Master Thesis Information Management

A comparison of governance models for cloud computing

With a case study on cloud IT controls for a telecom service provider

Name	**: Bram Reijnders**
Date	**: 27-07-2017**
Student ID	**: 1259523**
E-Mail	**:**
Study	**: Information Management**
Supervisor	**: Dr. E.A.M. Caron**
Second Reader	**: ir. R.J.M.A. Triepels**
Company	**: Telecom Service Provider**
Company info	**: The company is one of the largest telecom and IT service provider in the Netherlands. They offer multinationals and other enterprises a broad range of services and products: consulting, workspace management, cloud services, data centre capacity and other network-related ICT solutions.**

Abstract

Cloud computing offers many advantages such as scalability and cost reduction. A downside is that it brings new risks such as availability and data privacy risks. To minimize this risk IT governance models exist.

The question is how the IT governance models differ from each other in relation to cloud computing. Governance models could be best-practice and/or security frameworks. The models discussed are COBIT, ISO 27000 series, ITIL, ISAE 3402, COSO and CCM. Each of these frameworks has its own unique characteristics and by complementing each other they cover all cloud specific related risks that are known at this time.

A helpful tool for organisations which is developed by Becker and Bailey (2014) is the Cloud Governance Dial. By following the six steps of this dial the risks related to certain business processes or applications can be analysed and the appropriate governance model to cover each risk can be chosen. Additionally, a case study took place on cloud IT controls for a telecom service provider where a use case was applied to the dial. The results were useful, but not complete. The Cloud Governance Dial could use some optimisations and changes, such as including the GDPR.

The GDPR is a new regulation created by the European Union which becomes active next year and affects every company active in the EU that processes personal data. Many organizations currently struggle with complying with this regulation. So far it is unknown what for impact this regulation will have on the current business processes of a company.

With cloud computing, clients have difficulties to check how their data is handled and don't get insight in the very fine levels of security policy administration the cloud vendor has. In order to gain trust from the client, transparency from the cloud vendor is needed. This can be offered by means of certifications, but also by maintaining a personal relationship between the client and vendor. During this research was found that the amount of transparency provided does influence a prospects decision making when choosing a cloud vendor.

Table of Contents

1. Introduction

Cloud computing is a powerful technology to perform massive-scale and complex computing (Hashem et al., 2015). It offers advantages such as virtualized resources, parallel processing and security. Additionally, enterprises can benefit from reduced infrastructure management maintenance costs, efficiency, and improved user access (Lu et al., 2013). There are a wide variety of major companies that offer cloud computing such as Google, Amazon and Microsoft (Harvey, 2016). According to Gartner (2009) cloud services are offered on three different levels:

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

Taking google as an example, on the SaaS level you have the Google Apps, on the PaaS level you will find the Google App Engine and, finally, on the IaaS level there is the Google Cloud Storage.

There are several deployment models for the cloud: Public Clouds, Private Clouds, Community Clouds and Hybrid Clouds. The first two are the most common forms. It is expected, however, that the hybrid cloud model will get a more important role in the near future. The hybrid cloud is a combination of the public cloud and private cloud. With the public cloud model the cloud infrastructure is made available to the public and is operated for groups of organizations with similar service requirements, while with the private cloud model the infrastructure is operated solely by a single organization (Papazoglou, 2012). The key difference between the last two is that public clouds offer tremendous elasticity, which means “the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible” (Herbst et al., 2013), which leads to improved business agility and speed, lower costs, speed to serve and high performance computing (Kisker, 2010). However, private clouds offer less risk. Therefore, the likelihood of a data

security, privacy, and control breach is higher for the public cloud compared to the private cloud. To minimize this risk, audit frameworks and IT governance should exist. For the rest of this paper, the combination of audit frameworks and IT governance will be called governance models.

1.1 Problem statement

The central research question is:

> *"How are the IT governance models different from each other in relation to cloud computing?"*

The sub questions are:

- *How are the IT governance models different from each other without cloud computing?*
- *What risks does cloud computing bring?*
- *What are the challenges major cloud computing companies face when adopting IT governance models to meet their quality standards?*
- *Case study: How can the current service levels, quality frameworks and certifications be retained or complemented with cloud specific quality and security frameworks when offering application services based on public cloud infrastructure, while keeping the management tooling on the private infrastructure?*

1.2 Business relevance

As previously mentioned, cloud computing offers advantages such as business agility and speed, lower costs, speed to serve and high performance computing (Kisker, 2010). Many companies that currently only offer private cloud services must adapt to the competitive environment and start to also offer their services for public cloud services to stay relevant in the market. Many challenges are faced to achieve this transition, one of them being the way IT auditing and IT governance takes place. How

can a company provide services for the public cloud and keep, for example, their SLA's, ISO- and SAP-certifications they obtained by offering private cloud services? What arrangements do you as a service provider make with a large cloud computing hosting company like Amazon? One example being: How do you get your data back out of the cloud after terminating your contract?

1.3 Scientific relevance

Cloud computing has the potential to transform a great part of the IT industry by delivering services such as utility computing (Fox et al., 2009). 2The main issue that arises with information security in the cloud environment is the enterprise's loss of control and loss of governance over assets and information. This is the reason why Information Security is considered to be the main drawback that could prevent organizations from adopting cloud computing (Gens, 2009). Having the correct IT governance models could solve this.

1.4 Research design/method

The first two supportive sub questions will be answered using information available from previous academic research. Additionally, the way the telecom service provider manages their IT governance models will be taken into account as well, since these will be extensively discussed in the case study later. The third supportive sub question will be answered by getting in touch with major cloud computing companies such as Amazon and Microsoft. Questions will be asked regarding how they deal with the challenges they face with information security in the cloud. This will be followed by an in-depth analysis of the results. Finally, a case study will be done to check how the current service levels, quality frameworks and certifications can be retained or complemented with cloud specific quality and security frameworks (COSO, COBIT, ITIL, ISO 27000, ISAE 3402, CCM) when offering application services based on public cloud infrastructure, while keeping the management tooling on the private infrastructure. This will be done by making a comparison between the frameworks to find out how they differ from each other in relation to cloud computing. The IT governance models will be tested to see if they comply with the requirements needed to be suitable to be used with

cloud computing, while offering the same service levels without. Finally, a use case from the telecom service provider will be applied to the cloud governance dial developed by Becker and Bailey (2014) to test its effectiveness. After having done the case study answering the main problem question will be possible and advice can be given accordingly.

1.5 Structure of the paper

The remainder of this paper is organised as follows. The literature review starts with Chapter 2 which focusses on Cloud computing. This is followed by Chapter 3 where different IT governance models will be analysed. Having reviewed both Cloud computing and IT governance models makes it possible to talk about Cloud governance (CG) in Chapter 4, which is also the last chapter of the literature review. Chapter 5 an analysis will take place of the governance models and is followed by a case study in Chapter 6. Finally, the discussion and limitations will take place in Chapter 7 and the conclusion and recommendation can be found in Chapter 8.

2. Cloud computing

Figure 1 shows a brief overview of all the functionalities that current information technology services have and the additional features that Cloud computing bring, which were mentioned in the introduction of this paper. Cloud computing drastically reduces the upfront costs of computing that are normally associated with deploying leading-edge IT services (Staten, 2009). These costs are dramatically reduced due to one of the two major trends that are currently happening in information technology: IT efficiency. Cloud computing offers highly scalable hardware and software resources that can be shared by different end users, each of whom can use it its own way (Marston et al., 2011). The flexibility of the infrastructure allows balancing the computing loads while more people make use of the systems. The other major trend in information technology is business agility. Cloud computing can be used as a competitive tool for rapid deployment, parallel batch processing, use of compute-intensive business analytics and mobile interactive applications that respond in real time to user requirements (Kim, 2009).

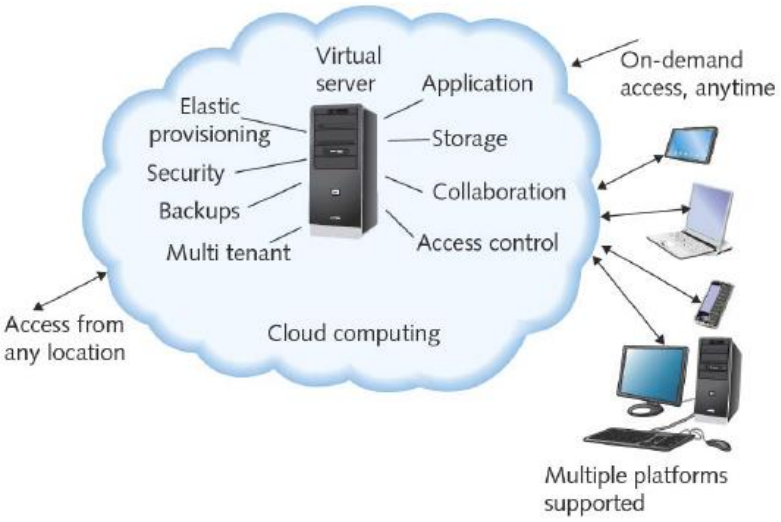

Figure 1: Cloud computing overview (Lalond, 2013)

Cloud computing, however, is not a matter of simply adding an endless number of servers. Most business applications rely on consistent transactions supported by Relational Database Management Systems (RDBMS) which do not scale. These require different architectures of storage, memory and processing (Hofmann & Woods, 2010).

A research done by KPMG (Lepeak, 2011) has shown that initiatives in the field of governance are the primary means for companies to improve a sourcing relation. Many

organizations look for guidance when creating a technology roadmap. They need to know which applications are best positioned for moving to the cloud and how these changes can be implemented while having the least disruption possible. Marginal functions, such as IT Management Applications and Personal applications, are often outsourced to the cloud while core activities are kept in-house (Dillon et al., 2010). Additionally, opposed to other sourcing alternatives, there needs to be more attention for compliance, security and risk aspects in the service level agreements, because services are being managed outside the clients' company, giving clients less control over their data than in other scenarios. The security check-list should include all aspects of security requirements including legal issues, physical security, policy issues and technical issues when adopting the cloud (Cattedu, 2010).

2.1 Risks Cloud Computing

Risk is a very important factor to take into consideration during the deconstruction of the cloud. During a research done by Westerman (2006), which was funded by the Center for Information Systems Research (CISR) department of the Massachusetts Institute of Technology (MIT), four key enterprise IT risks were described:

Availability – integration management. Architecture must be designed beforehand and should clearly indicate the spaces to be filled with the cloud services at all levels. The integration management of cloud services includes coordinating the interoperability of in-house and cloud services, applications and infrastructure. SLAs must contain rules regarding cloud uptime to ensure continuity. Ways to achieve availability are business continuity and disaster recovery.

Access – risk management. New areas including data handling, interface management, multi-tenancy, and security and legal compliance for sensitive data require risk management. Well defined SLAs could address most of these risks. Information protection, knowledge sharing and preventing malicious attacks are all ways to optimize access.

Accuracy – data integrity and regulatory compliance. Different classes of data may be subject to different policies and legal rules. Cloud Service Providers (CSP) have several

ways to show their clients that they handle their data carefully and correctly. This could be done my means of certification, audit controls, trust and transparency of controls or a combination of these. It is a challenge for CSPs to comply with all international regulations and policies which is necessary for trans-border information flows. To achieve a high level of data accuracy and consistency regulatory compliance is necessary.

Agility – corporate cultural impact. In the past IT services were seen as a costly utility which were necessary. Nowadays, with the uprising of cloud computing, IT services are more often seen as a strategically aligned tool for reducing costs, but also as a driver for innovation and contributing to business value. Part of agility is the ability to implement major strategic change.

These four key enterprise IT risks were later used as a foundation for research done by others and similar key risks were found by Moeller (2007) whom did a portfolio view of enterprise risk management for COSO. Taking care of these four key enterprise IT risk factors should help the CSP to take care of the security issues that customers should raise with vendors before selecting a cloud vendor according to Gartner (Brodkin, 2008):

- *Privileged user access (Access)* – Gartner says it is important to ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.

- *Regulatory compliance (Accuracy)* – Customers themselves are responsible for the security of their own data even when it is held by the CSP. Whenever the CSP does not undergo external audits it might be a better idea to look further.

- *Data location (Availability and Access)* – As a customer you have no idea where exactly your data is hosted and might not even know in which country. Gartner tells prospects to ask the CSP if they are willing to commit to storing and processing data in specific jurisdictions and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

- *Data segregation (Access and Accuracy)* – Data in the cloud is usually placed in a shared environment. It is important to find out what the CSP does to segregate the data.

- *Recovery (Availability)* – Even though Cloud computing is advertised as being available anywhere and anytime, it is important to know what will happen with your data in case of a disaster.

- *Investigative Support (Access)* – Since multiple customers use the data warehouse of the CSP, it is important to find out how the CSP log every event in case an investigation is necessary for your own company.

- *Long-term viability (Agility)* – It is important for customers to know the CSP will exist for many more years and will keep adapting its strategy to the constantly changing environment.

- *Vendor Lock-In (Agility)* – Often not considered when looking for the right CSP are the possibilities to obtain the data back from the cloud in case the contract is terminated. Termination could occur due to multiple reasons: Changes in ownership, bankruptcy, soured relationships, data security and privacy breaches, fall behind its competitors, prolonged outages. Changing from CSP could also result in compatibility related issues with data, program and operation systems.

As can be seen above, all security issues mentioned by Gartner are covered by carefully considering the four key enterprise IT risk factors. The security benefits and risks will be discussed in a bit more detail.

2.2 Security Benefits

Cloud computing offers several security benefits according to Cody et al. (2008):

- The first advantage is that standardized interfaces are very common in cloud computing. Since many users make use of the same hardware and software, the

number of things that need to be secured are limited, making it easier to focus and allocate resources. This in comparison with non-cloud users, each using their own hardware and adjusted software.

- The second plus is the benefits of scaling. The same amount of investment for deployment of standard IS policy, filtering and patch management can provide a better protection for a wider audience.
- Finally, the last benefit is the rapidity of response to security attacks. Cloud computing providers are better capable of dealing with security attacks due to their specialization in data hosting opposed to individual companies.

In addition, Catteddu (2010) mentions some additional security benefits:

- More timely, effective and efficient updates and defaults. Updates can be rolled out many times more rapidly across a homogenous platform than in a traditional client-based system that relies on a patching model.
- Benefits of resource concentration. The concentration of resources is a disadvantage for security, but the advantages are an easier and cheaper application of many security-related processes and physical access controls due to scaling.

2.3 Security Risks

Besides the security benefits just mentioned, there are some important security risks that need to be considered when making use of cloud computing mentioned by Goo and Huang (2008):

- First, some clients of cloud computing providers have difficulties to check how their data is handled and therefore don't know if the data handling happens in a lawful way.
- Secondly, clients sometimes don't get insights in the very fine levels of security policy administration of the standardized interfaces cloud providers offer, mentioned as one of the benefits for security before, increasing the risks of a breach.

- Thirdly, SLA's created in the early stages might still have some gaps in security defences, making the client uncovered for certain liabilities. Deletion of data might be impossible to be carried out when the client asks for it, since hardware resources are often being reused and the many contracts.
- Finally, malicious insiders could offer much higher damages in the cloud, due to some roles that are high-risk by their nature and scope.

Another research done by Mosher (2011) found that data privacy risks, availability risks, service provisioning risks, malicious activity risks and regulatory compliance risks could negatively affect cloud computing security.

One of the last things business managers think of when implementing cloud computing is to have a revert strategy ready in case when the quality of service goes down or when the risks get too high. It is important to keep knowledge of all critical information and processing assets that are in the cloud. Additionally, there needs to be enough skills in-house to be ready to set up internal systems and services again when necessary. Finally, backups of critical cloud-based assets should happen on a regular basis (Speed, 2011).

For public cloud clients there is an extra risk to be aware of. It is important for these users to keep their valuable information encrypted and to stay alert at all times. Encrypting your data these days is a very common thing to do. However, there is still a risk when the data is being decrypted for processing, even while this is often only the case for a really short moment. Using traditional IT services, the use of intrusion detection, alerting and prevention techniques have been very common. With cloud computing, many of these tools are managed by the cloud provider, which is another risk to keep in mind when choosing for a public cloud provider (Speed, 2011).

Overall, transferring your data to the cloud brings many risks associated with the implementation and use for an organization. It is important for businesses to not only recognise the risks, but also create a strategy to manage and mitigate these (Paquette et al., 2010). This can be done by creating an optimal SLA contract design and well developed cloud governance (Bhoj et al., 2001).

To create a strategy to manage and mitigate these risks, it is important to know that there are three types of controls being: preventive, detective and corrective (Kliem, 2004). When looking at the cloud an example of preventive control is a firewall. An example of detective control is a logging tool that alerts the user when something unusual is happening. Finally, an example of a corrective control could be disaster recovery in case a data centre where your data is stored got damaged due to a natural disaster.

Every company wants to focus on prevention, but it is important to have controls in place for detection and correction as well in case something goes wrong with the prevention control. When looking at the cloud in specific, clients have less control over their data and therefore rely more on the controls the cloud vendors have to offer. The cloud vendor is responsible till the virtualisation when offering an IaaS service, making the client only responsible for the data. This means that some of the controls that were first managed by the client are now managed by the cloud vendor instead.

When taking a closer look at the detective control type this can take place either manually or automatically. Manual control is very time intensive, but still manageable for small companies with not much data. However, large CSPs have many clients and hold a lot of data which makes automated logging the only possible option. Therefore, it is necessary to automate processes such as logging

Finally, it is important to keep in mind that there are two levels of controls: general IT controls and application IT controls. General IT controls being IT governance models such as ISO and COBIT, while application IT controls are controls mechanisms on the application layer such as controls within SAP. It is possible that when making the transition to the cloud, the general or application IT controls required need adjustments.

