Trust in the cloud

Loes Pross
Business Administration
Faculty of Behavioural, Management
and Social Sciences
8th of December 2016

MASTER THESIS
MSc in Business Administration

Trust in the cloud

Author

Loes S. Pross
Study program: Business Administration
Faculty of Behavioural, Management and Social Sciences
Student no.: 1532863
E-mail: l.s.pross@student.utwente.nl

Graduation Committee

Dr. Ir. A.A.M. Spil
Prof. Dr. M. Junger

Hengelo, 8th of December 2016

Acknowledgements

The document you are about to read is the final result of my Master Thesis project, conducted to obtain my Master's Degree in Business Administration from the University of Twente. With this thesis the program is completed and it concludes my education. The writing of this thesis has been a learning process. Both academically in the field of Business Administration and personally in experiencing challenges along the way. Personally, this process came with some hurdles I had to take and it has taught me to believe in myself and keep on going.

The completion of this project would not have been possible without the help and support of others. In the first place, both my supervisors Dr. Ir. A.A.M. Spil and Prof. Dr. M. Junger deserve a big thanks. They helped and advised me and gave me constructive criticism and support. Furthermore I would like to thank the people who participated in the case studies and the expert that helped me validate and complete the finding of this research for their contributions and their candour.

I would also like to thank my parents and sisters for their feedback, support and believe in me during these past months and for all the years before. Now that this thesis is finished I am confident that my student-career is behind me and I am ready to enter the world of professionals.

Abstract

The presented study is an examination of trust in cloud computing for organizations in the Netherlands. In this report the following research question will be answered: "*What are the attributes of cloud computing for an organization to trust a cloud provider?"*

To answer this research question, a literature research was conducted followed by multiple case studies and an expert interview. The literature research was conducted to gather the attributes of cloud computing for an organization to trust a cloud provider and to propose a research model based on the literature and two main adoption theories. In order to test and validate the research model multiple case studies were held and an expert interview was conducted.

According to the proposed research model trust is expected to have an influence on the adoption of cloud computing, with security, standards and certification, and reputation influencing the level of trust. Besides trust quality, divided into system quality and service quality, and compatibility also are expected to have an influence on the adoption of cloud computing by organizations.

Eight organizations agreed to participate in the multiple case studies. In the multiple case studies the interviewees were asked questions regarding the use of cloud computing and their trust in cloud computing. In addition to the multiple case studies an expert in the field of cloud computing was interviewed as an extra validation of the results of the case studies. The results show that the organizations and expert concluded that security is one of the most important attributes. Although the cloud providers do need to work on their security level. The case study showed that the organizations are hesitant in using the cloud for their core business or private-sensitive information, which makes them use cloud computing in a smaller extent than they could have. While the expert mentioned that a cloud environment in most cases is more secure than your own and you should use it, even for the private-sensitive information. The expert also mentioned that certification and standards show the quality of the cloud provider. The organizations request a more dynamic certification and standards of the cloud provider so the transparency will be increased and a certain level of security can be guaranteed. The continuity and with that the reputation of the cloud provider is of an importance to the organizations when choosing a cloud provider. Concluding the results also show that the compatibility of the cloud environment with the systems of the organization is not validated. The overall quality of the cloud is of greater importance to the organizations and expert. . The quality of the system should meet the quality of their own systems if not exceed this quality in order to adopt cloud computing. Organizations require great service quality with a 24/7 helpdesk from the cloud provider. Not being able to access the cloud environment for even a few hours can be devastating for an organization. Organizations also expect some personalized service of the cloud provider and not being just one of the hundred organizations that have employed their cloud computing service.

Looking at the attributes, no single attribute on its own can explain the trust and adoption of cloud computing. A trusted cloud provider may also not score on all of the attributes. Therefore a right balance between the different attributes is required for a cloud provider to ensure trust from organizations. This research shows that there is not one attribute or sample of attributes that explains the trust in all cases and that every organization and situation allows for a different combination of attributes.

The trust in cloud computing and the increasing adoption of cloud computing is a widely debated topic, our study showed the perspective of organizations and their trust in cloud computing. In order to explain the attributes they require for trust and adoption of cloud computing. Looking at the literature study and research model no single study had encompassed all the attributes that were used in our research. With this our research aims to have practical and academic contribution and can serve as a guideline for future research.

Table of Contents

List of Abbreviations

CIA	Confidentiality, Integrity and Availability
CSC	Cloud Service Certifications
DDos	Distributed Denial of Service
EC2	Elastic Compute Cloud
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
IT	Information Technology
IS	Information Security
ISO	International Organization for Standardization
PaaS	Platform as a Service
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
SaaS	Software as a Service
SLA	Service Level Agreement
TAM	Technology Acceptance Model
TOE	Technology-Organization-Environment framework
VPN	Virtualized Private Network

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Problem statement

"Cloud computing is one of the biggest growing segments within the Information Technology" (Subashini & Kavitha, 2011, p. 1). In the popular press cloud computing was in 2011 described as the next big thing and "a major technology disruption" (Weber, 2011, p. 1). Cloud computing has since then grown and its use has increased. Cloud computing is the new paradigm for "hosting and levering services over the Internet" (Zhang, Cheng & Boutaba, 2010, p. 7). It is clear that cloud computing has versatile opportunities for companies and that it is an emerging technology. However when decisions on cloud computing for organizations are made, trust is one critical obstacle for the adoption of cloud computing (Arpaci, 2016).

Adopting cloud computing also has a lot of advantages to offer for organizations; "it dramatically lowers the cost of entry for smaller firms trying to benefit from compute-intensive business analytics that were hitherto available only to the largest corporations; it can provide an almost immediate access to hardware resources, with no upfront capital investment for users, leading to a faster time to market in many organizations; cloud computing can lower IT barriers to innovation, as can be witnessed from the many promising start-ups, such as Facebook and YouTube; cloud computing makes it easier for enterprises to scale their services – which are increasingly reliant on accurate information – according to client demand; and cloud computing also makes possible new classes of applications and delivers services that were not possible before" (Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2011, p. 178).

Even with these advantages there still remain trust issues for organizations with the adoption of cloud computing. The IT departments of many organizations feel "more comfortable with supporting old mainframes and enterprise software instead of supporting their company's business strategy" (Weber, 2011, p. 1). A lack of trust is a key inhibitor to the adoption of cloud computing (Pearson, 2013). Organizations have fewer concerns about the health of the servers, but have more concerns regarding the security and privacy of their content in the cloud. Organizations feel that by brining their environment to the cloud they will face a higher security and privacy risk than if they keep running things the old fashioned way. While cloud providers claim that the cloud is more secure than whatever organizations are using now (Talbot, 2010; Kshetri, 2013). There remains a gap between the cloud providers' claims on the quality and safety of their system and the users', in this case organizations', view on the quality and safety of the system.

The aim of this research is to provide a better understanding of the trust issues organizations have with cloud computing and the attributes organizations require in order to trust a cloud provider with its content.

1.2 Research Question

This research aims to develop theory regarding the attributes organizations require in order to trust a cloud provider with their content. The following research question will guide the proposed study:

What are the attributes of cloud computing for an organization to trust a cloud provider?

In doing so, the proposed research aims to investigate the experiences organizations have with cloud computing and providers, their level of trust in cloud computing and providers, and the attributes organizations require for cloud computing.

The attributes in this context are meant as the standards organizations have regarding a cloud environment in order to trust it with their content. If these standards are met the organizations have the trust in the cloud environment and provider to use cloud computing for their organization and therefore adopt it. The proposed research will therefore examine the attributes of cloud computing for an organization to trust a cloud provider.

In addition to the central research question the following guiding question have been formulated, in order to guide the process:

1. What types of cloud environments are there for organizations to choose from?
2. What are the keys issues with the adoption of cloud computing?
3. How do these key issues influence the degree to which an organization adopts cloud computing?
4. To what extend do organizations trust cloud providers?

The first guiding question seeks to inform on the different types of cloud environments and what options organizations have to choose from. The second guiding question seeks to reflect the key issues organizations have regarding the adoption of cloud computing as indicated in the literature; an example is security. The third and fourth guiding questions seek to reflect the outcomes of the case studies and therefore the trust issues the interviewees and organizations have with cloud computing and adopting it.

Chapter 2 Literature review

2.1 Planning of the literature review

An extensive literature review provides an overview of the current academic insights in the area of cloud computing. An analysis and review of the existing academic literature gains insights and gives guidance for the research (Tranfield, Denyer & Smart, 2003). The method for a systematic literature review by Wolfswinkel, Fortmueller, and Wilderom (2013) was used. The method of Wolfswinkel et al. (2013) means defining criteria, searching with these criteria, refining the sample, analysing the content and presenting the content. For the systematic research the database of Scopus was used. Within Scopus only the Social Sciences and Humanities section was used. The search criteria are stated in Table 1.

Document type	Articles
Subject areas	Computer Science; Business management and accounting
Language	English
Source type	Journals
Search terms	Cloud computing AND Trust or Cloud AND Trust

Table 1 Search criteria for the systematic literature review in Scopus

Besides Scopus also Google Scholar and Google Books were used to find the needed literature. The same search terms applied here. Throughout the search articles, abstracts, titles, and conclusions were read as well as forward and backward citations checks were performed. The articles that remained are used as the core of this chapter.

2.2 Cloud Computing Literature Review

2.2.1 History of Cloud Computing

In 1961 in the MIT Centennial talk, John McCarthy said that "If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility … The computer utility could become the basis of a new and important industry", this implies the underlying concept of cloud computing (McCarthy, 1999).

Nowadays there is a growing trend of cloud computing and therefore many definitions have evolved in the literature. The most used and prominent definition of cloud computing is introduced by the American National Institute of Standards and Technology (NIST).

"Cloud computing is 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." (Mell & Grance, 2011, p. 2).

Besides the introduction of the underlying concept of cloud computing in the 1960s by John McCarthy, also the characteristics of cloud computing were explored. In 1966 Douglas Parkhill did this for the first time, in his book The Challenge of the Computer Utility. In his book Parkhill provides a vision for computing in the future where it is a utility just as any other, e.g. phones, electricity: always available when needed (on-demand) (Parkhill, 1966).

The real history of the term cloud comes from the telecommunications world. Where in the nineties telecommunication companies started to offer virtualized private network (VPN) connections. The VPN services were the replacement of dedicated point-to-point data circuits, which had the disadvantage of wastage of bandwidth. With the VPN connections the telecommunication companies

offered the same quality service, but at lower costs and with which they were able to switch traffic that enabled balance of the utilization of the overall network. Cloud computing now is the extension of the VPN concept by covering servers and network infrastructure (Harauz, Kaufman & Potter, 2009). But not only the VPN connection has made an impact on what cloud computing is today, also other recent technological advances have made this possible. The three core technologies that have made this possible are: virtualization, multitenancy and Web services (Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2011). These technologies made cloud computing as an utility possible, but even more important made it economically feasible and are the drivers behind the evolution and adoption of cloud computing (Creeger, 2009).

Since the sixties and the introduction of the concept by John McCarthy cloud computing has developed itself. In the history of cloud computing the arrival of Salesforce.com in 1999 is one of the first milestones (Harauz et al., 2009). Salesforce.com delivered enterprise applications through a simple website. In 2002 Amazon followed with the development of Amazon Web Services, with this they provided a suite of cloud-based services including storage, computation and even human intelligence through the Amazon Mechanical Turk (Harauz et al., 2009). In 2006 Amazon followed up with the launch of Elastic Compute cloud (EC2), which is a web service that allows individuals and small companies to rent computers on which they can run their own applications. The latest milestone for cloud computing came in 2009 with the development of Web 2.0, which made Google and others to start to offer browser-based enterprise applications, such as Google Apps (Ambrust, Fox, Griffith, Joseph, Konwinsky, … & Zaharia, 2009).

