Towards a compliant and secure cloud: Cloud migration, swapping providers and contractual aspects

Anders Sand Frogner

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2012

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Abstract

One of the issues in the cloud today is the switching between different service providers. Cloud providers often deliver their services through specific platforms(API), with specific tools, customized and special file formats that could cause dependencies. The cloud customer could potentially become dependent of the cloud provider. This is called a provider "'lock-in"', and could potentially hinder the migration process, the further development of the cloud technology, and the enabling of cloud computing technology for businesses and organizations.

We are attempting to improve security, avoid the "'lock-in"' problem, and ensure compliance in cloud computing and cloud environments through the improvement of business resilience and business continuity. Security, compliance, business continuity and business resilience are all aspects that influence trust between actors in a cloud computing environment. The trust issue hinders a lot of different organizations and business to take the step into the cloud environment. This issue of trust, along others, creates uncertainty for organizations and businesses considering moving their storage, applications or services into the cloud. This thesis aims to solve or improve this particular issue, and with it, enable more secure cloud computing.

The thesis results and findings aims to help organizations and businesses with the planning process, to help keeping their data secure, and successfully migrate/swap providers. The results and findings are concluded upon two different case studies of two cloud customers. The findings from these case studies are presented through security checklists, lists of SLA/Sec-SLA metrics and through a modification of a conceptual model.

A solution or improvement of these issues will enhance trust in cloud computing and enable more organizations and businesses to enter the cloud, utilize its efficiency and benefit from its low cost service on demand.

Sammendrag

Et av problemene i skyen i dag er vanskeligheten av veksling mellom ulike tjenestetilbydere. Skytilbydere leverer ofte sine tjenester gjennom spesifikke plattformer (API), med spesifikke verktøy, tilpassede og spesielle fil-formater som potensielt kan forårsake avhengigheter. Disse avhengighetene kan skape det som kalles en tilbyder "“lock-in"’(lås), og kan potensielt hindre kunders flytting mellom tilbydere, videreutvikling av skyteknologi, og hindre aktivering av skyteknologi for bedrifter og organisasjoner.

Vi prøver å forbedre sikkerheten i skyen ved hjelp av rettningslinjer og guider for å unngå "‘ lock-in "’(lås) problemet, og sikre migrering mellom skytjenester og skymiljøer gjennom forbedring av virksomheten overlevelsesevne og kontinuitet. Sikkerhet, migrering, kontinuitet og overlevelsesevne er alle aspekter som påvirker tilliten mellom aktørene i et skytjenestemiljø. Tillit spørsmålet hindrer en rekke ulike organisasjoner og bedrifter til å ta det siste steget inn i skyemiljøet. Tillit, blant annet, skaper usikkerhet for organisasjoner og bedrifter som vurderer å flytte sin lagring, applikasjoner eller tjenester inn i skyen. Denne oppgaven tar sikte på å løse eller forbedre disse problemene, og med det, aktiverer sikrere skytjenester.

Avhandlingens resultater og funn har som mål å hjelpe organisasjoner og bedrifter med planprosessen, for å hjelpe å holde sine data sikre, hjelpe med migrering/bytte av tilbydere. Resultatene og funn konkluderte ut i fra to ulike case-studier av to skykunder. Resultatene fra disse undersøkelsene er presentert i form av sjekklister, lister/tabeller med SLA/Sec-SLA målenheter og gjennom en modifikasjon av en tidligere utviklet konseptuell modell.

En løsning eller forbedring av disse problemene vil øke tilliten til cloud computing og at flere organisasjoner og bedrifter til å gå inn i skyen, utnytte dens effektivitet og dra nytte av sin lave pris tjeneste på forespørsel.

Acknowledgements

I would like to thank my supervisor Bernhard Hämmerli for supporting me and providing me with guidance during my work with cloud computing, to help define my research questions, provide me with sources of information and to point me in the right directions.

During my entire run of the master degree, and especially during my work on the thesis at the Master Lab at Gjøvik University College, the support and discussions with my classmates have been of great help. I would like to direct a special thanks to two spesific classmates and friends for their support, cooperation and help during the last five years, Lars Arne Sand and Gaute B. Wangen.

Finally I would like to thank my entire famliy, and especially my mother for support, motivation and help during the work with the master degree and the thesis.

Contents

List of Figures

List of Abbrevations

SaaS - Software as a Service
PaaS - Platform as a Service
IaaS - Infrastructure as a Service
SLA - Service Level Agreement
Sec-SLA - Security Service Level Agreement
QoS - Quality of Service
TTP - Trusted Third Party
API - Application Programming Interface
MTA - Multi-tenancy architecture
NIST - National Institute of Standards and Technology
LDAP - Lightweight Directory Access Protocol
FEIDE - Felles Elektronisk IDEntitet
VM - Virtual Machine
IP - Internet Protocol address
NIDS - Network Intrusion Detection System
NIPS - Network Intrusion Prevention System
ASP - Application Service Provider
SSL - Secure Socket Layer
SLO - Service Level Objective
ID - Identification

1 Introduction

1.1 Topic covered by the project

The work performed and presented in the thesis is centered around cloud computing, and the cloud environment. We will attempt to better the security and compliance of cloud computing through solving or improving problems regarding trust. We will take an in-depth look at contractual agreements between cloud provider and cloud customer, privacy laws and regulations, and the use of external/outsourced expertise. This is done through case studies of cloud customers and cloud environments. We will also propose guidelines, checklists or requirements for businesses and organizations going into the cloud, or swapping between cloud providers.

1.2 Keywords

Compliance, Trust, Privacy, Private Cloud, Public Cloud, Governance, Scalability, Security, Scaling an application, SaaS (Software as a service), PaaS (Platform as a service), IaaS (infrastructure as a service), Hybrid Cloud, Legal, Economics, Community Cloud, Security, Risk. Keywords gathered from Google and CSix Cloud Computing[10].

1.3 Problem description

When using cloud services, businesses and organizations will have to trust a third party or technology. Introducing a third party to your confidential information is difficult. How can they do this and why do they need to do this? Do cloud customers trust the technology, do they trust the third part and do they trust the communication channel the information travels? Trust is a security and compliance issue in cloud environments and cloud services, and is delaying many organizations and businesses in the transfer towards enabling cloud technology and environments. To enable a secure and compliant cloud we need the cloud customer to interact and contribute.

Another issue in the cloud is switching between different service providers. Cloud providers often deliver services through spesific platforms(API), with spesific tools, and customized and special fileformats. The cloud customer could potentially become dependant on the cloud provider. This dependency is called a provider "“lock-in"”, and could potentially hinder the migration process. There are several different reasons for why a cloud customer would want to swap provider. Economic reasons like bankruptcy, strike, increased subscription fee and/or increased cost of spesific services. A bankrupcy could also be caused by natural disasters and catastrophies like floods and waterdamage, earthquakes and fires. A change in the customers business that requires other types of services. All these aspects could trigger a wish for a new cloud provider. How can you make sure your information follow your switch of providers? How can customers even be sure their data is safe during this transaction?

1.4 Justification, motivation and benefits

Cloud computing serves large benefits to efficiency, which in return would yield greater economic returns. Cloud computing allows customers to access almost any service, at any time and anywhere they want. It is a further development of application and service hosting, and is most likely the future within computing. As stated by a paper from Berkley[11] there are certain security issues that need to be solved before companies safely can store their information in the cloud.

Solving the trust issue, or at least make it better would further the development and use of cloud computing. Service level agreement review and checklists, the help of external expertise and the possibility to switch between providers are steps along the way that would need to be solved to achieve this. The technology is more or less in place, but the arcitechture, standards and policies are lacking.

Enabling a more secure and compliant cloud will ensure that more businesses use the cloud environment and technology. The cloud could be saving these businesses costs on infrastructure, expensive maintenance and the expense it is to keep in-house expertise.

1.5 Research questions

To get a clear understanding of what has to be examined and researched, three research questions is defined.

1. How can businesses and organizations securely and efficiently plan and perform migration to/or swapping between cloud computing service providers without the loss of business resillience and business continuity?
2. How can cloud customers contribute to enable a secure and compliant cloud environment?
3. Can effective swapping of providers and a more secure and compliant cloud environment, enhance trust between cloud customer and provider?

1.6 Scope and boundaries

Security is a broad field, and for this thesis we will focus on security from a management point of view. This excludes technical solutions such as cryptography, algorithms and other technical areas, problems, research and solutions.

We will limit the study and research to norwegian and european cloud customers. Angling the case studies to Norwegian companies as this is by far the easiest solution for the information gathering phase of the case studies included in the thesis.

1.7 Summary of contributions

The summary of contributions presented in the thesis:

- Guidelines and recommendations for customers that need or want to change providers
- Guidelines and recommendations for organizations/businesses that want to enable the use of cloud technology
- Scenarioes of when cloud customers should contact external expertise

- Improve the trust and compliance issue for the organizations/businesses that want to use cloud technology

1.8 Thesis outline

The thesis is divided into several chapters. The thesis covers several different areas and the chapters serve as method to achieve a top-down approach. The thesis outline presents the reader with the content of these different chapters.

- Chapter 2 presents the background information on cloud computing needed for this thesis. The chapter is divided into three sub sections, Cloud Computing definitions and benefits, History of cloud computing and Security.
- Chapter 3 presents the thesis related work done by previous research on the field of the thesis scope. The chapter is divided into six sections, Definitions and Characteristics, Cloud Computing Models, Swapping Providers, The legal aspect, SLA and Trust Management.
- Chapter 4 contains the choice process of scientific methodologies.
- Chapter 5 contains the description of, and how the methodologies were used to solve the research questions.
- Chapter 6 contains the work done on the subject of swapping providers. This includes two independent case studies and recommendations and checklists of cloud provider selections and migration. The chapter is divided into four sections, Case Study: University Innlandet, Case Study: Narvik Municipality, Selecting the Provider and Discussion on Swapping Providers.
- Chapter 7 contains the work done on the subject of Service level agreement. This includes service level agreements based on the case studies from chapter 5 and use case scenarioes for external expertise. The chapter is divided into three sections, Service Level Agreement Recommendation, External Expertise and Law and Discussion.
- Chapter 8 contains the modification of a conceptual trust model. The model is modified to include the findings and results based on the first two research questions. The model should contribute to answer the third research question. The chapter contains one section, SLA based Trust Model.
- Chapter 9 presents an extended discussion of the findings and results.
- Chapter 10 presents the conclusion of the master thesis.
- Chapter 11 presents suggestions for further work.

2 Background

This chapter is included to inform the reader of the main definitions and aspects of cloud computing. The term cloud computing will be used and mentioned regularly throughout the thesis, and it is important that the reader has the same understanding and knowledge of the term (and the technology) as the author.

2.1 The Cloud

Throughout the thesis we base our understanding of cloud computing on several definitions. One of these definition is delivered by Lizhe Wang and Gregor Von Laszewski in a paper published in 2008: "‘A computing Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and persvasive way'"[12]. This is a somewhat technical definition of what cloud computing is. But, since this thesis is focusing on the management point of view, we will need a supplement of this technical definition with a definition adjusted towards management. The Gartner groups definitions of public and private clouds are well suited to establish a common understanding: The Gartner groups definition of a public cloud: "‘A style of computing where massively scalable IT-enabled capabilities are delivered ’as a service’ to external customers using internet technologies’"[13]. The Gartner groups definition of a private cloud:'"A form of cloud computing where service access is limited or the customer has some control/ownership of the service implementation"'[13]. There exists a lot of different definitions of cloud computing, and the mentioned definitions are just a selected few. NIST has also published their own definition, it is a two-paged definition, and the thesis has used the NIST definition regularly to grasp the subject of cloud computing. The NIST definition is complete, but comprehensive. "‘Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.'"[14].

2.1.1 Cloud computing benefits

The mentioned definitons 2.1,[13],[14],[12] sums up all the different aspects of the cloud, and how it works. These understandings of the term "‘cloud computing'" is the definitions that this thesis and all its research has been based upon.

There are several reasons why cloud computing is on its way to replace the former "‘in-house'" servers, services and infrastructure. To understand why the development has been directed more and more towards cloud computing we will have to look at some of the benefits surrounding the service.

Some of cloud computing benefits include:

1. User-centric interfaces[12]
2. On demand delivery and pricing[12]
3. Quality of Service guaranteed through SLA[12]
4. Autonomous system[12]
5. Scalability and flexibility[12]
6. Low cost in user equipment (thin clients)[15]
7. Versatility[15]
8. High reliability[15]
9. High extendibility[15]

These benefits come true with the use of different types of technologies used, such as: Virtualization technology which can be flexible, and techniques within this technology such as VMware, can offer infrastructure on demand while techniques like "‘VPN"’(Virtual Private Network) can offer a customized network environment to access the resources created through VMware(or other virtualization techniques)[12].

2.1.2 Cloud computing service models

With the benefits in place, it is important to know the different types of services the cloud offers. The different services are distinguished through models.

There exists three different types of cloud computing service delivery models, SaaS, IaaS and PaaS. SaaS 3.2.1 is a model for delivering software and applications through the cloud. IaaS 3.2.3 is described as delivering different types of infrastructures for lease to customers. This includes servers, storage, hardware and also networking components. PaaS 3.2.2 is a development service where the customer can create different types of software with the tools and liberaries delivered through the service.

The idea behind cloud computing is basically a pay on demand pricing model delivered through outsourced IT services(can also be hosted in-house as a self-hosted private cloud2.1.3). The IT professionals and their respective companies handles the actual servers, infrastructure, applications and services which they rent to businesses and organizations(unless it is self-hosted in a private cloud). The customer and user has less responsibility, and need less technical knowledge to be able to do their job[16] The idea was, and still is, that these businesses and organizations that rent computer services through the internet will save money and workhours on outsourcing most of the technical computer work, while still remain in control of their own applications, data and service use. The big difference between the cloud and the previous outsourcing alternatives like the grid and ITO is the "‘great deal of computing resources that is available, and scalable, at a low cost"’[16]. The provider will deliver hardware, software and infrastructure on demand[16].

2.1.3 Cloud computing types

There exists four different types of cloud computing, private cloud, public cloud, hybrid cloud and community cloud.

Private cloud

A private cloud will provide the customer with his own physical servers. This enables a complete data segregation, and no resource sharing with other cloud customers. This comes at a cost, as the private cloud is the most expensive cloud solution. The private cloud can either be hosted by a trusted third party, or it could be hosted by the company utilizing the servers(a self-hosted private cloud)[17].

Public cloud

In a public cloud the customer needs no self owned architecture or servers, and since the customer needs no architecture there is no need for any expensive investment. The services of a public cloud is also easy to implement as they are often only a swipe of a creditcard away(a truth with some moderation as the migration towards a cloud can end up with difficulties). The cloud customer will be protected with a high level of security, probably higher and tighter than any self-hosted business/organization ever would or could have. This is certainly the case when talking of large cloud provider companies like google, amazon, etc. As stated by NIST, a public cloud(cloud computing) has certain characteristics, "'on-demand scalability of highly available and reliable pooled computing resources, secure access to metered services from nearly anywhere, and displacement of data and services from inside to outside the organization"'[18].

Hybrid cloud

A hybrid cloud is a mix of both the private cloud and the public cloud[17]. The hybrid cloud type gives the customer the oppertunity to select and keep parts of their data and services to be segeregated on the private cloud, while at the same time have the ability to scale their use of the public cloud[17]. If the workload on the private cloud is to intense, the cloud customer can chose to scale up the resource need and use from the public cloud resource pool[19].

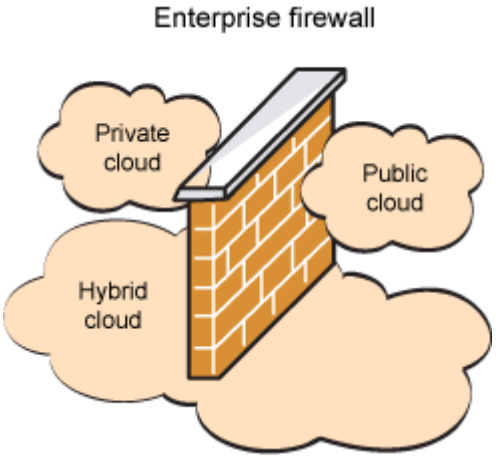

Figure 1: Cloud types [1]

Community cloud

The community cloud requires a trust based relationship foundation with other companies. In a community cloud several companies will work together with the same resourcepool, somewhat equal to the public cloud, but there still exist a hundered percent segeregation of data and the resource pool will not be shared by a non-trusted company.

2.1.4 Cloud computing Security

Security is a broad field, and for this thesis we will focus on security from a management point of view. This excludes technical solutions such as cryptography, algorithms and other technical areas, problems, research and solutions.

Computer security is always evolving, criminals and non-criminals alike will make attempts to surcumvent any security implementation. Security professionals will then be working as "'fire fighters"' to put out fires and to plug the potential holes in security. Computer security in the cloud is difficult to apply compared to older and more known technology. The cloud and the new problems that arises with new technology has increased security conserns at an alarming tempo as the technology itself is in a constant change. "'The rapid growth in the field of 'cloud computing' also increases severe security concerns"'[20].

We will investigate several aspects of the clouds management security issues, e.g. trust3.6, migration3.36, selection of providers876 and contractual agreements7.

2.1.5 History of cloud computing

Previous research, in what is now called cloud computing, had its origin in 2007[12][21][15]. Cloud computing is basically a predecessor to grid computing[16]. The big difference in cloud computing compared to previous methods and technologies are the great number of distributed computers instead of how these types of services previously used to be hosted(local PC/Server and the remote server rental)[16].

The idea and technology behind the cloud relies on several methods and technologies to be able to work as intended[16][15]:

1. The distributed technology used in the grid
2. High quality storage
3. Web 2.0
4. Viritualization
5. Distributed computing
6. Parallel computing

The development of new technology and techniques were needed as storage in the regular data centers and remote servers could no longer meet the need of todays companies and businesses[15]. The power consumation and the hardware cost pushed pricing on storage. This development happend continuosly as the need for more storage space increased[15].

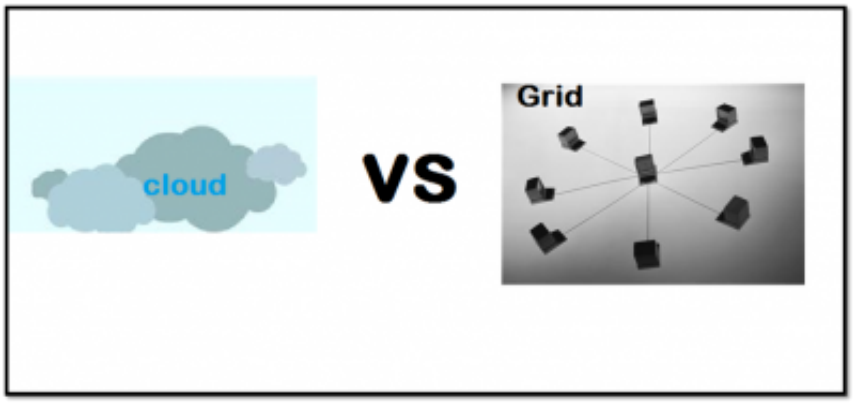

Figure 2: Cloud vs Grid computing[2]

Grid computing, as mentioned, initiated the technology of distributed computers. "“Grid computing provides a series of distributed computing resources through LAN or WAN"”[16]. The users within a grid can share computer resources to utilize and complete tasks that require amounts of resources that was previously not attainable through a local PC or a local/remote server. Cloud computing took this a step further, and with the available technology evolved into on-demand resource provisioning[16][15]. Grid computing is also less fail-safe as it relies more on the software used. One of the main differences between the two technologies is the resource management. While in grid computing the user would schedule a task for the grid to complete, while the cloud user would apply resources from the resource-pool to complete the task[16]. Cloud computing will also utilize virtualization to cut the strain on the physical resources. The cloud are able to automatically decrease or increase the resource pool(up until the upper limit of the physical resource pool) through virtualization in a way that is not possible through grid computing. Grid computing still has its areas of use, but they are often specialized for heavy tasks such as animation[16]. Some researchers belive that the grid capabilities and technology more and more will be integrated with cloud computing to form a world wide grid[16].

3 Related work

The chapter of related work includes all literature that was studied and found nessecary to answer the research questions 1.5 presented in the thesis introduction. The different cloud models 3.2.1 3.2.2 3.2.3 was studied to better answer the first and second research question 1.5. The study of related work regarding the models was conducted to learn the differences in the models regarding swapping of providers and the differences in security and compliance requirements. Related work surrounding the swapping of providers 3.3.3 was studied to better answer and supplement the first and third research question, but also to supplement the second research question 1.5. This includes known problematic issues such as provider lock-in and migration of data between providers. The section including the legal aspect of cloud computing 3.4.8 was studied to understand and supplement compliance issues with privacy laws. The compliance issue is both customer and provider related and the related work on this area helps supplement and answer the second research question 1.5. The section describing and elaborating the subject of Service level agreement(SLA) 3.5.4 is included and studied to help answer the second and third research question regarding customer contribution to security and compliance and if this helps enhance trust. The section of trust and trust management 3.6 was studied during the literature study, and included in related work to help answer and supplement the research done on all of the research questions 1.5. The related work is included to grasp the state of the art of the problem 1.3.

3.1 Definitions and Characteristics

All definitions are gathered from the NIST[5] draft, and are all relevant to specify before continuing with the related work. Several of the definitions are further described in this chapter, and it is important to form an understanding of the different subjects before elaborating in depth of the related work.

1. On-demand self-service:'" A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider'".
2. Broad network access:'" Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms(e.g., mobile phones, laptops, and personal digital assistants(PDAs))'".
3. Cloud Software as a Service(Saas):'" The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure'".
4. Cloud Platform as a Service(PaaS):'"The capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider'".
5. Cloud Infrastructure as a Service(Iaas):'"The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include

operating systems and applications"'.

6. Private cloud:"'The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise"'.
7. Community cloud:"'The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns(e.g., mission, security requirements, policy, and compliance considerations)"'.
8. Public cloud:"'The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services"'.
9. Hybrid cloud:"'The cloud infrastructure is a composition of two or more clouds(private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability(e.g., cloud bursting for load-balancing between clouds)"'.

3.2 Cloud Computing Models

The following sections will describe the different cloud service delivery models, and present related work and research done on the different cloud models. To understand how the swapping of cloud provider process is conducted, it is important that we know what types of services that is delivered through cloud computing, and any surrounding details of these services. We need to know if the different cloud computing models create issues when swapping cloud providers. It is also important that we identify any differences in the types of cloud models to be able to answer the second research question 1.5. To understand how cloud customers could contribute to security and compliance we need to know how the services they pay for are delivered, how they function and how they differ from each other.

3.2.1 SaaS(Software as a service)

This section details a brief description and overview of the SaaS cloud service delivery model.

