jamk.fi

How to self-assess and audit application deployment in public cloud?

Pinja Koskinen
Vesa Simola

Masters thesis
XXXXX 2018
Cyber security
Master's degree programme in cyber security

<table>
<tr><td rowspan="3">Author(s)
Pinja Koskinen, Simola, Vesa</td><td rowspan="2">Type of publication
Masters thesis</td><td>Date
Month Year</td></tr>
<tr><td>Language of publication:
English</td></tr>
<tr><td>Number of pages</td><td>Permission for web publication: x</td></tr>
<tr><td colspan="3">Title of publication
Title
possible subtitle</td></tr>
<tr><td colspan="3">Degree programme</td></tr>
<tr><td colspan="3">Supervisor(s)
Last name, First name</td></tr>
<tr><td colspan="3">Assigned by</td></tr>
<tr><td colspan="3">Abstract</td></tr>
</table>

Contents

1 Introduction

1.1 Background of the study

The cloud sign in network and software diagrams has been used for many years to indicate and abstract myriad of details concerning message flows, protocols and communications acreoss 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. (Kris Jamsa, 2012)

In their papar ”Cloud computing and security” Xingming Sun,Zhaoqing Pan and Elisa Bertino gave us 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 amongst several customers or services. To put it another way, cloud computing is similar to large pool of resources that are abstracted and virtualized to provide computing, storage, applications and services that are 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 things 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.(Xingming Sun,Zhaoqing Pan and Elisa Bertino, 2018)

There is seemingly some consensus that by placing all customer data and services in cloud would mean that successful attacker could gain access to large quantities of confidential information, meaning that the risk of data loss of security breach is higher in cloud than in traditional enterprise datacenters. This idea has its basis in the thinking that the cloud service provider and its infrastructure is more lucrative target than traditional data center. On the other hand, there is con-

sensus that cloud can be more secure than traditional datacenter. Reasoning being that it is easier to protect larger quantities of services in fewer locations and it would also be easier to use the latest technologies of protection in centralized manner. Also, given that costs tend to increase as more security is implemented , econimics 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 injurity, statements such as ”the cloud is risky” do not deliver any useful security information. Instead,these kind of statements should include propabilities and measured impacts to give one any value when making decissions.(Raymond Pompon, 2016) This controversy of cloud computing is further illustrated by Tim Mather, Subra Kumaraswamy and Shahed 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. Principle is that while we constantly hear the choir of ”cloud computing good” we also get to hear the ”could security bad” verse. Mind the gap meaning that one has to watch his step. Yet it is apparently not clear what is wrong with the cloud security.(Tim Mather, Subra Kumaraswamy and Shahed Latif 2009). This thesis tries to find answers to what that might mean and what should be taken into an account when evaluating ones cloud posture.

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

Criteria-referenced self-assessment is a concept where individual or organization gather information about their abilities or progress, then compare that data to explicitly defined criteria or standards and then amend or improve their practices and understanding of the topics based on the results. Purpose of the self-assessment is to detect areas where organization or individual is strong and on the otherhand, to find weaknesses to improve on. It is stated that feedback plays cruzial role in learning. (Heidi Andrade, Anna Valtcheva, 2009) The lack of feedback in education environment is largely due to 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.(Heidi Andrade, Anna Valtcheva, 2009).

There is some research suggesting that just by exposing the students to rubric may improve students

insight on the subject matter and also to increase the quality of their work. But even better results can be gained by actively engaging the student to utilize the rubric to self-assess their work. (Heidi Andrade, Anna Valtcheva, 2009). Similarly to this, we hope that this self-assessment criteria created in this theses would be usable and approachable enough to be similarly useful. So, the ultimate goal of the study was to create self-assessment questionaire for cloud computing security. 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).

1.3 Methods of the study

By answering to a question such as ”what kind of information we’re trying to come up with this research?” we can come up with a reasonable research method (Vilkka 2015). The answer to that question and hence the goal of this thesis was to come up with a self-assessment criteria to evaluate ones cloud posture in terms of security. To this end, research was done by first doing qualitative research utilizing literature avaible to us and the topics other researchers had found noteworthy, this was done to come up with reasonable background information to use as a basis for the self-assessment.

Practical part of the research was to actually implement the self-assessment questionaire that is handled as an separate attachement of this thesis.