Grid computing has made evolve the concept of cloud computing and also grid is often used as a backbone of cloud computing. With grid computing the focus was on an infrastructure that delivers storage and computing resources, this has shifted to an economy-based focus which aims to deliver more abstract services and resources (in the cloud) (Messerschmidt & Hinz, 2013).

With the emerge of cloud computing as a viable and on-demand platform, many users from various backgrounds are sharing virtual machines to perform their daily activities (Harauz et al., 2009). Also many players in the industry have made their move towards cloud computing and implemented it.

2.2.2 Characteristics of Cloud Computing

In the previous paragraph the definition of cloud computing by Mell & Grance (2011) was mentioned. Following their definition cloud computing consists of five essential characteristics, three service models, and four deployment models. The five essentials characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

As mentioned cloud computing has three different service models, Cloud Software as a Service (SaaS), Cloud Infrastructure as a Service (IaaS) and Cloud Platform as a Service (PaaS).

- SaaS is a software distribution model, in which the customers are provided with a particular piece of software. The cloud provider runs the software and enables the customer to access it, but the customer has to feed the data and instructions (Weis & Alves-Foss, 2011). In SaaS the users are faced with less responsibility than compared to IaaS and PaaS. In the case of SaaS "service levels, security, governance, compliance, and liability expectations of the service and provider are contractually stipulated, managed to, and enforced" (Zargari & Smith, 2014, p. 150). The management of the infrastructure of the cloud is therefore handled completely by the cloud provider.
- IaaS is an on-demand service of compute power and storage space. IaaS can provide customers server, disk storage, database and operating system, among other things (Kshetri, 2013). The users of IaaS are not able to manage or control the underlying cloud infrastructure (Zargari & Smith, 2014). The users do have access and control over the storage, applications, and certain network components. An example of a big IaaS provider is Amazon with its Elastic Compute Cloud (EC2), which will be described in section 3.2.
- PaaS provides customers an application environment. The applications are developed and executed by cloud vendors and the platforms provided by them. Facilities that are provided for

customers with PaaS are security, application serving, database management, and workflow management. Examples of well-known PaaS vendors are Google, with the Google App Engine, Salesforce.com, and Microsoft with the Windows Azure platform (Kshetri, 2013).

Differences in the service models do have an influence on the types of cloud computing related services and products that can be offered by the cloud service provider. But even more importantly the differences in the services models also have an influence on the risks and the degree a cloud service provider is responsible for the maintenance and management of it (Mell & Grance, 2011).

The four deployment models according to the paper by NIST are community cloud, hybrid cloud, private cloud, and public cloud (Mell & Grance, 2011).

(1) The private cloud is a cloud infrastructure for exclusive use by a single customer or organization, hosted either internally or externally and managed by a third-party, internally or a combination of them (Mell & Grance, 2011).

(2) The community cloud is a cloud infrastructure that is shared between several communities or customers with common concerns (e.g., security requirements, mission, compliance considerations, and jurisdiction) and hosted either internally or externally and managed by a third-party, internally or a combination of them (Mell & Grance, 2011). Compared to a private cloud the costs of a community cloud are spread over more users.

(3) The public cloud is a cloud infrastructure that is made for open use by the general public. The public cloud can be owned by an organization such as a government organization, business, academic, or even a combination of these organizations. The public cloud "exists on the premises of the cloud provider" (Mell & Grance, 2011, p. 3). Customers of the public cloud generally have access to it via the Internet, since the cloud providers own and operate the infrastructure at their datacentre. Examples of public cloud providers are Amazon, Microsoft and Google. In contrast to the other deployment models the public cloud is often offered to customers for free.

(4) The hybrid cloud is a cloud infrastructure that is a composition of two or more cloud infrastructures (private, community or public) that remain separate entities but are bound together offering the benefits of these multiple cloud infrastructures. The two or more cloud infrastructures are "bound together by standardized or proprietary technology that enables interoperability" (Jansen & Grance, 2011, p. 3).

The four deployment models of cloud computing are of significance when we look at the potential products and services that are cloud computing related that stakeholders now are able to offer. These products and services differ depending on the deployment model an organization is using or is considering to integrate. The four deployment models give an organization each a different level of control over their data. Higher risks for the organizations are associated with community or public clouds (Jansen & Grance, 2011). Therefore it requires organizations to do a proper evaluation of the risks before choosing one of the deployment models.

Following the definition of cloud computing by Mell & Grance (2011) the five essential characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

- *On-demand self-service* is one of the five essential characteristics of cloud computing. According to Mell & Grance (2011) it is on-demand self-service when "a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider" (p. 2). By adopting cloud computing end-users want to remotely store their data and use the on-demand storage service, without having the burden of local storage (Burda & Teuteberg, 2014). Cloud computing therefore offers the benefit of having continuous availability to archived data, which can be accessed simultaneously from different devices anywhere at anytime.
- According to Mell & Grance (2011) *broad network access* means that "capabilities are available over the network and accessed through standard mechanisms that promote use by

heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)" (p. 2).

Zaghari & Smith (2014) mentioned the accessibility of multiple datacentres worldwide as one of the big benefits of cloud computing. By having this access the number of hardware components and applications at run time can be reduced. Amazon was one of the pioneers in cloud computing with its Amazon Elastic Compute Cloud (EC2), which provided users a huge amount of storage space that could be accessed from any location connected to the Internet. As mentioned in section 3.3.1.1 according to Burda & Teuteberg (2014) cloud computing provides users with the ability to access it simultaneously from various devices, such as mobile phones and tablets, at anytime and anywhere.

- According to Mell & Grance (2011) *resource pooling* occurs when "the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the consumer demand" (p. 2). With resource pooling there is a sense of location independence, since the customers have no control and knowledge over the exact location of the provided resources. Customers may have the ability to specify the location at a higher level of abstraction (e.g., datacentre, state or country) (Mell & Grance, 2011). Examples of resources are storage, memory, network bandwidth, and processing.

  However, Mell & Grance (2011) may have mentioned resource pooling as one of the five essential characteristics of cloud computing and also as a big advantage for adopting cloud computing in 2009 they noted that the resource pooling in the cloud may result in questioning the data confidentiality and integrity (Mohammed, 2011). The average citizen may be ignorant to the security issues of the cloud, but most organisations are not that ignorant. Therefore organisations are not fully using the online services of cloud computing. In the past there have been several cloud failures that lead to major problems for the customers, examples are Amazon with a lost of service due to the lightning strike (Metz, 2009), Microsoft's data loss (Lonescu, 2009), and the first crash of Microsoft Azure cloud (Clarke, 2009).
- *Rapid elasticity* can be described as "capabilities that can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time" (Mell & Grance, 2011, p. 2). Users can, for example, automatically request additional space in their cloud. Cloud computing is setup to provide users with a seamless service. Therefore the service appears to be automatically and infinite for the users (Zargari & Smith, 2014). There are still some concerns about the rapid elasticity of cloud computing, since the requests of users have an impact on the system. The request the cloud provider gets can require a precise administration and can also be demanding. Some argue that therefore there should be a monitoring tool to control the requests to keep providing the benefits it can with rapid elasticity.
- The fifth essential characteristic of cloud computing is *measured service*. Measured service is described by Mell & Grance (2011) as "cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of utilized service" (p. 2).

  Cloud providers are measuring the service to deliver the customer a precisely configured product. Therefore cloud providers will measure, for example, the network bandwidth, memory utilization or any other aspect of the cloud solution. This allows them to deliver the customer a service that meets the customer's expectations. At the same time the cloud providers provide themselves with numbers, which allows them to measure the costs of the cloud and their return on investment (McLarnon, Robinson, Milligan & Sage, 2014).

Figure 1 presents an overview of all cloud services, deployment models and the central characteristics of cloud computing.

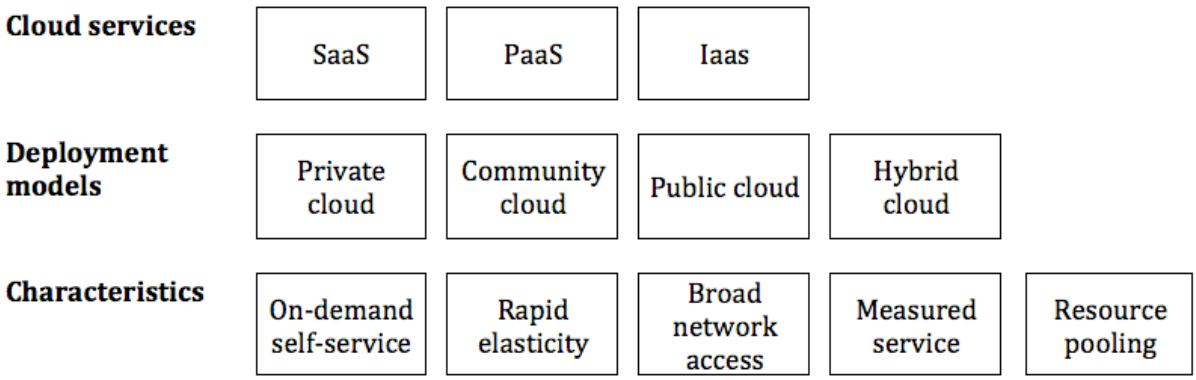

Figure 1 Overview cloud computing

2.2.3 Status quo on cloud computing

Research by Lins, Grochol, Schneider and Sunyaev (2016) discusses the cloud service certifications (CSC's) that have been developed in response to the security, privacy, and reliability concerns of organizations. But even with this certification there remain challenges for cloud providers and organizations. To have this certification widely adopted the providers and auditors "need the motivation and expertise to participate in continuous monitoring and auditing" (Lins et al., 2016, p. 68). In the final recommendation of Lins et al. (2016) they therefore also state: "the ever-changing cloud environment, fast technology cycles, regulatory changes, and increased adoption of business-critical applications demand highly reliable cloud services. Dynamic certification of cloud services can prove providers' high level of reliability and security to potential customers. However, methods to efficiently and continuously assess cloud services are still in their infancy. Organizations such as the Cloud Security Alliance and EuroCloud are developing processes and techniques for continuous auditing of cloud services. We believe that dynamic certification is a step toward more trustworthy and transparent cloud computing environments" (p. 70).

Research by de Hert, Papakonstantinou & Kamara (2016) discusses the cloud computing standard ISO/IEC 27018. In their research they mostly focus on the protection of personal data in the cloud and therefore on the consumer level. The impact of the ISO/IEC 27018 standard on business is not discussed. But it shows that the standard is intended to use in the market "granting a competitive edge to certified providers, provides concrete incentives to implement – to the benefit of the broader data protection purposes" (de Hert et al., 2016, p. 28).

The research by Rangasamy and Somasundaram (2016) is on the trust in grid computing system. In their research they use different types of trust, such as service provision trust, behavioural trust, identity trust, and reputation trust. They state that the trust in the providers' honesty, success rate, competence, reputation and availability will influence the decision of the customer to access them.

Arpaci (2016) studied the intention of students on using mobile cloud storage services. In this case the growth and use of mobile devices is substantial and therefore also the use of cloud services due to the limited storage in these devices. The study found that in contrast to other studies that "perceived security and perceived privacy are directly related to trust in mobile cloud services and indirectly related to attitudes and behavioural intentions toward using such services" (Arpaci, 2016, p. 156).