Description

SaaS is the delivery of applications and software as a service, and is defined by NIST: "'“The capability provided to the consumer is to use the providers applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."'[14]. SaaS has developed from ASP and dates from the turn of the century (early 1990s) where it was known as "'web Services"' or simply, application hosting[22]. SaaS is as a way of achieving software on demand, delivered through the internet[23][24].

Figure 3: SaaS Model[3]

SaaS in its modern form is a generally new concept, and todays mainstream SaaS solutions started to emerge around 2005-2006 when the internet gained speed and the customers were used to dealing with web-delivered services[23]. As mentioned, SaaS is deployed over the internet and is deployed to run behind a firewall on a LAN or a PC. SaaS is basically a convenient rental of computing resources. It is a sourcing alternative that allows organizations the use of different applications on demand and with scalability.

A list of the important characteristics and benefits from SaaS[22]:

1. Accessed through the web
2. Subscription pricing
3. Vendor support
4. Low customization
5. Managed/Frequent upgrades
6. Success based revenue model
7. Shift to service-based mentality

According to the NIST definition[14], the consumer(user/customer) has limited control, this includes limited control of the infrastructure, servers, OS, storage, application capabilities(except from limit user-specific application configuration[23]). The cloud provider is the one that is actually running the hardware and software[19].

The users of SaaS is delivered the use applications on demand, application data management, backup and sharing between subscribers, all operated and provided by a cloud service provider. Software is hosted by the vendor and offered to the customer as a subscription[23]. Subscription fees get calculated based on the number of users, the time in use, per-execution, per-record-processed, network bandwidth consumed, and quantity/duration of data stored, which results in a cost-effective infinite scalability[23]. In other words, it makes it possible to scale the amount of software access based on the requests. The scalability is one of the more important aspects that makes the cloud envir-

onment attractive to its customers. The customers of the services do not need to invest in infrastructure, upgrades and the investment it is to employ personell to operate or support the infrastructure.

The different types of SaaS customers/subscribers include, but is not limited to:

1. Organizations (e.g. Google apps, Amazon PayGo, Microsoft SaaS)
2. Private end users (e.g. Facebook and gmail)

The need, and the possibility for customization is reduced when operating through SaaS[22]. It is also limited what customizations you are able to perform[22]. The need is mainly reduced because the provider actually performs the hosting, as mentioned earlier. The customer will not need to customize servers, databases or applications. At the same time, the ability to customize at will, is also limited. When the customer hands the control to a third party provider, the customer give away the ability to customize at free will. There still is some customization of application in SaaS, but the provider limits what you can customize and what you can not customize.

Another benefit from SaaS is the externally managed and frequent updates[22]. The provider has responsibility to manage and keep the systems updated. Any update or patch issue is "“outsourced"” to the cloud provider, and is of less or no concern for the customer as long as the updates are done smoothly.

We have mentioned the subscription based fees and payment model used for SaaS. This shift of payment option (away from the traditional way of buying licenses) changes the whole dynamic of the customer - provider relationship[22]. The provider will need to continuously satisfy the customer with good service and a working environment to keep the customer paying the subscription fee. Theoretically, the customer can at any time cancel the subscription and move onto a competitors cloud environment. We will take a closer look at cloud dependencies and provider swapping later in this thesis3.3.16.2.7.

Authentication and Identification

Most cloud services providers provide means of security for the cloud connections. We will not go in detail regarding the technical security surrounding SaaS in this thesis, as it is outside the scope. But, it is important to take note of the authentication and identification issues that exists in a cloud environment. Authenticating and identification in the cloud is a subject being heavily researched at the moment 4. As an example we can mention the standard use of user name and password authentication, which could prove to be insufficient. However, as mentioned, there is ongoing work and research on security in the field of cloud computing[25] and SaaS security.

Subscriber/Provider interactions

The examples given in the NIST standard[5] illustrates how the SaaS dynamics with subscriber and provider interactions work. A provider generally offers several different software application solutions to multiple different customers. Let us consider an example 5, something as simple as a text based program. The SaaS provider has to deliver this service to two different organizations at the same time, and each organization has several employees that could access this specific service at the same time. The different applications are named "“Apps"” and given a letter each, e.g. "“A, B, C"” which represent three different software applications. The clients are the users attempting to access these applications. The box labeled "“available"” are the different available execution processes

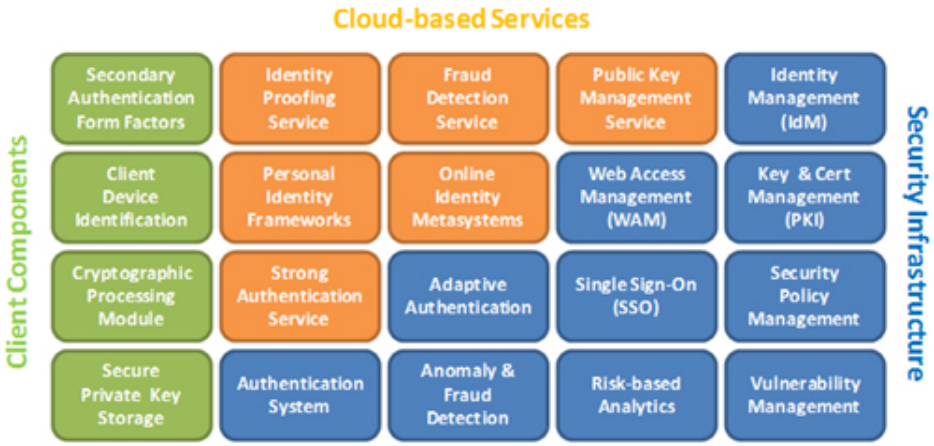

Figure 4: User authentication example[4]

of these applications. Each client attempts to access these application through a network connection. When the clients are successfully connected to the providers servers they will request to run an application. Each client will then be given their own execution process of whatever application they requested to run. E.g. Client 1(C1) requests to run two different applications(B and C) and is given the execution resources 1 for application B and execution resource 2 for application C. When client 2(C2) now want to access application C, this client is given execution resource 3. With this resource management one can distribute the execution of the same type of application to an unlimited amount of different clients (as long as there is server and bandwidth resources available). This example is re-constructed from the abstract interaction example within the Software as a Service chapter found in the NIST standard[5].

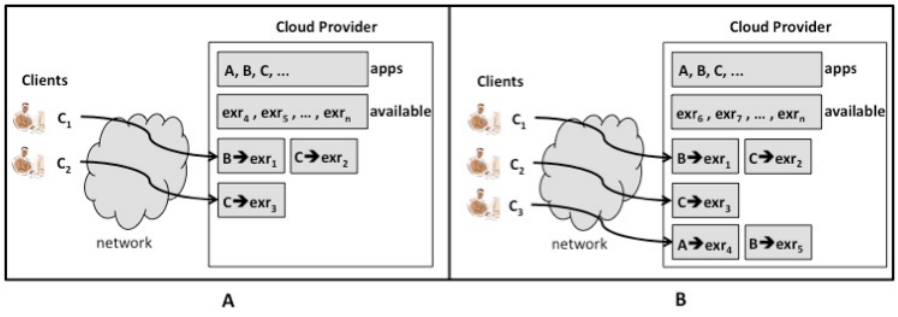

Figure 5: Abstract interaction - NIST[5]

In the SaaS model the provider is the one with control. The provider has full and total control of the lower layers, this includes Hardware, Operating system and Middleware. The cloud provider also has full administration control of the top layer which is applications, while the user/subscriber normally only has limited administration and user level control over the application layer.

MTA architecture

The idea behind MTA is that the providers only host one instance of an application on its servers, while each user experience this as if they were running their own application or instance. A SaaS example; Facebooks servers are hosting the application itself, while each user has the experience of being logged on to a separate instance/application. The MTA model is a form of virtualization where the application differentiate between customers and partition the configuration and data of the application such that each user works within their customized virtual application instance(tenance)[26].

Configurability

The configurability options within the SaaS architecture is made in a way that the designers of the application should be able to use just one instance of code-base when developing an application, while each user have the ability to configure and make changes that suits their specific needs[23]. This allows users to have their own unique experience, even if the code is the same. The configurability should be easy to develop by the designers and fulfill any need of the customers. The configurability is an important part of the multi-tenancy architecture because it allows for individual needs and modifications, making SaaS an applicable solution to many different types of customers[23].

SaaS risks

SaaS applications are often limited to tailer for specific needs[27], and has limited configuration capacities. A customer of a SaaS depends on the SaaS provider to make any necessary changes, as the customer is often restricted to make any major change to the service. The provider also decides upon and controls the security for a SaaS[19], the customer has limited to no influence. In a SaaS the customer risks exposing and losing business-critical information. The less control the customer has, the higher is the risk of something unexpected and unwanted happening. The customer has no guarantee for who handles or looks at the customer data, other than it is someone from the provider.

SaaS can also create dependencies. These dependencies are often based on either interface or file format of the data handled in the cloud. This could result as a vendor-lock in with potential high switching costs[19].

As with any of the cloud service delivery models, a customer has to evaluate potential compliance issues before using the service.

3.2.2 PaaS(Platform as a Service)

This section of the thesis will briefly describe and present the reader with the state of the art and related work regarding the cloud service delivery model, Platform as a Service(PaaS).

Description

The 2011 NIST cloud definition defines PaaS as the following: "“The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment."'[14].

PaaS provides the customer with a development environment through programming

languages, libraries, services and tools as mentioned in the NIST definition. "“PaaS provides the development and execution platform for user applications in the cloud"'[28]. This platform is virtual which allows the customer to not be concerned of the physical computer and the network interfaces[29]. With PaaS a customer can use middleman devices(cloud provider) to develop own programs and applications, and deliver it to the customers users(own customers) through the internet[16]. Platform as a Service can also be used to give clients platform access which enables them to put their own customized software and applications on the clouds[20].

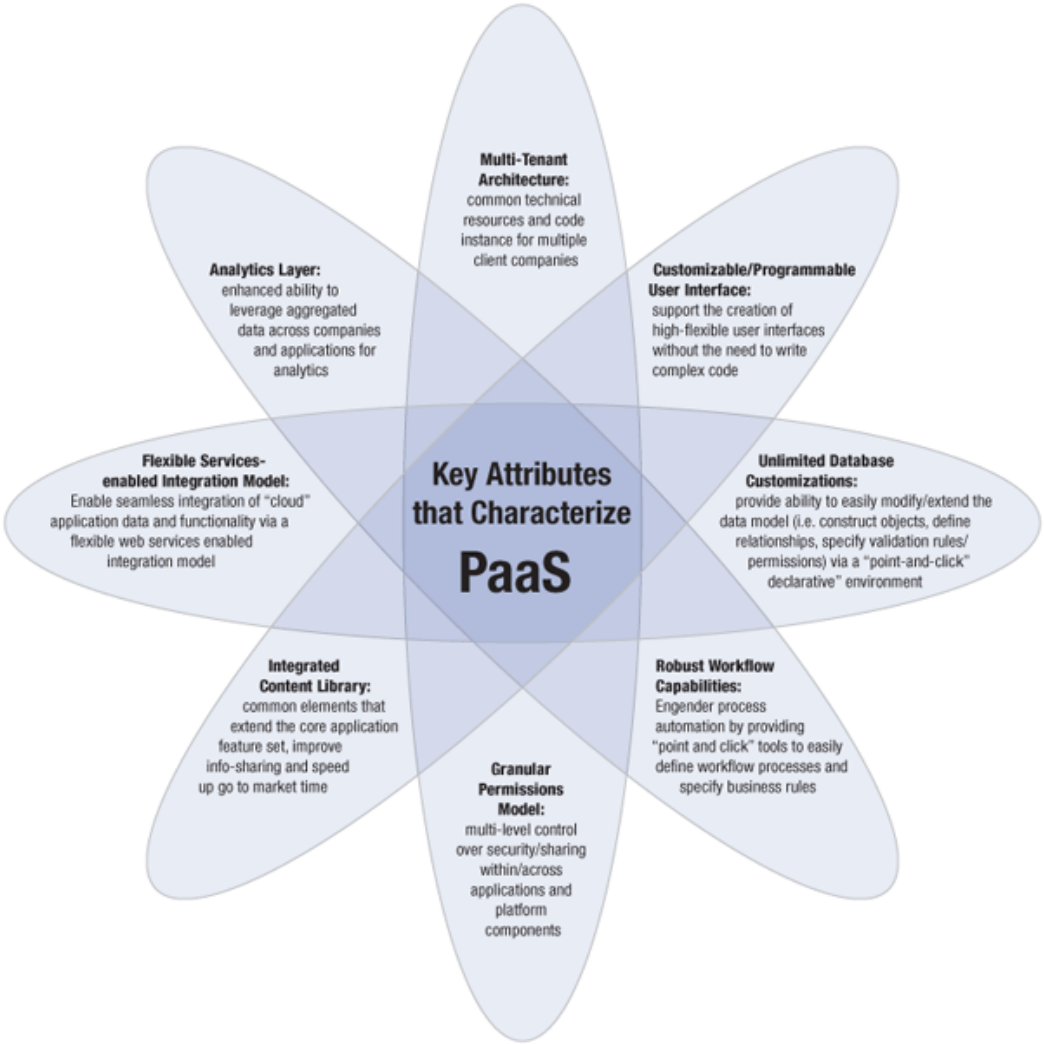

Figure 6: PaaS key attributes[6]

The key attributes and characteristics of the PaaS service delivery model is presented in the PaaS illustration figure6.

As with any cloud service delivery model in a public cloud there is less cost accompanied with PaaS than self hosted alternatives. There is less cost bound to the purchase of infrastructure, and the scalability options in the public cloud. There is also the benefit of reduced time-to-market(the time it takes to push the created applications and programs to the market and the customers of the developed applications and programs)[27][29].

"'Application components or building blocks allow for a fast and easy creation of new SaaS applications"'[27]. A cloud customer subscribing to PaaS could easily create, access and distribute their newly developed application.

The development process is done through the interaction with the PaaS servers through browser windows on a thin client[29]. This easy form of access is another benefit of the PaaS model. Thin clients are cheap, the accessibility is achievable with little investment, and the web interface is often easy to operate. The cloud provider could also offer integration platforms/methods, these integration methods would ensure that the migration of old "'legacy"' information and data is more or less seamless[27]. This method could also possibly be of use when migrating away from a cloud provider, but, the provider is less likely to help the customer with this process. We will touch upon this later on in the chapters of swapping cloud providers 3.3.3, s6.2.7.

Multi-tenacity is described in the sub-section of SaaS3.2.1. Multi-tenacity in PaaS basically works in the same way, but, it "'...is realized through underlying tiers of applications and database servers."'[27]

PaaS and trust

There has been examples of PaaS used in trust based models and frameworks, Brown and Chase[30] proposed an example in 2011. The thesis will take a closer look at trust, trust management and trust modeling in the section of trust management 3.6 and the chapter of modeling 8.

PaaS risks

Like SaaS, PaaS is not risk free. Migrating towards a PaaS solution could prove to present the customer with a long learning curve for its employers. The employers of the cloud customers would have to spend time to adjust and be accustomed to the new development and provisioning environments and tools given by the cloud provider[27]. When using PaaS, developers could be restricted to the APIs made available by the cloud provider, and the customer will often have to deal with a closed platform[27]. These dependencies could create a provider lock-in. The provider lock-in can potentially be costly to migrate from.

As with any other cloud computing service, there exists potential compliance issues with PaaS. The applications and programs created by the cloud customer could potentially include information that could be restricted by national privacy laws or regulations. But, it is of course less of an issue, as most application programming do not necessary need such types of information to function properly, it is avoidable.

3.2.3 IaaS(Infrastructure as a service)

This section of the related work part of the thesis will take a brief look at what IaaS is, and how it operates.

Description

"'IaaS refers to on-demand provisioning of infrastructure resources"'[31]. The NIST definition on cloud computing defines IaaS as "'The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage,

and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)"[14]. These definitions includes (what previously was called)server rental(computing/VM), storage and storage space, and as mentioned limited set of selected network components in a cloud environment. Within this "“package"” the different software(tools) to deliver these types of services are included[32]. IaaS is simply described as a form of a hosting service. The provider of this hosting service will provide the customer with the same opportunities that are available with self owned hardware, and the necessary tools required to control the software used on these virtual hardware[32]. This could include application control and file/data management tools. The service normally includes (scaling of) storage space, bandwidth and memory[32].

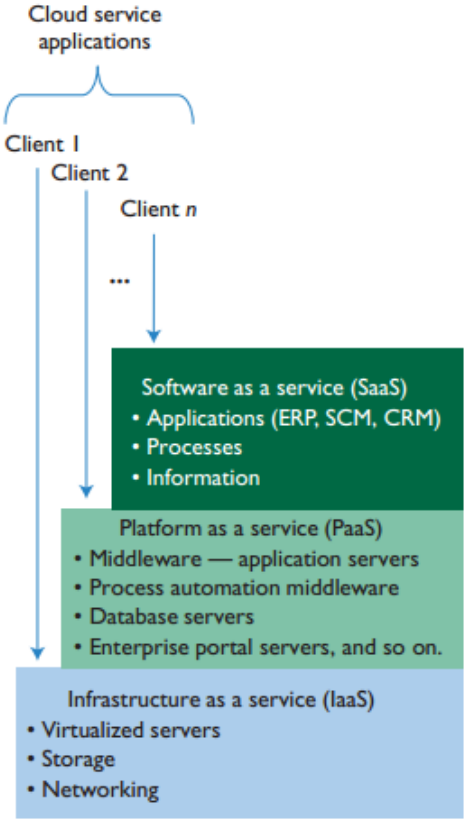

Figure 7: The conventional cloud stack[7]

IaaS is at the lower end of the cloud stack, as shown in the illustration figure of the cloud stack 7. The customer gains a tremendous control of the system or service they pay for, this includes control of security measures[19]. The customer gain flexibility to secure data, and to implement the needed degree of security, but, this comes at a cost. The customer gain this flexibility, but is also responsible for any and all of the security measures them selfs[19]. With this control and flexibility, the customer will also have to be responsible for any patching and software updates[19]. This also include any type of configuration of operating system, host-based and network based firewalls and ids, and also applied applications that run on their subscribed system[19]. The customer will also be responsible for the integration of all aspects of an application they deploy. This could

be e.g. databases and plug ins.

Multi-tenancy works as described in SaaS section, except that it is handled at the hypervisor level and "“in IaaS, tenants share infrastructure resources like hardware, compute servers, and data storage devices"”[33]3.2.1.

The most important benefits, characteristics and components of IaaS include:

1. Utility computing service and billing model
2. Automation of administrative tasks
3. Dynamic scaling
4. Desktop Virtualization
5. Policy-based services
6. Internet connectivity

Subscriber/Provider interactions

The customer of the IaaS will need the ability to establish a secure connection to the service at any desired time, and at any desired place. The service has to be low cost and easy to use[32].

Architecture

IaaS is hosted through physical servers inside different data centers. Each data center has several physical servers, and each physical server hosts and executes one or more virtual machines. The cloud customers will be given and assigned their own virtual machine(s) by the operators and administrators. The customers can control and operate these VMs at free will. The customers using the virtual machines have no insight or visibility into the virtualization layer, the physical server or the data center where their VM is located[34]. The cloud provider can move or migrate the different virtual machines inside the physical servers, the data center and even between data centers[34].

IaaS risks

With IaaS the customer has to manage the hosts security, this includes patches, configuration, log management, host based IDS and firewall[19]. This is much like the customer hosting its own data center/server. But, in IaaS the customer has no option for NIDS/NIPS, limited SSL options, no outbound fire walling, often only one IP address per instance, and IaaS is often delivered with a flat network[19]. In IaaS the customer has to rely on hardware and network support from the cloud provider, and this could of course be an issue[35]. Leaving this out of the customers control could potentially mean a decrease in the quality of delivery compared to a self-hosted alternative, and a increase response time in problem solving queries[35]. There is also a compliance issue as to the location and origin of the IaaS delivery[36]. Data segeragation and resource sharing with other cloud customers could also be a problem[36] with regards to sabotage and industrial espionage. "“Data may leak between competiting companies"”[36]. This is a problem in the public cloud and with the viritualization of hardware and machines.

3.3 Swapping providers

To help answer the first research question 1.5 we will look at related research and work that touch upon migration towards the cloud, selecting the right provider for the cloud customer and the process of swapping providers. It is important to identify the problem area found in previous research, and also how this process is conducted both in the cloud and previous hosting alternatives. We also need to identify what aspects these processes contain.

3.3.1 The problem

A paper presented by several researches at Berkely[11] in 2009, states that the second most important issue to solve to make cloud computing viable is the 'Data Lock-in' issue. Data lock-in could create problems for customers of cloud services, and the issue can make potential customers delay their planned use of cloud technology. The data lock-in issue is created by different dependencies in the cloud 3.2.1, 3.2.2, 3.2.3. These dependencies make the cloud customers dependent on the solutions, architecture and technology from their providers. These dependencies could come in the form of a proprietary file formats[37], (API dependency or) no available API[38], virtualization technology[8] or with different types of tools[19]. The providers has no real incentive to change this. As they get customers, they will most likely keep a hold of these customers for a long time due to this particular issue. But the providers also risk getting fewer customers with technology and policies that create dependencies and vendor lock-in. Cloud customer could start to avoid providers with dependencies and lock-in issues. If large parts of the cloud provider business use a form of vendor lock-in there is no real move or migration of customers from one provider to another[19].

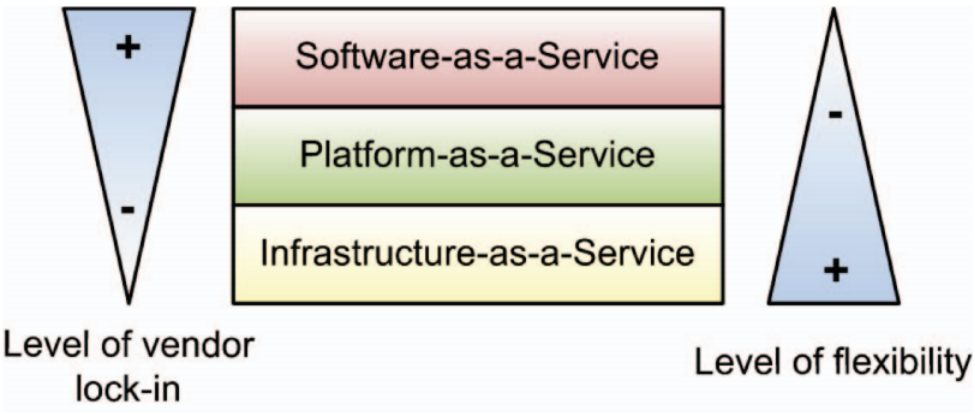

Figure 8: Vendor lock-in illustrated in the cloud stack[8]

The different cloud service delivery models create different levels of dependencies 8, 3.2.1, 3.2.3, 3.2.2.

The customers should optimally not be having having difficulty extracting their own data and programs from one service provider to another. The paper by several researchers at Berkley[11] presents us with what they believe is an obvious solution to the problem, standardizing API. Some form of technical standardization will probably have to be in place, however, we will try to look for solutions to this particular problem with the help

of management tools, guidelines, best practices and planning. Until we get a common standardization, there exist a need for other possible solutions.