2 General overview of cloud

Cloud service is generally understood as a product that consists of services hosted in the Internet. This could include servers, networks, storage systems, software applications and other services. These products could be running from 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. Also, in some cases users may share

files, data and information between several systems and other users via the cloud infrastructure. (Suikkanen, 2013 s8)

To name a few higher level motivators that might push companies towards cloud, let us consider the following (Tim Mather, Subra Kumaraswamy, Shahed Latif 2009):

- Initial investment is more manageable than buying complete set of infrastructure.
- 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, s7) Cloud hosting can be done in few different manners: Private cloud, public cloud, hybrid cloud and community cloud. (Suikkanen, 2013). Aforementioned deployment and hosting models are discussed next.

2.1 Cloud hosting types

As a concept, cloud computing can have multiple hosting types that differ from each other, these can be seen as ways of delivering the computing service. We will next describe some of the different characteristics of these hosting types as they do impact their ideal usecases.

2.1.1 Public cloud

Public cloud is hosted on the service provider facilities and all maintenance, modifications and upgrades are done 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 customer the options of choosing from several geographical locations from which to run their service. (Juha Ahlgren

2012, s12). The economy of scale can mean that the public clous 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. (Saara Suikka, 2013, s11)

2.1.2 Private cloud

Private cloud is understood as a service that is being operated by a service provider as a service to be used by single customer. Private cloud tends to use the same techniques as public cloud but they are configured to help the customer organization be more responsive and efficient in the IT resource usage than with traditional IT operation model. (Saara Suikkanen, 2013 s11) There are generally two types of private clouds, ones that are hosted on the customer premises and then there are those that are hosted on service provider 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 single customer organization. (Juha Ahlgren 2012, s10). Infrastructure on public cloud on the other hand is shared among the various customers of a service provider. (TAMOU, Aikaterini, 2014, s6).

2.1.3 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. Meaning that customer uses private cloud under normal circumstances but during peak load some or all parts of the service can be transported to public cloud.(Juha Ahlgren 2012, s13)

2.1.4 Community cloud

Fourth and final form of cloud is the community cloud. Community cloud is a multitenant cloud setup that is utilized by several organizations that may share a common interest or computing concerns. Such concern could come in a form of a compliance requirement, audit requirement or that the organizations require high speed access to common data, for example research organizations working on a common project. (Saara Suikkanen 2013, s12)

2.2 Cloud deployment models

2.2.1 Infrastructure as a service

Infrastructure as a service 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. (Saara Suikkanen, 2013 s13) 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 administative tasks can mostly focus on server side level like operating systems management and maintenance and third party software maintenance. (Kavis, Michael. ”Infrastructure as a Service”. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). John Wiley & Sons. 2014. Books24x7. <http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=62597> (accessed September 25, 2018), Infrastructure as a Service). 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, Michael. ”Infrastructure as a Service”. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). John Wiley & Sons. © 2014. Books24x7. <http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=62597> (accessed September 25, 2018), Infrastructure as a Service). So, it is worth to emphazise that while customer has limited or no control of underlying architecture that is used to provision the cloud based services, customer is still responsible for proper use and care of the cloud resources, for

example the configuration of an application. (STAMOU, Aikaterini, 2014,s5)

2.2.2 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. All the parts of the software infrastructure must be provided by the customer. To ease this task PaaS providers can provide software platforms to certain level. Typical software platforms can be for example databases, logging and payments services, which can be used via various APIs (Kavis, Michael. "Platform as a Service". Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). John Wiley & Sons. © 2014. Books24x7. <http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=62597> (accessed September 25, 2018)) 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, which would provide an API for containers for automatic scalability. Containers are relatively new concept in computing but they are used to package the application and its dependencies in to a 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 deployment as it eliminated the need for customer owned infrastructure for the deployment of a software application. (Saara Suikkanen 2013, s14)

2.2.3 Software as a service

Software as a service is a method of delivering software application from cloud via Internet 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 for the service provider. The advantages to the customer is 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. (Kavis, Michael. "Software as a Service".

Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). John Wiley & Sons. © 2014. Books24x7. <http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=62597> (accessed September 25, 2018)) Naturally, the SaaS services can not be used for software that require any heavier tayloring than just predefined configuration changes. A real-life example that illustrates the stacking of cloud services and the SaaS could be a email service that has its customer specific frontends 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, Michael. "Software as a Service". Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). John Wiley & Sons. © 2014. Books24x7. <http://common.books24x7.com.ezproxy.jamk.fi:2048/toc.aspx?bookid=62597> (accessed September 25, 2018)). Key point to understand the SaaS model is that customer has no control of the underlying software deployment or the computing infrastructure in SaaS model. (STAMOU, Aikaterini, 2014,s5). This is essential differentiator between SaaS and PaaS.

3 Security in cloud

As with any environment business continuity planning and disaster recovery planning apply, regardless if the service is ran on-premisses or in cloud. (Halpert, 2011). Hence, we'll start this chapter by describing business continuity plan and disaster recovery plan before diving further into the recognized risks.

3.1 Definition and importance of business continuity and disaster recovery plan

Business continuity plan is clear plan that aims to ensure that critical functions of a given organization are capable to operate in case of a disaster. Business continuity plan should identity the essential resources such as personnel, systems and infrastructure that is required to run the essential emergency business operation and how to later on reestablish all the business functions. (Childs, 2008) Disaster recovery plan is usually coupled with the business continuity plan, but 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 customer needs to recover in case of disaster taking place. RTO has direct impact on the budjet and resourcing required to recovery operations. As an example, if customer is to assume RTO of 3 hours, it is essential to invest hefty amount of money on a recovery site and make sure that it is operational with in the three hour window. If inturn, customer is expecting three week 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 we have available before operations must continue, RPO is translated into to the amount of data that is acceptable to loose in case of disaster. RPO can give indications as to how robust infrastructure is required to run the service. 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 ”inflight” 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 decission makers to state that security is their primary concern with cloud computing. (Tim Mather, Subra Kumaraswamy, Shahed Latif, 2009). Some general level challenges of cloud computing are identified as follows by Ben Halpert in his book 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 recidency is a factor as different countries and regions have different requirements for information handling.
- Multitenancy is what allows the economics of scale, it is also a compliance consideration when same infrastructure is shared amongst 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 agreenments.
- 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 model. Tim Mather, Subra Kumaraswamy and Shahed 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. High speed 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 addresssed 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 into 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 to outsourced data center.
- Changes in IT organization has to have the skills needed to operate the cloud environment and on the other hand IT organizations role 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, but this does not remove the need for compliance and security. (Raghu Yeluri, Enrique Castro-Leon 2014). Next, we'll discuss some of the security concerns of different cloud deployment models starting from the more general ones towards more deployment model specific ones.

3.2.1 Requirements set by regulation

Combining the relative freshness of cloud as a concept and that there are many service providers to choose from it is unfortunate that there is not all that much rules and guidelines for cloud implementations. It is likely that in the future there will be more regulation for cloud services but 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 service providers, but downside to this is that it could also lead to a situation where the cost benefits of cloud would shrink as customer would likely have to pay the bill of implementing the requirements defined by regulators. (Halpert, 2011)

To better understand the rugalatory aspects in cloud computing we first need to define what is meant by regulation. The dictionary definition of regulation states that regulation is a rule or directive made and maintained by an authority (Oxford dictionary, 2018). To broaden the meaning we can look at Ben Halperts book Auditing Cloud Computing: A Security and Privacy Guide from 2011

where he gives the following, quite descriptive, definition: A regulation is a rule or law, hence there should be consequence for not abiding, and that there shall be policing in a form of compliance. Basic idea of regulation is broadly protective, for example to protect assets such as stakeholder value or citizens. (Halpert, 2011)

Halpert 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, federal and EU.

In Finland we have this thing called Katakri that essentially is a auditing tool for authorities. Katakri can be used to evaluate the capability of organization when it comes to security of information that is classified as confidential. (Katakri, 2015) Another fine example of regulation that is effecting us in Finland is the EU General data protection regulation, or GDPR for short. 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, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en as viewed on Jan 2019)

Now that we have established what regulation is we can think of reasons why rulation exists. Ben Halpert 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 processes was defined but not implemented, resulting in damage to shareholders. After this incident 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 was already in place. Using these already defined best practices allowed PCAOB to quickly setup the audit criteria and guidelines. This re-

sulted in Sarbanes-Oxley compliance program. (Halpert, 2011).

