tampering with the log entries • Logging is done to a remote system • Custom applications (if applicable) implement their logging according to an applicable standard	
Reference	3.12.7	
Examples	• Logging is configured and not left on defaults. • SIEM system or similar log filtering and analysis tool is deployed. • Logging is configured to send logs to a remote log server. • Logging is part of the specification of the custom application.	