An article by Brian Hayes[39] brings up issues regarding the ownership of data, and if you can bring your data a long with you as you switch service provider. He also raises questions to what is supposed to happen to data if a customer fail to pay their bills, and if the customer have the ability to "'‘really"' remove old documents. Google, one of the larger cloud service providers in the world, mention in a white paper[40] regarding cloud security how they as a company handles customer data once the customer decides and confirms to delete an object. The data will be removed, making it unaccessible from that users interface[40]. Further, Google will delete objects from their servers, and remove any stray and remaining pointers[40]. Once the pointers and the data itself is removed the dereferenced data will be overwritten with other data over time[40]. They also make sure to put their retired disks through a data destruction process. This data destruction process is a complete logical wipe(full write of the disk with all zeros). The NIST draft[5] suggests that any customer should require that their provider offer these types of described deleting mechanisms.

Data Preservation is also mentioned in the NIST draft[5]. The draft from NIST[5] mentions that most providers state to have no obligation to preserve any data or information stored by customers if customers access to the services is closed or terminated. Customers service could e.g., be terminated or closed by the provider if the customer fails to pay the bill, or go back on any signed agreement. If the service is discontinued by the customer voluntarily, providers generally state that they will keep their data for around 30 days before starting the deletion process. Once a customer or provider has terminated the service delivery it could prove hard to regain the stored data if the provider has ensured dependencies.

NIST[5] mention these issues(lock-in, ownership, data preservation) as problems that needs to be solved. Some standards has already been developed, Open Virtualization Format[41] and the Cloud Data Management Interface[42]. But, there is a need for further development, and experience is needed to reduce the cost[5].

The NIST draft[5] also mentions the problem with the transfer of files between providers. A provider needs to offer proper credentials to another provider before a transfer can take place[5]. The NIST draft[5] also mention the need for standardization of format for the object(s) that is to be transferred. We will take a closer look at this in related work regarding the swapping between service providers 3.3.2.

3.3.2 Swapping between Service Providers

When swapping cloud providers, or migrating to the cloud from an internal solution the customer could potentially come across several problems and issues. When swapping provider or migrating towards the cloud the customer could experience a knowledge gap. Knowledge from the previous providers is not automatically transfered to the new provider(the same fact applies for migration from internal solutions to a cloud provider)[43], the IT experts that worked on the customers system and services will most likely stay with their previous employers[43]. In fact, the previous provider would normally have little to no interest in helping or aiding the customer or the new provider in any part of the swap process[43]. This will lead to a challenging relationship between the three parties, the customer, new provider and the old provider.

Add to this, around 25 percent of all outsourced contracts made are discontinued and given to new providers[43]. These numbers can tell us that a switch of cloud provider is a relevant problem to be addressed.

The cost of a swap between service providers can often turn out to be expensive[43]. The cheapest choice is more often then not, to stay with the current provider, while switching is the second most costly choice, and back sourcing as the most expensive and least desired choice[43]. The high cost of a switch often leads it to be a less viable choice.

Reasons to swap providers[44]:

1. Dynamic changes in the customer landscape
2. A shift in management risk tolerance
3. Changes in the supply market
4. Supplier rationalization
5. Natural Disasters[19]
6. Political conflict[19]
7. Compliance[19]
8. War[19]

3.3.3 Cloud broker

A way to avoid the lock-in issue, or ensure that the customer get the needed help in migration and swapping processes could be through a cloud broker. The cloud broker is a part of what is thought to be a solution to some of the issues and problems that has been plaguing the cloud[9]. In a paper by Buyya, Yeo and Venugopal(2008)[9] they envision a solution through a global market with cloud service brokers. The cloud service broker that exists in the market today, is working more or less as Buyya, Yeo and Venugopal envisioned back in 2008. The cloud broker serves as an intermediary between the cloud customer and the cloud provider[9] for resource allocation and negotiation[45].

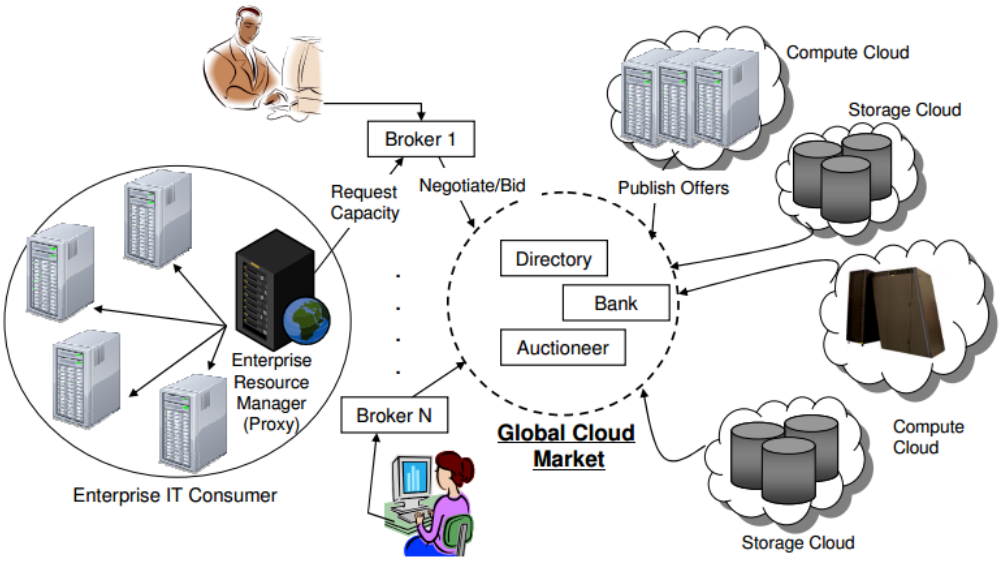

Figure 9: Cloud brokers in a global cloud market[9]

The broker mediates between the cloud customer and the cloud provider, this includes negotiating of SLA, metrics, service delivery and other potential business needs cloud customer could have[9][45]. The broker could handle a swap of provider(switch of data centers)[9].

3.4 The legal aspect

This section will list, consider and discuss some the more relevant European and Norwegian directives and laws that one would have to consider when moving into the cloud or when switching between cloud providers and data centers. Both the first and second research question requires literature study that covers the privacy laws and regulations that is applicable for cloud providers and cloud customers, and to figure out what can and can not be done with a service level agreement. We need to figure out any regulations and/or boundaries that is applicable and possibly restrictive towards the cloud customer.

Since most directives, regulations and laws that is applicable to cloud customers, in both the European Union and in Norway, is focused on privacy, it is important to have a understanding of what privacy actually is. We will use the following definition of privacy: According to Alan Westin[46] privacy can be interpreted as: "'... the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'". Privacy in a cloud environment is important for several reasons. First of all, all companies or organizations that are cloud customers has to ensure they are compliant with the national privacy laws, directives and regulations applicable for their location and region. Without this compliance they could be forced to stop using the cloud service, either temporary or permanently, which could result in unwanted and unexpected costs. The compliance can even be spread across multiple jurisdictions because of the dynamic nature of the public cloud[36].

The companies using cloud services also have to consider the risk of industrial espionage [36], and the requirements they them selfs set on the privacy of their data. If the cloud customer store their customers data in the cloud, they need to ensure the privacy of these customers data. Breaches in privacy could cause severe cost and loss of reputation to a company. One thing to remember is that the companies acting as cloud customers will have to help "'cover the bill'" of failures in compliance or privacy breaches by the cloud provider. The cloud customer will be held accountable by their customers and the national data protection inspectorate. This could result in a loss of reputation, business ideas and work hours. The economic costs connected to these losses could end up being detrimental.

3.4.1 Directive 95/46/EC

The European Union has created its own directive(the Data Protection Directive or directive 95/46/ec) that is addressed towards all its member states. The directive is rather old, as it was created the 24th of October as far back as in 1995[47]. However, this outdated directive[48] is still applicable for todays technology and the problems and issues regarding data and data control in the cloud. What is important is to be able to recognize the more relevant aspects of the directive and its different definitions.

Objective of the directive

The idea behind the directive is to better secure privacy[46] through secure data and data processing within the European union and its member states. The improved security of data will improve and uphold the fundamental rights and freedoms of natural person, and their right to privacy[47]. The directive was also created to make sure that member states would be unable to prohibit or restrict free flow of personal data across their borders(as long as privacy and security is ensured).

Definitions

Before we can take a deeper look at some of the directives paragraphs, it is important to mention and get an understanding of some of the directives more important definitions. Personal data, defined as "‘’personal data’ shall mean any information relating to an identified or identifiable natural person, the "‘data subject"; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological mental, economic, cultural or social identity;"’[47]. The definition is broad, and could leave room for different interpretations. However, the data is personal when it can be used to identify, or link the information/data, to an individual. This is applicable even if the person or organization holding the data is unable to produce the link.

The second definition is regarding the processing of personal data. The definition is as follows: "‘processing of personal data (’processing’) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;"’[47]. The definition cover any type of handling of personal data, whether or not it is done automatically or manually.

Definition "‘c"’, "‘’personal data filing system’ shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographic basis;"’[47]. This definition concerns the storage of personal data, and covers all the different types of storage.

The directive continues with definitions for controller, processor, third party, recipient and the data subject’s consent which can be found under definitions in the directive [47].

It is important to note the clear difference the directive has between the controller and the processor. Data controller is defined as "‘party that defines the purpose and the means of the processing, while the data processor is more or less defined as "‘the dumb performer"[49]. In a cloud environment some of the problem and confusion comes from the fact that a cloud customer can be both the processor and controller.

The Directive paragraphs

Section 2 of the directive states that "‘whatever the nationality or residence of natural persons, respect their fundamental rights and freedom, notably the right to privacy"’. As an example, in Norway the breach of privacy is punishable by law[50]. The "‘Personal Data Act"’ and the "‘Personal Data Regulations"’ sets several restrictions to how and what data the service providers can work with, look at and share.

At the same time, the EU directive "‘section 3"’ makes sure that one of the fundamental parts of the union treaty[51], the free flow of goods, persons, services, capital

and data between its member states(while safeguarding the fundamental rights of individuals). This is further enhanced in section 4,5 and 6 of the directive[47]. The sections in the EU directive leave much up each individual member state, and their individual laws on privacy. As seen in section 9, that states that every member nation is to be given a "‘room to maneuver"’ regarding privacy regulations and laws, this is also mentioned in section 32 and in 18 where the directive wants to ensure that individuals are not deprived of entitled protection through national/community laws "‘(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;"’. These national/state laws has proven to be contributing to restricting data flow and the economical growth once anticipated. These laws are still a problem for the European Union and the cloud, as national laws still dictate the flow and handling of information and personal data. As of now(Q1/Q2 - 2012) several laws within different member states are considered outdated[48]. The European Union are working on a new strategy for cloud computing and personal data protection that will result in a reform of the 95/46/EC directive[52].

The directive further ensures that any processing of personal data of either persons, public authorities, enterprises, agencies or other bodies has to be informed that their personal data is being processed as stated in section 25[47]. According to the directive one also has the right to "‘consult the data, request corrections and even object to the processing"’[47]. For any cloud customer, this paragraph of the directive is important. If any provider inside the European Union process any of the customers personal data, they are obligated to inform the customer. This paragraph[47] should ensure that the customer at any time knows who handles their personal data, in what circumstance and for what purpose. This is important to know for any cloud customer to reach compliance and ensure data privacy.

Providers within the European Union is also restricted by the directive[47] to not store any information about their customers that is unnecessary. The information stored has to be "‘adequate, relevant and not excessive to the purpose they are processed"’. The purpose of the storage of data has to be determined when the data was collected[47]. What this means is that data collected for a specific purpose can not be used for any other purpose than what it was collected for. This is to prevent the information being abused for a secondary purpose for which the information was not intended. E.g. customer data collected to create control and overview of billing is used for advertisement purposes.

The European Union is a legal maze for both service provider and customer as of now, as each individual state, nation or community is encouraged to enforce their own privacy laws(to a certain extent), as mentioned in section 19. This is a major issue for anyone wanting to switch providers, or make the move onto the cloud services. Consider a company that rents several cloud services in one EU state for storing of personal data. Now, the company would have to make sure that the country hosting the cloud provider has satisfactory privacy laws. The cloud provider could also outsource some of the storage to another EU member state, or perhaps even a third country, e.g. load balancing. This other EU member state or third country could have insufficient privacy laws compared to what the company and its customers need. Add to this complexity the switch between

providers. If some of the companies data has been stored in a third country, how can you be sure you are able to extract all of these data?

Data export to third countries

According to the EU directive, section 20[47], any handling of data by a person or organization in a third country outside of the union must not stand in the way of the protection of individuals. The degree and level of protection which is mentioned in the directive. This is however something the subscriber/customer needs to make sure before committing to any agreement or contract as these nations does not automatically follow the directives delivered by the European Union. "section (20) in the directive[47], Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;"‘[47]. The member state law where the customer is residing is determining whether or not the customers data can be exported to third countries[47]. As stated by the paragraph, any third country must not stand in the way or differ from the customers origin nations privacy laws.

When does the EU directive apply?

It is quite common for data to be transfered in the cloud, and with it, personal data. Migration to a cloud provider requires data to be transfered from outside the cloud into a cloud. A cloud provider could transfer the data around the cloud to improve the storage area(load balancing). The data could also be transfered for accessibility, and between providers in a swap of providers, and also back on in-house hosting solutions. As an example of cloud data transfer; Google apps transfer data in the cloud according to where the customer access data. As a more specific example: a Norwegian customer want to access cloud data while on a business trip in India, the data is first transfered to India, then become accessible for the Norwegian customer currently residing in India. This could of course lead to compliance issues.

It is important for any potential cloud customer wanting to move onto the cloud or switch between providers to know when this European directive comes into play to ensure compliance. At the moment there is only really one directive that directly controls the data flow of cloud services in the EU, the 95/46/EC directive[47]. The directive, and its regulation to the flow of personal data was when created, considered necessary to protect its citizens. But, in the cloud, data can rapidly change data center, and with that, nation, even continent. This could happen without the customers knowledge of the exact location of their data. The 95/46/EC[47] does restrict this with the protection of law. Therefor it is important for customers to have a complete understanding of where and when the directive is applicable.

Peter Hustinx, a European Data Protection Supervisor has in his interpretation of the directive given a three-point list of cases where the law is applicable or non-applicable[53]:

1. Cloud provider established in the EU - or acting as a processor for a controller established in the EU - will in principle be applicable by EU law
2. Cloud provider which uses equipment (e.g. servers) in one of the EU member states,

or are acting as a processor for a controller using such equipment - will also be applicable

3. Cloud provider in other cases - even if it mainly and mostly targets European citizens - would not be applicable by EU law

Discussion on 95/46/EC

The directive is getting old, and was not developed with cloud computing in mind. The directive was actually developed in the pre-internet era, were centralized computing and processing was the norm. The transfer of data between nations, which is normal in a cloud environment, is difficult with the current directive. The difficulty of data transfer out of a EU member nation, and also transfers coming from, or going to a third country(USA, Asia) is evident. Another known issue is the definitions of processing, and "“data processor"” and "“data controller"”. Both the consumer and the provider can be put in either or both of these categories. This makes the directive a source of confusion when considering the legal aspect. There is a reform of the directive in development, and this is much needed before we can take full advantage of the possibilities given through the cloud environment.

3.4.2 Directive 2002/58/EC

The 2002/58/EC is a directive that builds upon and "“particularizes and complements"” the 95/46/EC directive[54][55]. Mainly the directive expands the 95/46/EC on the subject of processing and transfer of data[54].

According to the directive all cloud providers are required to assure the nessecarry security measures and also inform all its subscribers of potential inherent security breach risks[54][55]. As a potential subscriber and customer one should make sure to require this information if it is not given. The cloud providers are also required to take suitable action to restore the normal level of security for new and previously undetected or unpredicted risks[54][55]. This directive is made to restrict the cloud providers, and as such is not that important to cloud subscribers. It is however important to be aware of the directive, and the way it helps protect cloud users. E.g. Article 5 in the directive[55] states that "“the use of electronic communications networks to store information or to gain information stored in the terminal equipment of a subscriber or user"” "“must be accompanied by specific and understandable information related to the purpose of processing that information. Additionally, the user or subscriber must have the option of refusing such processing"”[54]. As mentioned by Valentina Pavel Burloiu[54] this greatly helps the subscriber and customer with their right to privacy.

The directive is also applicable when changing between data centers and different cloud providers. The directives article 6.1 states that except for billing purposes, providers that delivered services and stored traffic data that is directly related to the customer has to be deleted and removed or made anonymous when the purpose of transmission is aborted or canceled[55][54], this also applies to location data. There are exceptions to article 6.1, but as a customer one would have to agree to let the provider keep the data, and the customer would also be able to withdraw this agreement at any time.

According to article 12.1 of the directive cloud providers are required to inform any customer of their mentioning in any directory and the purpose of such register if their personal data are used or could be inquired[55][54]. "“Subscribers also have to be in-

formed about the search options this type of file has in its electronic version"'[54][55]. The subscriber is even given the right to decide whether or not if their personal data should be included, and also the right to "'verify, correct or withdraw such information"'[54]Article 12.2[55].

3.4.3 Directive 2006/24/EC

This directive focuses on "'the retention of communications data generated or processed in connection with public available electronic communications services"'[56]. Public available electronic communications services are easier to access and use, but does not cater to organizations and businesses of a medium to large scale. These types of services are still under European and national law, but requires no contractual agreements. The lack of any form of specified contractual agreement removes any additional safety net businesses normally have with private cloud services.

3.4.4 OECD and other international privacy guidelines

The OECD privacy guidelines are voulentary, and as such, one can not demand any organization or business to implement them. It is important to know of their existence, and that international corporations could choose to follow these regulations. The guidelines are outside the scope of this paper, but the paper will still mention what is considered to be the guidelines main recommendations regarding the trans border data flow.

1. Member countries are to consider in their legislation the implications for other member countries of domestic processing and the re-export of personal data (paragraph 15)[57].
2. Member countries should take "'all reasonable and appropriate steps"' to ensure that trans border flows of personal data (including transit of data) are uninterrupted and secure (paragraph 16)[57].
3. Member countries should refrain from restricting trans border flow of personal data between themselves, except where the recipient country "'does not substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation"'. A member country is also allowed to impose restrictions "'in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection (paragraph 17)[57].

3.4.5 APEC Privacy Framework

The Asia-Pacific Economic Cooperation is another regulatory tool "'which is a set of privacy principles that members economies may implement voluntarily"'[57]. The Asia-Pacific area is outside the scope of this paper, but it is still worth mentioning that such a cooperation exists. For further information and analysis of this framework[58] one should study the framework itself[58], and different analysis of the framework[57]. The APEC cooperation has also released a document for data transfer between members and non-members[59].

3.4.6 Data export from one nation to another within EU

If you as a customer rent cloud services from another European member state you would have to make sure that the nation where the cloud provider is localized has sufficient privacy laws, or at least has servers or equipment that is localized within the EU. As

long as the provider is located in the European Union the provider would need to follow the European directive on privacy laws, however, as mention the directive leaves it up to each nation to produce their own privacy laws and uphold the level of privacy demanded by the EU directive. It is recommended that whatever contractual agreement that exists between customer and provider, the customer should make sure that they know every aspect of the given nations privacy laws and directives. It is also a good idea to compare this with their own nations privacy laws and directives to decide if these are sufficient and compliant.

3.4.7 Safe Harbor

The Safe Harbor agreement[60] was made between the EU and USA in 2000. The agreement states that companies from USA that want to handle sensitive information from the EU(or EU states) has to follow a set of principle set by the American government based on the EU directives. However, the safe harbor should not alone be a reason for why any EU member state should send their information to a third country.

3.4.8 Norwegian law

It is important for Norwegian customers to know when the Norwegian Personal Data Act and Regulations applies. First of all, according to the 3th paragraph in the Norwegian Personal Data Act[50], the law is applicable if the handling of personal data is done entirely or partly with the use of electronic equipment[50]. The law applies to anyone handling personal data within Norway, and also anyone using any aid(s) in Norway(paragraph 4)[50]. However, if the processing or transfer of data is not done with systems or organizations/businesses stationed in Norway, only transferring through the country, the law does not apply[50].

The data that is being processed or handled has to be defined in paragraph 1 and/or 2 of the "'Personal Data Act'"[61][50].

According to Norwegian law(paragraph 2 and 4 in the "'Personal Data Act'", the customer of any cloud service is the processor or handler of data, and has all the responsibility to ensure that any sensitive data is processed, handled and stored according to the Norwegian law[61][50].

Before the actual handling of data takes place there would need to be agreed upon several accept criteria for potential risks. These different levels of accept criteria is decided by the Personal Data Regulations[62]. According to paragraph 2-4 and 2-2 of the Personal Data Regulations[62] the customer of the cloud service is responsible for setting the desired risk criteria for the data they want to outsource to any cloud provider[62].

If a cloud customer should fail to be compliant with Norwegian laws and regulations, the Norwegian Data Inspectorate has authority to force changes to the cloud customers usage of the cloud environment.

3.5 SLA

SLA can be described as a contractual agreement between two parties. The SLA has been used to formalize the roles within the contract, and state the expectation, penalties for violations and other terms[63]. The contract is in place to create a certain assurance to both the users and the providers of the cloud services[64]. With large service providers the SLA is often pre-defined and the customer often has to agree to the terms if he want to rent their services, however the SLA can also include negotiated terms. No matter if the SLA is pre-defined or created through negotiations, the agreement serves as a Quality of Service between provider and consumer and should be considered with great care.

3.5.1 Definition and requirements

SLA is defined as "(...) a formal negotiated agreement between two parties. It is a contract that exists between the service provider and the customer. It is designed to create a common understanding about service quality, priorities, responsibilities, etc"[65][66].

The following are the main requirements of the SLA[64]:

1. SLA format should clearly describe a service so that the service consumer can easily understand the operation of the services
2. Present the level of performance of service
3. Define ways by which the service parameters can be monitored and the format of monitoring reports
4. Penalties when service requirements are not met
5. Present the business metrics such as billing and stipulate when this service can be terminated without any penalties being incurred

3.5.2 Sec-SLA

The regular SLA contains metrics and agreements regarding network throughput, delay, availability/up-time, package loss and other performance measurables. The SLA and Sec-SLA basically differs in the way that the Sec-SLA focuses on security and security measures. Security measures can be the protection against malicious code, security backup, security policies and protection against unsolicited electronic messages[66]. The Sec-SLA concept is not new, but it has to be done differently in the cloud than it would be on older technologies.

According to Chaves, Westphall and Lamin[66] the Sec-SLA should be developed by following the following three steps:

1. "“Policy Analysis: Any data available in the enterprise that could give support to create Sec-SLAs can be evaluated in this step"”
2. "“Architecture Analysis: In the previous step, a set of preliminary service level agreement categories was obtained. Now, when possible, these categories are applied in an architecture analysis activity. The objective is to analyze the customer’s infrastructure and to find the requirements that could be met directly into elements like web servers and firewalls"”
3. "“Interviews: To collect on what are the security concerns in the user’s point of view"”

The results from these three steps is meant to create a list of categories that will help

in obtaining and creating a sec-sla[66].