2.4 General Data Protection Regulation

The 25th of May 2018 the General Data Protection Regulation (GDPR) will be implemented, which was developed by the European Parliament, the European Council and the European Commission with the intention to strengthen and unify data protection

for every citizen within the European Union and because of the risks associated with cloud computing. This new regulation will be replacing the EU Data Protection Directive from 1995 and adds several new principles and guidelines (EUGDPR, 2017). For example, they implemented the requirements for data portability and a stricter concept of consent (Blackmer, 2016). Probably the most noticeable change is the extended jurisdiction of the GDPR. The new regulation will apply to all the organizations that process personal data of data subjects residing in the European Union, regardless of the company's location. This means that it does not matter where in the world a company that is located in the European Union processes its data, it still must comply with the GDPR. The same counts for organizations that do not reside in the European Union. Whenever these companies process data of European citizens, they do have to comply with the GDPR (EUGDPR, 2017). Updated regulations were necessary for several reasons:

- The need to get rid of the discrepancies in national laws;
- Lower the organisational costs for companies that need to deal with multiple data protection authorities;
- Higher level of standards for privacy protection per individual;
- Update the law and principles accordingly for new privacy challenges that showed up between 1995 and now, such as social media, cloud computing and big data.

Since the implementation date is getting close, it is important for companies to look at the future and be one step ahead. Companies should have a new compliance landscape ready for all the processes in the organization to avoid any problems the day the new regulation is being enforced.

2.5 Cloud Service Providers

There are many CSPs that offer cloud computing services to organizations. Most offer services ranging from Infrastructure as a Service till Software as a Service. Amazon, Google, Microsoft and SAP belong to one of the larger providers in this area (Harvey, 2016). Table 1 gives an overview of what each of these four providers has to offer.

The differences in table 1 can be explained. Google is relatively new to offering cloud services which explains why some services and certifications are not available yet. Amazon is the largest cloud service provider today with a lot of experience which explains why all the certificates and services mentioned in the diagram are included.

Certificates/Services	Amazon	Google	Microsoft	SAP
ISO 9000 series	✔		✔	✔
ISO 27000 series	✔	✔	✔	✔
ISAE 3402	✔	✔	✔	✔
CCM	✔	✔	✔	✔
SaaS	✔			✔
PaaS	✔		✔	✔
IaaS	✔	✔	✔	✔
SAP	✔	✔	✔	✔
Microsoft apps	✔		✔	
Oracle	✔		✔	

Table 1: Cloud Service Providers overview

3. IT governance models

Because of several high profile incidents of corporate fraud and failure in the past couple of years, corporate governance has gotten much more important than before. With IT becoming more often one of the fundamental tools of an organisation this lead to a new type of governance: IT governance (Mcleod, 2013).

ISACA developed a helpful guide which separates IT governance into five different domains (ISACA, 2013) which are:

1) *Framework for the Governance of Enterprise IT*
   The IT governance framework needs to be in continuous alignment with the enterprise governance and the key drivers directing the company's strategic planning, goals and objectives

2) *Strategic Management*
   Business strategy must drive IT strategy. The strategies of business and IT should be aligned properly.

3) *Benefits Realization*
   IT governance helps business realize optimized business benefits by means of effective management of IT investments.

4) *Risk Optimization*
   Identification, management, mitigation, communication and monitoring of IT related business risk are integral components of governance activities.

5) *Resource Optimization*
   IT requires sufficient, competent and capable resources to meet business demands and to meet current and future strategic objectives.

3.1 Overview of IT governance models

There already exist many control frameworks and models. None of them, however, includes all the available IT controls. Analysing them together shows us the "what, how, and scope" of IT governance and that some repetition between the frameworks is present (Becker, & Bailey, 2014).

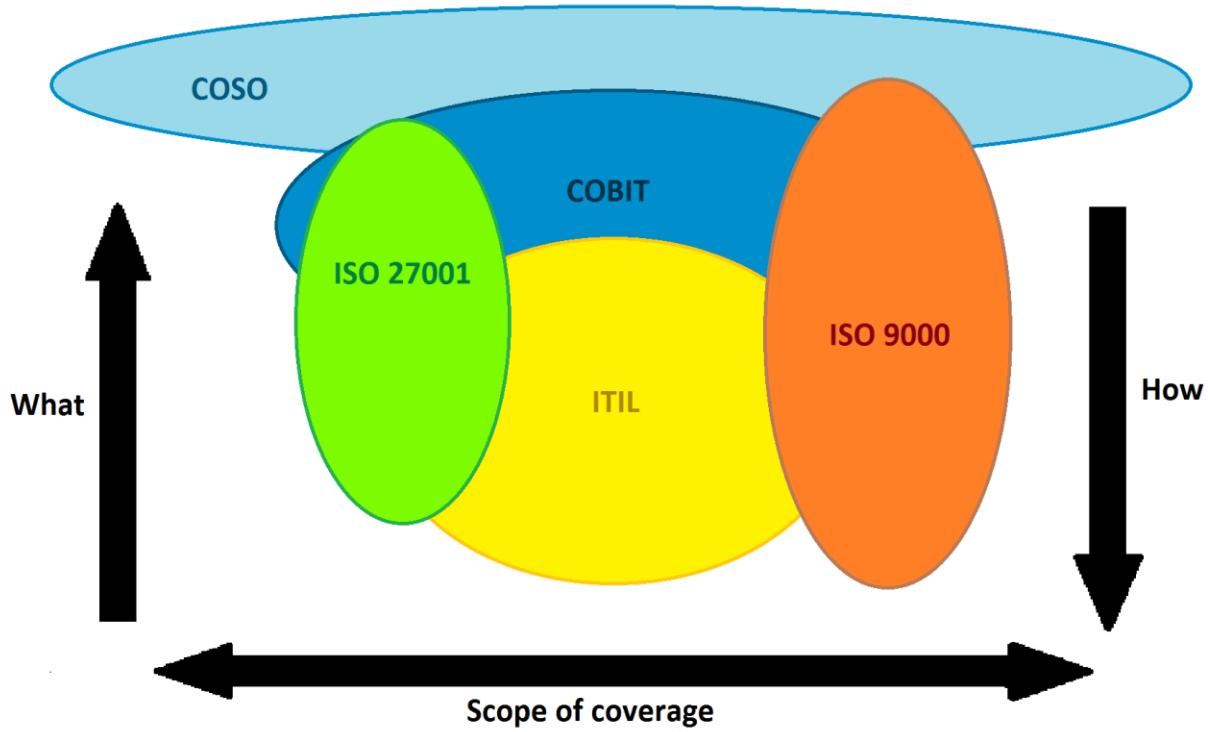

Figure 2: General "what, how, and scope" of IT governance models (Nguyen, 2010)

Figure 2 shows the relationship between some popular IT governance models, which will be explained briefly in the upcoming paragraphs. This figure is based on a general analysis and widely accepted by many business people and researches. Making use of more governance models at once leads to a higher scope of coverage, which is why in many companies there is more than one IT governance structure/framework being used. Each structure/framework has its own principles which need to be followed which could cause some complex situations.

Frameworks	Type	Covering	Goal	Implementation
ITGI/ISACA **COBIT** (business-oriented)	Best Practice (process-based)	*What* 4 Processes and 34 Domains	Measuring and assessing IT controls	Take into account broad view of whole system, then implementation
ISO and IEC **ISO 27000 Series**	Security Standard (Combination of standard and best practice)	*What* 10 Domains (ISO 27001)	IT Governance	Take into account broad view of whole system, then implementation
UK Government **ITIL**	Best Practice (IT service-based)	*How* 9 Processes	Improve internal IT services	Checklists and guidelines (Easiest to implement)
IAASB and IFAC **ISAE 3402** (Similar to SAS70)	Assurance Standard	*How* 5 Domains	Document that external parties of financial service organisations have adequate internal controls	Analyse the current situation, then implementation where necessary
COSO **COSO**	Internal Control	*What* 5 Key components, 17 Principles	Combat Corporate Fraud	Implement at business unit, division, subsidiary or entire organization level
CSA **CCM**	Security standard	*How* 13 Domains	Provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.	Take into account broad view of whole system, then implementation

Table 2: Overview of IT governance models

Table 2 shows a brief overview of the IT governance models seen in figure 2 and two additional frameworks which are relevant for cloud computing. All this information in the table is obtainable by visiting the websites of the owners which are mentioned above each framework in the first column.

As mentioned earlier, each framework offers different IT controls and thus has different goals and way of implementation. Figure 2 is a visualization of table 1 and looking at the third column *Covering* explains the placement of the "what, how, and scope" axis.

For example, COSO consists of five very broad defined key components that cover many different topics, which results in a very wide scope. This is followed by COBIT which consists of 34 different domains. Each domain covers only a very small part of the whole scope opposed to COSO's key components, but due to the number of domains the scope is still very wide. The wide scope comes at the expense of the "what and how" of both frameworks. Many different topics are covered, but for each specific topic not much explanation is given what to look out for or how to prevent something from happening.

The ISO 27000 series and ITIL, opposed to COBIT, have only a few domains, but these domains consist of many processes which gives a detailed understanding of the "what and how" of the topic discussed. The ISO 27000 series focusses on what should be covered to achieve a security standard while ITIL tells you how best practice can be achieved following their framework.

Each framework will be briefly discussed in the next subparagraphs to give more understanding of what their goal is and what exactly each framework has to offer. In chapter 5 a new figure similar to figure 2 will be made which will show the relationships of the frameworks with the "what, how, and scope" in relation to the cloud and will include ISAE 3402 and CCM, which were not included in figure 2.

3.2 COBIT

COBIT was first released in 1996 and stands for Control Objectives for Information and Related Technology. The latest version, COBIT 5, was published in June 2012. According to ISACA (2012) its mission is "to research, develop, publish and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals." Initially, COBIT was an audit framework but eventually evolved in a powerful IT Governance control model.

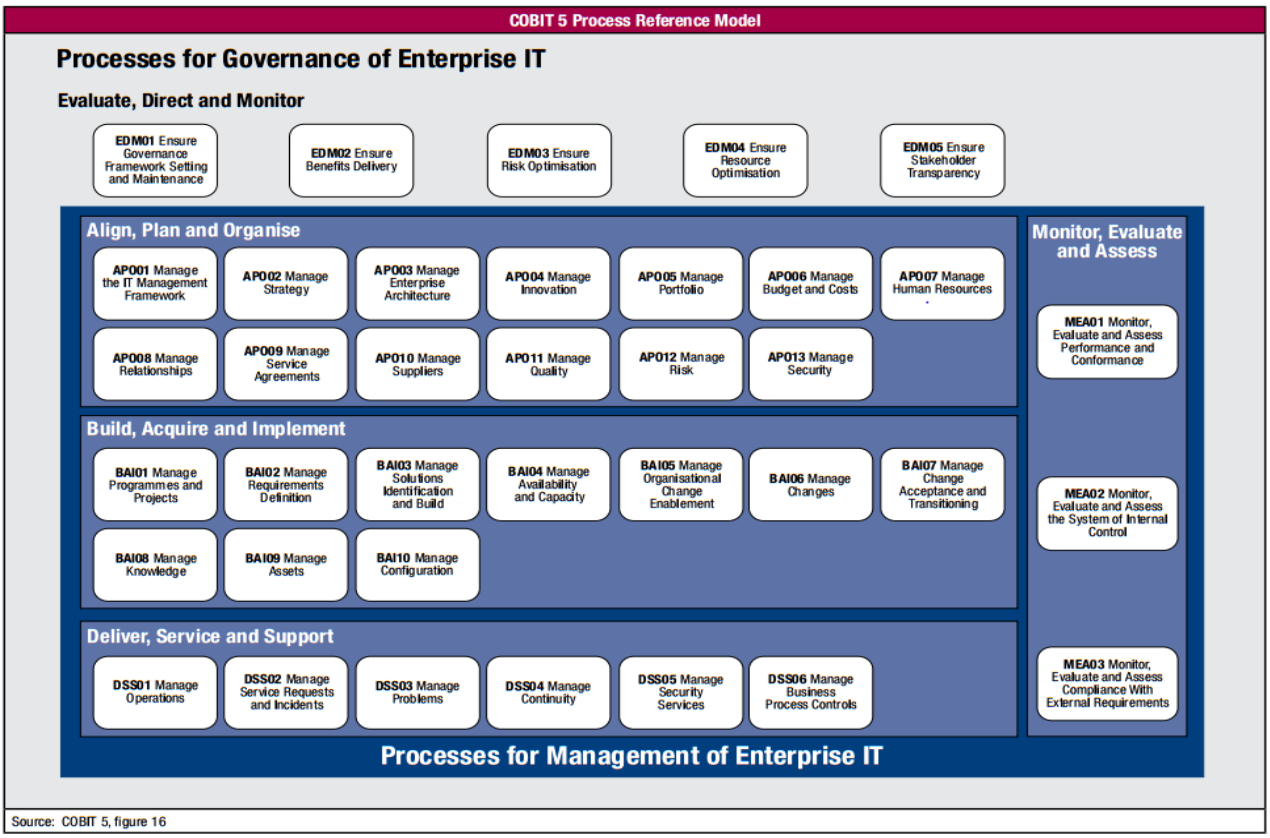

Figure 3: COBIT Framework (ISACA, 2012)

As seen in figure 3, the COBIT 5 framework evaluates, directs and monitors on the governance level ensuring enterprise objectives are achieved. Management plans, builds, runs, and monitors activities on the management level to achieve enterprise objectives.

The process “DSS05 Manage Security Services” is relevant for information security governance. The advantage of using COBIT as IT governance structure/framework is that the DSS05 process is part of a wider framework, which means it will seamlessly integrate with the other processes in an organization (Von Solms, 2005). A disadvantage, given by Von Solms (2005), is that the COBIT information security governance processes are not always very detailed by means of “how” things in a company should be done.

3.3 COSO

COSO was created in 1992 as a result of several large audit failures that occurred during the 1980s. The Committee of Sponsoring Organizations said that the COSO framework “defines internal control as a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following three categories: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations” (Simmons, 1997). These three categories do overlap, yet they are distinct from each other. The framework consists of eight components for internal control which can be seen in figure 4. An empirical examination of COSO as an internal control framework for information technology done by Tuttle and Vandervelde (2007) found that covering COSO’s conceptual model onto audit relevant assessments confirmed internal consistency between the fundamental constructs of COSO.

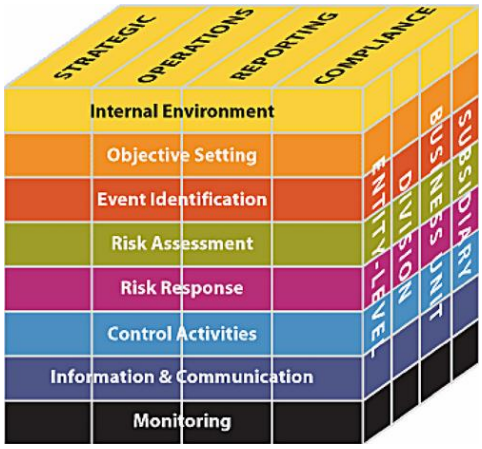

Figure 4: COSO Framework (COSO, 2004)

3.4 ITIL

The Information Technology Infrastructure Library (ITIL) is a framework outlining the best practice in ICT Service Management which was originally made by the UK government. The latest version, ITIL V3, was published in 2008 (Case, & Elephant, 2007). As seen in figure 5, the framework is based on continual service improvement. In a study done by Potgieter et al. (2005) was found that when an organization uses the ITIL framework it increases both customer satisfaction and operational performance.

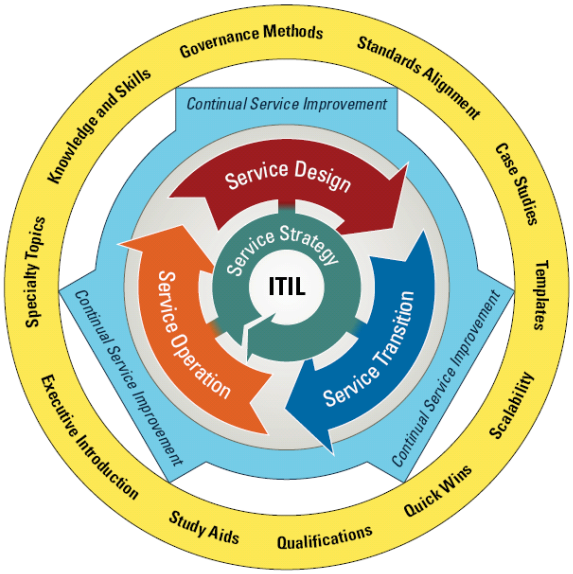

Figure 5: ITIL V3 (Suhairi, & Gaol. 2013)

3.5 ISO27000/9000

ISO is the international standards organization which is an independent, non-governmental international organization with a membership of 164 national standards bodies (Disterer, 2013). The ISO 27000 series of standards offers cloud risk assessment tools. ISO 27001, for example, is the best practice for Information Security Management Systems (ISMS). ISO 27017, which is still in development, will include cloud-specific security controls, besides the information security controls present in ISO 27002 (Beckers et al., 2011).

The ISO 9000 series of standards offer the guiding principles for the prevention of defects through the planning and application of best practices at every stage of the business, ranging from design till the installation and servicing (Rahman, 2001). ISO 9001, which is relevant for CG, provides the definitions of the characteristics and associated quality evaluation process to be used when specifying the requirements for and evaluating the quality of software products throughout their life cycle (Becker, & Bailey, 2014).

Both ISO series of standards show relevancy regarding IT governance and cloud computing. Where the ISO 27000 series offer cloud risk assessment tools, ISO 9000 focusses on the governance for cloud software requirements and quality, making them complement each other.