2.3 Trust

Trust is a concept that has been around for quite a long time. It is as old as the history of mankind and the existence of the human social interactions (Wang & Emurian, 2005). Trust is according to the Oxford English Dictionary (1971) defined as "confidence in or reliance on some quality or attribute of a person or thing, or the trust of a statement" (p. 3423). In the literature however researchers have a difficulty in operationalizing trust and disagree on the basis definitions. This is likely due to trust being an abstract concept that is often used with related concepts (Wang & Emurian, 2005). Besides trust is also a multi-faced concept that incorporates behavioural, cognitive and emotional dimensions (Lewis & Weigert, 1985). Research on trust in cloud computing has shown that trust is not easily defined and many definitions of trust exist within computer science (Artz & Gil, 2007; Mayer & Davis, 1995). The definition of trust by Zaheer, McEvily and Peronne (1998) that received regular mention will be used in this research.

"Trust is the expectation that an actor can be relied on, will be predictable, and will act fairly" (Zaheer et al., 1998, p. 143).

The definition of trust according to Zaheer et al. (1998) allows for the possibility of betrayal. They view it as an inherent feature of trust. The probabilistic element of trust is for persons to make a "leap of faith" by placing confidence in, in this case, a cloud provider, without knowing for certain that the providers' future actions will not produce unpleasant surprises.

Besides the definition of trust by Zaheer et al. (1998) more recent research has shown that trust in an online setting can be classified in two types: system trust and interpersonal trust (Hew & Kadir, 2016; Hsu, Chang & Yen, 2011; Leimeister, Ebner & Kremar, 2005; Ratnasingam, 2005).

"System trust is the belief resulting from the reliability and reliance of an information system while interpersonal trust refers to the belief resulting from the feeling of secure for other parties in the social exchange" (Hsu et al., 2014, p. 237).

On the other hand the research of Uusitalo, Karppinen & Juhola (2010) argues that there is a difference in 'hard' trust and 'soft' trust. Hard trust involves "authenticity, encryption, and security" (Uusitalo et al., 2010, p. 713). Whereas soft trust involves "human psychology, brand loyalty, and user-friendliness" (Uusitalo et al., 2010, p. 713). Therefore trusting the cloud computing and the cloud provider involves a lot of issues. Lin and Varadharajan (2007) mentioned that 'soft' trust is based on trust relationships through social mechanisms and 'hard' trust is based on security mechanisms. These types of trust are inline with the concepts of trust Hsu et al. (2014) introduced. For our research a distinction between 'hard' and 'soft' trust is used. Hard trust is the trust that is established via security, certification, and encryption (Head et al., 2001; Lin et al., 2004; Uusitalo et al., 2010). Soft trust is the trust that is derived from mechanisms like reputation, experiences and quality (Head et al., 2001; Lin et al., 2004; Uusitalo et al., 2010).

2.4 Trust and cloud computing

Due to the broad definition of trust and cloud computing the relationship between both will be elaborated further. Trust and cloud computing is a widely discussed subject due to thigh risks involved for organizations that rely on cloud computing. In 2011 Amazon.com's web service business had a widespread failure, which took down many Internet sites and made them inaccessible for hours. In an interview with the New York Times Campbell McKellar, founder of Loosecubes, a website that was not available due to Amazon.com's failure, said "clearly you are not in control of your data, your information" (Cain Miller, 2011). Although the cloud has benefits that are significant, interruptions like these are major for an organization. With risks like these and challenges in the trust of cloud providers accompanied with concerns for lack of transparency, security, privacy, reputations issues, and diminishing user control, many trust-related discussions appear (Kim & Yoon, 2012). A cloud provider saying "trust me" to organizations does not necessarily mean that organizations will respond with "we trust you".

Regarding the two types of trust and cloud computing. The issues of 'soft' trust cannot be as easily resolved. It concerns the quality of the service, the reputation the provider and cloud computing has, and trust in their privacy (Head et al., 2001). Organizations may also be concerned about whether the cloud provider will stay in business for some time (Jarvenpaa et al., 1999). The continuity of the organization with their reputation can have an effect on the amount of trust organizations have.

While these are all concerns regarding the 'soft' trust organizations also have concerns that relate to the 'hard' trust. A lack of trust can also be generated by the "perceived lack of clarity in service level agreements (SLAs) and security and privacy policies, standard terms and conditions, and sometimes the immaturity of cloud services" (Cattedu, 2015, p. 1). The concerns on 'hard' trust deal with the safety and it focuses on technological solutions to resolve these concerns (Head et al., 2001).

2.5 Risks of cloud computing

Although cloud computing has advantages for organizations there are also risks that involve the adoption of cloud computing and may therefore hinder the adoption of cloud computing. Literature research showed three risks receiving regular mention: confidentiality, integrity and availability. These risks are in the information security known as the CIA-triad. In Figure 2 the CIA-triad is shown.

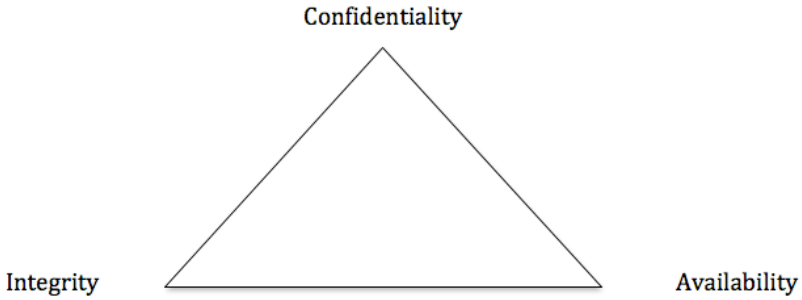

Figure 2 CIA-triad

The CIA-triad has for several decades been used as a conceptual model for computer security and information security (Whitman & Mattord, 2012). The origin of the CIA-triad can be traced back to 1975 when Saltzer & Schroeder stated that at time three categories of threats to information were distinguished by security specialists: unauthorised information modification (integrity), unauthorised information release (confidentiality) and unauthorised denial of use (availability). The term CIA-triad appeared in 1986-1987 as a term coined by the Johnson Space Center, USA (Parker, 2010). Since then the CIA-triad has rapidly gained popularity among information security practitioners and is now a general accepted foundation of information security. Information security requires that the three components of the CIA-triad are upheld. Information systems, like cloud computing, need to ensure that only the organization that is authorized to use it can access the information and no third parties are able to access it (confidentiality). The information stored in cloud computing need to be protected against unauthorised actions in the cloud like accidental and undesired modifications or deletion (integrity). And of course being able to access the system anywhere at anytime, whenever the organization or user needs their services (availability).

Confidentiality

According to Arias-Cabarcos, Almenárez-Mendoza, Marin-Lopez, Diaz-Sanchez & Sanchez-Guerro (2012), Kshetri (2013), Morales-Sandoval, Vega-Castillo & Diaz-Perez (2014), Zargari & Smith (2014), and Lian (2015) confidentiality is one of the biggest concerns regarding cloud computing. One of the first security services that are required in a cloud is confidentiality. When a cloud provider ensures confidentiality, the provider also does not learn any information about the customer's data (Morales-Sandoval et al., 2014). Some providers do use cryptographic technology to protect customer's data. But there still are some inconveniences. According to Zargari & Smith (2014) there are many privacy protection acts that do have limitations regarding to obtaining information from the cloud. In these privacy protection acts government agencies and private litigants may be able to obtain

information from a third party, since these privacy protection acts see the third party as the accountable one instead of the creator of the information. An example is the USA PATRIOT Act which permits U.S. law enforcement agencies to access cloud computing services that are hosted, controlled, and/or maintained by U.S. companies (Zargari & Smith, 2014). The lack of development in cloud-related legal enforcement mechanisms and systems allows the privacy and security issues, and with that the confidentiality, to fall into a legally grey areas (Kshetri, 2013).

Integrity

Weis & Alves-Foss (2011), Arias-Cabarcos et al. (2012), Li, Raghunathan & Jha (2012), MacKay et al. (2012), Kshetri (2013), Morales-Sandoval et al. (2014), Zargari & Smith (2014), and Lian (2015) argue that integrity can be a concern when adopting cloud computing. Integrity is "guarding against improper information modification or destruction" (Arias-Cabarcos et al., 2012, p. 519). As Morales-Sandoval et al. (2014) also mentioned, cloud computing may have big advantages and is so convenient that organisations are willing to trade it for the disadvantages it has, but most organisations such as government organisations cannot do this due to obligations as preserving the integrity of data. Therefore organisations require the security of the integrity of data of their cloud services.

According to Zargari & Smith (2014) integrity is one of the five goals that should be satisfied to guarantee the customer of security of the cloud service. They propose data encryption and colouring options to uphold data integrity and user privacy. However, not every cloud provider uses data encryption and colouring options for their cloud services and security services, as integrity cannot be guaranteed. Not every cloud provider offers these options because of the costs and the overhead it creates (Zargari & Smith, 2014). Encryption is the primary method to use for upholding integrity, but it is extremely expensive for the cloud providers and therefore not always used (Weis & Alves-Foss, 2011).

Availability of data

Another big concern regarding cloud computing is the availability of data (Arios-Cabarcos et al., 2012; Kshetri, 2013; McLarnon, Robinson, Milligan & Sage, 2014; Zargari & Smith, 2014; Lian, 2015). Availability of data is "ensuring that a system is operational and that it is accessible to those who need to use it, so the business purposes can be met, the loss of availability is often referred to as "denial-of-service"" (Arios-Cabarcos et al., 2012, p. 519). Lian (2015) argues that the availability of data influences the extent to which customers will adopt cloud services. Kshetri (2013) even argues that availability of data even is one of the topmost concerns for organisations when deciding to adopt cloud computing, rather than the total costs. When comparing cloud computing to traditional media, it does offer several advantages, such as continuous availability. Although the cloud provider may offer continuous availability, there are still inevitable risks such as hacker attacks, loss of data access or even unintentional downtimes (Burda & Teuteberg, 2014). Therefore the availability of data remains a concern for organisations when deciding to adopt cloud computing.

Chapter 3 Adoption Theory Review

In this paragraph there will be elaborated on two main theories explaining adoption. These adoption theories will give insight in how the adoption of an innovation, like cloud computing, can be enhanced and how it will affect organizations.

Before any adoption theory can be discussed, its needs to be determined what is meant with the term innovation. If we look at it in the broadest sense an innovation can be any new idea. Rogers (1995) defines an innovation as "an idea, practice or object that is perceived as new by an individual or other unit of adoption" (p. 11). In this case it does not matter if the idea, practice or object is objectively new, what matters is the perception of novelty. Also should be noted that innovation does not necessarily mean that the new idea, practice or object is better or more beneficial (Straub, 2009).

A majority of studies in the field of cloud computing investigated the adoption of cloud computing and its determinants (Low et al., 2011; Chong et al., 2012; Morgan & Conboy, 2013; Lian et al., 2014). In these studies several models and theories have been used to explain the adoption of an innovation. Low et al. (2011), Morgan & Conboy (2013) and Lian et al. (2014) employed the Technology-Organization-Environment (TOE) framework by Tornatsky and Fleisher (1990) to study the factors influencing the adopting of cloud computing in organizations, such as hospitals and high technology firms. Since this research also studies the adoption of cloud computing in such organizations the TOE framework is used. However, the adoption of an innovation can fail if the individual users within the organizations are not willing or slow in adopting the innovation (Sharma et al., 2016). The Technology Acceptance Model (TAM) by Davis (1989) explains the factors influencing the intention to use for individuals.