One of the big differences with the use of Sec-SLA and SLA in the cloud is the fact that the cloud itself is dynamical, on demand and changing. For a Sec-SLA to work in a cloud environment it has to have the same capabilities as the environment it is created to guarantee quality for. The definition of metrics and the monitoring process will have to be done on demand[66]. The SLA itself would also have to be made ready for agile changes[66].

3.5.3 SLA Metrics

The Sec-SLA and the standard SLA should both include metrics. Metrics should be both quantifiable and they should be measurable[66]. Both customer and consumer will want to control and check that the metrics given in the SLA is delivered at a desired level. Sec-SLA metrics can e.g. be Password management, Backup policies and Repair time. The metrics are in place to check and measure that the quality of services that is promised gets delivered. The metrics serve as check points for both the provider and the customer.

SLA metrics for IaaS, PaaS and SaaS and general SaaS terms has been proposed by Alhamad, Dillion and Chang[64]. This includes metrics such as scalability, availability, reliability and many more[64].

3.5.4 WS-Agreement

WS-Agreement is created by open grid forum(OGF), (and can be an alternative to SLA). This agreement specifies guarantees, obligations and penalties in case of violations according to the agreements made in SLA and Sec-SLA[64]. The WS-Agreement should include names, context and terms[64], where the name section should include the name of all the different services and preferably a unique ID for each service[64].

Information regarding service provider, domain, service and other service specifications is presented in the context section[64]. The terms section describes and details information about the terms of services and the given guarantees[64].

SLO, the service level objective. The SLO is described and mentioned in the WS-agreement as the different obligations both provider and consumer has if the agreements are not followed/violated[64]. The obligations and/or penalties that follows a breach of the agreement should be detailed and if possible overlooked by a lawyer or someone with good knowledge of the juridical aspects.

Negotiation

There are several different negotiation techniques and methods. Cloud consumers can review the SLA given by the provider, ask for changes, sign the agreement or terminate the negotiation. Cloud customers can also hire a trusted third party agent or company to negotiate for them[64]. The agent or company would be someone who has experience within the field, and probably have lawyers and technical experts to help review the terms of the SLA. They can also at a later stage, when the SLA is signed, help monitor the SLA metrics. Customers could also hire agents and experts within the specific field of cloud the customer wants to rent(SaaS, IaaS, PaaS), and have these agents/experts review the SLA and its terms. The idea is that you would have to negotiate the terms based on what services the customer wants. E.g. the SLA agreement might be very different from when the customer only need to rent SaaS to the need of IaaS and PaaS together.

3.6 Trust management in the cloud

This section describes related work and research on trust management and how trust influences the enabling of cloud computing technology. The third research question is studied and partly answered through study of literature on trust and trust management in the cloud.

Trust is a huge issue in cloud computing. But before we start exploring different research regarding trust, it is important that we have found existing definitions and research on what trust actually is. Trust is a psychological state, or act of faith. "“Confidence and reliance in something that is expected to behave or deliver as promised"”[67][68].

Now that the understanding of trust is known, we can continue to explain and show related work that will affect or be used in the thesis regarding trust.

The "Above the Cloud"”[11] paper lists "“reputation fate sharing"” as their obstacle number nine of the top ten issues regarding cloud services that would need to be solved. Even if reputation may not be the first that comes to mind regarding trust, it is actually potentially detrimental to most companies. A bad act by the service provider or another one of its customers could affect the reputation of the entire cloud, including other customers. Handing their reputation handling over to a third party is based on trust. The paper[11] suggests creating reputation-guarding services. It also mentions legal issues regarding legal liability(who is to blame).

In 2008 Gartner[13] published a research paper that included several of the management considerations that should be taken into account when working with third parties and cloud providers. This includes strategy development, transparency demands, legal assessments and IT risk issues. All these aspects help build trust towards the cloud provider, and should be taken into consideration.

NIST are working on a standard[5] related to cloud computing. The draft includes information security and in this draft they suggest hardware as a support for trust. NIST states in their draft[5], that SLAs generally place the security risk on its customers. This includes unauthorized modification, disclosure of data and service interruptions caused by malicious activity. This is not helping the potential customers to increase their trust in the different cloud providers. The draft also mention several recommendations for the customers when entering a third party cloud environment. E.g "“Security, Criticality, and Backup"”, "“Subscribers should carefully examine the SLA for any disclaimers relating to security or critical processing, and should also search for any comment on whether the provider recommends independent backup of data stored in their cloud"”[5]. The draft also mentions that any customer who is not pleased with the current SLA, or think that the default SLA do not address all their needs should discuss changes and modifications to the SLA before reaching any form of agreement 3.5. Having the SLA in order is important for any customer to be able to trust their provider.

NIST has included a bullet point list of technical aspects that the customer can require from any provider to ensure a higher level of trust in SaaS[5].

1. Data Protection: Analyze the SaaS provider’s data protection mechanisms, data location configuration and database organization/transaction processing technologies, and assess whether they will meet the confidentiality, compliance, integrity and availability needs of the organization that will be using the subscribed SaaS application.
2. Client Device/Application Protection: Consistent with the FIPS 199 impact level of

the data being processed, protect the cloud subscriber's client device(e.g., a computer running a Web browser) so as to control the exposure to attacks.

3. Encryption: Require that strong encryption using a robust algorithm with keys of required strength be used for Web sessions whenever the subscribed SaaS application requires the confidentiality of application interaction and data transfers. Also require that the same diligence be applied to stored data.
4. Data Deletion: Require that cloud providers offer a mechanism for reliably deleting data on a subscriber's request.

The NIST draft[5] also includes similar lists for PaaS and IaaS.

In a paper published by the University of Tokyo[69] they present and name areas of the cloud that make it insecure. These insecure areas are related to the trust of the cloud environment, and the authors present what they believe is a modeled solution to these insecurities. Another trust model, domain-based[70] novel security model, has modeled trust based on "“Trust decision"” and "“Trust update"”. They also proposed a novel security framework based on the independent trust management module for cloud environments. Another trust framework worth mentioning[71][72] was created by researchers from the Hewlett-Packard laboratories in Singapore. Their framework is based upon a data centric detective approach to increase trust and security in the cloud. The paper is moving away from standard preventive controls and towards detective controls. These detective controls(file-centric and data-centric logging mechanisms) is proposed to increase accountability, trust and security in the cloud. Another model proposal is based on a "“Family gene based Cloud Trust model"”[73]. There is also done research from the providers point of view. Even if we will focus on the customer/subscriber in this thesis, it is important to note and to know that there is also done research on trust where the question asked is whether the customer can be trusted[74] and not forgetting research that increase trust on both parts through modeling[75].

4 Choice of scientific methodology

This chapter will present the different scientific methodologies that is viable for each of the research questions 1.5. Each research question and the viable methodologies will be discussed in separate sections. This includes what results each method is expected to produce. The chapter will conclude with the preferable methodologies to answer each of the research questions.

4.1 Research question 1

The first research question asks how customers can swap between providers while at the same time keep resilience and business continuity 1.5. We aim to form a hypothesis and/or gather some general information that can be used to help cloud customers make the correct choices and desicions when swapping cloud providers or migrating to the cloud.

Qualitative and Quantitative research methods

There exists four viable general approaches for qualitative research methods, and of these four methods (Action research, Ethnography, Grounded Theory and Case Study) the case study is the most relevant scientific methodology for research of information systems[76][77]. The research questions that is best solved through qualitative methods will be best answered with the case study approach. Quantitative research methods are generally poorly suited to answer this specific research question because of the complexity of human experience and the amount of variables needed. It would make any quantitative method difficult for the first research question as long as it is not accompanied with a qualitative study.

Case study

A case study is research that focuses on a intensive analysis of one particular event, incident or phenomenon[78]. A case study can be based on either quantitative or qualitative data, or a mix of the two[78]. The case study is an empirical inquiry, and the approach does not follow any rigid protocol or set of rules. A case study will normally be done with the collection of empirical information through interviews and the research of text, documents and notes. The study can be done without any form of direct observation of events.

All these points make the case study methodology a suitable match to answer the research question. We will use an illustrative case study. This type of study focus on being descriptive, and uses one or more scenarios or instances of a type of event to illustrate a situation.

The limited time to perform the research restricts the use of the other qualitative research methods. The research would require multiple interviews or surveys, and the issue is to get a hold of enough knowledgeable subjects for the research to succeed within this limited time.

To be able to answer the research question, it is probably best suited to use the information gathering tools presented through the case study approach. One way to ex-

tract the needed information would be mainly through the use of interviews, and the addition of a study of notes, organizational structure and other project documents. With depth-interviews it is possible to find subjects that has already experienced the process of swapping providers. Their organizations should also have documented their process. With interviews and document study, the case study should be complete, and it should be possible to discuss and analyze the approaches used to answer the research question.

Literature study

A literature study is basically a study on previous work and research. The literature study includes evaluation, review and comparison of literature and previous research. The literature study benefits the research with the insight and knowledge of others. A literature study will enhance and supplement the information gathered of the swapping of providers through the case study. Related work and previous research will help answer any anomalies or regularities in the techniques or processes revealed through the information gathering process.

4.2 Research question 2

The goal of the second research question is to figure out if the cloud customers them self can improve the security and compliance of their cloud usage, or if they are slaves to their cloud providers desicions. We want to present potential improvements the cloud user can conduct to better and improve the situation.

Qualitative and Quantitative research methods

Much like the first research question, we are dealing with information systems, and the same requirements for methodology will be present. The reasoning that applied to the first research question methodology will also apply for the second research question 1.5. Following the same arguments and conclusions, we are left with the exclusion of quantitative research methods and left with qualitative research methods.

The thesis will focus on gathering information to solve the research question and for the creation of a hypothesis based on personal experience through interviews, document study and literature. Quantitative studies and methodologies are not suitable for this research question as the answer requires personal experience which will produce a large amount of variables.

Case study

The second research question will be solved by building upon the case studies used to solve the first research question, and serve as a second instance of a illustrative case study. The limited time, and the lack of opportunity of inclusion from subjects utilizing cloud technology excludes action research and ethnography from the qualitative methodologies pool. The use of case study as a methodology to answer the research question allows for the next best thing, experience, personal opinions and perhaps expertise from case study subjects that already use or plan to use the cloud technology.

Gathering information from organizations and businesses that has experience within the use of cloud computing is essential to be able to answer this research question. We will use this experience to gain knowledge from both positive and negative "'lessons learned'" by these experiences. A case study will reveal the methodologies and processes in use to enhance and highlight their compliance and security(if they have any).

Interviews and document reviews will be used to build the case study. Choosing in-

terviews as a information gathering methodology lets the thesis author directly tap into the experience and competence used by the organizations/businesses being studied. Interviews will be the information gathering tool of choice for this research question, document reviews will be used as a supplement to cover potential aspects left out by the interview method. This should cover all aspects of the process.

Literature and document study

Literature study will enhance and supplement the information gathered of the swapping of providers through the case study. Related work and previous research will help answer any anomalies or regularities in the techniques or processes revealed through the information gathering process.

4.3 Research question 3

The third research question is based on the two previous research questions. The aim of the question is to answer or present an idea of whether or not the results from the two previous research questions can improve the trust relationship between the cloud customer and the cloud provider.

Qualitative and Quantitative research methods

The two previous research questions builds hypothesis that could be attempted confirmed through quantitative methodologies. But, the aim of the research question is to further build upon that hypothesis by attempting to include parts of the answers of these previous research questions to further develop the hypothesis. To further develop the hypothesis the research question will be answered through the use of qualitative modeling. Qualitative modeling will show if the inclusion of the results from research question 1 and research question 2 will have any improvement or effect on the trust relationship between cloud customer and cloud provider.

Modeling

The third research question is inspired by, and builds upon previous conceptual trust models. The methodology for this research question will have to be modeling if the previous models are to be improved. The modeling process will present and show the results and hypothesis's gathered from the two first research questions. The model will answer the third research question by further developing the hypothesis. The model will not prove the hypothesis, it will only contribute to further development and research within the area. To prove the empirical information and hypothesis one would apply a quantitative method, but as mentioned, this will not help answer the research question.

4.4 Conclusion of methods

This section lists the conclusions of methodologies to be used for the different research questions. The concluded methodologies is further explained in the chapter of method description 5.

Research question 1

The choice of methodologies for the first research question:

1. Case study
   - Interview
   - Theory/document/notes study

Research question 2

The choice of methodologies for the second research question:

1. Case study
    - Interview
    - Theory/document/notes study
2. Literature study

Research question 3

The choice of methodologies for the third research question:

1. Literature study
2. Case study
3. Modeling

5 Method description

This chapter presents the descriptions of the methods presented in the chapter of "“Choice of scientific methodology"” 4, and how these methodologies will be used to answer the research questions 1.5. During the chapter "“Choice of scientific methodology"” we discussed and concluded with the methodologies of choice. For the first and second research questions, case studies are concluded to be the most suited 4.1, 4.2 methodologies. The information gathering phase of these case studies are completed through the use of interviews, document study and a literature review 4.1, 4.2. For the third, and last, research question the methodology chosen is modeling 4.3. The modeling methodology makes it possible to further develop previous models 4.3.

5.1 Case study

We will conduct two different case studies 4.1, 4.2 of two organizations/businesses that has experienced, or are experiencing a provider swap or a migration of cloud services. Two case studies are required to cover the entire subject required to answer the first two research questions. This includes cloud customer contribution and swapping between cloud providers/cloud migration. The research questions differ in such an amount that the case studies also has to differ to be able to cover all aspects. The case studies will be differentiated through some of the criteria chosen for each of the case studies.

5.1.1 Criterias for case studies

The companies studied need to fulfill certain criteria. The criteria are set to make sure that the choice of cloud customers/companies for the case studies contribute to answer the research questions.

Case study 1

The first case study is performed to help answer the first research question regarding the swapping of providers, and to some degree the second research question regarding cloud customer contribution. To be able to cover the research questions the case studies will have to fulfill a set of criteria. These criteria are set based on the problem description 1.3, related work 3, and the research questions 1.5.

The organization/business has to fulfill a criteria of using or renting private cloud services. The company will have to buy/or have bought services from a provider(hybrid cloud , private cloud) or deliver/plan to deliver its own services (through a private self-hosted cloud). The private cloud operates differently from the public cloud 2.1.3, and it is important that one of the two case studies revolves around the private cloud. The criteria is included to map any potential differences or similarities between private and public cloud with regards to the research questions 1.5.

To be able to answer the first research question 1.5 the organization/business being studied for the first research question has to be in, or been through a process of swapping providers, or in a migration process of (cloud) services. We want to study a company that has discovered positive and/or negative aspects of this process, and perhaps learned

something through their practical experience. We will draw upon their experience and gained expertise based on their "“lessons learned"".

It is important that the organizations/businesses being studied has encountered problems or issues regarding the swapping of providers or migration of services. Without this criteria the case studies will not result in any findings or results. This statement is true mainly because of the approach we are using towards the cases studies. We aim to gather information on both the smart/correct moves and desicions,the pitfalls and lessons learned by the cloud customer. This criteria ensures that most aspects of both the first and the second research question is covered, and that the two case studies can be compared when discussing the results and findings. It is easier to learn from mistakes than it is to learn from doing something correct.

Criteria for the first case study:

1. Private cloud
2. Swapping/Migration of cloud provider/services
3. Problems and setbacks during the swap/migration process

Case study 2

The second case study 2 is conducted to help answer the second research question regarding customers contribution to compliance and security in the cloud, and to some degree the first research question. These criteria are set based on the problem description 1.3, related work 3, and the research questions 1.5.

The organization/business being studied has to be involved with a public cloud provider, and be in the process of either swapping between two different public cloud provider, or in the process of migration from in-house systems towards a public cloud provider. The public cloud criteria differentiates from the private cloud criteria for case study 1. This is done for the two case studies to be comparable when discussing the results and findings, and to discover any differences in public and private cloud with regards to the research questions.

Like the first case study, it is important that the company being studied is in, or been through a process of swapping providers, or in a migration process of (cloud) services. This is to discover any positive or negative experiences with the process.

It is important that the organizations/businesses being studied has encountered problems or issues regarding the swapping of providers or migration of services. Without this criteria the case studies will not result in findings or results. To uncover findings and results it is important to discover any problems, issues or pitfalls with the swap or migration process. This way we can use these problems to learn from others mistakes, and give guidance to new potential cloud customers.

The second case study includes criteria to ensure answers to the second research question, this includes SLA/Sec-SLA contractual agreements and the use of external expertise. The SLA/Sec-SLA contractual agreement is in place to make sure that the second business/organization to be studied has entered into a contractual agreement including either SLA metrics or Sec-SLA metrics, or both.

The last criteria specifies that the use of external expertise is required for a business/organization to be evaluated for the second case study. The use of external expertise can be achieved with either lawyers, revision companies or other engineering companies.

One of the scenarios is enough to satisfy the criteria. We want to study the potential influence a third party could have to the cloud environment, either in the form of customer contribution or in the migration/swap process.

Criteria for the second case study:

1. Public cloud
2. Swapping/Migration of cloud provider/services
3. Problems and setbacks during the swap/migration process
4. SLA/Sec-SLA contractual agreements
5. Use of external expertise

5.1.2 Information gathering for case studies

In the chapter "“Choice of scientific methodology"' we concluded and identified information gathering and information analytic methodologies 4.1, 4.2. This section will describe which variants of these methodologies we will use to conduct and analyze the case studies, and how we will use these methodologies.

Document study

The document study will be providing a preliminary study for the planned interview 4.1, 4.2. The documents would need to be from the primary source or from secondary sources(delivered from primary source), in other words, it has to be close to the origin of the study. The case study will start with a thorough review of all related and relevant documents either from the primary source or delivered from the primary source. These types of documents include organizational structure documents, planning documents, contractual agreements and potentially published documentation(either academia or media). These documents will be used to form a general idea of the organization/business, and also the involvement with cloud computing and cloud environments. When the document study is completed, we should have formed a general idea of the company being studied and the relationship with cloud computing, and be ready to produce questions for the interview.

Semi-structured Interview

One of the information gathering methodologies for the case studies is the use of interviews. With a traditional interview the interviewer would have to stick to a strict script of questions, and could potentially miss important information. Through the use of semi-structured interviews the interviewer is able to ask the prepared questions, while at the same time open for discussions and follow-up questions. The choice of the semi structured interview is made to be able to gather empirical data based on a interview form that encourages discussion. The interview will have several pre-determined questions to make sure the information gathering process covers the research questions. The pre-defined questions will however leave several questions open for discussion, and the interviewer will encourage discussion during the interview. If the recipient of the interview replies any question with what could potentially open for a discussion or follow-up questions, the interviewer will adapt to the situation and attempt to encourage a discussion or another follow-up question.

Analysis

The case studies, and the information found during the information gathering, would need to be analyzed to identify potential findings. The analysis process is used to highlight important findings and facts found during the study[79].

During the analysis of documents and interview answers it is important to identify the facts surrounding the case studies[79]. In other words, every surrounding detail and fact that could affect the case should be accounted for. This could include organizational structure, pressure from management, the economic basis and any other potential influence. The facts and information found in the documents could be in the form of pictures, tables and graphs. This kind of information should not be neglected during the analysis. Identifying the facts is a process that requires the study of all potential important facts and at the same time being able to select the correct facts and disregard less important facts. If, for some reason, parts of the case studies facts or numbers are unavailable, we will make assumptions based on the available information[79].

Statements, judgments and decisions made by individuals associated with the cases should be analyzed thoroughly and questioned[79].

Once the facts surrounding the case studies have been identified, it is equally important and vital to be able to identify the key issues or issues[79]. If the case studies should uncover multiple issues it is important to be able to differentiate between the major issues and the trivial issues. If the analysis discovers more issues than expected they will be ordered based on importance and relevance to the research questions. If the list of issues should exceed to more than thirty, the less important and relevant issues will be excluded from findings and results. This is done because of the restricted time limit of the thesis, and to increase the focus on the most important and relevant issues. The major issues discovered during the analysis of the case studies will be used to answer the first and second research question. The cloud computing environment is multi disciplinary, and it is important to identify if the problems are caused by either IT, compliance(law) or business management(the problem could also be differentiated through management, technology and organizational issues[79]). The discovery of the issues disciplinary origin can help the analysis distinguish how the problem occurred, and how to prevent it from happening again.

When the issues and problems that affect the studied companies is identified the thesis will proceed to suggest and specify alternative course of actions[79]. Some of these alternatives for course of action will when evaluated, be used to help contribute to answer the research questions, which is partly answered by the recommendation of the best course of action.

It is also important to identify and recognize the different aspects and actions the studied companies did correct. The correct actions, as well as the incorrect ones will both help answer the research questions.

5.1.3 Literature study

To answer all the three research question, to supplement the case studies, and to generally obtain a better understanding of the subject at hand, the thesis author will continuously conduct a literature study. The literature used has to fulfill the following criteria:

1. Be relevant to the research questions

2. Be relevant to cloud computing

5.1.4 Presentation of analyzed data

Description of the different methods used to present the findings discovered from analyzing the case studies and the literature.

Checklists

Both case studies has criteria which ensures that the two different companies being studied either has recently completed a swap of provider/migration, or is in the process of swapping providers/migration of cloud services. The findings and results based on this criteria will enlight the way the companies that was studied planned for, and performed this swap/migration. These methods, and the alternative course of action/suggested course of action will be presented through security checklists for the selection/swapping of provider/migration process.

Use cases

The second case study has criteria that involve the use of external expertise. The thesis will present results and findings based on this criteria through several use case scenarios. The use case scenarios will represent situations and scenarios where it would be beneficial for cloud customers to contact and/or buy services from external experts. The use of use cases will illustrate the actual scenarios that took place during the case studies, in detail.

Metrics table

The second case study focuses on the public cloud, and the contractual agreements needed to enter a cloud computing relationship with a cloud provider. This relationship of trust and security need some form of measurable for quality of service. The results and findings regarding the business needs and contractual agreements will be represented through metrics tables.

Conceptual model

Both of the case studies has criteria regarding the swap of provider/migration. The findings from these case studies, plus the supplement of a literature study will contribute to answer the third research question. The idea, concept and results from these studies will be used to present a conceptual addition to previous and already discovered models of trust and quality of service monitoring.

5.1.5 Conclusion of methodologies

To answer the first and third research question, and to fulfill the criteria set for the first case study, the thesis author has decided to conduct a case study of the project University Innlandet. The information gathering phase will be conducted with the head of the IT-department of Gjøvik University College. This is done for easy access of a interview subject, while at the same time, reaching someone who has great insight in the University Innlandet project. The interview will be done in person.