3.6 ISAE 3402

ISAE 3402 is globally recognized standard for assurance reporting on service organizations. It requires management to provide a description of its system. Additionally, a written statement of assertion is required by management regarding the state of its internal controls (Fanning, 2014). A major difference between the previous mentioned ISO 27001 and ISAE 3402 is that ISO 27001 is a certification and does not have a testing framework, while for an ISAE 3402 audit the financial statements are the basis and the assessed framework (SasConsult, 2017).

There are two types of ISAE 3402 reports (Elifoglu et al., 2014):

- *Type I*: This report includes management's description of a service organization's system and the suitability of the design of controls at a given moment in time.

- *Type II*: This report deals with the design and operating effectiveness of controls for a time period, such as a month or quarter. Type II is usually preferred due to its scope.

The auditor's task is to publish a report which is called: Service Organization Control (SOC). This report focusses on the design and description that may be relevant to the user entities' needs. These reports can be divided into three different forms (Elifoglu et al., 2014):

- SOC 1: These reports require a detailed description of the service organization's controls that are likely to be relevant to a user entity's internal control over financial reporting system along with a written assertion by management. Service organizations such as payroll processing and medical claim processing are the best candidate for SOC 1 reports.

- SOC 2: The SOC 2 reports are intended to deal with the problems that are related to the expanding computer based service entities, examples being data centres and cloud computing. It provides assurance about confidentiality, processing integrity, privacy, security and availability to the users that use the service. When SOC 2 is combined with the ISAE 3402 type II report a description of the service auditor's tests of controls and the results of these tests will be given.

- SOC 3: Opposed to SOC 2, which is not distributed to other users such as sub-vendors without the permission of service organization, SOC 3 reports are a general-use report that can be freely distributed. SOC 3 reports can only been made as type II reports, while the other two versions can also be designed using the type I report method. The SOC 3 report provides only the auditor's report on whether the system achieved the trust services criteria. No descriptions of tests and results or opinions are given on the description of the system. Usually, when a company successfully completes an ISAE 3402 SOC 3 type 2 report, it can place a certificate on their website.

Suhairi and Gaol (2013) did research regarding the effectiveness of the new ISAE 3402 framework and concluded that there is scope of improvement in the new standards. The new auditing standard is, however, still missing a guide of specific control objectives which can be found in the ISO27001 and COBIT frameworks. They recommend using the COSO or COBIT report as a reference for service auditors and their clients when making use of this new framework.

3.7 CCM

The Cloud Control Matrix (CCM) is designed by the Cloud Security Alliance to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The matrix should establish a better understanding and trust level between the cloud customer and cloud provider (Saxena, 2013).

The CCM delivers a controls framework that consists of thirteen domains which put emphasis on business information security control requirements, reducing and identifying consistent security threats and vulnerabilities in the cloud, provides standardized security and operation risk management, and seeks to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud (Cloud Security Alliance, 2017).

One of the domains deals with compliance concerns for regular audits, inspections and reviews of data, objects, application, infrastructure and hardware at regular intervals. These audit activities need to be planned by the cloud provider and the stakeholders should agree with this in advance (Saxena, 2013).

Cloud computing also results in a higher level of virtualization. The data may be under the organization's logical control, but may physically be present in the infrastructure owned and managed by another entity (Vormetric, 2017). The Data Governance domain handles all the possible scenarios of data theft, retention, leakage, misuse, disposal and related risks. The ownership of data and objects containing data are defined in this domain.

Additionally, the Cloud Control Matrix outlines policies and procedures for management authorization for development and acquisitions of new services, databases, applications, systems, facilities, operations and infrastructures. When changes are made to the production environment these need to be documented, tested and approved before implementation takes place. A program needs to be established for the systematic monitoring and evaluation to ensure the standards of quality are met for all software developed.

Furthermore, the other domains focus on the employees, the physical locations, the legal aspects of cloud services, risk management and continuity and availability.

3.8 GDPR

The General Data Protection Regulation (GDPR) created by the European Union will be implemented next year and it is important that companies use the right frameworks that are compliant with the new regulation.

Under GDPR a company is always legally responsible to protect personal data from alteration, loss or unauthorised processing, even when employees use cloud services that are not approved or controlled by the organisation. For this reason an organisation must (Terstegge, 2015):

- Know which personal data are processed by users of cloud services;
- Identify the cloud applications used by the organisation's employees;
- Prevent personal data from being stored or processed in unmanaged cloud services;
- Protect personal data when stored or processed in cloud services.

Terstegge defined six questions which help clienteles that want to use the cloud in their business to find out if the provider is GDPR compliant:

1) Do you know where your cloud apps process and store data?
2) Does the app adequately protect personal data from loss, alteration, or unauthorized processing?
3) Have you executed a data processing agreement with the cloud apps you are using?
4) Does the app only collect "necessary" data and limit processing of "special" data?
5) Are you sure the vendor forbids the use of personal data for other purposes?
6) Do you know if you can erase the data when you stop using the app?

When looking at the models that were just discussed the ISO 27000 series, in specific ISO 27001 and ISO 27002, seem to be the most compliant with these new regulations (Henning, 2016). The GDPR does not say that companies must comply with the ISO 27000 series, but it provides a framework to handle concepts such as security policy and objectives, risk definitions and assessment, commitment for continuous evaluation and documentation (Bartolini et al., 2015). For this reason, it is recommended for every company that has to fulfil the GDPR requirements to securely handle personal data to comply with ISO 27001 and ISO 27002. They do, however, not cover all rules of the

GDPR. This raises the question whether the other rules, which are not covered by ISO 27001 and ISO 27002, will affect the way business takes place.

3.9 Hypotheses related to IT governance

To summarise, cloud computing offers several security benefits but also some security risks which were mentioned in section 2.3. Most IT governance models were developed before the existence of cloud computing. This raises the question whether these frameworks can effectively take care of these new security risks. This leads to the following hypothesis:

Hypothesis 1: The IT governance models discussed in chapter 3 effectively deal with the cloud specific security risks mentioned in section 2.3.

The GDPR was developed to create more digital privacy for all individuals within the European Union. Several requirements must be met. The question is whether the GDPR will make it necessary to change business process of a company. The following hypothesis is formulated:

Hypothesis 2: The General Data Protection Regulation significantly impacts the current cloud specific business processes of a company.

4. Cloud governance

Governance in the cloud requires defining policies and implementing an organizational structure with well-defined roles for responsibility of information technology management, business processes, and applications as these elements are moved out of the traditional IT environment in the cloud (Becker & Bailey, 2014). Governance is not a one-size fits-all proposition, the structure and the scale must take into consideration the maturity, culture of the IT organization, complexity and enterprise goals. Moving IT governance to the cloud increases the difficulty of effective governance (Dreyfuss, 2009). Clients have to accept the control of the service provider on a number of important issues and areas of the business process (Mangiuc, 2011).

4.1 Extending IT governance to the cloud

According to Dreyfuss (2009) the new cloud environment is very different from traditional outsourcing and requires a new approach to governance and management. There are important risks that should be analysed before migrating to the cloud such as:

- Internal threats;
- Horizontal audit compliance;
- Performance metrics;
- Security;
- Accountability and responsibility.

To deal with internal threats, standards, interfaces, controls and integration requirements should be addressed with policies and procedures that tell how everything fits together. Horizontal audit compliance gives an overall view of all business units and unifies the information streams which help businesses to find vulnerabilities across the company. Measuring performance internally and externally offers insight into areas that have been identified for IT-business alignment and can serve as an early warning system for risk and security, which is important when dealing with the SLAs that are made between the CSP and the client. Additionally, organisations often want to be sure

that security control is present when moving to the cloud which can be shown by means of certifications and transparency.

Achieving accountability in the context of cloud computing requires mechanisms that result in trust and security. These mechanisms range from auditing, tracking and reporting and monitoring till contracts and service level agreements. It is the customer's responsibility to enforce these mechanisms and to ensure successful implementation. Some IT responsibilities are taken away from the client, but governance is not one of them. The customer must be able to monitor the data handling practices of the provider by means of certification and control activities (Mangiuc, 2011).

A tool developed to clarify the roles and responsibilities associated with cloud deployment is the RACI matrix, the abbreviation stands for:

- Responsible: Who is responsible for a task;
- Accountable: Who will be held accountable for task completion;
- Counsel: Who will provide the information needed;
- Informed: Who is dependent of the information.

Based on the previous literature the following hypothesis can be formulated:

Hypothesis 3: The IT governance models cover the risks faced when migrating to the cloud.

The question is: Till what extend are the IT governance models already developed to deal with the changes that come along when extending IT governance to the cloud? Having an answer to this question for each framework helps us in finding the differences between the frameworks in regards to the cloud.

4.2 Deconstructing the cloud

The Cloud Governance Dial created by Becker and Bailey (2014) allows the organization to align the cloud solution with stated business values and deliver that added value through optimal resource allocation and performance management.

To build such a model, they first had to deconstruct the cloud to get a better understanding. The deconstruction started assessing each application domain or business process individually using the Cloud Computing Service Delivery and Deployment Model (Cloud Security Alliance, 2009) and asking the following questions:

1. What (process) is moving to the cloud? (Application domain or business process)
2. How will it be delivered? (SaaS, PaaS, IaaS)
3. How will it be deployed? (Public, Private, Hybrid)

Having given an answer to these questions results in a cube. The next step for deconstructing the cloud is to position the cube within the Cloud Cube Model developed by Rebollo et al. (2012) which can be seen in figure 6. To do this, four more questions need to be answered:

1. Where will the data be located? (Internal or External)
2. Who owns the technology, services, and interfaces? (Proprietary or Open)
3. Are there expectations of collaboration and data sharing?
4. Who is managing the delivery? (Insourced or Outsourced)

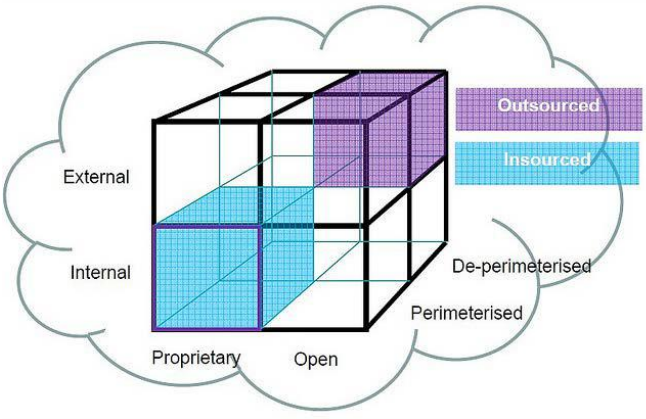

Figure 6: Jericho Forum Cloud Cube Model (Jericho Forum, 2013)

Having answered all above questions will lead to a set of governance challenges. Not every outcome will lead to specific ERM and Control frameworks. Many risks management and control objectives are common in many cloud outcomes.

4.3 Cloud Governance Dial

The Cloud Governance Dial developed by Becker and Bailey (2014), focusses on the five IT governance domains while producing the associated product as they apply to cloud adoption. The processes can be visualised as six dials as seen in figure 7 and are as follows:

1. Process: What is moving to the cloud;
2. Delivery: Identify IT governance domain objectives and deliverables;
3. Deployment: How will it be delivered;
4. Cloud Formation: How will it be deployed;
5. ERM: Determine the cloud formation;
6. Control: Cloud governance.

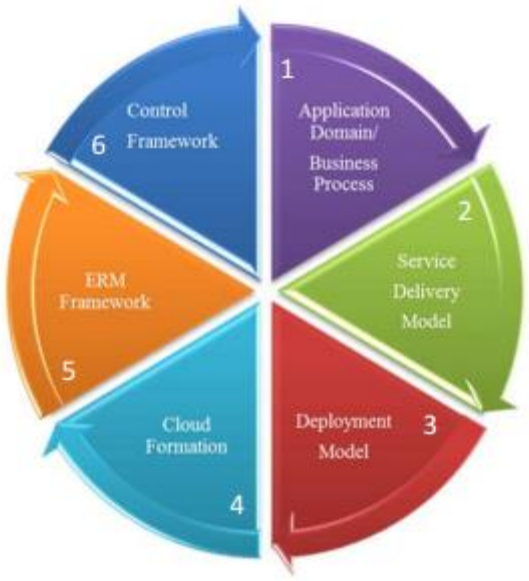

Figure 7: Cloud Governance Dial (Becker, & Bailey ,2014)

As the model, which can be seen in figure 7, shows, several other steps are necessary before the CG for a specific case can be selected. It needs to be clear which type of service the user is interested in (SaaS, PaaS, or IaaS) and the type of cloud (Private, Public, or Hybrid) they want to use. Based on the first four steps, the risks mentioned in chapter 2 can be elaborated on in more detail for the specific case during step 5. During step 6 the current IT governance framework should be reviewed and modified based on the results from step 5. According to Becker and Bailey (2014) it is often not needed to replace an effective, well-designed IT governance framework.

The Cloud Governance Dial is a new model which, to our knowledge, has not been tested in practice thus far. Therefore, the effectiveness of the model is still questionable and the following hypothesis can be formed:

Hypothesis 4: The Cloud Governance Dial is a viable model to meet IT governance goals and achieve alignment with corporate governance.

4.4 Cloud Service Providers

In chapter 2.5, Amazon, Google, Microsoft and SAP cloud services were compared to find out the differences between the companies regarding certifications and service offerings. It was noticeable that each of these companies has a different governance mechanism in place.

4.4.1 Amazon Web Services

Amazon Web Services (AWS) offers a security platform that includes: Infrastructure Security, DDoS Mitigation, Data Encryption, Inventory and Configuration, Monitoring and Logging, Identity and Access Control, Penetration Testing (Amazon Web Services, 2017). When looking at AWS Cloud Compliance in specific, there are many different certifications and frameworks they offer with their services. The certifications and frameworks AWS has to offer for their services and that were reviewed in this literature are: ISO 9000/27000 series, ISAE 3402 SOC 1/2/3 and they completed the Cloud Security Alliance STAR Self-Assessment, got an CSA STAR attestation and certification for CCM.

Around 2010, AWS first released a new type of deployment model called Virtual Private Cloud (VPC) to differentiate itself from other CSPs. This model is supposed to create a seamless and secure bridge between a company's existing IT infrastructure and the Amazon public cloud. Since there is a combination of the public cloud and private cloud it is a hybrid cloud model. The connection between the IT legacy systems and the cloud is secured via a Virtual Private Network (VPN). Additionally, AWS offers a set of isolated resources for the VPC, while still benefiting from the pay-per-use model. As a result, there is a balance between control (Private Cloud) and flexibility (Public Cloud) (Dillon et al., 2010).

4.4.2 Google Cloud Platform

The Google Cloud Platform (GCP) offers a rich set of capabilities around access control, auditing and encryption key management to enable customers to defend against external attacks and manage insider access risk. The Google Security Model consists of: Information security team, physical security at data centres, server and software stack security, data security and many platform security features (Google Cloud Platform, 2017). Focussing on the compliance Google offers for their services, they comply with the following frameworks and certifications that are mentioned in this paper: ISO 27000 series, ISAE 3402 SOC 1/2/3 and they completed the Cloud Security Alliance STAR Self-Assessment for CCM.

4.4.3 Microsoft Azure

Microsoft has as guiding principle for their security strategy to “assume breach”. They have many methods for securing customers’ data being: Auditing and logging, cybercrime, design and operational security, encryption, identity and access management, network security and threat management (Microsoft Trust Center, 2017). When looking at compliance, Microsoft Azure offers the following frameworks and certifications: ISO 9000/27000 series, ISAE 3402 SOC 1/2/3 and they completed the Cloud Security Alliance STAR Self-Assessment, got an CSA STAR attestation and certification for CCM.

4.4.4 SAP

SAP regularly checks compliance through external reviews and audits and follow one common framework, including data security and privacy regulations, worldwide (SAP Cloud Trust Center, 2017). Their framework and certifications offering varies a lot. ISO9000/27000 series, ISAE 3402 SOC 1/2/3 and the Cloud Security Alliance STAR Self-Assessment are all included.

4.5 Transparency

When deciding which public cloud provider to go for, it is important to look at the transparency they offer. Providers have different methods to provide transparency (Speed, 2011):

- *Nondisclosure agreements*:
  Many cloud providers don't like to share much information on their architecture, security and controls with outsiders. However, when there is a prospect that would like to make use of their services, a nondisclosure agreement could be signed and the information needed to convince the prospect could be given resulting in possibly a new customer.

- *Independent auditor reports*:
  Many CSPs ask independent auditors to assess the design and operation of the controls used by the service provider and to make these assessments available for their customers in the form of an independent audit report.

- *Certifications*:
  An easy way to compare providers is by looking at the industry certifications. Some relevant certifications related for cloud computing providers are ISO 27001, ISO 27002, and ISO 31000.

Besides transparency offered by CSPs, some standard services should be provided. Kaufman (2009) proposes in his study that providers should offer at least: strong access control, regularly scheduled data backup and archiving services and trusted encryption mechanisms. Offering this should give more assurance to the clients and trust in the providers.

Security-as-a-service and governance-as-a-service (InfoWorld, 2009) are a must for cloud computing, which requires solutions that address the need for policy-driven enforcement, segmentation, isolation, governance, and service levels (Farrell, 2010).

For clients transparency given by the cloud service provider is very important. The question is, however, whether this influences a client's decision making or this becomes negligible when a cloud service providers excels in other important factors. This leads to the following hypothesis:

Hypothesis 5: The amount of transparency provided by a Cloud Service Provider does influence the potential client's decision making.