This 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.

3.2.2 Global data recidency

To add insult to injury, it should also be stated that compliance with regulation can be a complex topic in multinational setting as there can be significant overlap amongst 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 United States and regulation is strict concerning what information is deemed as acceptable to collect, where it must be stored, not to mentioned where it may be processed. This is illustrated by EU Council Directive 95/46 that limits the transfer and processing of personal data outside borders of the european union. It is important that the service provider has solid strategy and planning 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. Also customer should make sure that proper controls and policies are inplace to ensure that the privacy issues are not violated.

3.2.3 Division of responsibility

Based on the security concerns identified above it is essential to understand the concept of division of responsibility. 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 Jiafu Wan,Kai Lin,Delu Zeng, Jin Li, Yang Xiang, Xiaofeng Liao, Jiwu Huang and Zheli Liu in their conference papaer on SPNCE 2016. 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 of 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 this is a factor worth considering.

Another aspect to this division of responsibility is pointed out by Donna R. Childs 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 providers offerings as much as they can. Reasoning being that if 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. Meaning, that in the end it might not be enough to just change some portion of customers service, but to actually make other far more signifficant changes. When the disaster strikes it is not a good posture to have ones hands tied like this. One approach to lessening this risk is to make sure that the customer has good lines of communications with the candiate service providers and possibly their management as well. This can be accomplished by taking part in information sessions organised by the service provider as these can be a good opportunity to interface with the senior management of the service provider 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 customer would appreciate service providers recommendations.(Childs, 2008).

Assuming the 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 straight forward one being 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 more tight is to include formal attestation clause at the end for executite to sign. Second, bit more invasive approach is to request the service provider to include additional documentation alongside the answers. These documents could be screenshots, access-control list configurations, outputs of vulnerability scans and so forth, they can be used as additional proof that the controls are implemented. 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 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. (Raymond Pompon, 2016).

3.2.4 Segregation of duties

Just like with customers own IT environment, customer should ensure that the service provider is adequately safeguarding against issues related to segregation of duties concerning the cloud service that is being offered to customers. To definition of this problem with segregation of duties could be described as cases where single user is able to both initiate and approve an action. Sumner Blount and Rob Zanella gave the following example of this in their book "Cloud Security and Governance: Who's on your cloud?" in 2010: As an example accounts payable administer who can both establish a new vendor record, and approve paymets 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, review of the service providers policies, strategy and abilities in this field is important. (Sumner Blount, Rob Zanella, 2010).

3.2.5 Importance of incident response

Dispite all the implemented controls and righteous plans and ideas for security and availability, the bad thing will eventually happen. This could include various things such as attempts at attacking the environment, successfull 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. Customer should know the procedures of creating, following and reporting of incidents. Customer shouls ask questions such as how is the customer notified and what kind of visibility is given to the customer to gain more information on incidents detected by the service provider. Does the service provider have a proper plans to act on a PR disaster, such as loss or leak of credit card information? Possible the single most important question to ask is to verify that the service provider and their plans on incident response are consistent with the plans of the customer?

(Sumner Blount, Rob Zanella, 2010)

Its 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 secutity incident response team (CSIRT) should be established. CSIRT needs to be able to:

• Analyse notifications of events

• Respond to the event if this is required, based on the analysis

• Escalate the issue as requried and by predefined procedures

• Reporting 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.(Ronald L. Krutz, Russell Dean 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 inplace to prevent attacks from succeeding? Does service provider implement regular risk analysis, what kind of patch management and host security scheme they have and what kind of user training and education takes place in matters of security? Detecting 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 behaviour to understand what is normal? What kind of log management and analysis tools are being used and how? How the detection processes is tied to the communication processes with the correct parties? Assuming that the service provider can detect the attack cus-

tomer should then investigate their capabilities to contain the threat. For this purpose 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 service providers capability of post-incident actions custor might ask things 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? And also, what corrective actions could be taken to prevent similar incidents from taking place in the future, and how these improvements would be communicated? (Ronald L. Krutz, Russell Dean 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 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, but with likely additional costs involved. It is essential to understand how the platform-of-choice implements the multitenancy, 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 doing maintenance. (Halpert, 2011). It should be also noted that the highest level of access to the infrastructure is 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, multitenancy 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 multitenancy issue. (Bond, 2018) Ben