To answer the second and third research question, and to fulfill the criteria set for the second case study, the thesis author will conduct a case study of Narvik Municipality. The literature study will be used to supplement the findings from the case studies, help answer the research questions, and to generally increase the understanding of the subject. We will conduct the interview part of the information gathering phase with the head of

Narvik IT-department. The head of Narvik IT-department has made several appereances in media regarding the cloud migration process, and has great insight in the Narvik Municipality IT-department. The interview will be conducted over telephone.

6 Swapping cloud providers

This chapter includes the two different case studies that was conducted after discussing and concluding methodology 4, 5. These two case studies were conducted to answer the research questions 1.5. This chapter includes a description of the scenarios, description of the particular case studies, results from the information gathering phase and a analysis based on the results from the information gathering phase, and is summarized with a list of key findings. The chapter continues to discuss and conclude on the findings, and the findings and results from the descriptions and the analysis of the case studies are later on implemented and presented through checklists, SLA metrics and use cases representing external expertise scenarios.

6.1 Case study: University Innlandet

University Innlandet is a project of merging three large Colleges residing in the same region. The three university colleges are Gjovik University College, Hedmark University College and Lillehammer University College. The project of University Innlandet is a cooperation between these three university colleges in Hedmark and Oppland together with the Hedmark and Oppland counties. Between these colleges there are six different campus areas; Elverum, Evenstad, Rena, Hamar, Gjovik and Lillehammer. The merger will result in a combined University for the whole region. The norwegian state does not subsidize any resources to the merger, so the project is dependent on external regional investments. The main reason for the merger is the statistical numbers showing the region surrounding the university colleges as being low, or poor, on value creation, research and education. The competition for applying students, and research resources will be diminished and the colleges want to cooperate better through this merger. The projects intention is to create better capability through better education possibilities[80]. A part of this process is to merge the data centers and the IT-departments. There is also hope that the merge will save money, increase efficiency and effectivity.

The university will have a total of 15000 students, 1500 employees after a potential merger. This will have some effect and possible implications on the IT department(s). As of today there are three data centers and IT-departments, one in Lillehammer, one in Elverum and one in Gjovik. This case study will investigate the different aspects of the merger, what has been planned, what has been done, and what challenges they are currently struggling with, and what challenges they have been through.

The data centers can be defined as a private self-hosted cloud. This case study will be used as a practical example of how a switch or merger could be done, alternative courses of action and what challenges exists.

6.1.1 Planning and ideas

The planning process for the merger has been going on for several years now, and is already approximately 1-2 years delayed. The planning within the IT-departments was mainly done through several brainstorm sessions were the different leaders of the IT-departments had discussions regarding the different problem areas. These brainstorm-

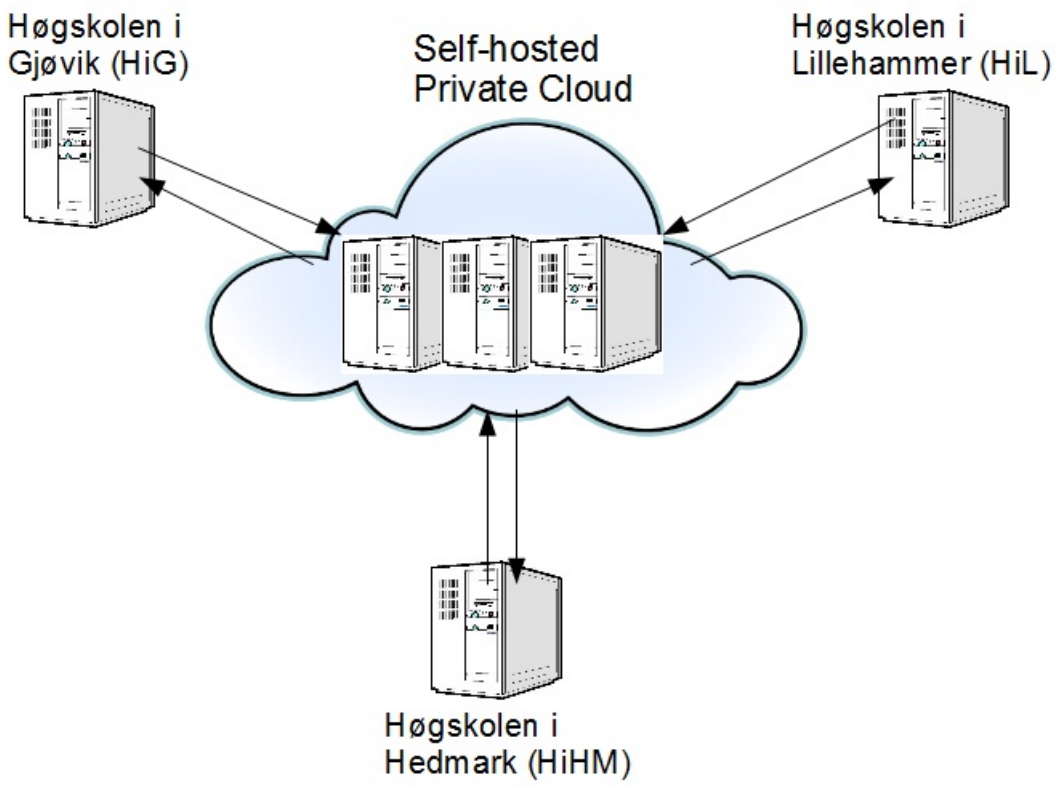

Figure 10: Self hosted private cloud

ing sessions was conducted to let every IT-department leader express their thoughts and ideas, also to make use of the extensive experience that exists between the IT-departments. The brainstorming sessions was also used to settle any differences and opinions on system specific matters.

The different IT-departments are now working on preparing their systems for a fluid transition. The infrastructure is in place, this includes: cables, network, electricity, cooling ventilation, fire safety, rooms, doors[81]. This also includes fast fiber connections between the different data centers. One of the more prominent challenges they have faced while planning is the issue of users and the unique user IDs used in the different services and systems. This case study will further explore and explain this problematic challenge in the section regarding services 6.1.3.

6.1.2 Private self-hosted Cloud

The data centers(server and server infrastructure) used by the different university colleges are self owned. This means that they are their own "‘provider"’ of both services, infrastructure and storage. Migrating services and/or data between self owned servers will exclude some of the potential problems that comes with the cloud types like public cloud and outsourced services. No matter how one would look at public cloud services, it is a outsourcing service, and leaves a lot of a organization or business value in other businesses hands. This problem is more or less eliminated when using a private self-hosted cloud. When outsourcing or using cloud services one has less control of the companies

own data, but at the same time less responsibility. However, one can compare the two. Problems regarding different platforms, different services and the migration of different types of data in this merger of private clouds, will be equal to the problem one would face when swapping public cloud service providers.

6.1.3 Services

Based on the interview with the IT-manager at Gjovik University College 5, one of the problems, and one of the only practical problems remaining for the merger to happen is the merger of services.

User names, and user name generation has proved to be difficult for the merger, and creation of University Innlandet. Lillehammer Univeristy college and Gjovik University college both use the same method for user generation. The user name is based on the year the student started at the school, plus the use of a running number. As soon as a new student is registered at the University college all the students information are automatically transfered to a ldap database(FEIDE), where the students user name, e-mail address, authentication web areas and access rights are generated, given and pushed out to the approximately 40 different individual systems. This system is simple and easy, and in addition to that, it makes it possible to make changes on one system that would automatically change the information in all of the individual systems.

In Hedmark University College they only use the running number for generation of users. According to the IT-manager at HiG, Hedmark University College are already using usernames with thirteen digits or letters. Unless this is gradually changed before the merger is to take place, it will mean that every user of the system would need a new user name. Consequently, all data would also need to be migrated. The data migration is troublesome and hard work, but with the infrastructure in place, it is doable. At the time of this case study there exists no concrete solution to the user and user name situation. If no solution other than the creation of new users are presented, the IT-departments would still need to map all the former user names("“Legacy"” user names) with the new user names in a way that the old data is not lost. This is problematic when the service is outsourced.

The database of students attending the university colleges for the entire region is outsourced to Usit, the IT department of the University in Oslo. This complicates the entire process, and it is comparable to potential problematic dependency situations one could face in the public cloud. Since the database is outsourced the university colleges are dependent on the owner of the database to make changes to the users. If the University colleges owned the database them selfs they could easily add a region/campus code at the end of each user name to differentiate between potential duplicate user names.

In services and applications that are offered through cloud and/or outsourcing the provider have the opportunity to make the application dependent(either through tools, API/platform or file format). This would make sure the provider easier could keep their customers as the migration to another provider would be a lot harder and more costly, this is a real fear for University Innlandet. University Innlandet could still ask for adjustments better suited for their purpose, but the provider is free to ask whatever they want as compensation for this adjustment. By keeping their customers, and through costly adjustments the providers ensures a steady income. The university college case study touches on this subject area on the different services that is outsourced, e.g. the student

database, and the fronter service.

Fronter is used by all three different University Colleges, but as a part of the merger, the different fronter services would also needed to be merged into one single service delivery for the planned University. There is no existing plan for the University Colleges to leave the service, so Fronter could potentially claim whatever they want for the merge.

It is often easy to move onto the cloud (or go into outsourcing partnership as in this case study), the problem is getting the data back. In this case, every part of the merger is using the same service(fronter) for certain services. If any of the parts involved in the merger had used a different provider for these services the university colleges would have encountered dependency issues. One of the services would have had to discontinue, and the migration of this data could have proven to be difficult. Unless these providers claim a too costly price for the merger, the project might as well keep these outsourcing partners to avoid the dependencies and lock-in issues.

6.1.4 Storage

The head of the IT-department at Gjøvik University College claim that the infrastructure and the connection between the different university colleges are of a high quality, and according to HiGs IT-department: "“even better than most businesses internal connections"'. The plan for the storage and migration of data concerns duplication, hot and cold sites. Unless it is needed to migrate large amount of data 6.1.3, the plan is to copy important data to the other sites as a form of backup. The goal is to reach high levels of duplication and low levels of centralization. With this strategy they aim to increase quality on the services and the storage, and keep an even higher level of up-time and availability. The University would e.g. not be that dependent on a single electricity company for them to be able to deliver their services and data.

All privacy related and sensitive data is, according to the IT-department at the University College of Gjøvik, already handled in a satisfactory manner. The only sensitive data as of today is stored in a student database which is controlled through the use of strict routines. In the future there will potentially be more sensitive data created and/or stored by the faculties scientists, this data storage will be outsourced and will not be part of any data migration handled by the university colleges.

The amount of data will increase, and as a cause to this effect, there is planned to buy more backup tapes/disks to ensure and minimize the possibilities of data loss.

6.1.5 What did go wrong

The IT-departments of the different University Colleges have settled and organized their organizational structure, ironed out most of their differences, and solved most of the practical issues regarding the merger. The user name issue mentioned in the section "“Services"'6.1.3 does however remain unsolved. Apart from the user name / user ID generation issue there is only political issues that stands in the way of the merger, a long with the agreements with the providers for their outsourced services.

6.1.6 Trust

Trust is not that much of an issue in this case study, as most of the services and data handling operations are done within the different departments of the merger. There is some trust involved by the use of third party outsourcing, and this is somewhat comparable with cloud providers. As these outsourcing deals are already made, and will not

dramatically change as a part of the merger, we will not study these any further.

6.1.7 Analysis

The project is between three colleges, these three colleges want to merge to form a University. As a part of the merger they are merging the IT-department and the data centers. The data centers can be defined as a private cloud. The infrastructure is already in place, and as a result there are no big expenses or investments needed for the IT-departments. The funding needed for the project is dependent on private regional investments. Since the private cloud is self-hosted the knowledge and expertise are mostly in-house, and data segregation should not be an issue. The different IT-departments are currently working on ensuring a fluid migration/merger. The IT-departments ensures resilience and continuity through the duplicity of data and the low level of centralization.

One of the key issues is the user ID management. One of the colleges involved in the merger use a different user ID creation methodology which turns out to be a problem when it is attempted merged with the other two colleges with their ID creation methodology. This particular problem is caused by both management and technology. Another potential problem is the lack of organized planning and risk management procedures. The planning has mainly been done through brain storming sessions and meetings that includes the involved IT-department employees. The project should have business continuity and disaster recovery plans ready for the worst case scenario, it is not enough to just create duplicity and a de-centralization environment. The project could also have spent more time and resources performing risk management analyzes and perhaps evaluated other types of cloud solutions.

Since so much of the infrastructure already is in place, there is no real need for the project to use any sort of public cloud service. It would have been cost saving to attempt to centralize the IT-departments and operations, but it would have to come at the cost of business resilience and continuity, and is probably not worth it.

6.1.8 Summary of findings

The summary of findings will present the most important findings found during the case study of University Innlandet.

1. Dependant on outsourcing services
2. Username conflict (User ID generation unsolved)
3. Differences in outsourcing provider could have created dependencies
4. Keep their current outsourcing partners to avoid cost of switch
5. High duplication, low centralization(backup)
6. The importance of underlying infrastructure(e.g. bandwidth, servers, network...)

6.2 Case study: Narvik Municipality

In the spring of 2011 Narvik municipality decided to migrate their e-mail services from IBMs Lotus Notes to Google apps and their services. Narvik is a small municipality, and the resources available for their IT department is limited. After years of using Lotus Notes(e-mail system/service from IBM) they found it hard and expensive to hold on to the needed employees and knowledge to keep hosting the service in-house. The municipality wanted to deliver services to the rapid growing customer base who uses mobile

devices for their e-mail and similar services. IBM had solutions for this, but the cost accompaning the switch to, and use of these services was to expensive to justify the investment for the municipality. The municipality started looking at cloud possibilities and ended up with Googles alternatives, Google Apps.

The public cloud alternative is quickly implemented, it is cost effective as the municipality will not need any specific investment or cost associated with any infrastructure. The economic savings the municipality make from outsourcing services to the cloud was one of the main reasons for why they chose to migrate to the cloud, but the move was also made for better use of mobile devices and collaboration solutions.

The IT department tested the solution internally within their department for eight months before they pushed the solution out to the rest of the municipality. They gradually migrated to the public cloud and to cloud computing technology.

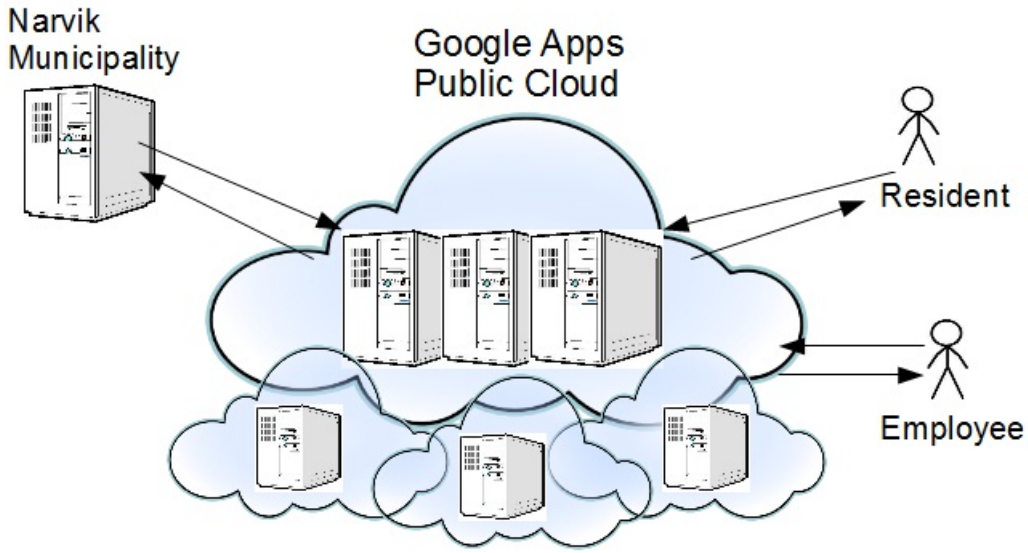

Figure 11: Public Cloud

A citizen of Narvik municipality was worried about the IT departments new solutions. The citizen delivered a formal complaint to the Norwegian Data Inspectorate. The Norwegian Data Inspectorate then required the municipality of Narvik to answer for what information they had stored in the cloud, and how they planned to handle sensitive information. After Narvik municipality presented the current agreement and SLA with Google and explained their handling of sensitive data, the Norwegian Data Inspectorate ended up denying Narvik further cooperation with Google and Google apps. Narvik municipality got a deadline to re-negotiate with Google and come up with a better solution for their handling of data. Narvik eventually requested a extension of their deadline and has been hard at work ever since. The response to the Norwegian Data Inspectorate is now delivered(May 2012), and awaiting reply.

6.2.1 Contractual agreements

When Narvik municipality contacted Google and requested delivery of cloud services, Google presented the municipality with a standard pre-defined contractual agreement. This is a general and standard SLA that Google send to all their customers. These contracts and agreements was according to the Norwegian Data Inspectorate not sufficient and did not cover/was compliant with the Norwegian privacy law. Particularly the physical storage location, and access rights, was among the larger issues requested answered and fixed. After re-negotiating with Google based on the requirements made from the Norwegian Data Inspectorate, the municipality and Google agreed upon a new customized and modified contract. The private re-negotiated contract/sla contains a lot of secret business information and can therefore not be shared to the public, this also limited our case study.

The municipality did discuss, evaluate and analyze the original SLA, but the need for a private and negotiated contract with Google, where more of Google's information were available and accounted for, became a need after the Norwegian Data Inspectorates queries. The new agreements were developed as a result of this.

Narvik municipality had help monitoring and reviewing the services, and the quality of service, delivered from Google apps through a trusted third party(revision company). The revision company presented the municipality with an audit and review of Google as a company. Audits of large companies like Google is hard to come by, and the revision company probably reviewed and controlled a previously conducted audit when they reviewed Google. Google is a large company, and they have large quantities of different customers. If every customer were to request a new audit, there would not be time for anything else than auditing. Large companies with a lot of customers often pay for their own audit(which could potentially be biased), and this audit is sent to the customers that request an audit.

Google also uses an open practical approach to their monitoring of QoS, Google have published several tools that can help customers monitor the quality of service they deliver. This should be coupled with a trusted third party to avoid possible biased monitoring tools.

6.2.2 Services

Narvik municipality are currently using several of Google's services and applications. The main application is Google Apps e-mail solution, but they are also using document services, draw-help applications, presentation and calculation tools. Several of these tools could potentially handle sensitive information, but the municipality would not use or handle any sensitive information in any of the cloud applications. However, especially the e-mail solution is hard to control. Since these applications has the possibility to handle this type of information, the routines, policies and control will need to be extremely rigid.

6.2.3 Sensitive data

Narvik municipality does not store, or plan to store sensitive data on the cloud or send sensitive information through the cloud provider. All the use of the different services will attempt to limit the amount of processing of personal data regarding the employees to name, telephone number, e-mail addresses and organizational affinity. There is of course no hundred percent guarantee that no sensitive data is stored upon the clouds, as the main application is a e-mail service, but Narvik municipality has several routines to

avoid it. They have heightened awareness around the subject of personal sensitive data. They try to inform every user through advertised information through their web page or e-mail. E.g. if they receive e-mail containing sensitive information they will never resend the same e-mail back to the sender with the reply, they will create an entire new e-mail. However, the Norwegian Data Inspectorate doubts the municipalities ability to restrict the inhabitants the sending of sensitive personal information per e-mail. The handling of sensitive data requires tight policies, routines and control 6.2.2.

6.2.4 Swapping providers

Narvik municipality also made sure they have ways of further migration and exit strategies from Google as a service provider. Google has published several migration tools and methods at a web page, dataliberation.org. Through the use of these tools there remains no real dependency of platform, service or file format from Google.

6.2.5 External expertise

The municipality contacted external expertise in the migration process from Lotus notes to Google. The use of external expertise resulted in a easy transfer of old data from the Lotus system to Google's cloud, Google also delivered migration tools that simplified the process. The company was a engineering company, and they helped the municipality with customization and to complete the swap.

Later on, after the intervening and queries from the Norwegian Data Inspectorate, Narvik contacted several lawyers, primarily a lawyer firm located in Oslo. They also had lawyer help from Google's offices in London and USA. These lawyers helped the IT-department and municipality to re-negotiate and customize the SLA with Google, and helped handle the queries and regulations from the Norwegian Data Inspectorate.

6.2.6 Analysis and summary

A problem with Google's services is that Google themselves can not guarantee for the exact physical location of the customers data. Google's cloud services work in a way that accessed data will be transfered and located in the location of where the data is last accessed. As an example, if a user of the municipalities system access their mail in China, that information will be temporary under Chinese privacy laws. As the final contractual suggestion is confidential, it is not possible to know how Google and Narvik Municipality decided to solve this problem, but as long as the data is only accessed in Norway, the data should be under Norwegian privacy law, and the contract would be compliant with this law. The compliance issue was this case study's most important issue.

We have no information on where Google stores the municipalities data, as the re-negotiated contract was kept confidential. However, Google is compliant with the standards and regulations required for Google to be a "'safe harbor"' 3.4.7, which indicate that some of their data could be located in the Americas, and that they are compliant with the EU directives. But, cloud providers can also perform load balancing which is a way of shuffling data to other areas of the cloud to decrease/increase the load of servers/data centers[36]. This could result in the data being located in other countries with laws and regulations that are non-compliant with the Norwegian laws and regulations.

The IT-department of Narvik municipality performed a risk analysis when they still discussed the migration from Lotus notes to Google apps, but they wished they had spent more time and resources before acting. However, Narvik municipality and its IT-

department has limited resources and manpower, and it is not easy to extend these analysis in small municipalities.

The municipality felt that the Norwegian law is a bit outdated. E.g. The Norwegian law requires one to be able to have an internal control at the data handler, which is almost impossible when using outsourcing providers or cloud providers located in other countries.

The planning and preparing phase of the migration/swap process should have uncovered that the standard SLA from Google was not compliant with the Norwegian privacy law. This could have been figured out at an earlier time. The SLA contractual agreement with Google had to be customized and modified, and after this process it will be harder to switch provider based on the fact that a new provider would require the same customization process. Another thing to note is that in this particular case, which is among the first of the public state organizations within Norway that moves into the cloud, make Google very interested in completing the arrangement. It could create a domino effect, with Norwegian customers choosing Google, if Narvik municipality get the green light from the Norwegian Data Inspectorate.

6.2.7 Summary of findings

The summary of findings will present the most important findings found during the case study of Narvik Municipality.

1. Exit strategies and planning
2. Importance of compliance
3. The use of external expertise
4. SLA negotiation
5. Dependencies
6. Service overlapping and limited audience testing
7. Change in routines and policies
8. Cost analysis

6.3 Selection of/or swapping Cloud Provider

This section use the findings from the case studies 6.1.8, 6.2.7 to help organizations and businesses evaluate the options of different cloud providers. This includes the first migration to the cloud and the migration between cloud providers. The findings will be presented in checklists 5. The checklists will cover what the potential customer of a cloud service should know, prepare and test for, a long with the most common pitfalls when selecting or switching cloud provider.