4.6 Summary of hypotheses

Table 3 shows a summary of all hypotheses:

	Hypotheses	Source
1	The IT governance models discussed in chapter 3 effectively deal with some cloud specific security risks mentioned in section 2.3.	(Goo & Huang, 2008) (Becker & Bailey, 2014) (Mosher, 2011)
2	The General Data Protection Regulation significantly impacts the current cloud specific business processes of a company.	(Blackmer, 2016) (EUGDPR, 2017) (Henning, 2016)
3	The IT governance models cover the risks faced when migrating to the cloud.	(Dreyfuss, 2009) (Mangiuc , 2011)
4	The Cloud Governance Dial is a viable model to meet IT governance goals and achieve alignment with corporate governance.	(Becker & Bailey, 2014)
5	The amount of transparency provided by a Cloud Service Provider does influence the potential client's decision making.	(Speed, 2011) (Kaufman, 2009)

Table 3: Overview of hypotheses

5. Governance models analysis

This research focuses on a limited number of important IT governance models. In figure 2, four different frameworks can be seen which are commonly used by companies being: COBIT, COSO, ITIL and ISO 27000.

Furthermore, two frameworks were selected based on relevant cloud computing auditing frameworks for this study and due to interest from the telecom service provider, being ISAE 3402 and CCM.

5.1 Overview of the Cloud Governance Dial

The Cloud Governance Dial by Becker and Bailey (2014) is used during the case study to find out whether the current service levels, quality frameworks and certifications can be retained or complemented with cloud specific quality and security frameworks. As previously mentioned, it is assumed that the application services will be offered on public cloud infrastructure, while management tooling will be managed on a private infrastructure.

During the literature review an in-depth analysis of the Cloud Governance Dial took place. The model is based on thorough literature research, but has not been used in practice yet to the best of our knowledge. By using the model during the case study the performance of the model will be tested. This way can be found whether the model is effective in its current state or if adjustments / optimisations for the model are necessary. For step 6, *Control*, an IT governance structure/framework should be chosen that takes of the risks mentioned in step 5, *ERM,* which were formulated based on the previous steps.

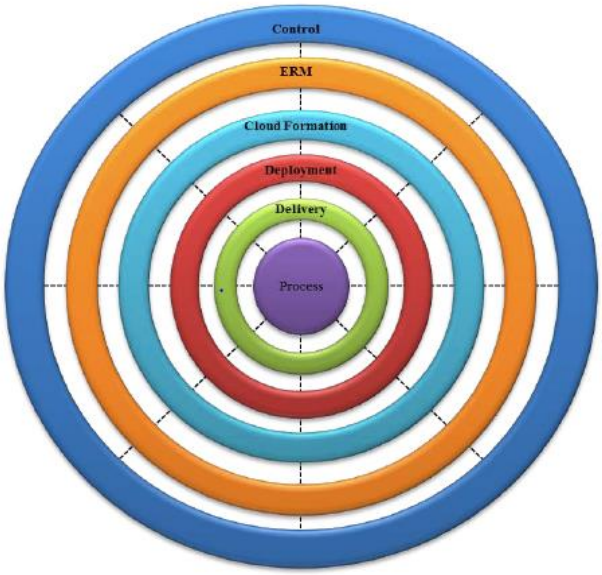

Figure 8: Cloud Governance Dial (Becker, & Bailey, 2014)

Figure 8 shows another visualization of the Cloud Governance Dial. To be able to choose the right structure/framework, more in depth research needs to be done to find out how the IT governance models differ from each other in relation to the cloud.

5.2 Cloud comparison IT governance models

As mentioned during the literature review, each framework is from a different type with its own goals and covering different domains. These differences are also noticeable when looking more specifically at the cloud contents of these frameworks.

Looking at Table 4a and Table 4b, which are based on available information on the websites of each framework and additional articles written by Isaca (2011), Horwath et al. (2012) and O'Loughlin (2014), it is clear that the definition of cloud computing formulated by the National Institute of Standards & Technology (NIST) is widely accepted, COSO being an exception. The definition of risk for each framework is defined differently, but they all mean the same in the end. The real differences between the frameworks starts to be visible when looking at the way each framework describes governance.

Both COBIT and COSO describe governance as risk management. Under COSO, the focus is to manage risk to be within its risk appetite. For COBIT, following the defined processes leads to appropriate risk management. Both ITIL and ISO 27000 series define governance as process alignment. For ISO, the alignments focus is between information security and business strategies, business objectives, value delivery and accountability. ITIL's alignment focus is between all the processes in the service strategy model. Finally, ISAE 3402 and CCM both describe governance as a set of compliance standards. For CCM these are cloud security standards and for ISAE 3402 there are process, management of processes and security standards.

Each framework got something different to offer for cloud computing. This can also be found in Table 4a and Table 4b. What can be seen is that this corresponds with the CG definitions. COBIT and COSO offer risk management for cloud computing. ISO and ITIL offer alignment in the business including cloud computing. Finally, ISAE 3402 and CCM provide compliance standards for companies that use the cloud.

Frameworks	Definition Cloud Computing	Definition Risk	Definition Governance	What does X framework offer for Cloud Computing?
COBIT	*A model for enabling 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.*	*The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise*	*The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved and ascertaining that risks are managed appropriately.*	*Produce a summary assessment of the business risks and achieved business value of an application, and help practitioners evaluate (often to a highly granular degree) many security or value issues.*
ISO 27000 Series		*The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of occurrence of an event and its consequence*	*Ensure alignment of information security with business strategies and objectives, value delivery and accountability. Supports the achievement of visibility, agility, efficiency, effectiveness and compliance.*	*Provide more detailed guidance and recommendations for both cloud service customers and cloud service providers.*
ITIL		*A possible event that could cause harm or loss, or affect the ability to achieve objectives. A Risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the Impact it would have if it occurred.*	*Governance is used to empower people, is agile, enables process automation and defines the measurement and control mechanisms that enables people to do their day-to-day jobs tactically to achieve the "IT governance" programs strategic objectives (the "what").*	*ITIL helps service providers with best practice guidance on the provision of quality IT services and the processes, functions and other capabilities needed to support them. ITIL can be capitalized on and provide a solid foundation for managing cloud based services and hybrid IT environments.*

Table 4a: IT governance models definitions and offerings

Frameworks	Definition Cloud Computing	Definition Risk	Definition Governance	What does X framework offer for Cloud Computing?
ISAE 3402	*A model for enabling 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.*	*Engagement risk: The risk of the auditor's exposure to financial loss and damage to his or her professional reputation.*	*Ensure that processes, management of processes and security comply with standards.*	*Provide a service organisation's management, user entities and other interested parties (clients, for example) with information about the controls the service organisation has in place.*
CCM		*The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise or organization*	*Ensure compliance with cloud security requirements by means of standards given.*	*Provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.*
COSO	*A computing resource deployment and procurement model that enables an organization to obtain its computing resources and applications from any location via an Internet connection.*	*Risk is the possibility that an event will occur and adversely affect the achievement of objectives.*	*A process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*	*By leveraging the COSO ERM framework, management will have an effective and consistent approach in identifying the universe of specific risks and risk responses that each cloud computing opportunity and decision entails.*

Table 4b: IT governance models definitions and offerings

Table 5a and Table 5b focus on the scope and benefits of each framework in regards to cloud computing. The scope, meaning the number of topics that are covered of each framework, is somewhat comparable with the scope of figure 2 where the framework relationships were discussed by Nguyen (2010). When only looking at cloud related topics, the scope of COSO is still very wide which is a result of having five general key components which take into consideration many cloud specific aspects. The same case is for COBIT, which has a wide scope when it comes to cloud computing and does not differ much from the scope coverage in figure 2. The cloud computing scope of ITIL is still IT service based and, as can be seen in Table 5a, focusses on best practices by means of flexibility, scalability, reducing costs and optimizing efficiency by leveraging new technologies. ISO 27000 series has a very narrow scope. This framework focusses on cloud security and both regulatory and legal requirements specifically. ISAE 3402 and CCM, which were designed as frameworks to be used with cloud computing, offer a wide scope when looking at cloud computing topics covered.

Each framework has its own benefits when it comes to cloud computing. Looking at the benefits COBIT brings to cloud computing in Table 5a it shows that it offers many. This shows once more that COBIT has, just as in figure 2, a wide scope, but again not each topic is described in detail.

The same would be expected with the COSO framework, since so far analysing this framework for the cloud has not shown many differences with the “what, how and scope” placement it has in figure 2. This, on the other hand, is not the case. When looking at the benefits COSO offers when used for cloud computing, many issues that were covered during the literature review are taken into account with a fair amount of detail included.

The benefits ITIL brings are all management related. This is not completely surprising, since ITIL is a best-practice framework that is focussed on improving internal IT services and is not specifically made for cloud computing in mind, which often involves external IT services.

As seen in Table 2, ISO is a security standard and the goal of ISO 27000 series is IT governance. When looking at Table 5a all benefits the ISO 27000 series offers in

regards to the cloud are risk related and many vulnerabilities that cloud computing brings are taken into account. This is in line with the placement of the ISO 27000 series in figure 2.

Finally, ISAE 3402 and CCM both offer many benefits to cloud computing. Keep in mind that ISAE 3402 is a framework that was created for accounting firms and is mandatory when cloud computing is part of their process in their company to guarantee adequate internal controls. Following the principles results in the benefits which can be found in Table 5b.

The CCM framework is explicitly designed for every organization that uses cloud computing as part of their company and assists these businesses in complying with most security requirements that relate to cloud computing. The benefits that result from the framework are all security related and of good quality due to very detailed domains.

Frameworks	Scope Cloud Computing	Benefits using X framework for Cloud Computing
COBIT	• *Strategic* • *Environmental* • *Market* • *Credit* • *Operational* • *Compliance*	• *Provide a good return on investment of IT-enabled business investments* • *Manage IT-related business risk* • *Establish service continuity and availability* • *Create agility in responding to changing business requirements* • *Achieve cost optimization of service delivery* • *Lower process costs* • *Manage business change* • *Manage product and business innovation*
ISO 27000 Series	*Helps organizations comply with numerous regulatory and legal requirements that relate to the security of information.*	• *Establish the risk management context* • *Quantitatively or qualitatively assess (i.e. identify, analyze and evaluate) relevant information risks, taking into account the information assets, threats, existing controls and vulnerabilities to determine the likelihood of incidents or incident scenarios, and the predicted business consequences if they were to occur, to determine a 'level of risk';* •*Treat, avoid and/or share the risks appropriately, using those 'levels of risk' to prioritize them;* •*Keep stakeholders informed throughout the process; and* •*Monitor and review risks, risk treatments, obligations and criteria on an ongoing basis, identifying and responding appropriately to significant changes.*
ITIL	• *Procurement and finance* • *Ability to scale quickly and reduce IT overcapacity* • *Leverages new technologies* • *Reduces IT ownership*	• *Business Relationship Management—form and uphold the cloud service provider and customer business relationship.* • *Demand Management—understand, anticipate and influence business demand for services. Carefully calculate demand to allocate the agreed budget within the financial management process.* • *Financial Management for IT Services—provide a cost-effective administration of the assets and resources used in providing IT services. Incorporate charging based on consumption when perusing cost analysis calculation.* • *Service Portfolio Management—describe a service provider's services in terms of the business value and needs. Create a portfolio for all potential external cloud deployment models.* • *IT Service Management—Asses the service provider's offerings, capabilities, competitors as well as current and potential market spaces to develop a strategy to serve customer needs.*

Table 5a: IT governance models cloud scope and benefits

Frameworks	Scope Cloud Computing	Benefits using X framework for Cloud Computing
ISAE 3402	*Operational processes and general IT controls. E.g. back-up/password-id policy and change management.*	*• Security – The system is protected against unauthorised access (both physical and logical).* *• Availability – The system is available for operational use as committed or agreed.* *• Processing integrity – System processing is complete, accurate, timely and authorised.* *• Confidentiality – Information designated as confidential is protected as committed or agreed.* *• Privacy – Personal information is collected, used, retained, disclosed and destroyed in conformity with the commitments in the service organisation's privacy notice, and with criteria set forth in generally accepted privacy principles issued by the AICPA.*
CCM	*Help organizations to comply with all security requirements that relate to cloud computing*	*Strengthens existing information security control environments by:* *•Emphasizing business information security control requirements* *•Reducing and identifying consistent security threats and vulnerabilities in the cloud* *•Providing a standardized security and operational risk management* *•Seek to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud.*
COSO	*• Unauthorized cloud activity* *• Lack of transparency* *• Security, compliance, data leakage, and data jurisdiction* *• Transparency and relinquishing direct control* *• Reliability, performance, high-value cyber-attack target* *• Noncompliance with regulations* *• Vendor lock-in* *• Noncompliance with disclosure requirements*	*• Cloud policies and controls* *• Assessments of the CSP control environment* *• Data classification policies and processes* *• Management oversight and operations monitoring controls* *• Incident management* *• Monitoring of the external environment* *• Preparation of an exit strategy* *• New disclosures in financial reporting*

Table 5b: IT governance models cloud scope and benefits

5.3 Overview of Cloud IT governance models

The analysis of IT governance models in regards to cloud computing, makes it possible to create a figure like figure 2, page 14. However, this time the scope is the amount of cloud domains that are covered by each framework. The “what and how” tells us the amount of detail each framework gives regarding how to address the issues in a specific domain and the level of detail it contains of each domain. Collecting the necessary data from Tables 4 and 5 to generate a cloud domain focused “what, how, and scope” figure leads to Table 6.

Frameworks	Risk domain	Governance by:	Cloud domains
COBIT	Business Risk	Standards	- Strategic Decision Making - Environmental - Market Positioning - Finances - Operational Processes - Security and Compliance
ISO 27000 Series	Security Risk	Processes	- Security and Compliance
ITIL	Event Risk	Processes	- Strategic Decision Making - Operational Processes - Finances
ISAE 3402	Engagement Risk	Processes	- Operational Processes - Security and Compliance
CCM	Business Risk	Standards	- Operational Processes - Security and Compliance
COSO	General Risk	Processes	- Strategic Decision Making - Environmental - Market Positioning - Finances - Operational Processes - Security and Compliance

Table 6: Overview of Cloud IT governance models

The new, cloud specific “what, how, and scope” frameworks are depicted in figure 9. The position of each governance model is, just like in figure 2, on an ordinal measurement scale for every attribute. As an example, COSO is wider than COBIT in regards to the scope of coverage. This means that COSO covers more cloud topics as opposed to COBIT, but does not tell exactly how many more.

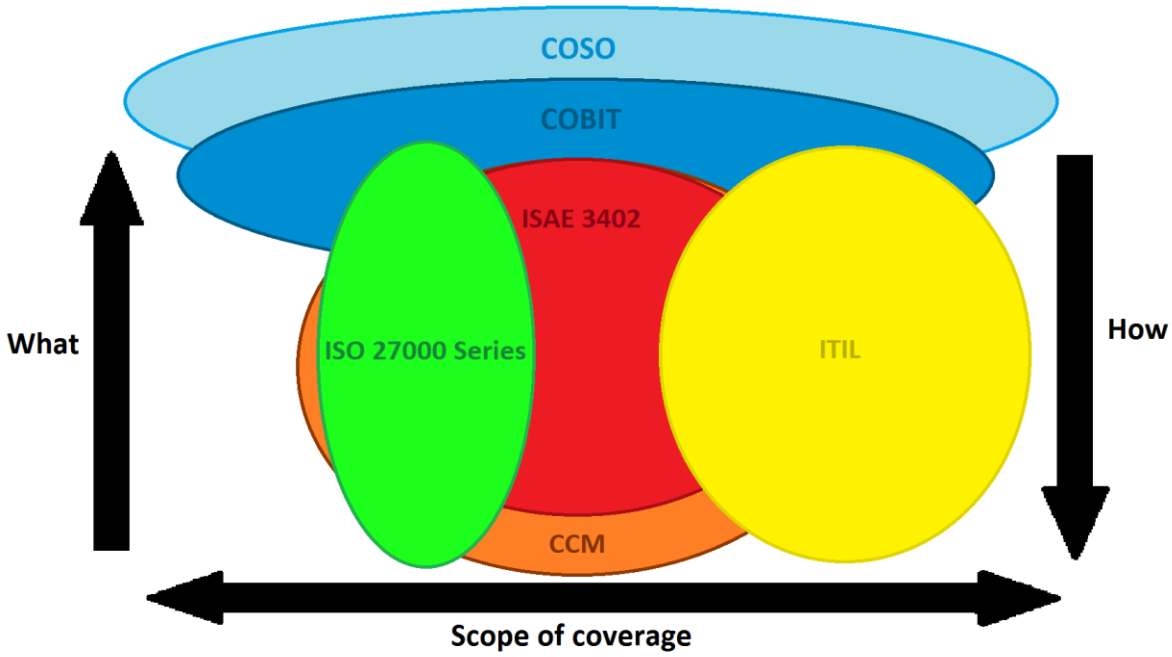

Figure 9: Cloud specific “what, how, and scope” of governance models

When comparing figure 2 with figure 9 it is important to keep in mind that for the former all domains, including the cloud, were considered for the scope. The scope of figure 9 is limited to the cloud specific domains only. This explains the different placements of the frameworks between the two, which are discussed briefly.

COSO’s placement is, just like figure 2, placed at the top. This is the only framework which is mentioned that covers all cloud domain risks on a general level. Just like every other domain, COSO again only addressed these with a moderate level of detail.

The scope of COBIT is again very wide. The same amount of cloud domains as COSO are covered. Both COSO and COBIT are frameworks that give guidelines. The difference between the two is that COSO manages this through general processes

while COBIT offers specific standards to achieve these guidelines. In addition, even though all cloud domains are covered by COBIT, the risk domain is limited to business risk. These two reasons are the reason why COBIT has a narrower scope than COBIT.

The position of the ISO 27000 series did not change much. The framework only covers the Security and Compliance domain of cloud computing. It does, however, give a very in depth “what and how” of this domain. Additionally, it takes into account how to comply with most regulatory and legal requirements for a company, but does not really consider how to handle the risks that external parties such as Amazon, Google, Microsoft or SAP could bring.