For this research the TOE framework and the TAM are used as a basic knowledge on the adoption of an innovation like cloud computing. The two adoption theories exclude one important variable; trust. Therefore in this research the TOE framework and TAM will be extended with the variable trust. Organizations have issues such as privacy and security that do play an important role in deciding whether to adopt cloud computing or not (Chong et al., 2012).

3.1 Technology Acceptance Model

The Technology Acceptance Model (TAM) was developed by Davis (1986; 1989) to explain computer-usage behaviour. TAM was adapted from Fishein and Ajzen's (1975) Theory of Reasoned Action (TRA). According to TRA beliefs influence attitudes, which leads to intentions, which then guides or generates behaviours. TAM has adapted this belief-attitude-intention-behaviour relationship to an IT user acceptance model. The goal of TAM is to "provide an explanation of the determinants of computer acceptance that is general, capable of explaining user behaviour across a broad range of end-user computing technologies and user populations, while at the same time being both parsimonious and theoretically justified (Davis, Bagozzi & Warshaw, 1989, p. 985).

TAM has a central argument that two beliefs, perceived usefulness and perceived ease of use, determine an individual's behavioural intention to use a system, which has been linked to subsequent behaviour (Taylor and Todd 1995; Sheppard et al 1988). TAM posits that perceived usefulness is influenced by perceived ease of use because the easier the technology is to use the more useful it can be. TAM also suggests that the key beliefs (perceived ease of use and perceived usefulness) mediate the effect of external variables. TAM has received extensive empirical support through application, replications and validations by researchers and practitioners (Adams et al., 1992; Chin & Gopal, 1993; Chin & Todd, 1995; Davis, 1993; Davis & Venkatesh, 1996; Gefen & Straub, 1997; Hendrickson et al., 1993; Igbaria et al., 1997; Mathieson, 1991; Segars & Grover, 1993; Subramanian, 1994; Szajna, 1994; Szajna, 1996; Taylor & Todd, 1995; Venkatesh, 1999; Venkatesh & Davis, 1996; Venkatesh & Morris, 2000) suggesting that TAM holds across technologies, as well as across populations, settings, and time. TAM has also been applied in various studies on e-commerce, online banking, 3G and m-

commerce (Chong, Chan & Ooi, 2012; Chong, Ooi, Lin & Tan, 2010; Wei, Marthandan, Chong, Ooi & Arumugam, 2009; Cheng, Lam & Yeung, 2006).

3.1.1 Key Elements

Perceived ease of use
Perceived ease of use is the "degree to which a person believes that using a particular system would be free of effort" (Davis, 1989, p. 320). This follows the definition of ease: "freedom from difficulty or great effort" (Davis, 1989, p. 320). Given that effort is finite resource, an application that is perceived to be easier to use than another application is more likely to be accepted by users (Davis, 1989). Because even when people believe that the technology is useful, they may still believe that the system is too hard to use. Therefore they believe that the benefits of the usage of the technology are outweighed by the effort it takes to use the technology. Davis therefore states "all else being equal, we claim, an application perceived to be easier to use than another is more likely to be accepted by users" (Davis, 1989, p. 320).

Perceived usefulness
Perceived usefulness is the "degree to which a person believes that using a particular system would enhance his or her job performance" (Davis, 1989, p. 320). This follows the definition of the word useful: "capable of being used advantageously" (Davis, 1989, p. 320). The system must, according to the definition, deliver some value. Perceived usefulness has been used in a large variety of previous research as a predictor of purchase intention (Bhattacherjee, 2000; Pavlou, 2003; Venkatesh, 2000). The value of a system, in this case cloud computing, derives in different ways including innovativeness and task ease enablement.

3.2 Technology Organization Environment Framework

The Technology Organization Environment (TOE) framework was developed by Tornatsky and Fleischer (1990). The TOE framework differs from other adoption theories since it provides a technological perspective and emphasizes the important influences of environmental factors and organizational characteristics. Previous studies have examined the adoption of cloud computing with the TOE framework (Alshamaila et al, 2013; Low et al., 2011; Lian et al., 2014). However these studies do not consider critical factors such as security, regulations and certification, satisfaction with their current systems and financials costs as a determinant of cloud computing service adoption (Hsu & Lin, 2015).

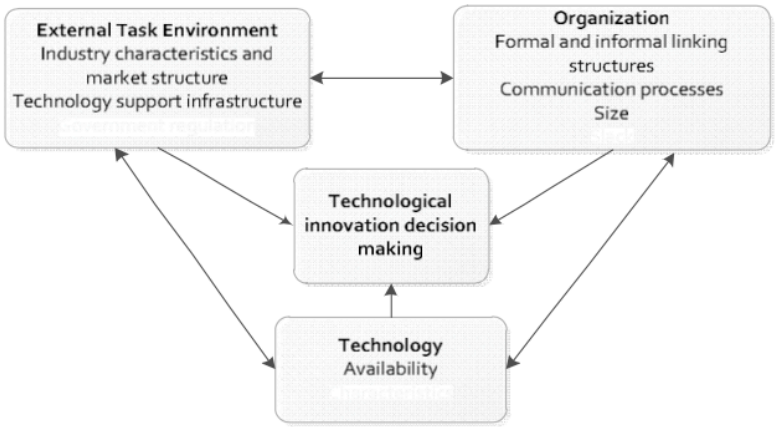

Figure 3 TOE Framework (Source: Tornatzky and Fleischer (1990))

The TOE framework was introduced and described in the book "The process of Technological Innovation" by Tornatzky and Fleischer (1990). The TOE framework focuses on the firm level of an adoption decision and how technology characteristics themselves can influence the adoption decision. In Figure 3 the TOE framework is shown. The organizational context of the framework describes the

characteristics of the organization, e.g. size, formalization, complexity of its managerial structure, and degree of centralization. The external environmental context of the framework describes in which area the organization conducts its business (DePietro et al., 1990).

3.2.1 Key Elements

Technology
According to the TOE framework tow types of technologies have influence on the adoption decision; technologies that are currently in use by the organization, and technologies that are available on the market but are not in use by the organization. The technologies that the organizations already uses influence the adoption decision because they show the limit and scope of the changes on a technological level that the organization can accept. The technologies that are on the market but are not in use by the organization influence the adoption decision because they indicate how the organization can evolve by adopting a new technology.

Organization
The organizational aspects of the TOE framework refer to characteristics such as size, structure and communication process. These organizational characteristics influence the adoption of an innovation in many ways. The structure of the organization influences the adoption decision and the communication process within the organization influences the adoption process. The behaviour of the top management of the organization can also have an influence on the promotion or prevention of the adoption (Baker, 2012).

Environment
The environmental aspects of the TOE framework refer to the structure of the industry, regulations, and the technological support infrastructure. The government regulations can either inhibit or support the adoption of a new technology (Baker, 2012). Therefore the impact of the government is not clear. The industry of the organization may predict the level of adoption. In rapidly growing industries the adoption may be higher, while in mature or even declining industries the adoption may be lower.

Chapter 4 Research Model

4.1 Research Model

Looking at the literature on adoption and cloud computing. Trust has a very important role in the adoption of cloud computing. In order to answer the main question: "*What are the attributes of cloud computing for an organization to trust a cloud provider"* attributes from the literature research were gathered. An explanation of these attributes and a description is given in the following paragraph. These come from the literature research on cloud computing, trust, the Technology Acceptance Model and the Technology Organization Environment Framework.

Articles	**Attributes**					
	Security	Standards & certification	Reputation	Trust	Quality	Compatibility
Arias-Cabarcos et al. (2012)	✓	✓	✓	✓		✓
Arpaci (2016)	✓	✓		✓	✓	✓
Burda & Teuteberg (2014)	✓		✓	✓	✓	
Chiregi & Navimipour (2016)	✓		✓	✓		
Järveläinen (2012)	✓	✓	✓	✓		
Hew & Kadir (2016a)		✓	✓	✓	✓	
Hew & Kadir (2016b)	✓			✓	✓	
King & Raja (2012)	✓	✓		✓		
Kshetri (2013)	✓	✓	✓	✓		✓
Lian (2015)	✓		✓	✓		
Messerschmidt & Hinz (2013)	✓			✓	✓	✓
Pazos-Arias et al. (2012)	✓	✓	✓	✓		
Rangasamy & Somasundaram (2016)		✓	✓	✓	✓	
Tehrani (2013)	✓	✓			✓	✓

Table 2 Attributes of cloud computing

Table 2 shows the attributes of cloud computing that were found through the research in literature. Based on the literature review this research proposes six attributes for cloud computing adoption. None of the studies that are summarized in Table 2 has integrated all of these six attributes. This research gap is also one of the motivations behind this research.

Previous research did not integrate all of the attributes shown in Table 2. This research wants to examine the attributes of cloud computing for an organization to trust a cloud provider. In order to determine the relationships between the attributes the articles from Table 2 and their research on the adoption of cloud computing and trust in cloud computing was used.

In chapter 2.3 the different types of trust, 'hard' and 'soft' trust were introduced and inline with this research has shown that security and trust are related (Lian, 2015; Chiregi & Navimipour, 2016). To complement the hard trust research has shown that standards and certification can also be a component of hard trust (Järveläinen, 2012; Raja & King, 2012; Kshetri, 2013; Lian, 2015). Lian (2015) mentioned in his study that standards and certification could ensure the security, while Kshetri (2013) mentions that standards specifically made for the cloud industry could enhance the trust of organizations and adoption of cloud computing.
While security and standards and certification seem to have an impact on the level of trust, the social aspects of trust should not be neglected. Burda & Teuteberg (2014) found in their research that trust can be increased through reputation. Research of Burda & Teuteberg (2014) also shows that overall

trust has a positive effect on the intention to use cloud computing. Arpaci (2016) argued that perceived trust has a significant effect on the attitude towards cloud computing.

To continue with the research of Burda & Teuteberg (2014), it states that if organizations positively perceive the service quality it would increase the trust in cloud computing and the provider and hence increase the adoption of cloud computing. In the research of Hew & Kadir (2016b) three types of quality are used: system quality and service quality. Other researchers also distinguish different types of quality and their influence on adoption (Tehrani, 2013; Rangasamy & Somasundaram, 2016).

Previous research by Beatty et al. (2001) on adoption in of an online environment showed that compatibility had a significant effect on the adoption. Tehrani (2013) also believed that compatibility is important for the adoption of cloud computing. Arpaci (2016) states that the compatibility of the cloud and the ease of use can serve as a meaningful predictor in the adoption of cloud computing. Whereas Kshetri (2013) states that compatibility can have a positive effect for cloud providers and their position in the cloud computing market. The more compatible their system is the lesser the chance that an organization or consumer will transfer to another cloud provider.

All the above-mentioned relationships between the attributes have contributed in the composition of the research model shown in Figure 4. In the next paragraph the definitions of the attributes will be defined and explained.