6.3.1 What cloud customers need to know

The checklist presented contains the suggestions of what a business or organization should know before performing a swap between cloud computing service providers or selecting a provider. The checklist is based on the findings from the two case studies. The different suggestions are put in no specific order, and not rated based on importance. Each suggestion in the checklist is further described in their own subsection following the checklist.

1. Current cloud providers platform, tool, file format or other forms of dependencies
2. SLA with both the current provider, and the SLA suggestion from the new provider
3. The different privacy laws (and other potential laws that could influence the transfer from one provider to another) in the topical areas of the previous provider, (the data transfer area/countries) and the new provider
4. The reason for changing providers
5. When the business/organization would need to contact external expertise (a trusted third party), normally lawyers or engineers
6. Viability of the cloud provider and ongoing support
7. The cloud providers ability to recover from failures

Nr	Description	Yes	No
1	Current cloud provider - API / Platform independent		
2	Current cloud provider – fileformat independent		
3	Current cloud provider – Tool independent		
4	Current cloud provider – Other dependencies		
5	Current SLA suitable for migration/exit		
6	New cloud provider – API / Platform independent		
7	New cloud provider – fileformat independent		
8	New cloud provider – Tool independent		
9	New cloud provider – Other dependencies		
10	New SLA suitbale for further migration		
11	New SLA metrics suitable for business goals and needs		
12	New SLA and cloud provider geographic location and privacy laws suitable		
13	Need for external expertise to complete the migration		
14	Risk identification and risk management completed		

Figure 12: What cloud customers need to know

Dependencies

When a customer want to swap between providers, one would have to transfer data/information or applications from one platform to another. Data and files can be stored in one type of file format on the origin-cloud provider, while the VMs and platform of the new provider uses another type of format. This can be as simple as how users and user identification are created 6.1.1. If this is done differently (e.g. one provider has user IDs represented by letters while the other provider uses numbers) by the two providers, conflict can arise. Another example could be API dependency, tool dependency and file format dependency. Organizations and businesses would need to know whether or not the provider swap is doable by checking for, and gain knowledge of potential dependencies. If the business or organization currently uses in-house hosting and are evaluating a switch to cloud computing, one could use the checklist to ensure further migration possibilities by avoiding the vendor lock-in issues 3.2.1, 3.2.2, 3.2.3.

SLAs, laws and regulations

The SLA3.5 of the current provider and/or the potential new provider has to be known in detail. The organization/business planning to perform a swap between providers will need to know if the SLA has any special clausal that states penalties for leaving the agreement or closing their business with the provider, e.g. if the customer want to leave the provider before the contract runs out. The SLA could also state what type of files or format the provider will deliver the customers data at the termination of the contract. The cooperation between the current and potential new provider could also be stated in the SLA. The SLA should also include measurable metrics 3.5.3 to ensure QoS, and should also state when a customer can leave if the provider does not uphold the promised QoS. The lack of knowledge of the signed SLA(and the new SLA the customer is about to sign) could be a potential pitfall, and it is of high importance that the customer has clear knowledge of its content.

For a Norwegian or European based company it is also important that the SLA ensures compliance with national privacy laws and regulations (e.g. Personal Data Act[50] and Personal Data Regulations[62] for Norwegian based cloud customers) and the current directives and regulations applicable for the region (e.g. 95/46/EC 3.4.1, 2002/58/EC 3.4.2 and 2006/24/EC 3.4.3 for European based cloud customers). The customers of cloud providers should have knowledge of what laws are applicable to their current cloud provider and their potential new cloud provider(and also what laws that are applicable to them as a customer). The customers should have knowledge of what processes and laws that applies to protection of their privacy in the location where their provider is located, and also the location of where their data are stored and their applications and platform is hosted(this does not have to be the same location as where the provider operates). This is particularly important when data is sent or stored, or when applications and platforms are hosted in another country than the customers origin. The customer need to make sure the new provider is compliant with the correct and current applicable privacy laws, regulations and directives.

Reason behind the swap

The customer should have a clear understanding of why they want to swap providers or migrate to the cloud. There should have been performed several considerations before initiating any swap of provider. This includes, but is not limited to: cost analysis, risk

analysis, disaster recovery plans, business continuity plans and plans for QoS monitoring.

External expertise

The customer should have knowledge of when to hire and/or listen to knowledge from external expertise. This is extremely important when considering the different aspects of the SLA, but should also be considered for the other parts of the transission process. This includes, but is not limited to: lawyers/legal help and engineers.

6.3.2 What businesses should test

The checklist presented contains the suggestions of what a business or organization should test before performing a swap between or migrating to a cloud computing service provider(s). The different suggestions are put in no spesific order, and not rated based on importance. Each suggestion in the checklist is further described in their own subsection following the checklist.

1. The amount of bandwidth that is required to transfer data and applications between providers, or from in-house servers.
2. If overlapping of provider services is possible
3. Gradually rolling out services
4. Performance testing

Nr	Description	Ok
1	Current bandwidth and transfer rate of data to new provider	
2	Current bandwidth and transfer rate of data from old to new provider	
3	Overlapping of services (when switching from old to new provider)	
4	Overlapping of services (when switching to a cloud provider for the first time)	
5	Testing services for a limited audience (when ok - e.g. gradually rolling out the cloud services to the rest of the organization and/or business)	
6	Performance testing models (e.g. measures the impact on increase and decrease in bandwithdt, storage scalability, process power etc)	

Figure 13: What businesses should test

Bandwidth

The customer and the provider(s) should test what bandwidth requirements the business/organization would need to transfer data within the wanted/required time slot. It should also be tested if the current bandwidth is sufficient for regular communication with a provider.

Overlapping

The possibility of overlapping of services when transferring (from old) to a new provider should be tested. The customer should attempt to convert a small part of their data, platform or applications to their new cloud provider before completing the entire transfer. This approach could be more costly, but could save the customer for a lot of issues and difficult challenges. If the swap between cloud providers or migration to a cloud provider is done gradually one would make sure that no matter what issues that arise, there is guaranteed availability through the previous provider or the in-house hosting solution

until the issues with the new provider is ironed out.

Limited audience testing

The potential cloud customer should test out and experience the services delivered from the provider before moving the entire organization or business into the cloud. Testing the services on a limited audience(parts of the business) before migrating could reveal potential flauds and errors while they still are in a small scale.

Infrastructure and performance testing

The infrastructure should be tested for increases and decreases in bandwidth, storage, scalability, processing power etc, and confirmed adequate before moving towards a new provider.

6.3.3 What businesses should prepare

The checklist presented contains the suggestions of what a business or organization should prepare before performing a swap between, or migrating to a cloud computing provider(s). The different suggestions are put in no specific order, and not rated based on importance. Each suggestion in the checklist are further described in their own subsection following the checklist.

1. Cooperation between the previous/current service provider and the new provider
2. Cost analysis of swapping cloud service providers
3. On-site/in-house backup of critical information and/or data
4. SLA negotiation and requirements with the new cloud service provider

Nr	Description	Ok
1	Cooperation between the old provider and the new provider	
2	Cost analysis of the swap of service providers	
3	On-site/in-house backup of critical information	
4	SLA negotiation and requirements	
5	Understanding of the policies of the new provider	
6	Changes in rutines, software and policies	

Figure 14: What businesses should prepare

Cooperation

The customer should do what ever possible to ensure that there exists cooperation between them selfs and the two provider(both the old provider and the new provider). This can be done through SLAs or through overlapping of services. There is often more incentive for the new provider to cooperate than it is for the old provider 3.5.

Cost analysis

A cost analysis should always be done to make sure that the swap of providers is profitable to the customer. The analysis should consider the cost of lowered QoS, availability and delays. The cost of not upholding parts of the SLA(and receiving penalties) and the cost of a potential release from a contract should be calculated and analyzed. It should also be calculated for an exit strategy when selecting a provider. The validity and prob-

ability of the providers economic survival should also be considered.

Backup

If the customer has the capability, a local backup of data should be the first move when transferring to the cloud or from one cloud provider to another. The customer should copy any critical data and information from the previous solution/provider before the move is initiated. That way the customer can be sure that the data is safe and will not be damaged or lost during the transfer process.

SLA negotiation

SLA metrics should optimally be open for negotiation. However, in most cases the customer is presented with a pre-written and defined SLA. If the SLA metrics are open to negotiation one would have to identify and define the most business critical metrics and try to incorporate those in the SLA together with the service provider. Should the SLA be pre-written and not open for negotiation one should make sure to perform a SLA review or audit to make sure that the business critical aspects and metrics are covered.

6.3.4 Avoiding pitfalls

If the above checklists are hard to apply, any business or organization should attempt to avoid the most common pitfalls in cloud computing. The following checklist contains "'a summary of'" the most common pitfalls one should aim to avoid.

Nr	Description	Ok
1	Migration possibilities	
2	Retrievable files and fileformat	
3	Geographic location of provider (servers and storage) / privacy laws	
4	Suitable SLA metrics	
5	Cloud provider viability	
6	Performance monitoring (TTP)	
7	Suitable security measures	

Figure 15: Pitfalls to avoid

Migration possibilities

Before buying services from any cloud provider the parties involved should agree upon exiting terms. These exit terms could e.g. be the way the customer would get their data back, and when the provider will delete the data. It should also be discussed what data the provider can keep after the business relationship is ended. Customers should also make sure that there is no platform or service dependency before entering any business relationship with a cloud provider. If there is no way around the platform or service dependency one should discuss the potential migration tools available (and assistance from the provider) to make the dependencies less vital.

Retrievable files

This subject is tightly coupled with the migration possibilities. The customer and the provider should agree upon the state of files and file format of the customers data when the business relationship ends. This will make the migration process easier for the customer, and minimize the problem of a vendor lock-in.

Privacy laws and location

It is important to know the physical storage location of the customers data. The privacy laws and regulations of the physical location could be a mismatch with the customers national privacy laws, and the customer need to be compliant. Without any certainty of the storage location there will exist doubt if the customers data and sensitive information is handled according to the customers requirements.

SLA metrics and performance monitoring

Without suitable metrics in the SLA there is no way of measuring if the customer is actually getting what he is paying for. To complete the investment of migration to the cloud or between cloud providers, the customer should have a method of measuring the quality of the service the customer is receiving. The optimal solution would be through monitoring tools from the provider together with evaluation and monitoring from a trusted third party(TTP).

Cloud provider viability

The customer should make sure that there is no apparent reason for why the potential new cloud provider could go out of business or continue support of the services the customer will pay for. An evaluation from a trusted third party(TTP) audit company could help prove or disprove the providers viability.

Suitable security measures

The security controls and measures implemented by the cloud provider would need to be sufficient and suitable for the type of information the customer want to store, and the services the customer want to use.

6.4 Discussion

Discussion on the "“case studies"” and "“selection of/or swapping cloud providers"”.

Case study: University Innlandet

The case study of University Innlandet 6.1 indicates the benefits from the use of a private cloud. The infrastructure is already in place, so there is no real increase in cost connected with investments to improvements of infrastructure, which normally is considered as one of the larger drawbacks of the private cloud.

It was also apparent that even the private cloud can have dependencies. University Innlandet had dependencies with regards to the user identification generation, and in smaller amounts dependencies from outsourced services. To ensure business continuity and resilience the project was structured as a de-centralized and duplicate system.

Case study: Narvik Municipality

Narvik Municipality 6.2 experienced that the public cloud is not without issues and complications. The use of a public cloud complicates the compliance with privacy laws. Especially when selecting large provider companies like Google. Narvik municipality experienced this complication when the Norwegian Data Inspectorate intervened with their cloud computing usage. The importance of extensive planning, and the ability and capacity to foresee and prepare for compliance issues was highlighted during this case study. The case study also revealed the utility value of hiring or contacting external expertise for several purposes. The case study underlined the importance of planning and preparing the entire process in detail and the importance of SLA audits and reviews.

Selection of/or Swapping providers

At the moment, there exists no branch standard on platforms(API), tools or file format within cloud computing, making switching of providers troublesome if not planned in advance. Customers risk getting stuck with a certain provider with a "'provider lock-in"' if their selection of provider process is not thoroughly planned. Providers use specific platforms for their services, making it harder to switch providers, and uses this to keep hold of their customers. Some providers, like Google, are attempting to lay the foundation for exit strategies and migration away from their own cloud services in hope of attracting more customers. However, until cloud providers either work together to form a standard, or get forced into a standard, customers will have to plan and weigh their options carefully within the cloud computing environment. The checklists created will help with the selection and planning process. The checklists are meant to give a start to companies assessing the option of cloud computing, or evaluating swapping providers.

7 Service Level Agreement

This chapter presents recommendations for reviewing and negotiating the service level agreement and the service level agreement metrics based on the findings from the case studies 6.1.8, 6.2.7 and the literature study.

7.0.1 Negotiation strategy

Large cloud providers(e.g. Google, Amazon...) will present their customers with a pre-defined SLA. But, if a customer has the option to negotiate or discuss some of, or each point of the SLA, this is highly recommended. By negotiation and discussing, the customer can more or less help define a SLA that is customized to their specific business need. However, this is normally not the case. To help customers know the different options and the difference in the providers SLA this thesis will present a way of reviewing the SLA through the use of external expertise 16, 17.

A review of the SLA should reveal the cause and effect of the different aspects of the SLA to the customer. The metrics tables 7.0.4 presented in this chapter will attempt to help guide the customer through the most important part of an SLA, and help the customer identify the parts of the SLA that is detrimental and critical to their business needs.

7.0.2 Expertise and knowledge

Based on the experience and knowledge gained from related work and the information and findings gained through the case study of Narvik municipality 6.2 6.2.7, we will present three scenarios where external expertise and knowledge could help the customer with the SLA, and with the migration process.

Scenario 1:SLA review and negotiation Use Case

The first scenario represents a SLA review and negotiation 16. When the customer has decided that they want to move towards cloud computing, or when the customer want to swap cloud providers it could prove to be beneficial for the customer to contact lawyers and lawyer firms to help review the SLA, the SLA/Sec-SLA metrics and how to avoid potential legal issues and penalties. If any dispute arises, either with the cloud provider or with national information security supervisors, lawyers are of great help. The potential cloud customer will request cloud services from a cloud provider. The provider will then respond with either a pre-defined SLA or a negotiable SLA draft to the customer. The customer will, together with help from lawyers, evaluate, review and audit the agreement. It there is room for negotiation, the lawyer will negotiate the SLA with the provider on behalf of the customer.

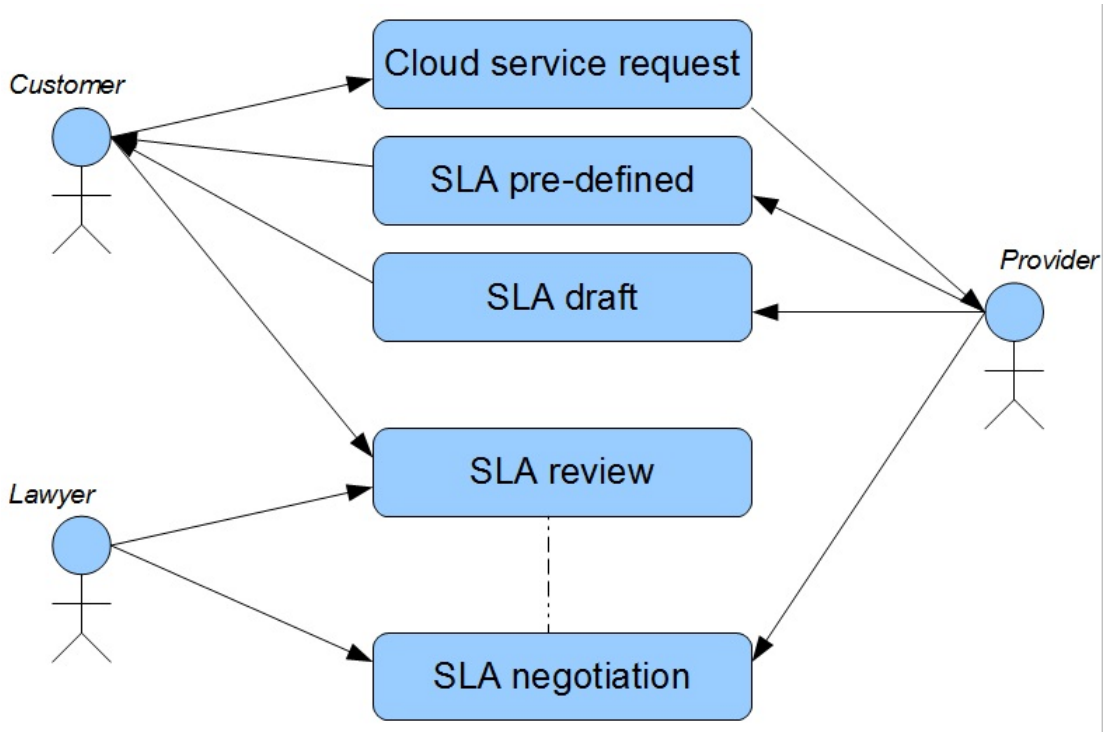

Figure 16: SLA Review and negotiation

Scenario 2:Revision/Audit Use Case

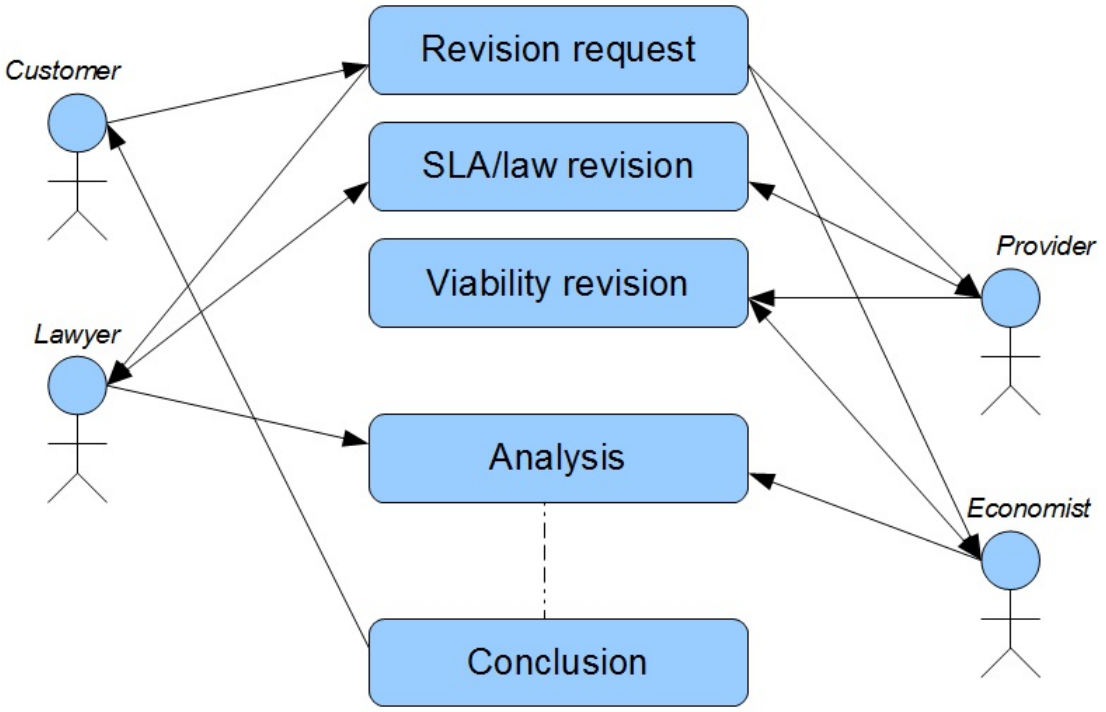

Figure 17: Revision

The second scenario represents a revision/audit 17. A revision or audit can help organizations and businesses avoid several pitfalls when choosing or swapping cloud providers. The revision will be done towards potential new providers to figure out the viability of the cloud provider, and that the new provider is compliant with privacy laws 7.1 3.4.8. The customer puts in a request for a revision to either a lawyer firm or a economist firm, the customer (or the lawyer/economist) will send information of the revision process to the provider. The lawyer will send a request for information regarding juridical matters and SLA contracts to the provider which the lawyer firm in turn will analyze and provide the customer with a conclusion. The economist will send a request for information regarding economics, customers and other potential economic influence factors to the provider which the economist firm in turn will analyze and provide the customer with a conclusion. This can be difficult with regards to large provider companies that is stationed outside the same country as the customer. The large providers (e.g. Google, Amazon...) provides the customer with a already completed audit performed by a third party. However, the assistance of lawyers can help the customer review this audit and deem the audit sufficient or non-sufficient. It is important to remember that audits performed to determine compliance with certain standards(e.g. ISO 27001 and SAS70) where the scope is definable, the providers can define a scope for the compliance audit them self [19].

Scenario 3:Migration Use Case

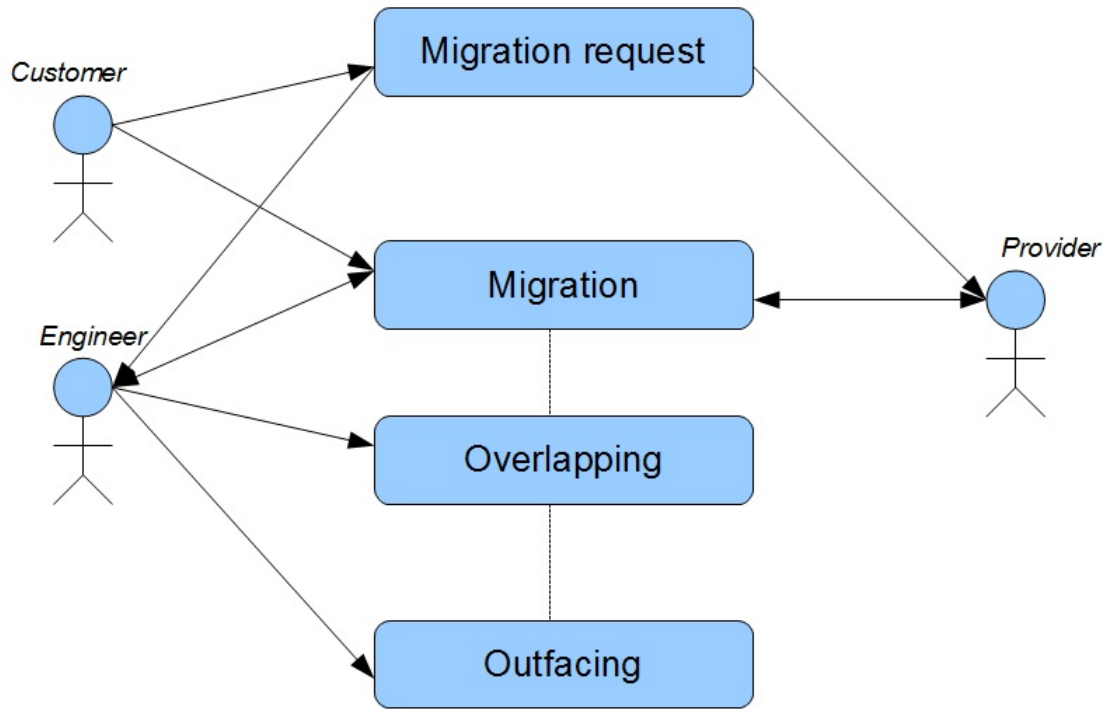

Figure 18: Migration

The third scenario represents a migration 18. The migration process can be difficult, especially for small or medium sized businesses and organizations. Help from outside

expertise can simplify the process. The use case presents such a scenario. The customer has decided upon a cloud provider to migrate to, and sends a request to both the new provider,(the previous provider) and the engineering company. The engineering company will help sooth the process with overlapping of old data and services, gradually introducing the customer to the new provider. If any problems should arise while the migration process is underway the customer can temporarily perform a "'roll back'" and go back to their former solution(previous provider), which ensures business continuity. The engineering company can also help the customer to establish the new cloud services for a limited audience within the company before they complete a full migration. The overlapping will continue until all services and data is successfully transfered onto the new providers cloud solution, and the outfacing process is done.