The one framework that moved significantly is ITIL. When focussing at the cloud domains the ITIL covers three of them. As previously mentioned, ITIL is a best practice framework that focusses on improving several IT services for the management. This is the only framework in this research that does not cover the security and compliance domain.

CCM and ISAE 3402 are two frameworks that were discussed in this paper, but not considered during the time figure 2 was made. Both CCM and ISAE 3402 were developed with cloud computing in mind. Both frameworks cover two specific cloud domains. The scope of CCM is wider than ISAE 3402 since the latter is a framework that was designed for accounting firms and therefore the coverage can be limited to what is important to ensure adequate internal controls.

6. Case Study at a telecom service provider

To find out how the current service levels, quality frameworks and certifications can be retained or complemented with cloud specific quality and security frameworks, a case study will take place. An explanation of the case study method, including the advantages and disadvantages this method has, can be found in Appendix A. During this case study it will be assumed that the application services will be offered on public cloud infrastructure, while management tooling will be managed on a private infrastructure. This case study will take place by comparing the private, hybrid and public cloud with each other and see if any differences or similarities are visible. After that, one use case will take place to test the Cloud Governance Dial.

6.1 Data sources

The data for the case study is collected from multiple sources. These sources are:

- The telecom service provider;
- Amazon;
- Microsoft;
- Current client of the CSP.

To collect the data, interviews took place and for that several questions were formulated. Whenever necessary, multiple qualified employees from different departments of the telecom service provider were questioned. This lead to comparable answers for each question which results in a more convincing conclusion.

All interviews took place at the location of the interviewee. The questions were given in descending order. All interviews were recorded after receiving permission to do so and were typed out afterwards for efficiency during the interview. The interviews can be found in the Appendix.

6.2 Questions interviews

As previously mentioned, the results of an exploratory case study will answer the hypotheses and problem statement. This is done by means of interviews with some of the participants mentioned in paragraph 6.1. This interview consists mainly of cloud

computing specific questions that should be addressed by the Cloud Computing user's auditors. The questions asked in the interviews result from the paper written by Elifoglu et al. (2014), the product service index that the telecom service provider provides to its customers, the Cloud Governance Dial, and as a result of analysing the frameworks in this research. The questions can be divided into multiple subtopics, which is in harmony with the security check-list required when adopting the cloud provided by Cattedu (2010):

- General: Some general questions regarding the current IT governance models and the transition from private to public cloud are asked.

- International Dimension and Privacy: Cloud computing has no real borders, the data of a company could be hosted anywhere in the world where different rules and regulations apply without being informed about it. Therefore, clear agreements need to be made between both parties.

- Security Breaches: This subtopic was addresses extensively in the literature review. There are security benefits, but also a lot of security risks to consider.

- Privacy and Encryption: Companies that hand out their data to a CSP want to be sure that their data is save. A way to do this is by making use of encryption. Additionally, there needs to be clear communication between the parties involved regarding who has access to the data due to privacy concerns.

- Audit Rights, Integrity and Availability: A client wants to be sure that the CSP does its best to provide the best service in the most secure way. Therefore, regular audits are necessary. Offering transparency is another way to improve clients trust. Finally, it is expected that the data in the cloud is accessible every day of the year and that outages are rare to non-existent.

- Exit strategy: What is often overlooked when two parties get to an agreement is what happens when the contract will be terminated. It is important to know what

> happens with the data that is in the hands of the CSP and how the client can transition the data to a different provider. Cloud providers speak different languages. All the major providers offer unique, and often proprietary, data storage (Hofmann, & Woods, 2010).

The questions are explorative and semi structured. The telecom service provider was given two set of questions. One with the focus on the private cloud and the other one focussed on the hybrid cloud. The questions were combined and can be found in Appendix B. The companies Amazon and Microsoft were both offered the same set of questions. Additionally, some questions were asked to a client of the telecom service provider to test the Cloud Governance Dial and to find out the importance of topics such as transparency for the client. These questions can be found in Appendix C.

Having the results obtained by these questions makes it possible to generate an answer to the question how the current service levels, quality frameworks and certifications can be retained or complemented with cloud specific quality and security frameworks when offering application services based on public cloud infrastructure, while keeping the management tooling on the private infrastructure and still comply with the requirements of the customer. Additionally, the Cloud Governance Dial can be tested to see its effectiveness and efficiency and conclusions can be made whether modifications in the model are necessary or not.

The following three paragraphs will be structured equally. First an overview will be given of the certifications that cover risks. This is followed by checking whether the vendors are GDPR compliant. After that the topics encryption, transparency and termination of contract will be discussed.

6.3 Hybrid Cloud

During an interview with a product manager from the department of Cloud Managed Services of the telecom service provider, an overview was given of how risk is handled and what type of Cloud Compliance Frameworks they use for managing the hybrid cloud. See Appendix D for the full interview. The telecom provider has the certifications ISO 9001, ISO 27000, and ISO 22301, which are externally audited together with the

General Counsel Office of the telecom service provider, for all managed hybrid cloud services. Some clients, such as accounting firms, require an ISAE 3000 statement. This statement is issued twice a year. A consultant from the telecom service provider, of which the interview can be found in Appendix F, informed me that there are many more certifications, but that this is different for each cloud and each product that is offered. Furthermore, the consultant said that their processes are ITIL based and that the architectures in the company use multiple frameworks such as COBIT to create their own environments which are offered to customers.

In addition to these international standards, the telecom service provider has developed its own internal standard in collaboration with Deloitte, a consulting firm specialised in auditing, which they named the Certified Compliance Framework (CCF). This framework guarantees that customers data resides at datacentres of the telecom service provider, which are all located in the Netherlands, and the systems are handled by Dutch administrators.

The CCF takes away many risks associated with cloud computing, however this framework is only offered when using a specific type of service, which is a virtual private cloud. When a company wants to make use of one of the larger service providers Amazon, Google, Microsoft or SAP the framework can't be guaranteed. For this reason the telecom provider developed managed hybrid cloud. The hybrid cloud combines the advantages of a virtual private cloud (security, reliability) with the ones of a public cloud (scalability, flexibility). This way the customer can choose the best combination of cloud service models based on the types of applications they want to host or develop. On the virtual private cloud level an additional layer of protection will be present with the CCF.

When being asked whether the telecom service provider is already GDPR compliant I was told by the product manager that only a few more adjustments were necessary to comply with the General Data Protection Regulation on their hybrid level. Since these adjustments are very limited business processes or performance does not seem to be affected by it. Furthermore, the consultant wanted to emphasize that as a telecom service provider they are an example for the rest when it comes to complying with such

regulations. From a cloud perspective, the GDPR doesn't cause many changes. As a supplier of cloud services, however, this regulation will influence several processes.

All data the telecom service provider holds is marked with the highest classification. Only named accounts have access and only when this is necessary to provide the required service level.

Even though Speed (2011) concluded in his research that most cloud providers encrypt their data, this does not always seem to be the case. One of the product managers from the telecom service provider told me this is not as easy as it seems. Data that is stored in the cloud and not being edited or used constantly is easily to encrypt. However, many applications that run in the cloud have data that needs to be available and is processed constantly and applying encryption on that level would severally impact performance. Additionally, the principal solution architect from Microsoft said during the interview that encryption services are available, but not often used since these are not mandatory and impact performance.

Transparency has been deemed as an important factor for prospects that orientate on their possibilities. The telecom service provider shares their audit reports directly with their customers to discuss these twice a year. Every employee is being screened and must agree with a Code of Conduct and sign a Non-Disclosure Agreement (NDA) when applying.

Integrity and availability are assured by means of back-up services and multiple security services that are being tested each quarter. These tests take place from external to internal, but also between tenants internally.

If a customer decides to terminate a contract, the telecom service provider will facilitate the customer in any way to get the data in the cloud back to the client. This topic, however, does not really get mentioned during the negotiations.

6.4 Private Cloud

During an interview with a security manager of the telecom service provider the same overview was given which was also shown for the hybrid cloud of how risk is handled

and what type of Cloud Compliance Frameworks are used. See Appendix E for the full interview. Just like the hybrid cloud, the private cloud has the certifications ISO 9000, ISO 27001, ISO 22301, ISAE3000, CCF and many more certifications which are different for each product that is offered.

For private cloud, there are no exceptions for when CCF cannot be applied, since no external parties such as Amazon, Google, Microsoft or SAP are involved, opposed to the hybrid cloud. A downside having a private cloud situation instead of a hybrid cloud, however, is that there is less scalability and flexibility. It is still possible to scale, but it will take longer for the CSP to fulfil the requirements since in general private cloud providers have less servers in inventory ready to be used.

Where the product manager of the telecom service provider said only a few adjustments are necessary for compliance with the General Data Protection Regulation on a hybrid level, the security manager still questions himself how compliance is going to be achieved. Due to the amount of logging that is required with the new regulation he thinks a completely automated process for this is required, which is not the case at this time.

Data is not encrypted on a private cloud level for now. According to the security manager this does not happen in practice yet at many different CSPs due to multiple reasons. One of them is that it affects performance. Another reason no encryption is used at the moment is the fact that if the encryption key gets lost, the data cannot be accessed any longer. The security manager finds encryption not necessary as long as there is enough trust between the CSP and the client.

When it comes to transparency for the private cloud the telecom service provider has obtained multiple certifications which are open to the public. These certifications are both internal and external audited. If a client wants to look into one of the reports they will have to visit one of the offices. A prospect customer can look into these reports after signing a non-disclosure agreement in advance, but situations like these rarely occur.

The security officer told me that when a contract gets terminated several institutions require evidence that their data is erased. For the private cloud this is proven by a signed piece of paper that says all the data has been erased and hardware has been shred. The interviewee thinks using a program like Blancco could significantly improve the trust between the CSP and the client since this third-party software is very trustworthy when it comes to erasing data. He thinks as long as the GDPR is not active, CSPs are not going to invest money in this process to save costs.

6.5 Public Cloud

Multiple public cloud server providers were approached, but only Microsoft offered to take of an interview. Therefore, the information from Amazon is collected from what is publicly available on their website.

6.5.1 Microsoft

During an interview with a principal solution specialist from Microsoft, which can be found in Appendix G, the same set of questions were used as for the telecom service provider. When asked how risk is handled and which Cloud Compliance Frameworks are used to handle these risks, a web page was shown which showed all certifications Microsoft Azure has at the moment. Some of these certifications are the basic ISO 9000 and 27000 series and ISAE 3000 series.

Furthermore, Microsoft is also Cloud Security Alliance (CSA) certified. Microsoft Azure differentiates itself by having country specific compliance. For example, there are two Dutch specific certifications being ‘BIR 2012’ and ‘NEN 7510:2011’ which they have acquired. The latter is important for organizations in the healthcare sector.

A known issue with the public cloud is that users do not know in which country their data is located. Microsoft has three different layers to show their customers that their data really is only in countries they have given permission for:

- Their first layer is ‘Microsoft over Microsoft’. In the Microsoft Azure trust centre a whitepaper can be found that says what they do for security, where they save the customer’s data and what certificates are applicable.
- The second layer consists of all certificates Microsoft Azure has acquired. All these certificates are from independent parties that have audited Microsoft. These certificates are accessible for all customers and proof that what Microsoft does is in regards to security and compliance is in fact achieved.
- The third layer is Microsoft’s Online Services Terms (OST). In this layer direct appointments are made between Microsoft and the customer.

If for some reason customers still do not trust that their data is safe after these three layers, there is always an option to encrypt their own data by themselves.

When mentioning the GDPR the principal solution specialist told me that Microsoft Azure has promised their customers that they will be GDPR compliant as soon as it becomes active till the virtualisation level. It is important to keep in mind that Microsoft is not responsible for the data, but only the infrastructure since it mostly offers IaaS services. Therefore, it is the clients responsibility to be GDPR compliant starting at the OS level and further.

Each service and server has its own type of encryption. Microsoft Azure also offers encryption for data in transit, but this will impact performance significantly. AES2500 bit is an example of encryption that is offered by Microsoft. It is also possible for users themselves to encrypt their data with tools such as Bitlocker which impacts performance less. Services like Office 365 are encrypted by default.

Transparency to customers is offered by means of certifications which are open to the public and were audited by independent auditors. Additionally, every customer is screened during the recruiting process and NDA’s must be signed. It is not possible to look into the reports of these certifications without being a customer.

There are standard protocols for when a company terminates his contract. The customer will be the owner of the data hosted on Microsoft Azure's servers for a long time, even after termination of the contract. In the OST can be found that the data will be deleted permanently after 90 days, but in practice this is often even longer unless the company explicitly asks the data to be deleted.

6.5.2 Amazon

AWS, just like Microsoft Azure, has many certifications such as ISO 9000 and 27000 series, ISAE 3000 series and is CSA certified. A full list of certifications give out to AWS by independent auditors is publicly available on their website and a lot of information can be found in their whitepaper: *"*Amazon Web Services: Risk and Compliance*"* (2017).

A lot of emphasis is put on control ownership. AWS controls the physical components and the customer owns and controls everything else, including control over connection points and transmissions.

AWS customers decide in which physical region their data and their servers will be located. Data replication will only take place in the same regional cluster and will not be placed in other regions. AWS will not move customers' data to another region without notifying the customer, unless this is required to comply with the law.

It is already confirmed by AWS that they will be GDPR compliant when the regulation will be enforced next year. They offer multiple services to help customers comply with the GDPR, since only the infrastructure layer is managed by Amazon, but not the data. Types of services Amazon offers are related to access control, monitoring and logging, encryption and the fact that they have a strong compliance framework and security standards.

Encryption is supported by AWS for multiple services. Customers are allowed to use their own encryption mechanisms, but are also able to use server side encryption which is offered by Amazon. Third party encryption technologies are also allowed to be used within the AWS data centres.

Transparency is offered by having multiple certifications that tell customers that AWS has effective physical and environmental controls in place. In addition, it is never allowed for a customer to have a data centre tour, since their data centres host multiple customers.

Based on the information publically available on the website of Amazon it is not exactly clear what procedures or protocols are in place if a customer decides to terminate its contract. If customers request to export data, this is possible by means of digital data transfer or physical *"snowballs"*. Customers have 30 days to collect their data after requesting termination of the contract. It is unclear what happens with the data after that period.

6.6 Testing the Cloud Governance Dial

Having analysed the private, hybrid and public cloud helps us in testing the Cloud Governance Dial, see section 4.3 and 5.1.

To test the effectiveness of the dial a simulation is required by means of a use case. In this use case we have SAP systems moving from a private to a public cloud environment. When the transition is complete, the idea is that some elements are still managed on the private cloud, but the application itself runs on the public cloud. This is a hybrid cloud solution.

Applying this use case to the six steps of the Cloud Governance Dial leads to the following answers:

1. Process: What is moving to the cloud?

Looking at the use case SAP applications are moving from a private cloud to a public cloud environment. No specific cloud service providers are mentioned and only the general risks associated with the private and public cloud will be considered.

2. Delivery: Identify IT governance domain objectives and deliverables.

With identifying the IT governance domain objectives and deliverables is meant how the SAP applications will be delivered. There are three different options to choose from which were explained earlier: SaaS, PaaS, and IaaS. For this use case the PaaS solution is the way it will be delivered. This means that the customer manages the data and applications and the cloud service provider takes care of the rest.

3. Deployment: How will it be delivered?

Again, there are three options to choose from: Public, Private and Hybrid. As previously mentioned, the idea is that the SAP application runs on the public cloud, but is still partly managed on the private cloud. This results in a hybrid cloud solution.

4. Cloud Formation: How will it be deployed?

This step consists of multiple questions which each need to be answered individually:

- **4.1 Where will the data be located? (Internal or External)**

  All the data for the SAP applications will be located external at a cloud service provider. The applications will be managed using the private cloud, but no data needs to be stored on the private cloud for this.

- **4.2 Who owns the technology, services, and interfaces?**

  The infrastructure will be owned by the public cloud service provider. The SAP services will be owned by the telecom service provider offering these services and finally the data itself is still owned by the customer.

- **4.3 Are there expectations of collaboration and data sharing?**

  The main point of this transition is to collaborate with a partner that is specialised in offering public cloud solutions. Because of this collaboration on a high level is required. The cloud service provider has the infrastructure and the telecom

service provider has the knowledge to manage SAP services. Due to the hybrid cloud situation data sharing is essential.

- **4.4 Who is managing the delivery? (Insourced or Outsourced)**

The delivery is managed by both the Telecom Service Provider and cloud service provider. Since the SAP applications are being moved from the private cloud to the public cloud it goes from insourced to outsourced. It could be argued, however, that, since there is still some managing taking place on the private cloud, there is a combination of insourced and outsourced.

5. ERM: Determine the cloud formation.

Having answered the first four steps makes it possible to collect all cloud specific risks associated with the answers given. In this use case SAP applications are moving from the private to the public cloud. Several risks are associated with this:

- First, how are you going to make this transition as smooth as possible? Customers that are using your service right now expect the same quality and uptime or better during and after the transition. It is important to consider all the changes that come along with moving to a new platform.

- Second, SAP has many different types of applications each of them managed different. Each application has bugs and flaws present which could cause security risks. In 2013 an exploit was discovered that misused one of their vulnerabilities which got patched soon after.

The second step told us that in this use case the service offered will be a Platform as a Service. This brings along several known PaaS specific risks (OWASP, 2009):

- *Business Continuity Planning and Disaster Recovery with PaaS vendor.*
  This means that the client is dependent of its vendor. If the infrastructure of the vendor gets affected this could directly influence the client's business processes.

Rules need to be in place to prevent this from happening such as disaster recovery.

- *Vendor Lock In.*
  PaaS vendors tend to dictate the database, storage and application framework used. If a customer has some legacy applications which are not supported, it will require the skills and infrastructure to run these which is a costly process.