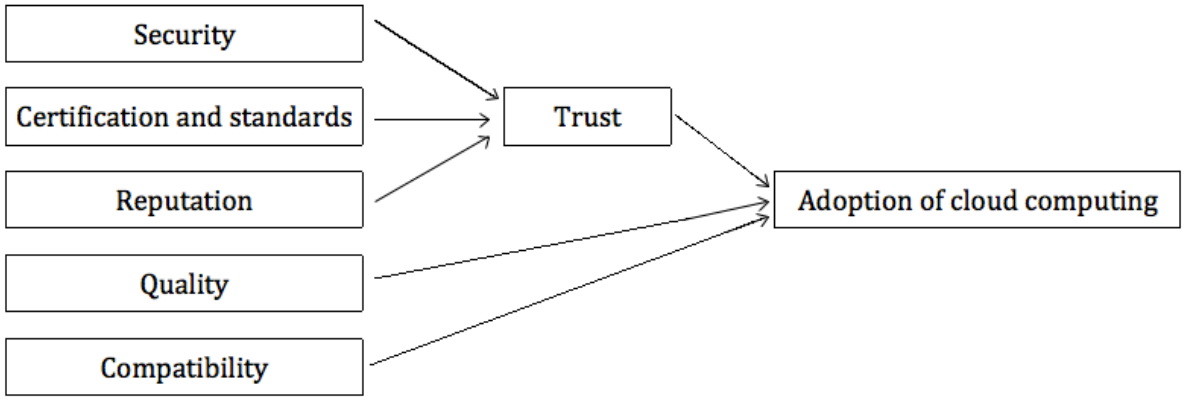

Figure 4 Research Model

4.2 Attributes

4.2.1 Security

Security is in the field of cloud computing defined as "the degree to which cloud computing is perceived as being more secure than other computing paradigms". Previous studies found that security is one of the main concerns about adopting cloud computing (Chong, Lin & Eze, 2009; Mohammed, 2011; Subashini & Kavitha, 2011; Sultan, 2011; Tehrani, 2013; Sharma et al., 2016). Security issues concern the confidentiality, integrity and availability of the system (Gorden & Loeb, 2002).

The security of the system influences the availability (Kim et al., 2013). For example, a system that is vulnerable for a Distributed Denial of Service (DDoS) attack or malicious software is unlikely to keep performing when it is compromised and will therefore affect the availability of the system (Yigitbasioglu, 2014). The integrity of the cloud provider influences the level of security the organizations feel the cloud environment has. Integrity refers to "the commitment level of the cloud computing vendor to honour obligations to the best of their abilities" (Sharma et al., 2016, p. 63). And last the confidentiality of the cloud provider refers to "the prevention of data access by unauthorized users" (Arpaci, 2016, p. 153).

4.2.2 Certification and standards

Concerns regarding breaches in cloud environments have started the development of cloud service certifications (CSCs) e.g. Cloud Security Alliance's Security, Trust & Assurance Registry, and EuroCloud Star Audit (Lins et al., 2016). In previous studies the demand for certification and standards for cloud providers was already demonstrated (Mohammed, 2011; Mackay et al., 2012; Kshetri, 2013; Kshetri, 2016). Research has shown "that trust can be built through supporting IT based mechanisms like certifications" (Sunyaev & Schneider, 2013, p. 34). These standards and certifications should also address the accountability of the organization and the cloud provider. Cloud provider do offer policies and Service Level Agreement (SLA) that should cover all the aspects of privacy and damages caused by breaches and especially the accountability for any privacy disclosure (Kshetri, 2013). However, these policies and SLA's do not adequate address the responsibilities of the cloud provider. Dynamic certification of cloud services could provide a high level of reliability and security to the potential customers (Lins et al., 2016).

4.2.3 Reputation

Reputation is defined by the Oxford English Dictionary (1971) as (1) "reputation is what is generally said or believed about a person's or thing's character or standing" and as (2) "a widespread belief that someone or something has a particular characteristic". In the field of cloud computing reputation is related to trust, but the two attributes are different. Reputation is "the aggregated opinion of a community towards that entity" (Huang & Nicol, 2013, p. 3). Where an entity with a high reputation is trusted by many organizations in that field. As Huang & Nicol (2013) also mentioned reputation is useful for cloud users in choosing a cloud service and provider, but it is inadequate afterwards.

4.2.4 Trust

Trust has previous already been defined paragraph 2.3 as "the expectation that an actor can be relied on, will be predictable, and will act fairly" (Zaheer et al., 1998, p. 143). This definition allows for a leap of faith that the organization needs to make towards the cloud provider. In order to make this leap of faith as small as possible the organizations do have some demands and factors that influence their trust regarding the cloud provider. In the conceptual model in Figure 4 is shown that security and the certification and standards, and reputation influence the trust from the organization to adopt cloud computing.

4.2.5 Compatibility

Compatibility can be defined as "the degree to which an innovation is perceived as consistent with the existing values, past experiences, and needs of potential adopters" (Rogers, 2003, p. 15). In the case of cloud computing and this research compatibility can be defined as the degree to which cloud computing is perceived as consistent with the culture and norms of the organization and the technical aspects of the environment of the organization. With compatibility also comes the perceived ease of use. If the organization believes that adopting the system is free of effort since it is compatible with their own technologies this would enhance the adoption of cloud computing.

4.2.6 Quality

The performance and quality of a cloud provider concerns aspects regarding the system and the service of the cloud provider. Within the attribute quality there is a breakdown in service quality and system quality.

System Quality

System quality concern aspects of the system like usability, reliability, response time, availability, and adaptability. A cloud provider could for instance have different ways to access the cloud storage, e.g., by mobile applications or other innovative features. The quality of the system also says something about the perceived usefulness of the system as Davis (1989) defined it " the degree to which a person believes that using a particular system would enhance his or her job performance" (p. 320). In the case of cloud computing for organization this means the degree to which cloud computing would enhance the performance of their organization.

Service quality

This factor is important for every organization. Given the impersonal nature of cloud computing service quality is especially important for the end users and their trust in the cloud provider. Factors that can be associated with service quality include quick responsiveness, empathy, following-up service, assurance and personalization (Lee & Lin, 2005).

Chapter 5 Research Methodology

In order to find the answer to the research question a method of data collection and analysis had to be determined. This chapter covers the way the data has been gathered and how it has been analysed.

5.1 Case study

The research will be conducted through an explanatory multiple case study. The use of case study is related to research that concentrates on one particular subject, in this case the trust in cloud computing. Case studies are preferred when the following conditions are met: the main research questions are "why" and "how" questions, the researcher has little or no control over behavioural events, and the focus of the study is a contemporary phenomena (Yin, 2013). As the proposed research meets all of these conditions, case study best serves our needs.

The definition of case study research used by Yin (2013) is as follows: "A case study investigates a contemporary phenomenon ('the case') in its real-world context, especially when the boundaries between phenomenon and context may not be clearly evident. […] The second part of the definition points to case study design and data collection features, such as how data triangulation helps to address the distinctive technical condition whereby a case study will have more variables of interest than date points" (Yin, 2013, p. 2).

For the multiple case study according to Yin (2013) theory is "developed" in the beginning of the research and is tested in the case study. This validation process also allows for new insights although it is primarily driven by the "developed" theory (Yin, 2013). With the multiple case studies the research model is examined. To validate the theory and research model that has been developed at the beginning of the research Yin (2013) presses for six to ten cases to get a high degree of certainty.

5.2 PRIMA model

The PRIMA/USE-IT model by Spil, Schuring and Michel-Verkerke (2004) was used for the conducted interviews. The theory of the model is based on the TAM model by Davis (1989), the UTAUT model by Venkatesh (2003), the Information System Success Model by Delone and McLean (2003), and the Innovation Diffusion Model by Rogers (1983). The model consists of five areas of analysis, namely; process, relevance, information needs, means and people, and attitude. The USE IT-model combines theories about adoption and diffusion of innovations and provides an interview model and questionnaire with which the success of an information system from a user's perspective can be predicted and evaluated. The USE IT-model presents two dimensions: the domain dimension and the innovation dimension. These dimensions were make the USE-IT model very suitable for studying the trust of organizations in cloud computing.

This qualitative research method is chosen to provide a more detailed understanding of the factors that influence the trust of organizations in cloud computing. The literature study complements the interview method with the attributes that will appear through the questions asked with the PRIMA interview model. Data is collected by interviewing several organizations using the PRIMA model. Different types of large professional organizations with experience in cloud computing have been selected. These organizations have employees with great knowledge on cloud computing and therefore can participate in this research.

As mentioned earlier, the model consists of five areas; process, relevance, information needs, means and people, and attitude. In the following section we explain what is expected to be measured by each construct. The validation of these expectations will follow in the discussion section.

The working **process** consists of a description of the activities the user performs completing certain tasks. By asking questions related to the process information on the process and working habits will give more insights in the experience of the user with cloud computing.

The **relevance** consist questions regarding what the value for the users of the cloud computing is. It is about the acceptance of cloud computing. The extent to which the users of cloud computing are expecting that it will solve problems and will help to achieve targets. It is also about the potential bottlenecks in the system and what kind of improvements the end users would like to see in the system.

Information needs is about which information the user would like to receive from the system and should align with the information the service delivers and captures. In the case of cloud computing information needs also means **information quality**. With information and data being the primary source of cloud computing information quality suits better. Within information quality we assume that there are some aspects that measure the information quality. These aspects are: timeliness, completeness, reputation, service and free-of-error.

Means and people examines the resources available to the users/organizations given the assumption that hardware and support enable effective use of the cloud computing. In the case of cloud computing, we will examine in what extent organizations already use cloud computing. The cloud computing system also has to joint with their current processes. Further, means and people also examines the perceived risks of cloud computing, like safety, privacy, and reliability.

Finally, the **attitude** section will expose whether or not there is resistance to this innovation. Resistance is not per definition positive or negative, but it exposes flaws in the system (Lapointe, & Rivard, 2005). With this the attitude of the end users of the system will be taken into account. What is the attitude of the end user of cloud computing pertaining to innovation and IT in general?

5.3 Data collection and analysis

The data collection and analysis of this research has been done through multiple case studies. The format of case studies was chosen due to the lack of knowledge in organizations on cloud computing. Most organizations that were approached for this research were not using cloud computing or did not have an employee in their organization with extensive knowledge on cloud computing. Therefore it was hard to find organizations that fit our criteria. From the organizations that participated in this research their expert on cloud computing was interviewed for the case study.

The PRIMA method was selected for the semi-structured in-depth interviews. The group of interviewees vary as they all work for different organizations. The semi-structured interviews makes sure that the difference in answers are due to the difference in interviewees rather than the differences in questions asked (Barriball & While, 1994).

The interviews were held one-to-one rather than in focus groups, since bias may occur when interviewees are influenced by strong opinions of others (Barriball & While, 1994). The interviews were also held face-to-face as there also might be a bias for not examining non-verbal communication in e.g. phone interviews. The interviews lasted between 30 and 60 minutes each. The sample size consists of eight organizations. This amount of cases allows for a comparison of results between cases (Diefenbach, 2009). The interviewee had to be an expert regarding cloud computing. To ensure confidentiality the interviews were held in a private room away from other professionals and anything that is discussed during the interviews remains between the interviewee and the researcher.

Organizations were asked to participate in this study that already had adopted cloud computing. With the interviews the organizations information was inquired on their opinions on different aspects of cloud computing. The questions asked to the organizations were adapted from the PRIMA model and previous research that has been published (Landeweerd, Spil & Klein, 2013).

The developed interview questions were aimed to capture the interviewees' opinion about cloud computing, their trust in the cloud providers and the factors that influence their trust in the cloud

providers. In order to measure the attributes found in the literature research each attribute should have at least one item in the interview model. The different constructs of the PRIMA model are also expected to make the attributes identified in the literature to appear, either directly or indirectly.

PRIMA construct	**Attributes expected to be measured**	**Example questions**
Process	Compatibility	Does your organisation use cloud computing at this moment? If so what type of cloud does it use?
Relevance	Compatibility System quality	What aspects of cloud computing do you experience as a bottleneck?
Information quality	Certification and standards System quality	What aspects of the system are important to you? Is the content safe with the cloud provider?
Means and people	Service quality System quality Reputation	Do you get sufficient support from the cloud provider? How important is the service and helpdesk of the cloud provider?
Attitude	Certification and standards Reputation Trust	Do you trust cloud computing and the cloud providers? Would you trust cloud providers with your own information?