7.0.3 Argumentation for external expertise

Engineers are not lawyers, and vice versa. It is difficult for someone who has specialized within a engineering field to have a full grasp of all the different privacy laws and regulations that exists throughout Europe, and the rest of the world. Any business or organization that plans a move to the cloud, or plan to move between cloud providers should contact external expertise in the form of lawyers or engineers that has specialized on the field in question(this is dependent on the in-house expertise of the business/organization). The case study of Narvik Municipality 6.2 shows findings that prove as a good example of the lack of juridical expertise, and what the cause of this lack of expertise was. Narvik Municipality had external help to the IT-department with the practical issues regarding the migration from the IBM solution towards Google Apps and Googles cloud environment. The SLA contract between Google and Narvik Municipality did not specify what physical location Narvik Municipality's data would be stored or where the services would be hosted. One of the inhabitants of Narvik Municipality delivered a complain to the Norwegian Data Inspectorate, which is a Norwegian national privacy protecting organization. The Norwegian Data Inspectorate interfered with the migration and demanded that Narvik Municipality should know the exact physical location of their data. The location of the data and services dictate the privacy laws the municipality and its inhabitants data would comply with, and these privacy laws are not neseccary compliant with Norwegian privacy laws, Narvik Municipality was suddenly in a position were they are not compliant with Norwegian law. Narvik Municipality ended up contacting a Oslo based lawyer firm. This lawyer firm, together with Googles lawyers from England and USA worked together to alter the original SLA agreement to better suit Norwegian privacy laws 7.0.2, 6.2.

The findings from the second case study clearly point towards a recommendation of early implementation of outside help in the form of lawyers or engineers.

7.0.4 SLA metrics

The SLA metrics are as mentioned measurable 3.5, and should be agreed upon to guarantee for a certain level of quality of the service delivered. Metrics can, and should be different depending on what type of business that want to rent the providers services, it is also dependent on what services the customer want to rent. The cloud is dynamic, and the SLA metrics should have some dynamic properties and capabilities 3.5.2. Despite the need for dynamical metrics, the SLA should include some or all of the following metrics. The following tables is made to help cloud customers better understand what metrics a

SLA should contain, and help the customers decide for them selfs what metrics they need and what metrics they should try to negotiate with the cloud provider. The metrics for the different cloud models 3.2 are created as a mix of regular SLA metrics and Sec-SLA metrics.

Nr.	Metric	Description	Unit
1	ID management / Authorization	Identification and authorization mechanisms – penetration test	Self defined units, (Yes/no)
2	Protection against malicious code	Application protection against execution of malicious code – penetration test	Self defined units, 1-5, low-high.
3	Password management	Cryptographic measures and policies	Self defined units, 1-5, low-high. Protect against threats – Yes/no
4	Customizability	Ability to change dependant on user and security	Yes/no
5	Scalability	Ability to change dependant on need and security	Yes/no
6	Sensitive data	Server house capable to transmit or process sensitive data	Yes/no
7	**Risk management**	**Grading of application security**	**Risk level, self defined units 1-5, low-high.**
8	**Portability / migration**	**The abilitiy to migrate between providers**	**Self defined units, scale easy-hard, (Yes/no)**
9	**Level of dependency**	**Different dependencies that could affect the service model and migration**	**Level and degree of dependencies, 1-5, (Yes/no)**
10	**Compliance**	**Compliance with laws, regulations, directives**	**Yes/no**
11	**Server and storage cost**	**Server requirements, Amount of storage requried**	**Self defined units**

Figure 19: SaaS Metrics

7.0.5 Metrics tables

The metrics tables 19, 20, 21 for each of the different cloud models 3.2, has been inspired by the metrics presented in the paper from Alhamad, Dillon and Chang on "“Conceptual SLA Framework for cloud computing"' [64]. Some of the metrics used are from this paper from Alhamad, Dillon and Chang [64] and other papers used in the related work of SLA 3.5, [66], [63]. Some of the metrics are created based on the answers during the semi-structured interviews of the case studies with HiG 6.1and Narvik municipality 6.2, and

the findings from these case studies 6.1.8, 6.2.7. The metrics based on these findings are marked "'bold'" in the tables. The following subsection will describe the metrics that is included based on the findings 6.1.8, 6.2.7 from the case studies. The metrics specified for each cloud service delivery model is not locked, and potential cloud customers should feel free to use metrics mentioned for one model for other models. E.g. If the potential cloud customer finds a SaaS metric suitable for IaaS or PaaS they are free to use this metric for the other two cloud service delivery model metric lists.

Nr.	Metric	Description	Unit
1	ID management / Authorization	Identification and authorization mechanisms – penetration test	Self defined units, (Yes/no)
2	Protection against malicious code	Application protection against execution of malicious code – penetration test	Self defined units, 1-5, low-high.
3	Password management	Cryptographic measures and policies.	Self defined units, 1-5, low-high. Protect against threats – Yes/no
4	Customizability	Ability to change dependant on user and security	Yes/no
5	Scalability	Ability to change dependant on need and security	Yes/no
6	Number of developers	The limit of developers working on projects	Yes/no (Self defined units 1-X)
7	Browser security	Adequate browser security – penetration test / security test of browser vulnerability	Self defined units (severity of potential vulnerability – risk management)
8	Server security	Adequate server security – penetration test	Self defined units (severity of potential vulnerability – risk management)
9	**Risk management**	**Grading of application security.**	**Risk level, self defined units 1-5, low-high**
10	**Portability / migration**	**The abilitiy to migrate between providers.**	**Self defined units, scale easy-hard, (Yes/no)**
11	**Level of dependency**	**Different dependencies that could affect the service model and migration**	**Level and degree of dependencies, 1-5, (Yes/no)**
12	**Compliance**	**Compliance with laws, regulations, directives**	**Yes/no**
13	**Infrastructure**	**Bandwitdth, network, servers QoS**	**Spesific requirements, satisfaction scale(1-5)**
14	**Server and storage cost**	**Server requirements, Amount of storage requried.**	**Self defined units**

Figure 20: PaaS Metrics

Portability/Migration/Integration

Even if this process is a bit static, it is important that the possibility for migration is under continuously evaluation. The possibility of migration of services/platform/infrastructure

is tightly coupled with dependencies, and the findings of dependencies 6.1.8, 6.2.7 in the case studies. The measuring unit could be a simple yes and no, or a self defined scale of portability/migration possibilities (e.g. easy - medium - hard).

Risk Management

Risk management is not a new concept, and is not a brand new metric suggestion, but is included in these metric tables based on the findings 6.2.7 in the second case study of Narvik Municipality 6.2. A risk management process should be conducted before selecting or swapping cloud providers, but it should also be a continuously process during the business relationship between the cloud customer and the cloud provider. Changes in services or delivery of services made by the provider could potentially affect the risk or threat level perceived by a cloud customer. The change in threat and risk could be measured in threat or risk levels, a more or less subjective scale introduced by the cloud customer.

Level of dependency

The degree, or level, of dependencies affecting the service delivery models should be continuity monitored. Findings regarding dependencies was found in both case studies 6.1.8 6.2.7, but particualary in the case study of University Innlandet 6.1. The measurable unit could either be represented through a yes and no, or through a scale of degrees of dependencies. The measurable unit should consider the current level of dependencies and the potential dependencies with the inclusion of new services or changes to services made by the provider.

Compliance

Compliance with different regulations and laws is important for the customer, and is to some degree, measurable. With the providers load balancing, the problem of shared jurisdiction, changes to location of storage and the change in politics, laws and regulations, the customer will have to continuously monitor compliance. The customer is either compliant or non-compliant, so the measuring unit will have to be a simple yes or no(compliant or non-compliant). The compliant issues were primarily findings 6.2.7 from the second case study of Narvik Municipality 6.2.

Backup

Low centralization, high duplication is one of the benefits University Innlandet 6.1 hope to gain by migrating and merging the IT-departments of the different colleges in the region. Backup as a security measure is of course nothing new, but is included in the metrics tables because of the findings represented in the first case study. Backup could be represented and measured with different types of units. Either through a simple yes and no, or a measurable unit of degree of backup. This scale could be self-defined on a scale representing the level of backup possibilities and opportunities.

Infrastructure

Bandwidth, network, servers and all aspects of infrastructure or delivery of infrastructure services is often mentioned as something that should be included in the SLA to control and validate the QoS delivered by the provider. The findings 6.1.8 from the first case study of University Innlandet 6.1 supported the inclusion of infrastructure in the SLA and SLA metrics. The units can either be specific bandwidth requirements, network and server availability, or general satisfaction of provider delivery.

Cost

The case study of Narvik Municipality 6.1 and the findings 6.2.7 of this study uncovered the use of cost analysis to predict the cost and migration to the cloud, and if it was worth the cost. Every cloud customer should perform cost analysis to make sure that the move to the cloud, or between providers within the cloud, is economically benefitial. The analysis should be conducted whenever there is a change in the relationship between the customer and the cloud provider. Any changes to services, SLA or cost of delivery should result in a new cost analysis. The metrics and the unit should be self defined and evaluate the different costs, and increased/decreases in the cost.

7.0.6 Monitoring

When Monitoring, or performing a revision of the SLA metrics, it is important to make sure the customer get the quality of service that was agreed upon during the negotiation and/or signing of the SLA. Customers should never trust blindly on cloud providers to deliver the promised quality of service.

To be able to control or monitor the services, the ability to monitor the metrics should be a part of the agreement and/or contract between the provider and customer. Some providers, like Google 6.2, deliver their own tools for monitoring to the customer, while other providers might chose not to. No matter if the provider delivers means of monitoring to the customer or not, the customer need to make sure that the monitoring is not biased in one way or the other.

One way of achieving a trustful monitoring could be to agree with the provider, that it is beneficial to both parts, to let a trusted third party monitor the SLA metrics. This trusted third party could be a revision or audit company(s) that has expertise in either law, engineering or both 6.2. This trusted third party would act like a SLA agent, making sure that the agreements of the contract is being overheld by both parties. Customers can also pay for their own revision or audit company, to make sure the provider delivers the promised quality of service 6.2.

Monitoring of metrics enhances the trust relationship between the customer and the provider.

7.1 Compliance

As a cloud customer it is important to have a certain overview of the different laws and regulations that is applicable for the region the customer is located, and ensure that the company is compliant with these laws. It is also important that the selected or potential cloud provider is compliant with the laws and regulations applicable to the customer.

7.1.1 The legal maze

The term legal maze is used in a lot of different literature to describe the issues regarding the EU directive 3.4.1, and all the different national privacy laws that reign in Europe. Any company need to abide by their own national privacy laws, but the problem arises when this company buys cloud services from a company abroad, as the privacy laws that apply to the cloud provider might not be covering the privacy laws of the cloud customer, making the cloud customer non-compliant. The potential cloud customer should have knowledge of the applicable directives, laws and regulations applicable for their region, e.g. for a Norwegian company buying services from a European cloud provider should have knowledge of the different EU directives 3.4.1, 3.4.2, 3.4.3, the laws and

Nr.	Metric	Description	Unit
1	Storage location	Applicable laws, physical location of storage area/datacenter.	Self defined units, dependant on area of operaion. (Yes/no)
2	Storage space	What systems the data will be stored upon. What fileformat data will be stored in, and what fileformat when recieveing the data. Options for scalability	Fileformat, systems, scalability. Self defined units, 1-5, low-high.
3	Security and privacy	Cryptographic measures, identity management, adaptive authorization, authentication, transfer of data, availability	Self defined units, 1-5, low-high. Protect against threats – Yes/no
4	Recovery	Disaster recovery plans, hot/cold sites.	Yes/no
5	Sensitive data	Server house capable to transmit or process sensitive data	Yes/no
6	**Backup**	**Backup images, where they are stored.**	**Self dedined units, 1-5, (Yes/no)**
7	**Risk management**	**Grading of networks, virtual images, data.**	**Risk level, self defined units 1-5, low-high.**
8	**Portability / migration**	**The abilitiy to migrate between providers.**	**Self defined units, scale easy-hard, (Yes/no)**
9	**Server and storage cost**	**Server requirements, Amount of storage requried.**	**Self defined units**

Figure 21: IaaS Metrics

regulations for the country were the provider is residing, and the Norwegian privacy laws and regulations 3.4.8.

7.2 Discussion

Discussion regarding the SLA review process, SLA/Sec-SLA metrics and external expertise.

7.2.1 SLA review process

The process is meant to be a very general starting point for companies without much knowledge or competance of the cloud and the cloud environment. Each company that decides to adapt the review process need to adapt the metrics 7.0.4, and make their own customizations and changes to the metrics tables for it to be a viable methodology. The metrics table are made as general as possible for it to be adaptable for most types of cloud customers. The process is not new, and neither are most of the metrics, as there exists

many SLA review processes. The thesis only added a small contribution in the inclusion of the Sec-SLA metrics based on the findings of the case studies 6.1.8, 6.2.7.

The sla review process presented in this thesis starts with negotiation strategies. Even if the large companies use standardized and pre-written SLA agreements, there is still room for negotiation, as found during the work on the Narvik Municipality case study 6.2.

7.2.2 External expertise

Based on the findings through the case studies 6.1.8, 6.2.7, the need for external expertise is relevant for organizations and businesses. Organizations and businesses that is not of large enough scale to afford in-house expertise on spesific areas could encounter issues and problems during the process of migration towards cloud services or between cloud providers. These companies need to know when to contact and hire external knowledge and expertise. Migration and adaption processes within the cloud include a lot of juridical questions and issues. The use cases of scenarioes of exteral expertise are created based on findings during the case studies of University Innlandet 6.1 and Narvik Municipality 6.2, and represent scenarioes where the subjects of the case studies contacted or wanted to contact external experts. The correct use of external expertise could save the cloud customer time and money.

7.2.3 Metrics

SLA and Sec-SLA metrics are hard to define. The cloud is dynamic, and the metrics has to be dynamic to some degree as well. The metrics would need to be scalable, and they would need to scale in the same rate as the delivered service. Optimally, any cloud customer should have the oppertunity to request changes in the SLA metrics table continously if needed, and with that in mind it is hard to look at the created tables as much more than a starting point, and as a base of operations. There is a lot of research left in the field of Sec-SLA and there is a need for scalable Sec-SLA to better fit the cloud environment. Ideas and development of SLA/Sec-SLA metrics are evolving continiously, and the presented tables 7.0.5 should not be used by customers as more than a start. The needed metrics could also be different based on the customers specific need. That is why it is also recommended to hire lawyers or engineers(as see fit) to accompagny the customer when reviewing and negotiating the SLA and its metrics. We did not follow the recommendations for metrics found in related work 3.5.2 as they would have required a more in-depth and hands-on analysis than what was possible with the time limit we had.

8 Modelling and analysing

The following chapter presents the attempt to solve the third research question 1.5 through an addition and improvement to a conceptual SLA-based trust model for cloud computing.

8.1 SLA-based Trust model

The model is conceptual and based on previous conceptual SLA trust models. The addition to the model created by Alhamad, Dillon and Chang[82], is the idea of dependencies and the possibility of migration/swapping providers. The model is envisioned to enhance trust in the cloud environment, if and when, it is materialized. The addition and model modification is based on the results from the first two research questions 1.5, the findings from the case studies 6.1.8, 6.2.7 and the presentation of these findings 6.3, 7.

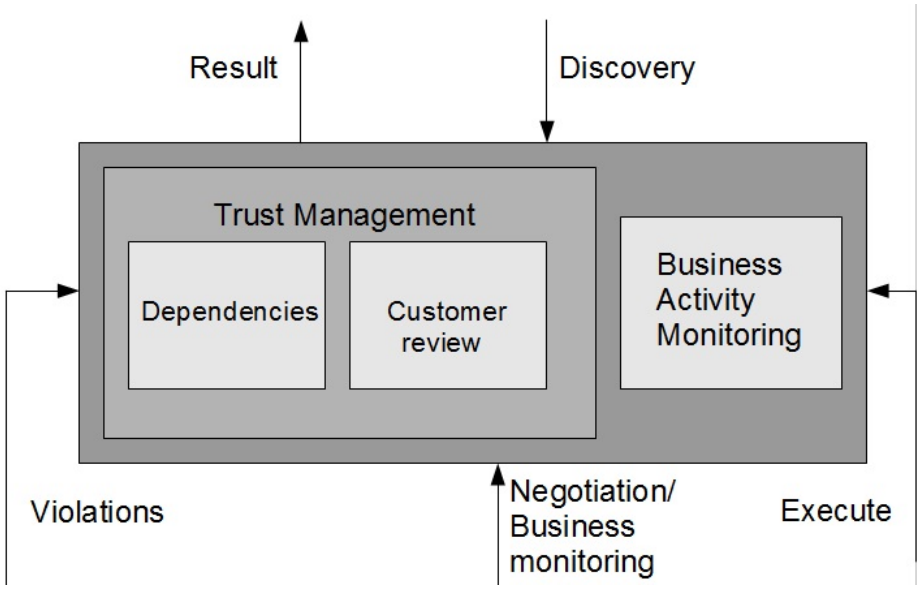

Figure 22: Dependencies in the trust model

8.1.1 Dependencies

The idea behind the addition of dependencies in the trust management part of the model, is for customers to send, not only their customer reviews, but also any dependencies they have experienced from the cloud provider, to a cloud service directory. The cloud service directory is a database that includes customer reviews of cloud providers, and information of the providers given by the providers(advertisement). The dependencies could be graded on a scale from 0-1, where 1 would equal full dependency, and 0 would represent zero dependency. In addition to the graded scale, the database could allow for the attachments of documents and notes regarding the level of dependency.

8.1.2 Trust management

The trust management is supposed to enhance trust through customer reviews and dependency review. The evaluation from customers will be sent to a database of cloud providers. The addition presented in this thesis requires users to point out dependencies and send this information together with the customer review. When the cloud provider directory has reviews and dependency information, any potential new cloud customer will have an easier task of selecting their best suited provider.

8.1.3 How portability and user contribution enhances trust

The portability, or ability to swap providers/migrate, increases trust in the cloud. It indirectly enhances trust through diminishing the need for trust. If cloud customers are free to migrate between service providers, the need for trust is less of an issue. A customer would still have to trust a third party with their data, and the confidentiality of this data. But a cloud customer will no longer be forced to stick with the same provider should there exist any mis contempt. The choice of a cloud provider would not be as detrimental as it can be in todays cloud environment. With this model, the user would be in charge. The customers decide what cloud provider that will be presented as the best through their reviews.

8.1.4 Discussion

The model can possibly be misused by false user reviews and a lack of dependency grading. Even if this is outside the scope of this thesis, the model would need some way of making sure that every previous or current cloud customer answers the reviews legit. Without legit user reviews and dependency grading the model would result in false recommendations. A newly started provider would also have a hard time getting their first customers, since they start of with zero reviews. Another negative aspect of the model is that it actually servers no purpose should the cloud providers agree upon a common standard for API, file format and other forms of dependencies. However, cloud customers and researchers can not wait until the providers themselves agree upon such a standard, and this model is hopefully a step in the correct direction.

9 Discussion

The goal of the thesis was to help businesses and organizations enable the use of cloud computing technology. This goal was attempted reached through presenting guidelines and recommendations for cloud computing customers that want to move onto the cloud, or move and migrate between cloud providers. The thesis also presented how customer them selfs could contribute to ensure a compliant and secure cloud, and guidelines and recommendations for these contributions. Last, but equally important, if these aspects could help improve the trust relationship between a cloud provider and a cloud customer. To reach this goal we had to include several information security management aspects, and look for solutions within business, information security and IT, and juridical parts of information security. Much like the enabling of a multi-disciplinary demanding cloud computing technology, the solution presented in this thesis was found through a multi-disciplinary study.

For the first research question, regarding the planning and execution of migration to a cloud provider or the swapping of cloud providers, we had to figure out what problems that could potentially stand in the way of such a process, and how we could solve these potential problems. To understand how such a process would formulate in practice we decided to conduct two case studies that was aimed at giving us insight and understanding of the problematic issues cloud customers had already experienced, and draw knowledge based on these practical experiences. The use of these case studies helped uncover several findings that we used to produce the mentioned guidelines and recommendations checklists for selection of/or swapping of providers. Since case studies are a qualitative study, we would of course prefer a supplement study that would research the quantitative data based on the findings from the qualitative study. But, the time limit of the thesis restricted the use of such a supplement study. The case studies gave us several expected findings on dependencies and the previous known problem of vendor/platform lock-in and how organizations and businesses possibly can avoid this lock-in. These findings were presented through several checklists created to guide the (potential) cloud customer in the selection of/or swapping of providers. This included what they should know, test and prepare for.

The case studies conducted was also used to help answer the second research question. The question asked how cloud customers could contribute to the enabling of a secure and compliant cloud environment. Through the case studies we found several findings, these findings suggested use of external expertise, and the several other aspects the customer them selfs could do to contribute to a more compliant and secure cloud environment. The use of external expertise was presented through several use case scenarios to illustrate the benefit a cloud customer could gain from such services. We also found interesting techniques and methods of ensuring business continuity and resilience through service overlapping and limited audience testing. Like the first research question, these case studies were conducted as qualitative studies, and a supplement study of quantitative qualities could be needed to confirm the findings and results.

For the third, and last research question, we used the results and findings from the previous research questions to see if we could improve upon a previously created conceptual cloud computing SLA trust model. We wanted to include the migration and swapping aspect, while at the same time include the customer contribution to the cloud environment. The idea behind the addition to the model was for the customers of cloud provider services to contribute with their perception and discovery of dependencies with different cloud providers. This dependency information directly affects the migration possibilities of cloud customers, and would be stored in a directory data base available for all potential cloud customers. Customers with specific experience with a certain provider(s) would contribute with this exact experience, improving the evaluation situation for new potential cloud customers when selecting their new cloud provider. The model is conceptual, and the addition is an idea, and is not materialized. For further development, the model will have to be materialized and tested in practice.