- *Lack of adequate provisions in SLA.*
  The upcoming National Institute of Standards and Technology (NIST) Cloud Computing Security publication will do a lot to standardise compliant cloud infrastructures which need to be followed

- *Meeting compliance demands and control risks when working with a PaaS vendor.*
  The PaaS vendor takes over a lot of the auditing required. If a company that has its data hosted at the vendor needs to comply with certain demands, they need to be sure that the vendor also is compliant. When looking for a cloud service provider it is important to look at the certifications obtained by each provider.

Answering the question mentioned in the third step of the Cloud Governance Dial made it clear in this use case we have a hybrid cloud solution. The main risks that a hybrid cloud solution brings are somewhat similar to the risks associated with PaaS. Compliance is again an issue with the same reasoning that was just given. Additionally, cloud security and loss of control are two other issues related to the hybrid cloud. Since the starting position of this use case is SAP already being present on the private cloud these last two issues have already been covered before. Cloud security is just as important for the private and public cloud. Loss of control, however, is a bigger issue on the public cloud than the private cloud, since on the private cloud level you still have a decent amount of influence and control over your data, while on the public cloud you have no control over your data at all.

This leads us to the fourth step which consists of four smaller questions that needed to be answered. The data will be hosted externally at the cloud service provider which results in the just mentioned loss of control. Furthermore, each of the parties owns a different part of the service. The cloud service provider such as Amazon or Microsoft owns the infrastructure, the Telecom Service Provider owns the services and the data is owned by the client itself. As long as the boundaries of the responsibilities between the parties are clearly defined, this should not lead to conflicts between the parties.

The third question in step four was whether there is collaboration and data sharing or not. In this use case this is definitely the case. To prevent conflicts and disruption of service, clear rules and agreements need to be in place before offering a service together.

The final question told us that the data is going to be outsourced which brings the risk mentioned before being loss of control. Again, clear rules and agreements need to be in place to assure the client the data is handled carefully.

6. Control: Cloud governance.

Now that the first four steps were analysed for risks during step five it is possible to find the required IT governance models that are needed. Going back to figure 9, which has been generated based on analysis of the frameworks mentioned in this paper, we are able to choose the frameworks that cover these risks.

ITIL as a best practice framework is necessary to assure business continuity and to ensure that the same level of quality is met after the transformation to the public cloud. In addition, having ISO 27000 series certifications is a must when offering cloud services. In addition, the Cloud Control Matrix would be a good additional security standard. This standard offers clear questions about many cloud security related topics which are not very difficult to understand and therefore easy to communicate with to your client and the client service provider. ISAE 3402 could be mandatory depending on the type of company you offer services too. It would be a good decision to already be ISAE 3402 compliant beforehand so it can be used as potential sales point for

prospects. COBIT could be an additional best practice that could be helpful for measuring and assessing IT controls but is not mandatory due to the Cloud Control Matrix.

In conclusion, the most important thing to take into consideration for this use case is to make clear rules and agreements between all parties involved before the transition starts. In most cases, only two parties are involved being the customer and the cloud vendor. In this case, three parties are involved being the customer, telecom service provider and cloud vendor. Therefore, questions such as *"Who is responsible for what?"* need to have a clearly defined answer so the same or even better level of service can be provided as a result. Since in the private cloud many of the same requirements for cloud security apply as for the public cloud, not many changes are needed in that area.

A possible scenario that shows the importance of clear rules and agreements is a conflict between the parties due to a data breach. For the customer, the reputation towards both the telecom service provider and the cloud vendor will be damaged. The telecom service provider does not have access to the datacenter and therefore must rely on the cloud vendor following the right procedures. Both parties have an interest with the customer by offering high quality service and therefore both would not like the blame for such an incident. If the right rules and agreements are made beforehand regarding responsibilities, no blame game can occur between the two parties.

7. Discussion and Limitations

The motivation for writing this thesis is based on findings of previous literature, as some of these seem to be extraordinary. In addition, these findings are relevant for current challenges that the telecom service provider is facing. Differences and similarities between their findings and the results from this thesis will be discussed accordingly.

Hypothesis 1: *The IT governance models discussed in chapter 3 effectively deal with the cloud specific security risks mentioned in section 2.3.*

The IT governance models that were discussed in chapter 3 were: COBIT, ISO 27000 Series, ITIL, ISAE 3402, COSO and CCM. When looking at the risks mentioned in section 2.3 and having analysed each of the above frameworks, which resulted in figure 9 on page 42, this lead to the following.

CCM has been proven effective by giving answers to many security risks that customer's face when moving data to the cloud such as where their data is located, how it is secured and how it gets encrypted. This is done by means of a questionnaire which is provided by the CSA and needs to be filled in completely to be CSA certified. During the interviews, both Microsoft and Amazon showed they are CSA certified. The telecom service provider did not show this type of certification, but has its own developed framework called CCF which is somewhat similar and audit by an independent party.

The ISO 27000 series has already proven its effectiveness with dealing with cloud specific security risks by purely focussing on the security and compliance domain and its certification is mandatory for any company that has cloud services being part of the process.

Furthermore, the best practice framework ITIL effectively deals with several cloud specific security risks such as availability risks by covering domains such as strategic decision making, operational processes and finances. This framework helps to ensure the same quality standards are met in the foreseeable future.

Finally, ISAE 3402 effectively deals with cloud security, availability, privacy and integrity. This is an especially important framework for accounting firms that make us of cloud processes, since it is a mandatory certification by law.

Frameworks such as COBIT and COSO are helpful to recognise cloud security risks, but need more input from its users than the other models to effectively deal with the risks. When looking at figure 9 on page 42 they are at the top of the figure which means these frameworks help companies find out what the risks in their company are, but does not guide the company in making these risks disappear and therefore own input is required.

As a result, the hypothesis is not completely accepted, since not all IT governance models discussed in chapter 3 effectively deal with the cloud specific security risks, unless input is given.

As seen in the literature review, there are many cloud specific security risks to consider. In general, the same types of risks are found by different academics. Because of this it could be said that these risks are commonly accepted to be aware of. Something to look out for, however, is that, as long as the cloud is changing, there is a chance that new risks will be discovered over time. The analysis of the IT governance models is based on risks that are known at the time of writing this thesis. However, the results could be different in the near future if new risks are discovered which are currently not taken into account by the governance models.

Hypothesis 2: *The General Data Protection Regulation significantly impacts the current cloud specific business processes of a company.*

Based on the interviews with the telecom service provider, cloud service providers and the client the GDPR does seem to significantly impact the current cloud specific business processes of a company, but it is yet unknown how big this impact will be. Every company is aware of the regulation and preparing themselves, but as the consultant from the telecom service provider mentioned, there are no clear boundaries given in the regulation. Large providers such as Amazon and Microsoft promise to be

GDPR compliant till the virtualisation layer as soon as the regulation becomes active next year.

Every business seems to be affected in some way by the GDPR. The client that was interviewed is not affected by the regulation when it comes to their customers, but their HR system, which contains personal employee data, is affected. This will be the case for almost every company in the European Union. It is imaginable that having a small employee database it is easy to comply with the new regulation, but that for big companies some serious adjustments need to be made which are costly and do affect the current business processes.

Based on the available information, it is not possible to either accept or reject the hypothesis at this point.

It could be argued that Henning (2016) made a bold statement by saying that the ISO 27000 series covers most of the regulation. The telecom service provider, Amazon and Microsoft all find it challenging to comply with the new regulation. If being ISO 27001 and 27002 compliant, which most companies are, would make a company also comply with the regulation, there wouldn't be any challenges for these companies at the moment. At this moment, it is far from clear what the best way is to comply with the GDPR. One way to create compliance is by trying to answer questions such as:

- Is personal data being stored or processed?
- Is it known where the data is located?
- How long has the data been there?
- Can it be permanently deleted?

If there are tools or procedures in places that makes it possible to give an answer to all these four questions a company could end up being GDPR compliant.

Hypothesis 3: *The IT governance models cover the risks faced when migrating to the cloud.*

During the analysis of the IT governance models discussed in Chapter 3 it has been clear that all models cover at least one of the cloud specific risks. An exception being

ISO 9000 which purely focusses on business continuity management and does not take cloud computing into account.

Governance models such as COSO and COBIT cover all risks, but not into much detail. Therefore, it is better to combine several other governance models such as ITIL, CCM and ISO 27000 series which results in a better compliance overall. The hypothesis is accepted.

Combining these models results in covering all the important risks that were mentioned by Dreyfuss (2009) when migrating to the cloud. This is in accordance with the available literature. In addition, Mangiuc (2011) developed a tool to clarify the roles and responsibilities associated with cloud deployment. This tool is used in the Cloud Governance Dial which will be discussed next.

Hypothesis 4: *The Cloud Governance Dial is a viable model to meet IT governance goals and achieve alignment with corporate governance.*

The Cloud Governance Dial, developed by Becker and Bailey (2014), was to our knowledge not tested in practice yet. Having applied a use case to the cloud governance dial showed that the dial is, till certain extent, a viable model to meet IT governance goals and achieve alignment with corporate governance. However, the model was created in 2014 and therefore already got outdated. Some adjustments are recommended to improve the model.

The first recommendation is to take the GDPR into account. This new regulation is affecting many companies. It is advised to make an additional step which addresses the GDPR and ask questions such as the ones mentioned on page 62:

Having answered these questions helps management to get a better overall view of how personal data is currently being managed and helps them find out whether measures need to be taken to be compliant.

The second recommendation is to split up step 4. Right now, the first three steps consists of relatively simple questions while the fourth step consists of four very

important questions. It is recommended to split up each question individually so each step is of equal length and equal importance.

The foundation of the model has been well executed due a thorough literature analysis done by Becker and Bailey. Many of the risks that are summed up during step 5 of the cloud governance dial are covered by the IT governance models. If the right questions are asked in the dial this could lead to a lot of efficiency in the process of finding the right IT governance models. For this reason, it is important to analyse the questions periodically and update where necessary.

In conclusion, the hypothesis is accepted, but improvements to the model can be made.

Hypothesis 5: *The amount of transparency provided by a Cloud Service Provider does influence the potential client's decision making.*

During the interviews it was clear that the telecom service provider, which offers private and hybrid cloud services, offers more transparency overall than public cloud vendors. A reason for this could be that big public cloud vendors have many more clients, are American based and are very protective about their infrastructure. Overall, customers of public cloud vendors have to suffice with the certifications, while for the telecom service provider more transparency is given by discussing the audit reports with its customers and having one dedicated person in the company who can be contacted for questions and issues, which results in more trust.

This is supported by the answer of the client when asked why the company choose a private cloud solution instead of a public cloud solution. The most important factor that they took into consideration for their decision-making process was that they wanted a contact point at the company they would be hosting their data and wanted to be sure to know where their data is located at any time. The telecom service provider proofs with their CCF framework and the fact they only have data centres located in the Netherlands that their data can only be located in the Netherlands. While public cloud vendors do promise that data will only be stored in locations you have given permission for, there is no way to check if this is true.

Therefore, the amount of transparency provided by a Cloud Service Provider does influence the potential client's decision making. The hypothesis is accepted.

A lot of past literature focussed on creating some sort of checklist for companies that want to start using the cloud by giving recommendations for these companies in regards to what to look out for when it comes to transparency. An example is the bullet points of Speed (2011) mentioned in the literature review. The methods to provide transparency mentioned in 4.5 do seem to have impact on a prospects decision making process and therefore are important to take into account for each cloud vendor.

7.1 Limitations

There were several limitations that had impact on this thesis:

- First, the time was scarce to do research. Due to this a limited amount of IT governance models were discussed, while in practice there are many more being used.

- Initially the plan was to interview Amazon, Google and Microsoft. Amazon and Google didn't respond to multiple requests. In the end, only an interview took place at Microsoft. Amazon, however, did have most of the required information available on their website, while Google did not.

- Due to circumstances, only one client of the Telecom Service Provider was interviewed, which limited the analysis for the transparency hypothesis.

8. Conclusion and Recommendations

This thesis has answered the research question “how are the IT governance models different from each other in relation to cloud computing?” by analysing literature, taking interviews and one use case. The following was found based on the discussion in Chapter 7. The first finding is that many IT governance models effectively deal with cloud specific security risks, but that this is not the case for every model. The second finding is that at this point it is yet unknown whether the GDPR will or will not significantly impact the current cloud specific business processes of a company. Third, the IT governance models that were discussed in this paper together cover all the risks that are faced when migrating to the cloud. The fourth finding is that the Cloud Governance Dial created by Becker and Bailey is a viable model to meet IT governance goals and achieve alignment with corporate governance. The final finding is that the amount of transparency does influence the potential client’s decision making.

8.1 Recommendations

Based on the findings, several recommendations for future research can be made:

- More IT governance models can be analysed and added to figure 9 on page 42 which results in more models being easily comparable by just looking at the figure.

- When the GDPR becomes active next year, it might be possible to measure its impact on cloud specific business processes. At the moment companies don’t really know how the GDPR will affect their business processes. This might be more clear and measurable when the regulation becomes active and is applied in practice.

- The Cloud Governance Dial was found to be a viable model. However, it is important that improvements, such as including the GDPR, are made. A dedicated research to this dial could result in a more viable model than it is right now.

- Transparency does seem to influence the decision making of prospects. During this research, however, the findings were based on a very limited analysis. A wider analysis with a large dataset could result in more reliable results.

In addition, recommendations for practice can be made:

- The impact of the GDPR should not be underestimated by any companies dealing with personal data. Even though the actual impact is unknown at this point, seeing in practice that big companies such as Microsoft and Amazon need to put in a lot of effort to comply, shows that this regulation has some serious impact. Businesses should carefully pay attention to how personal data is currently managed and what needs to change to comply with the new regulation.

- The Cloud Governance Dial is a helpful tool for companies to find out what the required IT governance models are to cover all risks associated with business processes or applications. It is important to note that the Cloud Governance Dial needs improvement so therefore should be used as an additional tool and not as a replacement.

Finally, recommendations can be made specifically for the telecom service provider:

- Based on the results from the use case it is very important to make clear rules and agreements between all parties involved before certain services are offered to prevent conflicts or reputation damage. Normally, only two parties were involved, being the client and the telecom service provider. In this new case, at least three parties are involved being the client, the telecom service provider and a cloud vendor such as Amazon or Microsoft.

- The CSA developed the Cloud Security Alliance STAR Self-Assessment which is already completed by companies such as Amazon, Google and Microsoft. This self-assessment is a simple questionnaire with about 40 questions regarding cloud governance which are very straightforward and therefore easy to understand for current clients and prospects. This way, more transparency is

given towards to the client which, as was found during this study, influences the potential client's decision making. Therefore, it is recommended to complete this STAR Self-Assessment.

- During one of the interviews was told that a few changes were still necessary before complying with the GDPR. It is recommended for the telecom service provider to ask themselves questions such as the ones mentioned during the discussion in Chapter 7 to find out whether the right tools and procedures are in place to ensure they are GDPR compliant as soon as it becomes active next year.

Literature

Amazon Web Services (2017). AWS Cloud Security. Retrieved, May 16, 2017, from: https://aws.amazon.com/security/

Amazon Web Services (May, 2017). Amazon Web Services: Risk and Compliance. Retrieved, July 11, 2017, from: https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

Bartolini, C., Gheorghe, G., Giurgiu, A., Sabetzadeh, M., & Sannier, N. (2015). Assessing IT security standards against the upcoming GDPR for cloud systems.

Becker, J. D., & Bailey, E. (2014). IT Controls and Governance in Cloud Computing. In Proceedings of the Twentieth Americas Conference on Information Systems (AMCIS '14) (pp. 1-8).

Beckers, K., Schmidt, H., Kuster, J. C., & Faßbender, S. (2011, August). Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing. In Availability, Reliability and Security (ARES), 2011 Sixth International Conference on (pp. 327-333). IEEE.

Bhoj, P., Singhal, S., & Chutani, S. (2001). SLA management in federated environments. Computer Networks, 35(1), 5-24.

Blackmer, W. S (2016, May). GDPR: Getting Ready for the New EU General Data Protection Regulation. Retrieved, May 9, 2017, from: http://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation/

Brodkin, J. (2008). Gartner: Seven cloud-computing security risks. Infoworld, 2008, 1-3.

Case, G., & Elephant, P. (2007). ITIL V3: Where To Start & How To Achieve Quick Wins.

Catteddu, D. (2010). Cloud Computing: benefits, risks and recommendations for information security. In Web application security (pp. 17-17). Springer Berlin Heidelberg.

Cloud Control Alliance (2017). Introduction to the Cloud Controls Matrix Working Group. Retrieved, April 13, 2017, from: https://cloudsecurityalliance.org/group/cloud-controls-matrix//#_overview

Cloud Security Alliance. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. Retrieved, May 4, 2017, from: https://cloudsecurityalliance.org/

Cody, E., Sharman, R., Rao, R. H., & Upadhyaya, S. (2008). Security in grid computing: A review and synthesis. Decision Support Systems, 44(4), 749-764.

Coso, I. I. (2004). Enterprise Risk Management. Integrated Framework.

Curtis, W. B. (2010). Cloud Computing: eDiscovery Issues and Other Risk.

Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: issues and challenges. In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on (pp. 27-33). Ieee.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.

Dreyfuss, C. (2009). Cloud-Enabled Outsourcing: New Ideas for Effective Governance and Management. Retrieved from Gartner database.

Elifoglu, I. H., Guzey, Y., & Tasseven, O. (2014). Cloud computing and the cloud service user's auditor. Review of Business, 35(1), 76.

EUGDPR (2017). GDPR Key Changes. Retrieved, May 9, 2017, from http://www.eugdpr.org/key-changes.html

Fanning, K. (2014). Cloud Software: How to Validate Third-Party Vendors. Journal of Corporate Accounting & Finance, 25(5), 25-30.