Halpert highlights that usually both consumer and service provider are internal to the organization, this allows more control over aspects of the cloud service, such as quality of service. Example of this is that internal 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.(Halpert, 2011)

3.5 Security aspects in hybrid cloud

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

3.6 Security aspects in Infrastructure as a service

It is key element to understand that the service provider has means to view the activities of any virtual machine running inside a infrastructure as a service cloud. (Halpert, 2011) Also, as stated above customer is responsible for implementing the required patching inside virtualmachines himself, this is true even while service provider would be patching the hypervisor level.

Another way to describe this is illustrated in the Cloud security and privacy book by Tim Mather, Subra Kumaraswamy and Shahed Latif 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 hypervisors, paravirtualization etc. This layer is maintained by the service provider.
- Customer gues OS or virtual machine virtual machine running some operating system and software stack. This is maintained by customer.

Above could also be considered another way of describing the the division of responsibility. This is

essential part on the other service delivery models as well.

3.7 Security aspects in Platform as a service

Key differentiatior between infrastructure as a service and platform as a service is that 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 had. Also, lower administrative overhead can be achieved by moving some of the maintenance burden from in-house staffers to 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 Kris Jamsa highlights the concern of risk of breach by the platform as a service provider. Its stated that if the service provider fails to be compliant with the service levels, performance availabilility and security of the application running on platform as a service might be at risk. (Jamsa, 2012). Michael P. McGrath states in his Understanding PaaS book that its not so much about platform as a service being fundamentally different, but customer just does not see all the actions taking place behind the scenes, such as monitoring, tweaking and constant improvement. 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. (Michael P. McGrath, 2012). Aforementioned statements are escalated when combined with the statements by Tim Mather, Subra Kumaraswamy and Shahed Latifas 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. Reasoning being that attackers could possibly utilize this information to implement attacks. (Tim Mather, Subra Kumaraswamy, Shahed Latif, 2009)

All the above points to the direction where 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. (Tim Mather, Subra Kumaraswamy, Shahed Latif, 2009)

3.8 Security aspects in Software as a service

Software as a service typically presents itself as a application hosted and developed by service provider and delivered over web browser. This allows customer to limit their needs of onsite data center based sofware and applications leading to less amount of administrative burder. (Jamsa, 2012). Kris Jamsa also states that as software as a service is likely multitenant this may lead to a situation where any customizing software as a service delivery might difficult, expensive and in some cases impossible. (Jamsa, 2012) Given that everything from physical hardware, hypervisors and application is hosted by service provider they also have visibility to all of the information of all of the customers of their software as a service offering. (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 customer may have. (Tim Mather, Subra Kumaraswamy, Shahed Latif, 2009)

3.9 Methods of improving security and availability in cloud

3.9.1 Service level agreenments

Service level agreenments also known as SLAs are sets of condition and terms defined in contracts between customer and the service provider. SLAs can be used to define and agree upon the service levels between 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 agreenments is given by Xingming Sun,Zhao-qing Pan and Elisa Bertino in their paper ”Cloud Computing and Security” in 2018 where they define

service level agreenment as means to assure quality, reliability, security and scalability of the cloud service. (Xingming Sun,Zhaoqing Pan and Elisa Bertino, 2018)

To succesfully utilize SLA 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 customer to choose from and to bind the contract upon. These could be considered as templates for the SLA. Customer then reviews these templates, selects one possibly modifying it and sends it back to the service provider for a review. Service provider then accepts, declines or sends modified version to the customer for a review. (Stamou,2014 s 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 specially 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 take into account the individual risk requirements of the customer but this can lead into highly tailored SLAs. (Stamou,2014 s14).