Table 3 Attributes expected to be measured by the PRIMA model

In Table 3 the attributes that are expected to be measured with each PRIMA construct are shown. Each construct measures one or more attributes. The final interview set-up can be found in Appendix A.

Due to confidentiality both the name of the interviewee and the firm were made anonymous. Each firm is randomly assigned with a code word based on the NATO phonetic alphabet. The data from each interview has been transformed into a story in which the main issues discussed during the interview are summarized. A conclusion of each interview has also been drawn. After the within-case analysis the cross-case analyse was performed in order to discover patterns across all cases. The patterns are then discussed in the discussion section.

Chapter 6 Case Analysis Results

This chapter will present the within-case and cross-case comparisons. Each of the eight cases has been presented with an overview of the main issues discussed during the interview. In the cross-case analysis the converging and diverging issues across these cases is revealed. These results are then used to answer the main research question: *What are the attributes of cloud computing for an organization to trust a cloud provider?*

6.1 Within-case analysis

6.1.1 Case 1: ALPHA

Size	> 1000
Type of organization	Healthcare
Interviewee's position	Head of Information Management and the IT department

As head of information management and the IT department of this healthcare organization the interviewee makes sure that the healthcare processes work. Not only the infrastructure for these processes, but also the data and applications. The information management and IT department make sure that the employees can use infrastructure, data and applications. The interviewee's work process consists of making sure the employees are provided with applications and data whenever they need it.

Case analysis ALPHA
ALPHA uses a private cloud within their organization. The private cloud is only used for certain amounts of data. The main reason for this decision is that the organization has information that is very privacy-sensitive and needs a secure environment. The organization does not have the trust in the cloud that it is that secure that these amounts of information can be placed in the cloud. Therefore ALPHA has chosen to adapt the cloud to a certain level. ALPHA uses cloud computing, but only places information in the cloud that is not privacy-sensitive.

The most important reason for Alpha to choose for cloud computing is the flexibility it has. *"We kind of buy some sort of certainty for up- and downscaling of the amount of space we need"*. Besides the flexibility the management of data is outsourced and that reduces the amount of costs for the IT department of ALPHA.

Privacy and security are the main risks of adopting cloud computing. With security comes privacy according to the interviewee. The main questions regarding the risks in cloud computing for the interviewee are: *"What happens with your data when it is in the cloud? If you put the data in the cloud and the provider goes bankrupt, who will be the owner of the data? What happens?"*.

When asked which components of cloud computing the interviewee would like to see improved security was appointed again. The interviewee thought it would be helpful if there would be more standards for cloud providers. Judiciary are, according to the interviewee, a lot of steps that need to be made to equal the practice of using cloud computing.

The trust in cloud computing is there until proven otherwise. *"If you do not trust the cloud provider you should not adopt cloud computing in the first place. It is in their own interest to maintain their reputation and image"*.
ALPHA does select their cloud provider very carefully. It is, according to the interviewee, their responsibility to choose the right cloud provider and therefore carefully considerate the different cloud providers. Organizations can choose to adopt a cloud with a cloud provider that is very cheap, but is the security at this provider as good as you expect? If the product, like a cloud, is very cheap there is

always some sort of catch. An organization like Alpha cannot have this and therefore carefully considerate which cloud provider they will choose for their cloud.

Case conclusion
In sum, the organization does have trust in cloud providers but security and privacy remain important issues. Flexibility and the low cost did attract the organization to adopt cloud computing. Privacy and security keep them from adopting cloud computing for other applications and data that are more privacy-sensitive.

6.1.2 Case 2: BRAVO

Size	>1000
Type of organization	Healthcare
Interviewee's position	Information Manager

BRAVO is a healthcare organization in which the interviewee works as Information Manager for the IT department. The organization works with very private-sensitive information and therefore is very careful with adapting cloud computing.

Case analysis BRAVO
BRAVO uses cloud computing for a very small percentage of their business, almost 90% of their business concerns very private-sensitive information that cannot be stored into the cloud. The small percentage of business that is used in the cloud concerns processes that are not the core business of the organization, e.g. their HR application is in the cloud.

"Trust in cloud computing and providers is little. In order to gain trust in cloud computing and providers we, as an organization, would need to invest in drafting contracts to ensure the security of the cloud". As an healthcare organization BRAVO's core business is not in cloud computing and therefore would nee to invest more in the IT department and there knowledge of cloud computing, providers and legislation. The interviewee does mention that a breach in data also can come from within their organization. In the past an employee has leaked some private-sensitive information. *"Therefore security is also always subject to human error".*

The information that is currently stored in the cloud for BRAVO is not their core business, therefore the service level the organization needs of the cloud provider is not that high. A 24/7 service and helpdesk is not necessary. In the case BRAVO would store their very private-sensitive information and core business in the cloud a 24/7 service and helpdesk would be demanded and required of the cloud provider. Without this information the organization cannot function.

The advantage of cloud computing is for BRAVO the reduced costs for the IT department and the flexibility it offers. The disadvantage of cloud computing for BRAVO, according to the interviewee, would be that the cloud provider does not have the same incentive and drive that employees of BRAVO do have when something goes wrong. *"When there is a hitch in the cloud, the employees of BRAVO could be addressed in person and would have the drive to work overtime to solve this problem as quickly as possible. From a cloud provider you expect the same service, but the employees that work there do not have the connection with your organization as the employees of your own organization".*

Case conclusion
In sum, the organization does use cloud computing but only for a small percentage of their business. BRAVO does not trust cloud providers with all of their information and would need to invest in investigating the regulations, legislation and requirements they would have towards a cloud provider. Therefore their core business remains, for now, in their own organization and IT department.

6.1.3 Case 3: CHARLIE

Size	> 1000
Type of organization	Education
Interviewee's position	Head of Information Management

CHARLIE is an educational organization in which the interviewee works a head of the Information Management department. The interviewee has the task of designing policies for this department. The interviewee has with its department an approach in which cloud comes first. Therefore everything that can be put into the cloud will be put in the cloud. This does not mean that everything has to be in the cloud, but the consideration will always be made.

Case analysis CHARLIE
CHARLIE uses cloud computing in their organization. Cloud computing is used very often within the organization due to their "cloud first" approach. Big and critical applications for their business are transferred to the cloud, but also little applications that are not that critical for their business like a payroll system is transferred to the cloud.

The risk the interviewee sees in cloud computing is privacy. *"The privacy of the cloud is not as good as expected for example, that can be a high risk for us as an organization. Also what happens when the cloud provider is not able to provide you with cloud computing anymore? What happens with your system and data? Is the organization able to get it back?"* Therefore the interviewee pleads for an exit-strategy. Therefore availability is also one of their main risks when adapting cloud computing.

Requirements CHARLIE has for the cloud provider are: continuity, availability, privacy, and linkable with their own systems and data. These requirements are, according to the interviewee, the most important for their organization. The importance of the service the cloud provider offers is dependent on the cloud purchased. *"For some clouds we only need an e-mail address that responds within a workday, other clouds need a 24/7 service desks that we can call"*.

Fully trusting the cloud provider is not possible according to the interviewee. In order to trust the cloud provider arrangements need to be made. *"In that sense it is good that legally more and more is required from the cloud provider. That gives us, user of cloud computing, a stronger case when something goes wrong"*. CHARLIE as an organization continually evaluates the contracts is has with cloud providers and also revises them when needed due to new legislation.

Case conclusion
CHARLIE uses cloud computing, but does not fully trust cloud providers. The interviewee mentioned that increasing legislation for cloud providers is a good thing that ensures organization and therefore increases the use of cloud computing. The biggest risk with cloud computing is privacy and the requirements for a cloud are: continuity, availability, privacy and linkable with their own systems and data.

6.1.4 Case 4: DELTA

Company size	> 1000
Type of organization	Education
Interviewee's position	Information Manager IT department

DELTA is an educational organization in which the interviewee works as Information Manager of the IT department. The interviewee has the task of designing policies for this department and negotiating with cloud providers. The organization does not have a cloud approach, but when certain systems or applications need replacement they will check whether or not cloud providers have anything to offer that fits their needs.

Case analysis DELTA
DELTA uses cloud computing within their organization. The interviewee mentioned that their organization only uses SaaS and does not use PaaS en IaaS. These two cloud services are at the moment too expensive for the organization to outsource to a cloud provider. The organization does use cloud computing for large applications that involve their core business, but also for smaller applications that do not involve their core business.

Important for DELTA when using cloud computing is the flexibility it has to offer. *"If we would do it ourselves the capacity always needs to be maximum, in the cloud we are able to upscale and descale our capacity when necessary"*. The interviewee mentions that it is a misconception that cloud computing is cheaper that doing it yourself. This relies on the type of cloud you, as an organization, want to use and the requirements it needs to have.

"The risks involved with cloud computing and providers need to be assessed with every cloud provider you, as an organization, want to work with. Every provider has something else to offer, which includes risks". For DELTA the security, privacy and responsibility of the cloud provider are important and requirements, but at the same time there can be risks when not fulfilling the needs of their organization.

For improving cloud computing and the services the cloud providers have to offer the interviewee believes that cloud providers need to be more transparent. *"If the cloud providers are transparent about what they can offer your organization and what gaps an organization itself may need to fill. Then a better consideration for adopting cloud computing can be made. A large organization, like ourselves does have the knowledge and experience to make these consideration, but smaller organizations do not always have the knowledge and experience to make the consideration without some transparency from the cloud provider"*.

The quality the cloud providers offer is not always the same. Sometimes there lacks some kind of standard. Some cloud providers are, according to the interviewee, just in the business to make money and do not deliver the service you might expect from them. Therefore careful consideration needs to be made when adopting cloud computing and an organization always should have its own requirements for the cloud provider.

Case conclusion
DELTA uses cloud computing for both large and smaller applications and amounts of data. The main concern with cloud computing is the security, privacy, and responsibility of the cloud provider.

6.1.5 Case 5: ECHO

Size	> 1000
Type of organization	Education
Interviewee's position	Manager IT department

ECHO is an educational organization in which the interviewee works as the manager of the IT department. ECHO has a strategy for their use of cloud computing and is aiming to work in 2020 entirely in the cloud.

Case analysis ECHO
ECHO uses cloud computing within their organization. Cloud computing is used for small applications, but also for very critical processes within their organization cloud computing is being used, e.g. the organization uses cloud computing for their registration system.

"As an educational organization we want to focus on our core business and do not have the idea that information services and IT support are our core business. These processes do not have to take place within our own organization and therefore can be outsourced to for example an cloud provider". ECHO does notice that the main issue with adopting cloud computing and doing as less as possible themselves, with information services, is the flexibility. Cloud providers also have a price for their flexibility and as an organization you need to make firm commitments with the cloud provider to ensure the flexibility while at the same time not paying the ultimate price.

The risks of cloud computing are, according to the interviewee, the services that do not always fulfil the needs and requirements. Another risk is the continuity of the cloud provider and the data or applications stored at the cloud provider. *"What happens when the cloud provider goes bankrupt? Is there some sort of exit-strategy?"*

Cloud providers could improve their service by contributing thoughts about how the cloud is able to integrate with the current processes of the organization. Certain amounts of flexibility in their service, not just hourly invoice for every question or request. Also being taken serious by the cloud provider and not seen as one other customer. The cloud provider should deliver a service that is more personal.

ECHO also has concerns regarding the maturity of a lot of cloud providers. The business in cloud computing has grown tremendously and therefore some cloud providers are not as mature in their business as may expected from them. The level of security and privacy at these cloud providers is not according to a lot of standards organizations have.