Farrell, R. (2010). Securing the Cloud—Governance, Risk, and Compliance Issues Reign Supreme. Information Security Journal: A Global Perspective, 19(6), 310-319.

Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., & Stoica, I. (2009). Above the clouds: A Berkeley view of cloud computing. Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, 28(13)

Gens, F. (2009). New IDC IT cloud services survey: Top benefits and challenges. IDC exchange, 17-19.

Goo, J., & Huang, C. D. (2008). Facilitating relational governance through service level agreements in IT outsourcing: An application of the commitment–trust theory. Decision Support Systems, 46(1), 216-232.

Google Cloud Platform (2017) Google Cloud Platform Security. Retrieved, May 16, 2017, from: https://cloud.google.com/security/

Harvey, C. (2016). Top 10 Cloud Computing Companies. In Datamotion. Retrieved, February 15, 2017, from http://www.datamation.com/cloud-computing/slideshows/top-10-cloud-computing-companies.html

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of “big data” on cloud computing: Review and open research issues. Information Systems, 47, 98-115.

Herbst, N. R., Kounev, S., & Reussner, R. H. (2013, June). Elasticity in Cloud Computing: What It Is, and What It Is Not. In ICAC (pp. 23-27).

Hofmann, P., & Woods, D. (2010). Cloud computing: The limits of public clouds for business applications. IEEE Internet Computing, 14(6), 90-93.

Horwath, C., Chan, W., Leung, E., & Pili, H. (2012). Enterprise risk management for Cloud Computing. COSO. [Online]. Retrieved, May 9, 2017, from: http://www.coso.org/documents/Cloud\%20Computing\%20Thought\%20Paper.pdf

InfoWorld. (2009). Special report. Cloud computing deep dive.

ISACA. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA.

Isaca, Information Systems Audit, & Control Association. (2011). IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud. Isaca.

Kaufman, L. (2009). Data security in the world of cloud computing. IEEE Internet Computing. 7(4), 61–64.

Kim, W. (2009). Cloud computing: Today and tomorrow. Journal of object technology, 8(1), 65-72.

Kisker, H. (2010). The global software market in transformation: Findings from the Forrsights software survey, Q4 2010

Kliem, R. (2004) Managing the risks of offshore IT development projects. *Information Systems Management, 21*(3), 22-27.

LaLond, A. (2013). Virtual Networks and Remote Acces. Retrieved, May 24, 2017, from: http://cis155al.blogspot.nl/2013/02/chapter-10-virtual-networks-and-remote.html

Lepeak, S. (2014). *KPMG Sourcing Advisory 1Q14 Global Pulse Survey* [Report]. Retrieved, March 6, 2017, from: http://www.kpmg-

institutes.com/content/dam/kpmg/sharedservicesoutsourcinginstitute/pdf/2014/1Q14-sourcing-advisory-global-pulse-report.pdf

Lu, C. W., Hsieh, C. M., Chang, C. H., & Yang, C. T. (2013). An improvement to data service in cloud computing with content sensitive transaction analysis and adaptation. In Computer Software and Applications Conference Workshops (COMPSACW), 2013 IEEE 37th Annual (pp. 463-468). IEEE.

Mangiuc, D. M. (2011). Enterprise 2.0-Is the market ready?. Accounting and Management Information Systems, 10(4), 516.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. Decision support systems, 51(1), 176-189.

McDonough, J. and McDonough, S., (1997). Research Methods for English Language Teachers. London: Arnold.

McLeod, S. (2013). The 5 Domains of IT Governance. Retrieved, May 24, 2017, from: http://www.longviewsystems.com/it-governance/

Microsoft Trust Center (2017) Security. Retrieved, May 16, 2017, from: https://www.microsoft.com/en-us/trustcenter/security

Moeller, R. R. (2007). COSO enterprise risk management: understanding the new integrated ERM framework. John Wiley & Sons.

Mortensen, H (2016). General Data Protection Regulation - Implementation in Danish companies. The Danish ICT and Electronics Federation, DI Digital

Mosher, R. (2011). Cloud Computing Risks. ISSA Journal, July Issue, 34-38.

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. Government information quarterly, 27(3), 245-253.

Nguyen, B. (2010). A comparison of the business and technical drivers for ISO 27001, ISO 27002, CobiT and ITIL. Retrieved, March 6, 2017, from: http://trongbang86.blogspot.nl/2010/11/comparison-of-business-and-technical.html

O'Loughlin, M (2014). IT service management and cloud computing. Axelos.

OWASP (2009, October). Cloud – Top 5 Risks with PAAS. Retrieved, July 4, 2017, from: https://www.owasp.org/index.php/Cloud_-_Top_5_Risks_with_PAAS

Papazoglou, M.P. (2012). Web Services & SOA. Principles and Technology. Pearson (2012)

Potgieter, B. C., Botha, J. H., & Lew, C. (2005, July). Evidence that use of the ITIL framework is effective. In 18th Annual conference of the national advisory committee on computing qualifications, Tauranga, NZ (pp. 160-167).

Rahman, S. U. (2001). A comparative study of TQM practice and organisational performance of SMEs with and without ISO 9000 certification. International Journal of Quality & Reliability Management, 18(1), 35-49.

Rebollo, O., Mellado, D., & Fernandez-Medina, E. (2012). A Systematic Review of Information Security Goverance Frameworks in the Cloud Computing Environment. Journal of Universal Computer Science, 18(6), 798-815.

SAP Cloud Trust Center (2017) Cloud Certification Compliance. Retrieved, May 24, 2017, from: https://www.sap.com/sea/about/cloud-trust-center/cloud-certification-compliance.html

SasConsult (2017). ISAE 3402. Retrieved, April 14, 2017, from: http://www.sasconsult.nl/isae-3402

Saxena, S. (2013). Ensuring cloud security using cloud control matrix. International Journal of Information and Computation Technology, 933-938.

Simmons, M. R. (1997). COSO based auditing. Internal Auditor, 54(6), 68-73.

Sinha, A., Jaiswal, A., Gupta, R., & Chaurasiya, V. K. (2011). SAS 70 to SSAE 16/ISAE 3402: An insight into outsourcing security and process controls, and significance of new service audit standards. ISSN 1931-0285 CD ISSN 1941-9589 ONLINE, 315.

Speed, R. (2011). IT governance and the cloud: principles and practice for governing adoption of cloud computing. ISACA Journal, 5, 17.

Staten, J. (2009). Hollow out the moose: reducing cost with strategic right sourcing. Forrester Research, Inc, 209.

Suhairi, K., & Gaol, F. L. (2013). The Measurement of Optimization Performance of Managed Service Division with ITIL Framework using Statistical Process Control. JNW, 8(3), 518-529.

Terstegge, J. (2015). Managing the Challenges of the Cloud Under the New EU General Data Protection Regulation. Netskope.

Tuttle, B., & Vandervelde, S. D. (2007). An empirical examination of CobiT as an internal control framework for information technology. International Journal of Accounting Information Systems, 8(4), 240-263.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both?. Computers & Security, 24(2), 99-104.

Vormetric (2017). Cloud Data Security Solutions. Retrieved, April 13, 2017, from: https://www.vormetric.com/data-security-solutions/cloud-data-security

Westerman, G. (2006, April). The IT Risk Pyramid: Where to Start with Risk Management. Center for Information Systems Research, Sloan School of Management, V(1D).

Yin, R., (1994). Case study research: Design and methods (2nd ed.). Beverly Hills, CA: Sage Publishing.

Yin, R.K., (1984). Case Study Research: Design and Methods. Beverly Hills, Calif: Sage Publications.

Zainal, Z. (2007). Case study as a research method. Journal Kemanusiaan, 9.

Appendices

Appendix A: Case Study

A case study is used to produce an answer for the hypotheses and problem statement. There are several categories for case studies, being (Yin, 1984):

- Exploratory case studies: Explore any phenomenon in the data which serves as a point of interest to the researcher. This type of study is meant to open the door for further examination of the phenomenon observed.

- Descriptive case studies: Describes the natural phenomena which occur within the data in question. According to a research done by McDonough and McDonough (1997) these studies may be in a narrative form.

- Explanatory case studies: Examine the data closely both at a surface and deep level to explain the phenomena in the data.

Zainal (2007) found several advantages of a case study. First, examination of the data is most often conducted within the context of its use. Secondly, variations in terms of fundamental, instrumental and collective approaches to case studies allow for both quantitative and qualitative analyses of the data. Finally, Zainal found that detailed qualitative accounts often produced in case studies not only help to explore or describe the data in real-life environment, but also help to explain the complexities of real-life situations which may not be captured through experimental or survey research.

Case studies don't only bring advantages, they also have their disadvantages. The first one being that case studies are often accused of lack of rigour. Second, case studies provide a very little basis for scientific generalisation since they use a small number of subjects, some conducted with only one subject. Third, case studies are often labelled as being too long, difficult to conduct and producing a massive amount of documentation (Yin, 1993).

Appendix B: Questions Private/Hybrid/Public Cloud

General

1) What IT governance models are used by your company for the private / hybrid / public cloud services?

2) What are the major differences, auditing wise, between private, hybrid and public cloud services, if any?

International Dimension and Privacy

3) How can the cloud computing user ensure compliance with laws prohibiting data from being stored in certain countries?

4) Is your company already compliant with the General Data Protection Regulation which becomes active next year?

Security Breaches

5) How will the Cloud computing provider identify, respond to, correct, and disclose data or other security incidents that negatively affect the user company and its customers?

6) What are the user organization's audit rights for data loss or data breach?

Privacy and Encryption

7) Who can access the user data when it is at rest or in transit on a provider platform?

8) What type and level of encryption is employed while the data is in transit or at rest?

9) What types of controls or procedures are in place to restrict privileged users within the Cloud computing environment from viewing or modifying the sensitive data stored in the provider's infrastructure?

Audit Rights, Integrity and Availability

10) What are the audit rights (or forensic privileges) for the user organization?

11) How do you deal with transparency?
    - Nondisclosure agreements
    - Independent auditor reports
    - Certifications

12) How often do regular audits, inspections and reviews occur?

13) How is integrity and availability assured?

Exit Strategy

14) What rules are in place when a company terminates his contract regarding the data saved on the private / hybrid / public cloud? (E.g. How does one get his data back, how does it get deleted?)

    Moving from one Cloud computing provider to another will be close to impossible because of compatibility related issues in data, program and operating system differences.

    Reasons for terminating a contract: Changes in ownership, bankruptcy, soured relationships, data security and privacy breaches, fall behind its competitors, prolonged outages.

Appendix C: Questions Client A Telecom Service Provider

1) What role does the Cloud have in pursuing the philosophy to be the favourite provider of essential, trendy and printed promotional gifts?

2) Can an example be given of a functionality (application/process) that you moved to the Cloud? What are the benefits of this now the functionality is in the Cloud?

3) What has made you decide to choose for a Private Cloud solution at KPN instead of a Public Cloud solution back when the decision was made? Has transparency played a role? (Transparency = Certifications, Audit reports)

4) Is there besides Product Compliance and Social Compliance also (IT) Security Compliance? If yes, do you have certifications for these? (Examples of certifications are: ISO, ISAE, ITIL)

5) What for guidelines are in place for carefully dealing with customer data? Has the General Data Protection Regulation (GDPR), which will come into effect next year, affect your business processes? (More information: http://www.eugdpr.org/)

Appendix D: Interview Product Manager Telecom Service Provider

General

1) What IT governance structures/frameworks are used by your company for the hybrid cloud services?

"Our hybrid cloud as a whole is one service which has the certifications ISO 9001, ISO 27001 and ISO 22301. Part of the hybrid cloud is the virtual private cloud which is, in addition to previous certifications, Cloud Compliance Framework (CCF) compliant. CCF was created in collaboration with Deloitte and is a framework based on our own risk analysis and an analysis of the most important frameworks on the market on IaaS, PaaS and SaaS level. It covers anything that we think a company wants to have secured when making the move to cloud computing. When we started to offer managed hybrid cloud, it was not possible to make these CCF compliant due to the heavy auditing from E&Y. This is why the managed hybrid cloud got their own certification being ISAE 3000. The idea is that at some point in the future CCF will become an extension of ISAE 3000."

2) What are the major differences, auditing wise, between hybrid and private cloud services, if any?

"ISO 27001 gets externally audited once a year by an external party in collaboration with our General Council Office. CCF gets audited much heavier by E&Y, since for every individual risk that is described a stamp has to be given. For ISO 9000 and ISO 22301 some interviews take place and it is necessary to show some stuff, but you do not really have to show evidence."

International Dimension and Privacy

3) How can the cloud computing user ensure compliance with laws prohibiting data from being stored in certain countries?

"We are now busy making Public cloud part of our services and this is what we struggle with right now. How are we going to offer a service where we know there will be differences between the guarantees that are given? Something that should be noticed is

that there is a difference between a client that takes the public cloud services themselves and lets us manage it or us taking the public cloud services ourselves and let it be managed by the customer, since there will be different conditions that apply. We have specific appointments with the suppliers, an example being that all our deals are under European rights. To achieve this though negotiations are necessary, since big providers such as Microsoft and Amazon prefer the American rights. A regular customer is not able to negotiate about these rights which means we can offer a customer a bit more assurance that are looking for compliance."

4) Is your company already compliant with the General Data Protection Regulation which becomes active next year?

"A few small adjustments are necessary. We have a meeting about this topic very soon."

5) How will the Cloud computing provider identify, respond to, correct, and disclose data or other security incidents that negatively affect the user company and its customers?

"There is a whole process for this executed by a special department. They agree upon what gets communicated and if it is going to be communicated at all. The responsibility also lays at the privacy. All security incidents are logged by the security team which is mandatory."

6) What are the user organization's audit rights for data loss or data breach?

"I do not know the details. But I can imagine there is a difference between a regular and big customer."

Privacy and Encryption

7) Who can access the user data when it is at rest or in transit on a provider platform?

"In the CCF we have written down that all the data gets the highest classification. We do not want to distinguish between what is privacy sensitive data and what not. Only named accounts have access and only when it is really necessary."

8) What type and level of encryption is employed while the data is in transit or at rest?

"There is no encryption. Perhaps in the near future this will be offered as a separate service. Encryption, however, would directly influence the application, for example performance."

9) What types of controls or procedures are in place to restrict privileged users within the Cloud computing environment from viewing or modifying the sensitive data stored in the provider's infrastructure?

"Named accounts make accessibility limited. Each account again has limited access. In general there are procedures when hiring employees and capturing procedures. We are busy centralising this."

Audit Rights, Integrity and Availability

10) What are the audit rights (or forensic privileges) for the user organization?

"In the contract it says they have the rights for a limited amount of audits with the costs being for the client. However, first we try to set up a meeting with our internal audit and if that does not suffice our external auditor E&Y will try to convince the client. If these two talks do not satisfy the client the last scenario is to let them do an audit themselves."

11) How do you deal with transparency?
    - Nondisclosure agreements
    - Independent auditor reports
    - Certifications

"We share our audit reports with our customers. Our audit takes place in two phases. The first audit takes place in May and these results are directly communicated with our customers. In November, the final version of this audit will be made and again will be communicated and discussed with our customers. In January, our customers receive a bridge letter for the months December and January which is necessary for the ISO 3402 certification. For employees, a Declaration of behaviour given out by the government is

mandatory and they have to agree with a Code of Conduct and sign an NDA when applying. We offer services with the highest classified data which are close to state secrets and those customers have accepted the amount of transparency we offer."

12) How often do regular audits, inspections and reviews occur?

"Two times a year for our certification by E&Y. First internal and then external. With Deloitte we maintain our CCF framework each year."

13) How is integrity and availability assured?

"Important to add to that is continuity. Our back-up services take care of the availability and continuity. The cloud is secured from the outside with by multiple security services. There is one entrance where all the data comes in which is highly secured. Each quarter Deloitte does several tests to check this security. This test takes place from external to internal, but also between tenants internally. We receive the results each quarter."

Exit Strategy

14) What rules are in place when a company terminates his contract regarding the data saved on the hybrid cloud? (E.g. How does one get his data back, how does it get deleted?)

"We want to facilitate our customer in the best way possible to bring back their data. This can be done by means of discs or any other medium. We will only cancel the tenant when they tell us they are done. We provide all possibilities, but the costs will be for the customer. This topic does not really get spoken about when the contract is signed. Every cloud has a solution for this, but the higher you get in the stack the harder it becomes to get your data out of the cloud. On hybrid level this is not an issue, but it will be at the application stack."

Appendix E: Interview Security Manager Telecom Service Provider

General

1) What IT governance models are used by your company for the private cloud services?

‘‘*For private cloud the frameworks we have the standard ISO 9001, ISO 27001 and ISO 22301 certifications. In addition, the Cloud Compliance Framework, a framework which was developed in collaboration with Deloitte, is an extra framework we provide for our customers.”*

2) What are the major differences, auditing wise, between private cloud services and public cloud services, if any?

“I looked into the required standards for both types of services and I have noticed only a few differences in controls and if you ask me personally I do not think a major difference between the two is necessary. I think from a customer perspective the most important thing is that the customer can hold on to its data by knowing where the data is located, who has access to it and by knowing who is collecting the data. This is not mentioned in the ISO frameworks, but is mentioned in the Cloud Compliance Framework.”

International Dimension and Privacy

3) How can the cloud computing user ensure compliance with laws prohibiting data from being stored in certain countries?

“This can only be achieved when your data is in the country where you have to comply with certain law. You will have to trust the legal prudence of that country.”

4) Is your company already compliant with the General Data Protection Regulation which becomes active next year?