3.9.2 Encrypt static data and in-flight data whenever possible

As stated earlier the very nature of cloud computing relies in the resource pooling, this on its own poses the question if cloud storage service is suitable as several customers utilize the same storage system. To lessen the risk of data leakage within the cloud customer should implement encryption to protect static data. For infrastructure as a service environment that could mean using encryption methods provided by service provider or encrypting the data using third party system. When using encryption it is essential to use appropriate encryption algorithms, at the time of writing this includes AES, customer should select the encryption algorithm based on actual need and so that it

is compliant with regulations. Encryption highlights the importans of managing the encryption keys in a 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. (Xingming Sun,Zhaoqing Pan and Elisa Bertino, 2018) I in their paper on ”A Formal Security Analysis of the Signal Messaging Protocol” from 2017 Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt and Douglas Stebila illustrate the use case for end-to-end encryption of communications. They state that in the past there has been attempts to improve security by encrypting the messaging between 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 that authenticate the customers 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 are 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 that there have apparently been flaws in the key management that undermine the security (Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, Douglas Stebila, 2017).

This just goes to say 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 requirementsi like PCI-DSS, ISO 11568 state that key management must be implemented. Proper key management should cover the whole life cycle of the keys and that different application requirements do not contradict the key management process, leading to vulnerabilities.(Mike Andreasen, Troels Norgaard, Alina Mot, Per Snowman, Axel Buecker, Carsten Dahl Frehr, Soren Peen, W. Craig Johnston, 2014)

3.9.3 Information hiding

In addition to traditional encryption 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 given piece of information this approach aims to hide the data inside ”junk

data" or split the data so that 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. Underlying principle being that attacker can only control the asset (in our example before, 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 in 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 it 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. Add that to the concept of splitting the information into number of parts stored in different locations and 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. (Peter Wayner, 2009)

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

3.10 Searchable encryption

To preserve confidentiality of data, it should be strongly encrypted whenever it is not within the secure boundaries. (Katakri) Thus it it is a natural conclusion that the data should be encrypted during the data transfer to and from cloud as well as while the data is at rest, if the cloud provider can not be considered as 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 the document database. Also 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. Hoang Pham, Jason Woodworth, and Mohsen Amini Salehi. Survey on Secure Search Over Encrypted Data on the Cloud. https://arxiv.org/pdf/1811.09767.pdf

3.10.1 Data redundancy

Had the cloud storage been an option at some decades ago, it would have been quite unlikely that we would have the same backup processes and mechanics that are actively in use today. Be that 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 the best practices of taking backup copies and storing those into off site locations from which the data could be restored if needed. (Marc 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 agreenment to increase availability and disaster recovery capability. (Raghu Yeluri, Enrique 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. (Ronald L. Krutz, Russell Dean Vines, 2010)

As same principles apply to cloud backup as to normal backup it is reasonable to review the traditional meaning to data backup. Backups are understood as a snaphost 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 data set and full backups are used as a baseline for other kind 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, but it has a downside when it comes to restores: 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 noteable 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 ran 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 further explain these 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. (k = m/n), finally store the n + m redundant coded data to multiple cloud storage facilities, final 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. (Xingming Sun,Zhaoqing Pan and Elisa Bertino, 2018)

It should be noted that while replication and backups give service provider the ability to comply with service level agreenments, they also include a risk of dispersed copies of data, credentials and so on floating in the cloud. In addition to ensuring that the aforementioned does not happen customer should make sure that if they decide to change service provider the backup copies and replicas are destroyed according to the agreenment. This can be difficult to achieve as there are no standard means of proving that certain dataset is actually properly destroyed.(Raghu Yeluri, Enrique Castro-Leon, 2014) One problem worth highlighting is the issue of medium and technology obsolescence. This is referring to new backup mediums developing and surfacing and customer 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 but it is worth noting nonetheless.(Marc

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 ains on 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 indexes, pointing to the actual data. (Daehee KimSejun, SongBaek-Young Choi, 2017).

3.10.2 Authentication

In the ”Cloud security: A comprehensive guide to secure cloud computing” from 2010 Ronald L. Krutz and Russell Dean Vines gave us the following definition: As usual, authentication and identification play major roles in most access control systems. To better understand what this is about lets give both of those terms 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, this usually is understood as username or logon ID to the given environment. Username or logon ID should not consist of users real name, job title or function, this 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, this is commonly implemented by using password. Authentication constructed of the three types listed below:

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

It is also possible to combine some of the above authentications mechanics and come up with something call two factor authentication. Example of this would be bank automate that requires both the card and the PIN code. (Ronald L. Krutz, Russell Dean, 2010)

3.10.3 Handling the 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 and this 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 (Teddy Hayford-Acquah and 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. (Gunnar Bøe, Vidar Faltinsen, Einar Lillebrygfjeld, 2011) Two routers using VRRP protocol act in active-passive manner to provide so-called first-hop redundancy (rfc5798, 2010). This approach, when combined with physically separate lines, provides protection from fiber cuts on the last mile and this 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 are accepting 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 won't purchase redundant connectivity but instead accept the risk of significant business impact and downtime. (Packetworks, 2016).