"When were fully operating in the cloud we definitely expect a 24/7 service and helpdesk from our cloud providers, without the cloud we cannot function as an organization. Therefore one of our requirements is a 24/7 service, although we do not operate as an organization 24/7". The interviewee mentions that at the moment not every cloud provider is delivering a 24/7 service and helpdesk. Towards 2020 these contracts will be revised and the same service will be expected and required from these cloud providers.

ECHO is investing, at the moment, a lot of time in revising the contracts with cloud providers. Contracts that have been made in the past need adjustments in order to serve the security the organization needs at the moment and in the future. More is expected from the cloud provider than in the past. ECHO even includes in some cases a penalty clause. This in order to ensure the service the cloud provider needs to deliver and to protect themselves.

Case conclusion
ECHO is progressive organization in terms of cloud computing. The organization is aiming to work in 2020 entirely in the cloud. Because the organization is so progressive in the case of cloud computing, it does have a lot of knowledge. It also invests in cloud computing and examining whether the clouds they are using are fulfilling the requirements of the organization.
The maturity of the cloud providers could improve according to the interviewee. Also the flexibility of the cloud provider and their services need some improvement in order to enhance the functionality of the cloud.

6.1.6 Case 6: FOXTROT

Size	> 1000
Type of organization	Government
Interviewee's position	Policy advisor of the IT department and Head of the IT department

FOXTROT is a governmental organization. The interview was held with two employees of FOXTROT, one is policy advisor for the IT department and the other is the head of the IT department.

The organization has a cloud first approach. Therefore anything that can be stored in the cloud will be stored in the cloud.

Case analysis FOXTROT

FOXTROT uses cloud computing within their organization. Within their organization there is a "cloud first" approach. When something can be stored into the cloud, they will carefully consider in doing so. But the organization prefers to have it in the cloud in the first place. The cloud is used for small applications with little impact on their privacy-sensitive information and with little impact on their critical processes. Since the organizations deals with a lot of privacy-sensitive information little of their applications and data is stored into the cloud. The means are there to make this percentage bigger.

The flexibility and scalability are one of the main characteristics of cloud computing that are important in considering using cloud computing. "*Besides the flexibility and the scalability, it reduces cost in the amount of personnel you have to have. The cloud provider manages the security and other technical aspects, which allows us to have less personal in the IT department"*. FOXTROT aspects a 24/7 service of the cloud provider and one of their requirements is that the cloud provider is located within Europe due to legislation. Another requirement is the security, the cloud has to be safe and a certain amount of encryption of their data is also expected. *"Encryption does increase the costs of a cloud provider and therefore cloud computing is not always cheaper than doing it yourself"*.

The risks FOXTROT experiences with cloud computing are privacy, this is the main issue they have with cloud computing and second comes the continuity. *"Privacy and security are very important for our organization. As an organization you are in control over your own data and application, when we outsource it to a cloud provider we do not have any idea and control over how the integrity is of the cloud provider. The contracts we make with cloud providers are therefore very important"*.

The interviewees do have trust in cloud providers if they meet certain requirements. The requirements the organizations has for cloud providers are: (1) availability of the cloud and to what degree of continuity the cloud provider can deliver, (2) confidentiality of the cloud provider and the cloud it offers, and (3) the integrity of the cloud provider. When the cloud provider meets these requirements the interviewees do have the trust in the cloud provider, to trust it with their data.

Case conclusion

In sum, the organization does trust cloud providers, but availability, confidentiality and integrity remain important issues. The flexibility and the low costs, in certain cases, attracts them to adopt cloud computing. Privacy-sensitive information and the risks involved as well legislation keeps them from adopting cloud computing one a larger basis.

6.1.7 Case 7: GOLF

Size	>1000
Type of organization	Electronic
Interviewee's position	Global IT-manager

GOLF is an organization that operates in the field of electronics in which the interviewee works as Global IT-manager. GOLF is an organization that operates worldwide.

Case analysis GOLF

GOLF uses cloud computing within their organization. The interviewee mentioned that the adopting of cloud computing only recently has started. Since a few years the organization is willing to adopt cloud computing. Before cloud computing was seen as unsecure and therefore not used within the organization.

The availability cloud computing has to offer, is what makes it very attractive according to the interviewee. Also the lower costs the IT department would have when storing its data in the cloud. The IT department could reduce the amount of employees in the case of using cloud computing.
The ultimate scenario, according to the interviewee, would be to have the data stored at two cloud providers. In that case there always is a back-up of the data that is stored in the cloud. "If a cloud provider unexpected looses its businesses and goes bankrupt, the data is located in another cloud and the risks are minimalized for us as an organization".

The risks concerning cloud computing are minimal according to the interviewee. *"At the moment more and more legislation regarding cloud computing is generated. Which makes it easer to choose for cloud computing."* The interviewee also mentions that the cloud provider has in most cases a higher level of security than most organizations since it is their core business. Besides the cloud provider also has an interest in keeping their reputation. When an organization experiences a data breach this also has an effect on the cloud provider and their reputation.

From the cloud provider GOLF expects a 24/7 service, since their organization not only in the Netherlands but worldwide operates. A helpdesk with 24/7 service is a requirement. Although it does depend on the data that is stored in the cloud. *"Certain data is rarely used and mainly serves as a back-up that is required. For these types of data in the cloud the service of the cloud provider could be less. Within our organization the requirement is to have 24/7 service, but in these cases it could have been less"*.

Case conclusion
GOLF recently started using cloud computing. The benefits of cloud computing are the availability and reduced costs for the organization. The risks are minimal due to the growing legislation in the area of cloud computing. GOLF trusts cloud providers with its content, since it is their own interest as well to deliver the best service as possible. Although the ultimate for GOLF is to have two cloud providers where they store their data in case of an emergency.

6.1.8 Case 8: HOTEL

Size	> 1000
Type of organization	Electronic and Information Technology
Interviewee's position	Chief Information Security Officer

HOTEL is an organization that operates in the field of electronics and information technology. The interviewee works as Chief Information Security Officer at HOTEL. The interviewee works on the information security of the organization. HOTEL does have a strategy for using cloud computing; *"when we need new features for our organization the first step is to examine whether a cloud provider offers these features. If so, we will put it in the cloud"*.

Case analysis HOTEL
HOTEL uses cloud computing within their organization. HOTEL has contracts for 80% with other organization that deal with very privacy-sensitive data. For these organizations HOTEL is not able to use cloud computing. Therefore cloud computing is used for the other 20% of contracts they have with organizations that deal with less privacy-sensitive data. Also cloud computing is used within their organization for e.g. HR.

Before deciding in whether to use cloud computing or not HOTEL classifies its data. Does it involve confidential information about their organization or one of the organizations it is working for? Does it include personal data? Based on that HOTEL designs the requirements a cloud provider needs to have. The requirements are tested at the cloud provider through a risk assessment.

The risks of cloud computing are tested through a risk assessment before the organizations teams up with the cloud provider. The security of the cloud provider is one of the main risks. *"When we store our data or applications ourselves we make sure the security is top notch, it that also the case when adopting cloud computing?"* Also where the cloud provider is located, it has to be in Europe and the organization wants to know how much other parties are involved.

"In my own experience a lot of cloud providers are not as mature as they should be in the field of security". The cloud providers need to invest more in security to improve the services they offer. Also the cloud provider can be more proactive according to the interviewee. A large organization like HOTEL knows what can be expected from the cloud provider, but also which processes they need to have in order to ensure the security of the cloud they are using. Smaller organizations are less familiar with the legislation and regulations for cloud computing. A cloud provider could in that case help the smaller companies by explaining what is expected from them and what processes need to be adjusted in order to meet the legislation.

A 24/7 service of the cloud provider is expected. "Your data should be watched and secured 24/7, therefore a service desk that is available 24/7 is a must".

With trusting the cloud provider the interviewee expects to be taken serious by the cloud provider. The cloud provider also needs to initiate adjustments in the cloud when their organization has serious doubts about certain features. Also the cloud provider is expected to deliver on promises that have been made.

Case conclusion
In sum, the organization does trust cloud providers after careful consideration and risk assessments. But trust is there to a certain extent, some data gets encrypted by their organization internally and is with this encryption stored in the cloud. The organization tries to minimise the risks as much as possible through different requirements for the cloud provider and by securing the access to the cloud (one time passwords, only assessable at their location etc.).

6.2 Cross-case analysis

The goal of this research is to find out what the attributes of organizations are in order to trust a cloud provider. A total of eight case studies were conducted. The participants in all of these case studies were familiar with cloud computing and already were using cloud computing within their organization. In order to answer the research question it was important to find out to what extent the organizations are using cloud computing. The organizations make thought-out decisions on whether to adopt cloud computing and to what extent.

The extent to which the organizations use and adopt cloud computing differs. Not all of the organization use cloud computing for their core business. Organizations ALPHA, BRAVO and FOXTROT do not use cloud computing for their core business. Organizations GOLF and HOTEL do use cloud computing for their core business, but the private-sensitive information is left out of the cloud. In Table 4 an overview is shown of the organizations using cloud computing for their core business or non-core business.

	A	B	C	D	E	F	G	H
Core			X	X	X		X *	X *
Non-core	X	X				X		

Table 4 Overview of usage cloud computing within organizations

When asked what the interviewees found the most important aspect of cloud computing all of them answered the security of the cloud. Any organization has some private-sensitive information, whether it is information on new technologies that need to stay private for their competitors or information regarding the personal data of their clients. Therefore the level of security of the cloud is of great importance to these organizations. Other aspects of cloud computing that are important are according to the interviewees: security, flexibility, service, reduced costs, and continuity. In Table 5 an overview is shown of the important aspects of cloud computing according to the interviewees.

Important aspects of cloud computing	A	B	C	D	E	F	G	H
Security	X	X	X	X	X	X	X	X
Flexibility	X	X		X	X	X		
Service	X	X	X	X	X	X	X	X
Reduced costs	X	X				X	X	
Continuity			X		X	X		

Table 5 Overview of the important aspects in cloud computing

As shown in Table 5 the service of the cloud provider is also a very aspect in cloud computing. Most of the organizations expect a 24/7 service from the cloud provider. Only those applications and services that are not regularly used in the cloud could serve with a service that is only available during business hours.

The interviewees were also asked what their attitude towards innovations in information technology is and whether their organizations embrace innovations quickly or are more of a laggard in adopting an innovation in information technology. The interviewees themselves have a very positive attitude towards innovations only their organization does not always allow a quick adoption of an innovation. Organization CHARLIE and ECHO do adopt innovations quickly in order to stay on top. The other organizations are more hesitant in adopting innovations, mostly due to the private-sensitive data they are working with and the fact that information technology is not their core business.

Trust in cloud computing and cloud providers is there for the interviewees to a certain extent. The trust in cloud computing and cloud provider arises, according to the interviewees, when the provider meets certain requirements of their organization. First, the organizations expect a level of security of the cloud provider. As already mentioned security is an important aspect of cloud computing. In order to check the security level of the cloud provider organization HOTEL performs its own risk assessment

at the cloud provider. Not every organization is in the position to do their own risk assessment at the cloud provider. Therefore, organization ALPHA, BRAVO, DELTA and ECHO would like to see more standards and certification for cloud providers. Their believe is that not all cloud providers are mature enough in the field of information security and that standards and certificates would help to increase the maturity of the cloud providers. Organization HOTEL who performs its own risk assessment for cloud providers also mentioned that currently there are some cloud providers on the market that do not meet the needs in terms of information security and are purely there to earn some cash without having concerns about security. Organization CHARLIE and FOXTROT mentioned that they verify the standards and certifications cloud providers have before adopting a cloud. The case studies show that organizations are interested in more dynamic certification as a step forward to increase the security and transparency of cloud environments, as Lins et al. (2016) also mentioned in their research.