The findings and results produced during the work on this thesis could potentially be adopted by organizations and customers residing in a situation of a move into the cloud, or between cloud providers. The findings suggest several ways the customer could help contribute to a more compliant, secure and trusted cloud environment. Optimally, the findings would have been through another process of quantitative study to confirm and guarantee the correctness of the findings.

10 Conclusion

The work that has been conducted for this thesis has resulted in guidelines and recommendations for customers that need or want to change cloud providers, and potential cloud customers that want to enable use of cloud computing technology. The work also resulted in a list of scenarios that represent contact with external expertise for the enabling of cloud technology, and swapping between cloud providers. We also describe how these results can be used to improve the trust relationship between the cloud customers and cloud providers through an addition to a conceptual trust model on cloud computing. We gathered findings and results from two different case study experiments. The case studies were performed on two different organization, one utilizing a private cloud, the other organization utilizing a public cloud. The findings were used to produce the mentioned results.

The guidelines and recommendations for the migration and/or swapping between cloud computing service providers provide the potential cloud customer with checklists for the selection of cloud providers. These checklists are meant to ensure business continuity and resilience through the planning process. The checklists are three-parted, one checklist containing information on what the cloud customer should know, test, prepare and what to avoid when selecting or switching between providers. By following these checklists and recommendations the cloud customer will have the opportunity to avoid any provider or platform lock-in, plan for exit strategies, and will be able to migrate to the cloud, or between providers.

Through the results presented in the thesis the cloud customer is able to contribute to enable a secure and compliant cloud. The guidelines and recommendations for negotiation includes several SLA metrics tables to guide the customer through the SLA and the process of refining and auditing this contract. The checklists, as mentioned, and the scenarios representing external expertise help the cloud customer contribute and to take the correct choices when enabling or using cloud computing. The guidelines aim to help the cloud customer by selecting a suitable provider, forming and negotiating a suitable SLA. Another important aspect is the contact with, and use of external expertise when needed, to ensure a secure and efficient migration/swap and to be compliant with the applicable privacy laws, regulations and directives.

A modification to an already existing trust model was created to prove that effective swapping of providers and cloud customer contribution could enhance the trust between cloud customers and cloud providers (on a conceptual level). The idea behind the addition and modification is to let customers of cloud providers report the amount and level of dependencies connected with the different providers based on experience. The reports will be gathered in a directive database for new potential customers to review.

All the research and study during the work on this thesis is qualitative, and since they are based on practical experience, they should be considered valid and useful for potential cloud customers in the same position as the companies and organizations studied. However, there is a need for a quantitative supplement study to confirm the found results.

11 Further work

Further work on the SLA requirements and metrics could be needed before a final judgment of their usefulness is confirmed. Metrics suggestions and guidelines regarding the legal aspect are only presented through two specific cases, which is enough to form a hypothesis, but a broader quantitative study would be needed to confirm their usefulness. The metrics could also benefit from being re-worked in cooperation with lawyers that has specialized on the field. The SLA metrics and Sec-SLA metrics should be split out and be in more detail, a questioner or depth interviews with different types of potential cloud customers could reveal what SLA and Sec-SLA metrics the average cloud customer seeks and find important.

The case study regarding the migration of data centers(private self-hosted cloud) differ from the study of customers switching cloud providers and customers using public clouds. There is a lot of potential for further work and research in creating a comparable collection of different case studies or other form of samples from customers that have been through the process of switching cloud providers. A collection of case studies of customers that have practical experience with cloud provider switching could help improve the checklists created for the swap process. Further studies should also include scenarios where organizations or businesses are trapped by a provider-lock and want to swap providers. It could also prove beneficial to do case studies or other types of research on the hybrid cloud to reveal any differences from the private and public cloud.

The model created to answer the third research question is on a conceptual level and would need more work before it could be materialized. There is also potential further work located in developing a model representing the SLA agent, the trusted third party and their communication with the cloud providers and the customers.

The case studies conducted has formed a basis for the forming of hypothesis regarding the checklists, metrics tables and use cases. A quantitative study would help in confirming or denying the hypothesis and the information found through the case studies.

Bibliography

[1] Amrhein, D. & Quint, S. APRIL 2009. Cloud computing for the enterprise: Part 1: Capturing the cloud. http://www.ibm.com/developerworks/websphere/techjournal/0904_amrhein/0904_amrhein.html. Last visited: 13.06.12.

[2] Azharuddin. NOVEMBER 2011. Difference between cloud computing and grid computing.

[3] Vertisage. 2010. Saas and cloud computing enablement. http://vertisage.com/s-saas.html. Last visited: 13.06.12.

[4] C.Chou, D. Authentification example.

[5] Mell, P. & Grance, T. 2011. The nist definition of cloud computing (draft) recommendations of the national institute of standards and technology. *NIST Special Publication*, 145(6), 1–2.

[6] Discourse, S. D. Key characteristics of a paas offering. http://www.siia.net/blog/index.php/2011/03/siia-members-only-issue-brief-key-characteristics-of-a-paas-offering/. Last visited 16.06.12.

[7] Papazoglou, M. & van den Heuvel, W. nov.-dec. 2011. Blueprinting the cloud. *Internet Computing, IEEE*, 15(6), 74 –79.

[8] Karatas, F., Bourimi, M., Barth, T., Kesdogan, D., Gimenez, R., Schwittek, W., & Planaguma, M. march 2012. Towards secure and at-runtime tailorable customer-driven public cloud deployment. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*, 124 –130.

[9] Buyya, R., Yeo, C., & Venugopal, S. 2008. Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In *High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on*, 5–13. Ieee.

[10] SiG, C. 2010. Cloud computing keywords. http://sites.google.com/site/csixcloudcomp/member_content/keywords.

[11] Fox, A., Griffith, R., et al. 2009. Above the clouds: A berkeley view of cloud computing. *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS*, 28.

[12] Wang, L., Von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J., & Fu, C. 2010. Cloud computing: a perspective study. *New Generation Computing*, 28(2), 137–146.

[13] Heiser, J. & Nicolett, M. 2008. Assessing the security risks of cloud computing. *Gartner Report*.

[14] Mell, P. & Grance, T. SEPTEMBER 2011. The nist definition of cloud computing. *Special Publication 800-145*.

[15] Zhang, S., Zhang, S., Chen, X., & Huo, X. 2010. Cloud computing research and development trend. In *Future Networks, 2010. ICFN'10. Second International Conference on*, 93–97. Ieee.

[16] Zhang, S., Chen, X., Zhang, S., & Huo, X. 2010. The comparison between cloud computing and grid computing. In *Computer Application and System Modeling (ICCASM), 2010 International Conference on*, volume 11, V11–72. IEEE.

[17] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. April 2010. A view of cloud computing. *Commun. ACM*, 53(4), 50–58.

[18] Jansen, W. & Grance, T. 2011. Guidelines on security and privacy in public cloud computing. *NIST Special Publication*, 800–144.

[19] Ensure & Neupart. MAY 2012. Cloud computing security - ccsk certification.

[20] Shaikh, F. & Haider, S. 2011. Security threats in cloud computing. In *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*, 214–219. IEEE.

[21] Alhamad, M., Dillon, T., & Chang, E. dec. 2011. Service level agreement for distributed services: A review. In *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on*, 1051 –1054.

[22] Ju, J., Wang, Y., Fu, J., Wu, J., & Lin, Z. JUNE 2010. Research on key technology in saas. 384 –387.

[23] Nitu. 2009. Configurability in saas (software as a service) applications. In *Proceedings of the 2nd India software engineering conference*, ISEC '09, 19–26, New York, NY, USA. ACM.

[24] He, H. dec. 2010. *Applications deployment on the SaaS platform*.

[25] Kelly, J. Cloud computing and cryptography.

[26] Tsai, W.-T., Shao, Q., Huang, Y., & Bai, X. 2010. Towards a scalable and robust multi-tenancy saas. In *Proceedings of the Second Asia-Pacific Symposium on Internetware*, Internetware '10, 8:1–8:15, New York, NY, USA. ACM.

[27] Rake-Revelant, J., Holschke, O., Offermann, P., & Bub, U. oct. 2010. Platform-as-a-service for business customers. In *Intelligence in Next Generation Networks (ICIN), 2010 14th International Conference on*, 1 –6.

[28] Wang, T., Zhou, X., Zhang, W., & Wei, J. 2010. Towards paas using service-oriented component model. In *Proceedings of the Second Asia-Pacific Symposium on Internetware*, Internetware '10, 18:1–18:4, New York, NY, USA. ACM.

[29] Lawton, G. june 2008. Developing software online with platform-as-a-service technology. *Computer*, 41(6), 13 –15.

[30] Brown, A. & Chase, J. 2011. Trusted platform-as-a-service: a foundation for trustworthy cloud-hosted applications. In *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, 15–20. ACM.

[31] Haji, A., Ben Letaifa, A., & Tabbane, S. oct. 2011. Implementation of a virtualization solution: Saas on iaas. In *Wireless and Mobile Networking Conference (WMNC), 2011 4th Joint IFIP*, 1 –5.

[32] Bhardwaj, S., Jain, L., & Jain, S. 2010. Cloud computing: A study of infrastructure as a service (iaas). *International Journal of engineering and information Technology*, 2(1), 60–63.

[33] JuniperNetworks. 2012. Securing multi-tenancy and cloud computing. `http://www.juniper.net/us/en/local/pdf/whitepapers/2000381-en.pdf`.

[34] Hay, B., Nance, K., & Bishop, M. jan. 2011. Storm clouds rising: Security challenges for iaas cloud computing. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, 1 –7.

[35] Khajeh-Hosseini, A., Greenwood, D., & Sommerville, I. july 2010. Cloud migration: A case study of migrating an enterprise it system to iaas. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, 450 –457.

[36] Hay, B., Nance, K., & Bishop, M. jan. 2011. Storm clouds rising: Security challenges for iaas cloud computing. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, 1 –7.

[37] Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. 2009. Controlling data in the cloud: outsourcing computation without outsourcing control. In *Proceedings of the 2009 ACM workshop on Cloud computing security*, CCSW '09, 85–90, New York, NY, USA. ACM.

[38] Fitzpatrick, B. W. & Lueck, J. November 2010. The case against data lock-in. *Commun. ACM*, 53(11), 42–46.

[39] T OGRAPH, B. & MORGENS, Y. 2008. Cloud computing. *Communications of the ACM*, 51(7).

[40] Google. 2010. Security whitepaper: Google apps messaging and collaberation products.

[41] Crosby, S., Doyle, R., Gering, M., et al. Open virtualization format specification.

[42] SNIA. SEPTEMBER 2011. Advancing storage and information technology. `http://snia.org/sites/default/files/CDMI_SNIA_Architecture_v1.0.1.pdf`.

[43] Alaranta, M. & Jarvenpaa, S. 2010. Changing it providers in public sector outsourcing: Managing the loss of experiential knowledge. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, 1–10. IEEE.

[44] Matthias Olzmann, M. W. Switching it outsourcing providers - a conceptual framework and initial assessment of critical success factors. *Service Computation: The third International Conferences on Advanced Service Computing*.

[45] Houidi, I., Mechtri, M., Louati, W., & Zeghlache, D. july 2011. Cloud service delivery across multiple cloud platforms. In *Services Computing (SCC), 2011 IEEE International Conference on*, 741 –742.

[46] Westin, A. & Blom-Cooper, L. 1970. *Privacy and freedom*. Atheneum New York.

[47] OCTOBER 1995. The european parliment - directive 95.

[48] JISClegal. AUGUST 2011. Report on cloud computing and the law for uk fe and he.

[49] Eecke, P. V. Cloud computing legal issues. http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf.

[50] Lovdata. Personopplysningsloven. http://www.lovdata.no/cgi-wift/wiftldles?doc=/app/gratis/www/docroot/all/nl-20000414-031.html&emne=PERSONOPPLYSNINGSLOV*&. Last visited 13.06.12.

[51] Union, E. 2006. *European Union: consolidated versions of the Treaty on European Union and of the Treaty establishing the European Community*. European Communities.

[52] Giannakaki, M. The eu data protection directive revised: New challenges and perspectives.

[53] Hustinx, P. APRIL 2010. Data protection and cloud computing under eu law. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf.

[54] BURLOIU, V. 2012. Cloud computing and the regulatory framework for telecommunications and information society services.

[55] JULY 2002. European parliament - directive 2002.

[56] MARCH 2006. European parliament - directive 2006.

[57] Kuner, C. 2010. Regulation of transborder data flows under data protection and privacy law: Past, present, and future.

[58] Cooperation, A. 2004. Apec privacy framework.

[59] Secretariat, A. & Cooperation, A. 2009. Guidebook on apec procedures and practices.

[60] JULY 2000. European parliament - safe harbor commission decision.

[61] Datatilsynet. 2011. Cloud computing - en veileder i bruk av nettskytjenester. http://www.datatilsynet.no/Global/04_veiledere/CloudComputing_veil.pdf. Last visited 13.06.12.

[62] Lovdata. Personopplysningsforskriften. http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001215-1265.html. Last visited 13.06.12.

[63] Faniyi, F. & Bahsoon, R. june 2011. Engineering proprioception in sla management for cloud architectures. In *Software Architecture (WICSA), 2011 9th Working IEEE/IFIP Conference on*, 336 –340.

[64] Alhamad, M., Dillon, T., & Chang, E. april 2010. Conceptual sla framework for cloud computing. In *Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on*, 606 –610.

[65] Forum, T. Service level agreement/quality of service overview. `http://www.tmforum.org/Overview/2016/home.html?linkid=29209`. Last visited 08.05.12.

[66] de Chaves, S., Westphall, C., & Lamin, F. march 2010. Sla perspective in security management for cloud computing. In *Networking and Services (ICNS), 2010 Sixth International Conference on*, 212 –217.

[67] Costa, A. & Bijlsma-Frankema, K. 2007. Trust and control interrelations: New perspectives on the trust control nexus. *Group*.

[68] Khan, K. & Malluhi, Q. 2010. Establishing trust in cloud computing. *IT professional*, 12(5), 20–27.

[69] Sato, H., Kanai, A., & Tanimoto, S. 2010. A cloud trust model in a security aware cloud. In *Applications and the Internet (SAINT), 2010 10th IEEE/IPSJ International Symposium on*, 121–124. IEEE.

[70] Li, W., Ping, L., & Pan, X. 2010. Use trust management module to achieve effective security mechanisms in cloud environment. In *Electronics and Information Engineering (ICEIE), 2010 International Conference On*, volume 1, V1–14. IEEE.

[71] Ko, R., Kirchberg, M., & Lee, B. 2011. From system-centric to data-centric logging-accountability, trust & security in cloud computing. In *Defense Science Research Conference and Expo (DSR), 2011*, 1–4. IEEE.

[72] Kiruthika, M. & Amirtha, M. A framework for accountability and trust in cloud computing.

[73] Wang, T., Ye, B., Li, Y., & Yang, Y. 2010. Family gene based cloud trust model. In *Educational and Network Technology (ICENT), 2010 International Conference on*, 540–544. IEEE.

[74] Sun, X., Chang, G., & Li, F. 2011. A trust management model to enhance security of cloud computing environments. In *Networking and Distributed Computing (ICNDC), 2011 Second International Conference on*, 244–248. IEEE.

[75] Neisse, R., Holling, D., & Pretschner, A. 2011. Implementing trust in cloud infrastructures. In *Cluster, Cloud and Grid Computing (CCGrid), 2011 11th IEEE/ACM International Symposium on*, 524–533. IEEE.

[76] Benbasat, I., Goldstein, D., & Mead, M. 1987. The case research strategy in studies of information systems. *MIS quarterly*, 369–386.

[77] Flyvbjerg, B. 2006. Five misunderstandings about case-study research. *Qualitative inquiry*, 12(2), 219–245.

[78] Baxter, P. & Jack, S. 2008. Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report*, 13(4), 544–559.

[79] Pearson. How to analyze a case study. http://wps.prenhall.com/bp_laudon_mis_10/62/15948/4082759.cw/index.html. Last visited 01.06.12.

[80] Landheim, H. 2011. Universitet i innlandet - hvorfor universitet i innlandet. http://www.innlandsuniversitetet.com/Om-prosjektet.

[81] IKT, A. 2011. Rapport - organisering av administrative funksjonsområder. http://www.innlandsuniversitetet.com/PageFiles/49707/Rapport%20fra%20IKT-gruppa%2030.09.11.pdf.

[82] Alhamad, M., Dillon, T., & Chang, E. sept. 2010. Sla-based trust model for cloud computing. In *Network-Based Information Systems (NBiS), 2010 13th International Conference on*, 321 –324.

A Appendix

Interview questions : Case Study University Innlandet

Who was involved in the swapping process, and which datacenters was planned combined/merged?
- Anything you would want to add?
- Follow-up questions

How was the planning process?
– Did you use any standards when planning?
– Anything you would want to add?
– Follow-up questions

Did you perform any switch or merge of any type of application service?
– What types of services?
– Why did you want to merge services?
– Did the switch or merge of services have any dependencies?
– Did it exist any other form of dependencies?
– Would you consider the systems and services to have a low «escape velocity»?
– Anything you would like to add?
– Follow-up questions

Did you/was it planned to perfom migration of stored data?
– What challenges did you face?
– Was any of the data considered sensitive?
– If data was sensitive, how was it planned to handle such data?

How were you planning for potential loss of data?
– Anything you would want to add?
– Follow-up questions
– Disaster recovery / Business continuity

Did you have any compliance issues?
– Norwegian privacy laws and regulations?
– Norwegian Data Inspectorate?
– Anything you would want to add?
– Follow-up questions

Do you/Did you have any form of services outsourced to third parties?
– If yes, how did you solve potential dependencies?
– Do/did any of the involved parties have different outsourcing partners?
– Anything you would want to add?
– Follow-up questions

Was / is there anything standing in the way for a successful/full migration?
– Anything you would want to add?
– Follow-up questions?

Interview questions: Case Study Narvik Municipality

What services did you plan to migrate to the cloud?
- Was it only e-mail services?
- What was your plan for the e-mail services?
- Would you use the e-mail accounts to send sensitive information?
- How do you plan to handle sensitive information?
- Did you plan/perform any transfer of data? (If yes, how was this done/planned?, what did you do with the old data?, How did you get old data into the cloud?)
- Anything else you want to add?
- Follow-up questions

Did you have any contractual agreements with google?
- Service level agreement?
- Was it possible to negotiate the SLA or other forms of contracts?
- Did you perform any analysis of the SLA before negoiating/signing the agreement? (SLA review/audit?)
- Did you perform any risk management evaluation of the SLA?
- Was the metrics pre-defined? Did you get any overview of the metrics? What metrics was the most important for you?
- Did you get any oppertunities for monitoring of the QoS?
- What QoS guarantees did you get?
- Did the SLA contain any clause(s)?
- Anything else you want to add?
- Follow-up questions

How did you migrate from Lotus Notes?
- Did you investigate the oppertunities for further migration/swapping of provider(away from Google)
- Are there any dependencies from using Google Apps? Did Google inform you of any dependencies?
- Did you have any dependency issues when migrating?
- Did you have any fileformat issues? Did you have any API issues?
- Anything else you want to add?
- Follow-up questions

Did you rent/hire/contact any form of external expertise during the migration/swapping process?
- Lawyers / Engineers / Others ?
- If not, did you contact any external expertise later on?
- Anything else you want to add?
- Follow-up questions

What would you have done differently?

Narvik Municipality Interview notes:

- Google, e-post, dokument tjenester, regneark, tegneprogram, presentasjonsverktøy er hva vi benytter i dag.
- Varsel om vedtak, utsettelse av frist, levert grunding svar m/hjelp av advokater fra Oslo, London og USA(Google sine advokater) Til behandling hos datatilsynet i løpet av Mai.
- Ingen sensitiv data påvirker.
- Ingen 100% garanti for interne rutiner på sensitive data. Økt oppmerksomhet på akkurat dette. Strenge rutiner. Flere aktiviter/info på hjemmesidene våre m/info om personopplysninger
- Informert publikum. Rutiner i form av sensitiv data in. Ikke returnere samme e-post. Lagre i eget system, utenfor sky.
- Overførsel av gammel data vha migreringsverktøy.
- Ferdig utarbeidet SLA. Generell. Public for alle. Nå er det direkte avtale med Google. Forretningshemmeligheter, konfidensiell.
- Gjennomgang av SLA under prosessen. Tredjepart revisjon vurderinger.
- SLA Metrics
- Datatilsynet – tilgjengelighet, e-post som tjeneste (ikke forretningskritisk) Vi kan leve uten.
- Monitorering av QoS gjennom tredjepart. Har også åpne verktøy løsninger fra Google. Gjennomsiktig rapport.
- Gode exit muligheter fra Google som leverandør av tjenestene
- Ingen spesielle avhengigheter fra Google
- Advokat/Ingeniør firma for hjelp med SLA/migrering/revisjon
- Advokat hjelp (datatilsynet)
- Risikoanalyse gjennomført, skulle brukt mer tid (alikevel en bra vurdering med flere gjennomganger) Vurdert mange parametere
- Lovteksten er utdatert
- Personvernsloven
- Internkontroll hos databehandler er vanskelig
- Mangel på kompetanse i Narvik
- Ingen operatør, men mekanisk elektronisk prosess, mer mot prosessering
- TTP

University Innlandet Interview notes:

- Hva er likt, hva er forskjellig?
- Org. Kultur er klar
- Universitetet, Oppland, Private aktører
- Kartleggingsprosess
- Fagfolk
- Lekasje av kompetanse i Hedmark / Oppland, trenger sterke høgskoler for at det skal andre veien. Flere Dr. Grader
- Data migrering tilbake
- Ledd avik, 15 år, spare noe på drift kostnader også
- 3 skoler, 1500 ansatte, 3 datasenter
- Store IT konsekvenser, 45 ansatte
- Lagring av data er ikke noe problem
- Felles bruker ID FEIDE LDAP, 40-talls forskjellige systemer, med forskjellige brukere
- Automatisk brukerkontroll
- Gigabit linjer mellom skolene, desentralisering er planen, ikke noen form for sentralisering.
- Brukermassen/autentiserin – studieadministrasjon
- Forskjellige bruker ID / navn skaper problemer mellom de forskjellige høgskolene som er involvert i prosjektet (Hedmark)
- HiG best forberedt, ulik kompetanse.
- Infrastruktur er på plass
- Studentdatabaser UiO
- Ulike synspunkter på tjenester/platformer som skal leveres
- 7-8 år siden sist forsøk på å slå sammmen, som slo feil
- Migrering/utrulling
- DR: Ikke avhengig av en strømleverandør
- Personaldata for studenter og ansatte, litt forskningsdata, har gode rutiner. Godt driftet. Dette er sensitive opplysninger/informasjon.
- Data ikke lagret lenge nok til å tape, kjøre på gamle løsninger en god stund til, Kjøre backup til andre campus, ingen tap siste 7 år.
- Politikk står i veien.
- Prosjektsidene til innlandsunviersitetet ligger på nett
- Outsource: Fronter + UiO database
- Alle tre høgskolene bruker fronter