Similarly, if cloud application is running in a "stretched" network infrastructure, e.g. 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 different kind, but with equally 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 decoupling 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 approaches have apparently been deemed as non-trivial and time consuming

tasks so 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 streched OSI layer 2 domain over routed network (rfc7348). While there are quite a few methods of implementing encryption in network it should be questioned if it is a sustainable choice to outsource application security to 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 networking 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 utilising encryption in DWDM (Arista, 2018) level. It should be noted that both MACSEC and IPSEC have 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 atleast 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 network level to implement the encryption, instead utilize sufficient encryption in the application level, just to be sure.

4 Self-assessment of cloud security posture

Before going further, lets briefly address the concept of criteria-based self-assessment and how one might approach the whole concept of self-assessment. 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 a 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, in a responsible way and also to monitor the evolution of those studies. (Tiia Kokkonen, 2012).

Just by reading the above statement and by replacing the words ”student” with ”cloud user”, ”education” with ”IT” and ”study” with ”application” we 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 a exercise in weakness finding that just consumes resources, Tiia Kokkonen points out that students should concentrate on the benefits of self-assessment. Similarly, an internal audit or self-assessment ran by the organization itself could be seen as means to improve the constantly developing security policy, using the finest controls for 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: Negavite culture pushes persons and organizations towards avoiding getting blamed for mistakes and managing just up to the letter of the law, not one bit further. Culture of safety on the other hand, is all about preventing the bad thing from taking place, this includes things like transparency and continous improvement. Also, in a safety culture, everyone acts as a 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. (Raymond Pompon, 2016)

4.1 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 bit here is that self-assessment is done by oneself, not by an external party (Oxford dictionaries, 2018). This is a key differentiatior 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. Organization that owns the data defines the minimum level of security. Au-

dit on the other hand is the process that measures how the organization is aligned with the given compliancy requirement at a given point in time. (Prashant 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 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 key to understand that the implementation of security in cloud is slightly different from what it is with on-premise or traditional deployments. (Prashant Priyam, 2018) Oxford dictionary definition of audit states that the audit is an official inspection of entitys accounts by an independent auditor. (Oxford dictionaries, 2018). Another definition of audit is given by Ben Halpert in his book Auditing Cloud Computing: A Security and Privacy Guide as follows: Audit is an 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. (Halpert 2011). We believe that the aforementioned statements highligh the difference of audit and self-assessment.

4.2 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 organizations security policy more effective. 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 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 risk, yet it will provably 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.(Raymond Pompon, 2016)

According to Raymond Pompon, 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 etc. Raymond 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 5 years
- Very Unlikely Assumed to take place less than once every 5 years

Raymond Pompon also proposes theree impact ratings: minor, major and critical. All three of those can also be split into three subcategories: confidentiality impact, integrity impact and availability impact. Example of confidentiality of minor scale could be under 10 database records of confidential nature being exposed internally without any proof of exploitation, while major impact of the same thing would entail that several internal employees with no authorisation having accessed these records. Critical rating would be under 10 data records being exposed externaly or more than 10 records exposed internally. Integrity impact follows the same guidelines but it essentially replaces the exposure of data with data being altered without authorisation and wether the alteration can be detected and corrected. Availability impact is slightly different concept, minor being several users having no access for 1-5 days, or customer facing service down up to an hour. Major availability impact could be characterized as customer facing service being down for more than an hour but less than a day, critical represents a situation where customer facing service is down for more than a business day. (Raymond 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 organization shall match its assets against attack surface, known weaknesses and implemented controls. For example, if company hosts 10 websites (assets) it might know that on average it is missing 2 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 phish-

ing test training (control). While the above gives us numbers it is likely that in the end something like security steering committee will make subjective calls, but 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.

4.3 Controls to assess

According to Chris Jacksons 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, IDS etc. that 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 confidentialiy.
- 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 Conclusions