“Personally, I am not focussed on this topic, but I do know KPN has been working on this a long time to comply with the regulation when it becomes active next year. This is mostly done by the compliance office. I do question myself how they are going to achieve this, since to me it seems very hard to achieve compliance. If anything looks

like violation of privacy you will need to know where the data is located, who has access to it, how long it has been there, if it can be deleted and much more. There are so many different things which need to be logged that an automated process is required."

Security Breaches

5) How will the Cloud computing provider identify, respond to, correct, and disclose data or other security incidents that negatively affect the user company and its customers?

"The privacy office has rules and procedures for exactly this in place. As soon as you have a suspicion of a security incident you must report this to the security office. They will do further investigation and will decide if it is necessary to report the case. This needs to be done within 24 hours, otherwise it will have consequences."

6) What are the user organization's audit rights for data loss or data breach?

"I can't tell you that, since I don't spend time on this subject."

Privacy and Encryption

7) Who can access the user data when it is at rest or in transit on a provider platform?

"I am not sure who can, but I am sure data is accessed when it is necessary. I did, however, never saw something like that happen myself. This topic does get more and more relevant these days."

8) What type and level of encryption is employed while the data is in transit or at rest?

"Encryption is mentioned in certifications like ISO, but does not happen on large scale yet in practice since no one dares that. Encryption also affects performance. I think the reason encryption is not applied yet on large scale is that customers trust the cloud service providers and if you have your data encrypted and happen to lose the encryption key you will have a big problem. That is why I think encryption on large scale is not happening yet, but I could be wrong."

9) What types of controls or procedures are in place to restrict privileged users within the Cloud computing environment from viewing or modifying the sensitive data stored in the provider's infrastructure?

"I am not able to give a good answer to that since I am not focussed on this topic."

Audit Rights, Integrity and Availability

10) What are the audit rights (or forensic privileges) for the user organization?

"Again, I am not able to tell you that, if you want an answer for this question you should contact someone from the security office."

11) How do you deal with transparency?
    - Nondisclosure agreements
    - Independent auditor reports
    - Certifications

"The certifications we have are open to the public and every customer could ask for these. If the client wants to have an actual look in the report they will have to come to one of our offices. A prospect customer might look into these reports when signing a non-disclosure agreement, but this rarely happens.

ISO is being audited by an external party. With ISO you get the freedom to decide how you manage the controls for each specific ISO certification and you also have to decide for yourself how often you do an internal audit. The auditor looks at how you deal with the ISO requirements, but not in detail. With other frameworks such as the ISAE3000 series, however, external auditors do check till a high level of detail how you achieve said requirements."

12) How often do regular audits, inspections and reviews occur?

"ISO auditing consists of two internal audits and one external audit each year. The results of these audits do not really get shared with the customer. By having the certificates most of the time we have proven enough evidence that we comply. If a customer asks about a detailed report of an audit, they can get a look into the report."

13) How is integrity and availability assured?

“I do not think I can give you the best answer to this question. I suggest you ask this question to one of my colleagues to get a complete answer.”

Exit Strategy

14) What rules are in place when a company terminates his contract regarding the data saved on the private cloud? (E.g. How does one get his data back, how does it get deleted?)

‘‘Many institutions such as banks want proof that all data is, in fact, erased when they decide to leave a cloud vendor. So far we proof with a signed piece of paper that all data is erased or the hardware has been shred.

There is, in my opinion, a better alternative for this which is a software program called Blancco. When using this software, which has been developed by a third party, you move all data that needs to be erased to a certain platform and let the software run. When this process has finished it gives you a report that proofs the data is erased. Blancco does not get used by cloud service providers at this point most likely due to the fact it costs money, but if you want real proof for your customer that their data is gone Blancco is a fair option. Not only does the client want the data gone, but also the cloud service provider themselves, so they are not able to get in trouble later.

With the General Data Protection Regulation becoming active next year I am sure companies are going to invest money into the exit strategy procedures. As long as the regulation is not active, customers do not ask for such type of software and better alternatives costing money this is not a topic being addressed at the moment.”

Appendix F: Interview Consultant Telecom Service Provider

General

1) What IT governance models are used by your company for the private / hybrid cloud services?

"Standard certifications we offer are ISO 27001, ISO 27002 and ISAE 3402. There are many more certifications we have, but this is different for each cloud so you really have to look at each product individually. I do know that CloudNL has many certifications.

Our processes are ITIL based and our architectures use several frameworks such as COBIT to create their own environments which they provide to their customers."

2) What are the major differences, auditing wise, between private, hybrid and public cloud services, if any?

"The main difference is that when a client uses the public cloud there is no way to get in as a customer and all you get is the certifications they offer. The more you move to the public cloud the less you have to invest into auditing. As an example, in the past you had to check your own car while nowadays you bring your car to the garage and assume that they did a good job. This can be related to the public cloud, you assume they are good at what they do. With the private and hybrid cloud services you have more control over the auditing process."

International Dimension and Privacy

3) How can the cloud computing user ensure compliance with laws prohibiting data from being stored in certain countries?

"When you make use of our service CloudNL we can guarantee the data will only be located in the Netherlands, since there are no servers in other countries for this service. If you use on of our other cloud services we offer where your data is kept at servers of for example Amazon or Microsoft, you will have to check their website to find out where your data is kept.

It is important to realise that the cloud provider is responsible till the virtualisation layer and till this point it gives guarantees by means of certifications. For the data itself the responsibility is for the customer. This means it is your decision to choose the right cloud service provider that gives you the most control for your data."

4) Is your company already compliant with the General Data Protection Regulation which becomes active next year?

"We are in the forefront here in the Netherlands. We as telecom service provider of course are an example for the rest when it comes to complying with such regulations. I am not sure whether we are already fully complying with the regulation, since the GDPR doesn't have clear boundaries.

From the cloud perspective the GDPR doesn't cause many changes. As supplier of cloud services, however, this regulation will influence the processes."

Security Breaches

5) How will the Cloud computing provider identify, respond to, correct, and disclose data or other security incidents that negatively affect the user company and its customers?

"First, all our employees get trained on yearly basis. Every year they get an online training what tells them what to do in case of a security breach. In case someone notices a real data breach, the Security officer needs to be called immediately. They will report this to the Dutch Data Protection Authority. Our company reports every incident to this institution, since we don't want to take any risks."

6) What are the user organization's audit rights for data loss or data breach?

"Customers are not allowed to perform audit themselves at our data warehouses. We have our own external auditor which customers can talk to and if they are not satisfied start a discussion with. No exceptions will be made. We get audited externally and other parties can trust these results.

As an example, imagine someone breaks into your house and your local police goes into your house for investigation. It would be weird if another police department in a later

stage again wants to investigate your house and if your neighbour wants to take a look, your whole street wants to take a look! You trust that the results from the first investigation from the local police are sufficient and other parties can rely on that information. We can't invite every single customer to have an audit at our data warehouse since that would end up chaotic."

Privacy and Encryption

7) Who can access the user data when it is at rest or in transit on a provider platform?

"Usually this is only the customer. Even when a server is defect and needs replacement, no one besides the customer is getting access to the data. The people working in the data warehouses only fix the infrastructure and are not able to access the data in any way, because this is secured by the client. We don't want to be able to access the data, since that would make us responsible."

8) What type and level of encryption is employed while the data is in transit or at rest?

"I do not dare to say that exactly. There are many encryption options and I do know that many cloud environments encrypt data at default, but I don't really know what type of encryption we offer. If we would offer in transit encryption, I would advise customers to use AES256, but I am not sure if we offer this service at the moment."

9) What types of controls or procedures are in place to restrict privileged users within the Cloud computing environment from viewing or modifying the sensitive data stored in the provider's infrastructure?

"None of the employees here is authorised to access the data. We do have administrators, but they are only able to access the back-end part to make sure everything is working, but are not able to access the data front-end."

Audit Rights, Integrity and Availability

10) What are the audit rights (or forensic privileges) for the user organization?

"The customer has the right to check the audit status at any moment and could request the report whenever they want. The client is able to take a look into the report, not the end-client. An end-client could be a user which has SAP as a service which is hosted on AWS. In this case SAP is the client which has the right to request the reports."

11) How do you deal with transparency?
    - Nondisclosure agreements
    - Independent auditor reports
    - Certifications

"Every employee is being screened and needs a statement of conduct. For extremely important customers such as the government we have dedicated teams which have extra screening. In the contracts with our clients we have multiple NDA's. For prospects, rarely small parts of reports are offered to get some insight in our certifications, but these reports are not available in public. Usually, the only thing the customer wants to know is whether we have a certification."

12) How often do regular audits, inspections and reviews occur?

"Yearly, monthly, weekly. This differs for each certificate. As an example the ISO 27001 certificate gets audited yearly. Once internal and once external."

13) How is integrity and availability assured?

"We simply guarantee our customers the promised availability and we comply with that. If we don't comply compensation will be offered."

Exit Strategy

14) What rules are in place when a company terminates his contract regarding the data saved on the private / hybrid / public cloud? (E.g. How does one get his data back, how does it get deleted?)

"As customer you are responsible for your own data. If you use the public cloud you know that your data will be saved on multiple servers. If you want to collect your data in that case it depends on how you managed your data and whether backups were made.

If I recall correctly somewhere in our service description we say that after terminating your contract after certain amount of days your data and account both get deleted.

In a public cloud environment it is difficult to guarantee your data is really destroyed, while in the private and hybrid cloud you have more options to achieve this. Because of this, it is important to not put your most sensitive data in the public cloud."

Appendix G: Interview Principal Solution Specialist Microsoft

General

1) What IT governance structures/frameworks are used by Microsoft for the public cloud services?

"We use many different IT governance models which can be found on both Microsoft and Azure trust centre. In addition to the usual ISO, CSA, ISAE certifications we also have two Dutch specific certifications being 'BIR 2012' and 'NEN 7510:2011'. I don't know the details of the first certificate, but I do know the latter is important for organizations in the healthcare sector. Every year we obtain more and more certifications."

2) What are the major differences, auditing wise, between private, hybrid and public cloud services, if any?

"In comparison with the private and hybrid cloud, we take responsibility up to and including the virtualization layer. Everything above that level, starting at OS level, is for your own responsibility. A big advantage of public cloud opposed to the other two types is the ability to scale rapidly on short term. With one simple click it is possible to be able to deal with much more demand than usual and with one more simple click it is possible to reverse this."

International Dimension and Privacy

3) How can the cloud computing user ensure compliance with laws prohibiting data from being stored in certain countries?

"We have three different methods to show the customer that their data really is only in countries they have given us permission for. In the Azure trust centre there are white papers that show exactly what we do. In this paper we explain what we do for security, where we save the customers data and what certificates are applicable. This is the top layer which could be summarised as 'Microsoft over Microsoft'.

The second layer consists of all our certificates. These are from independent parties that audit us. These certificates proof that what we tell them what we do is in fact

achieved. These reports are accessible for all our customers. Sometimes traditional companies come to us and their auditor asks us if they can have a look in our data centre. This is of course not possible, but by showing our certificates and reports this is most of the times sufficient information that is required. I have never seen a company not satisfied with the information we provide.

The third layer is our Online Services Terms (OST), which can be found on our website. The OST consists of appointments between us and the customer. On this level is promised to the customer that the data is only stored in a certain area and that the data is not given to other parties. In fact, we have never given Dutch data to other parties. The American government made six requests in 2016 to obtain data from the Netherlands but this was never successful. When the data is located in the Netherlands, both an American judge as a Dutch judge as to approve the request for certain grounds, which rarely happens.

There is actually a fourth layer for organizations that think that there are always backdoors by security agencies or other parties. For these businesses we offer encryption."

4) Is your company already compliant with the General Data Protection Regulation which becomes active next year?

"We made a promise to our customers that we will be GDPR compliant as soon as it becomes active till the virtualisation level. It is important to keep in mind that the rest, starting at OS level and further, needs to be GDPR complaint too but is not our responsibility. We do, however, offer assistance in this matter to be GDPR compliant."

5) How will the Cloud computing provider identify, respond to, correct, and disclose data or other security incidents that negatively affect the user company and its customers?

"I don't know the details of the procedures but these can be found back in the OST. We will communicate a description of the breach, the time period and the consequences of the breach with our customer. In addition, the name of the reporter, the name of which it

was reported to and the steps that were taken after that are noted. This whole process should happen within 5 business days."

6) What are the user organization's audit rights for data loss or data breach?

"Customers do not have permission to enter the data centre, even in case of a data loss or data breach. I don't know whether exceptions are made for large partners."

7) Who can access the user data when it is at rest or in transit on a provider platform?

"Almost no one is able to get access to the servers were the data is held. We have a responsibility scheme which is based on a least to know basis. We don't have administrators that have access to everything. Instead, they might get up to 30 minutes to make a change or repair a defect, which will be logged and has to be requested in advance. To give you an idea of the amount of people that work on this level: At the Dublin data centre work seven people in total.

In addition, all data in a data warehouse is scrambled. Some customers think that if you take one database from a stack you can read the data from this one database, but this is not the case.

At Microsoft we have a blue team and a red team. The blue team makes sure all data is safely secured. The read team is responsible to find any possible security flaws. We found that at most companies' theft happens by means of identity theft. This is why we always use multifactor authentication."

8) What type and level of encryption is employed while the data is in transit or at rest?

"This differs per service and server. We offer different types of encryption, but this should be a decision of the customer. We also encrypt data in transit, but of course this will impact performance. AES2500 bit is the encryption we apply. Bitlocker is another tool that customers can use that doesn't impact performance much. Office 365 is a service that is always encrypted."

9) What types of controls or procedures are in place to restrict privileged users within the Cloud computing environment from viewing or modifying the sensitive data stored in the provider's infrastructure?

"We have very strict rules regarding this matter. Everything that happens in the infrastructure is logged. The people that work at the data centre never get insight on the data that is one a database. We are the data processor, not the data owner. For us it is important that the customer can process its data whenever needed."

Audit Rights, Integrity and Availability

10) What are the audit rights (or forensic privileges) for the user organization?

"As I said previously, there aren't really. All businesses can have a look in our reports. In addition, it is possible to take a look in one of our data centres, but beforehand a box needs to be ticked that says it is just for looking around and not for audit reasons."

11) How do you deal with transparency?
- Nondisclosure agreements
- Independent auditor reports
- Certifications

"Each employee is screened during the recruiting process. In addition, NDA's have to be signed. We have three different of layers of business impact being: Low business impact, Medium business impact and high business impact. It is not possible for us to look into data of our customers. As mentioned in the first few questions, we have many certifications which were audited by independent auditor reports."

12) How often do regular audits, inspections and reviews occur?

"This differs for each report. All this information can be found online. Most of the times audits happen several times a year. We perform audits, inspections and reviews as often as we think it is necessary to assure compliance. We hope that some certifications will be combined in the future, since the number of certifications right now seems to be excessive."

13) How is integrity and availability assured?

“Storage of data happens at multiple locations, for example Amsterdam and Dublin. For the customer, however, only one of these locations is accessible. This way we can guarantee the availability we offer.

Amsterdam and Dublin are located in one Geo. We also have a Geo for America and Asia and Oceania combined. Soon Africa will be added as a Geo. Germany is also part of the Europe Geo, but is different than the other two locations. The infrastructure is hosted by a German party instead of us and an Azure layer is placed on top of it. This means that the infrastructure is not hosted by an American company, which could help in specific legal situations. We try to host everything on our own servers when possible.”

Exit Strategy

14) What rules are in place when a company terminates his contract regarding the data saved on the public cloud? (E.g. How does one get his data back, how does it get deleted?)

“We have standard protocols for this. What I know is that the customer will be owner of the data hosted on our servers for a long time, even after termination of the contract. In the OST can be found that after 90 days after terminating the contract, the data will be deleted. In practice, this time period is often even longer, unless the company wants us to delete the data earlier. This time period is so long, so companies have a lot of time to decide how to obtain the data back from the cloud.”

Appendix H: Interview Client A Telecom Service Provider

1) What role does the Cloud have in pursuing the philosophy to be the favourite provider of essential, trendy and printed promotional gifts?

"At the moment, half of our revenue is based on internet purchases. We started with having our systems on premise and connected these to the internet. These days we have sort of a mix, some systems are on premise and some parts of our business we have in the private cloud at the telecom service provider. Their platform is shared, but we have our own environment in that platform."

2) Can an example be given of a functionality (application/process) that you moved to the Cloud? What are the benefits of this now the functionality is in the Cloud?

"One example is our mail environment. First we had our mail application on premise and now we take this as a service from the telecom service provider. The benefits are that we don't need technical management anymore for this service and the solution really is a commodity. The functionality is the same as before, if not better. Now we can take advantage of every new development immediately, which in the past took years before we could take advantage of these. Another benefit is that the application service gets continuously managed by the telecom service provider."

3) What has made you decide to choose for a Private Cloud solution at KPN instead of a Public Cloud solution back when the decision was made? Has transparency played a role? (Transparency = Certifications, Audit reports)

"For us the most important factors we took into consideration for our decision-making process was that we wanted a contact point at the company we would be hosting our data and we want to know where our data is located at any time. With the public cloud we are not sure where our data would be located."

4) Is there besides Product Compliance and Social Compliance also (IT) Security Compliance? If yes, do you have certifications for these? (Examples of certifications are: ISO, ISAE, ITIL)

“We don’t have any certifications regarding this discipline.”

5) What for guidelines are in place for carefully dealing with customer data? Has the General Data Protection Regulation (GDPR), which will come into effect next year, affect your business processes? (More information: http://www.eugdpr.org/)

“We won’t be affected by this regulation when it comes to our customers. The only data we store are business addresses and contact details. No personal data like house addresses and birthdays are stored on our servers. When we look at our HR systems personal information about our employees can be found. For this we do need to comply with the new regulation. We still need to take a few steps to comply with this new regulation. We have our HR system outsourced to another company, so we will have to audit them to see if they comply.”