The interviewees also mentioned that there is also a level of trust in the cloud provider due to their own risks. Cloud providers also want to deliver the best service and security, since a data breach would also have an impact on their reputation and perhaps even their existence. The interviewees also take the reputation of the cloud provider into account in order to determine the continuity of the organization. CHARLIE, ECHO and GOLF mentioned continuity as an important aspect of cloud computing, whereas ALPHA and GOLF also mentioned that by delivering cloud computing the cloud provider itself also has a reputation to worry about. When asked how the organizations feel that they can examine the continuity of the cloud provider and the cloud most of them answered: “in order to address the continuity we look at the reputation of the cloud provider and the quality of their system”.

The interviews with the experts on cloud computing were also analysed regarding the attributes for cloud computing the interviewees and their organizations have for cloud providers. As Table 5 showed, security is the main attribute for businesses to trust a cloud provider with its content. If the security of the cloud provider does not meet their expectations or needs the organizations search for another provider. This applies to the trust in the cloud provider, if the interviewee or the organization do not have the trust in the cloud provider the search for a cloud environment continues.

The compatibility of the cloud environment with the organizations’ information systems is only mentioned by three of the eight interviewees. Other interviewees mentioned that if the cloud environment does not fit their needs and current system they would search for another provider for their cloud environment. As also shown in Table 5 the service quality of the cloud provider is of great importance to the organizations. Some of their processes may be dependent on the cloud environment and when something goes wrong they need immediate support and service from their cloud provider in order to keep their business running.

The interviewees mention the importance of trust in cloud computing and the cloud provider. Without some level trust there is no adoption of cloud computing. When asked what the interviewees believe trust in cloud computing is and how it is influenced the overall response was: the believe that the cloud provider keeps the promises that are made and that the cloud provider also does anything in its power to provide the cloud environment with the highest level of security, privacy and reliability as possible.

6.3 Expert interview

In this paragraph an overview will be given of the expert interview that was conducted. The expert interview was conducted with an expert on cloud computing. The interview was conducted to create extra context and strengthen the validity of the case studies. The outcome of the interview will be discussed in a descriptive way. The expert on cloud computing is an owner of an audit and consultancy company specialized in information security.

For analysing the trust issues with cloud computing, the expert first described his experience with cloud computing and attitude towards innovations in general. For his own business the expert uses cloud computing on a daily basis. Through the cloud the company receives data from the customers that needs to be examined. His attitude regarding innovations in general is very positive. *"In order to stay on top in this business you need to be ahead of the competition, which means introducing innovations to your organization in an early stage"*.

Attributes that are important to the expert in using cloud computing as a business are the security, with some certificates to prove the security to a certain amount, the performance, and the service of the cloud provider. *"The performance of the cloud provider is important, which means that the cloud has to respond fast and be able to upload and download large amounts of data in no-time"*. The service the cloud provider delivers is according to the expert one of the main requirements of many organizations. Organizations must be able to reach the cloud provider and their service desks at all time. *"If the cloud environment stops working, their own business may stagnate as well"*.

The main risk in cloud computing according to the expert is a breach in data of organizations. *"Other organizations trust these organizations with their data, when there is a breach in the data that is located in the cloud, their business will suffer from it"*. Therefore the security the cloud provider delivers is of great influence on the trust organizations have in them.
The expert mentions that small organizations are not able to produce their own server-site, due to the costs. *"A cloud provider can spent more money on security than a small organizations, since they are specialized in it"*. Larger organizations have more tools to create a similar environment as a cloud provider does. Therefore their considerations in adoption cloud computing may for them be of less importance than for smaller organizations. But also larger organizations are more pressed to use cloud computing, it's dynamic, fast and saves costs.

Regarding trust the expert mentions that a certain level of trust in the cloud provider is required, otherwise an organization should look for another provider to deliver the service. *"It is in their (cloud provider) interest as well to deliver a service with a high level of security. Their reputation is also affected in the case of a data breach"*. In choosing a cloud provider the expert looks at the standards and certifications and therefore level of security a cloud provider can offer, but also looks at the reputation the cloud provider has. *"For my own organization we choose a small cloud provider with a good reputation. The cloud provider knows us, can react fast when we need assistance and has knowledge about the systems and data we work with"*. For other organizations the expert also recommended looking at the reputation and certification and standards a cloud provider has.

6.4 Discussion

As mentioned in chapter 4 the attributes for cloud computing we expect to find with the conducted interviews are security, certification and standards, trust, quality, and compatibility. The cross-case analysis shows the attributes that were demonstrated in the case studies. In this paragraph the attributes that were expected to be demonstrated in the interviews are discussed and perhaps which attributes the organizations have that are not mentioned in the literature.

The *security* of cloud computing and the provider is the main attribute for cloud computing the interviewees mentioned. As can be seen in Table 5 all the interviewees agree that security is an important aspect of cloud computing and the expert also mentioned security as one of the main attributes. Due to the current security level in cloud computing some of the organizations are not willing to place core and critical applications and data in the cloud. The main concern for these organizations is the level of security and privacy of the cloud environment and provider. The interviewees of organization ALPHA, BRAVO and FOXTROT did mention that they do not use cloud computing for their core business due to the security issues they have with cloud computing and the lack of privacy there is according to them. Organization HOTEL and GOLF also keep their private-sensitive data out of the cloud due to the issues they have with the security and privacy of the cloud. This shows that the organizations really value the security of the cloud environment and also believe that the security level of cloud computing is not high enough for them, for now. Whereas the expert mentioned that the cloud provider has more resources to spend on security than most organizations do and therefore the security in the cloud is on a high level. Although this may contradict the believes of the organizations is does show the importance of security.

In the cross-case analysis the demand for *certification and standards* for cloud providers and cloud computing from the organizations is already shown. Some of the interviewees believe that cloud providers are not mature enough on the level of security and are therefore not always more secure than their own solutions. The certification and standards give the organizations the ability to compare the providers better and also give an extra assurance of their system. The interviewees of DELTA, ECHO and HOTEL did mention that the certification and standards that already do exist for cloud computing, like the ISO/IEC 27017, are not dynamic enough. The existing standards are a retrospective and only reflect the technical and organizational measures that were fulfilled at the time they were issued. These standards might not be met at a later moment in time, in which the standard is still valid. Therefore the certification and standards threatens their trustworthiness and reliability.

The value of *trust* in the cloud provider and their cloud computing service was well demonstrated in the case studies. All of the interviewees stated that trust in the cloud provider is key for adopting cloud computing. *"When there is no trust in the cloud provider, you should not adopt their service"* was the statement of the interviewee for the organization HOTEL. This demonstrates the overall feeling of all the interviewees. When there is no trust, all of the organizations will look for another provider or search for another solution. The organizations do believe that the cloud providers also have a great interest in keeping the cloud as secure as possible. Their *reputation* is also on the line as ALPHA, GOLF and the expert already mentioned. The reputation of the cloud provider was according to the expert also of importance; standards and certificates could enhance that trust by showing the quality of the cloud and the provider. The organizations uses reputation as a tool to validate the continuity of the cloud and the provider and in that context was an attribute to their trust in the cloud and the provider.

The *compatibility* of the system is not as expected in the literature a supported attribute for cloud computing. Only the interviewees from organization CHARLIE, DELTA and ECHO mentioned that the cloud environment should be compatible with their own information system. As the interviewee of organization DELTA said *"if the cloud environment is not compatible with our own systems we will search for a cloud provider that can provide us with an cloud environment that is compatible with our own systems and that fits our needs"*. Cloud computing is an emerging technology with also an emerging amount of cloud providers. This allows organizations like DELTA to search for a cloud provider that fits their needs and who can offer their organization a cloud environment that is

compatible with their own systems. Therefore organizations like CHARLIE, DELTA and ECHO are in the position to choose the cloud provider that fits their needs the most and relinquish the adoption of the cloud environment that is not compatible with their own information system.

As an organization that is dependent on the cloud for its data, the availability of the cloud is of great importance. One of the risks the organizations perceived was also the continuity and availability of the cloud. Not being able to access the cloud for a few hours on a business day can be devastating. It costs the organization a lot of money and maybe even their *reputation*. Therefore organizations require great *service quality* of the cloud provider and take the reputation of the cloud provider into account since they believe this has an effect on the continuity of the cloud and cloud provider. For most of their content in the cloud the organizations would like a 24/7 service of the cloud provider, only some content that is not used on a regular basis could have a service that is only available on business days at business hours. Besides the 24/7 service organizations also would like some personalization of the cloud provider. When they use the service it would be nice if the cloud provider would recognize their business and their specific needs. They are familiar with them, show empathy and have a good following-up service.

Chapter 7 Limitations and Future Studies

This research should be seen in the light of its limitations. The conducted case studies were done with organizations willing to participate in this research that also fit the criteria. Many organizations that were inquired to participate in this research did not have an employee in their organizations with extensive knowledge on cloud computing and providers. Also many organizations that were inquired had not adopted cloud computing yet. Therefore the sample size of our research may be biased since the interviewees come from organizations that are innovators in the field of cloud computing. The case studies are based on single case interviews, which also might influence the rigor of this research. However, all of the interviewees are experts in the field of Information Management and Security of their organizations and therefore can be considered as valuable sources (Yin, 2013).

The research has been limited to eight professional Dutch organizations. A larger group of organizations could have provided this research with different results, but as Yin (2013) also mentioned a multiple case study with six to ten cases allows for a high degree of certainty. Since the research has been done among larger professional Dutch organizations the results are only applicable to organizations that are located in the Netherlands. Organizations located in other countries may require other attributes and have other opinions regarding cloud computing. Beside the geographical area from which the data was collected, the bias may as well be in the industries of the organizations that were studied. The case studies were held among different types of large professional organizations and not restricted to a specific industry. This may be a limitation since every industry has its own characteristics and requirements. Also small and less professional organizations were not examined which also could have provided with other insights and results.

A future research in this field of study is highly recommended. Cloud computing is an uprising and ever-changing phenomenon and for a lot of organizations a new technology to adopt. Therefore I would recommend researchers to do further research on the attributes of cloud computing for organizations in order to trust a cloud provider. It is recommended to improve the research model used in this research by adding or removing some of the attributes and other constructs. New research could provide a better understanding of what the general attributes for organizations are regarding cloud computing. This is helpful for organizations and cloud providers to provide them a better understanding of the trust in cloud computing.

Chapter 8 Conclusion

This research combined an extensive literature review with a case study to develop an overview of attributes that are associated with trusting the cloud provider and adopting cloud computing. The attributes that were demonstrated in the literature review include security, certification and standards, reputation, trust, quality, and compatibility. Within the performed case studies the attributes were analysed through an interview with information management experts of different organizations. This showed that cloud computing is growing but at the moment still is a concept for the most innovative organizations. An interview with an expert on cloud computing was held to validate the results from the multiple case studies.

The cloud environment is fast, ever-changing and therefore requires cloud services that are reliable and secure. Dynamic certification and standards could provide a high level of reliability and security for the potential customers. An independent third-party for instance could audit providers on a more continuously basis on their security, reliability and trustworthiness.

If cloud providers want more organizations in the cloud or organizations to use cloud computing to a larger extent they need to work on their security level. The case study showed that the organizations are hesitant in using the cloud for their core business or private-sensitive information, which makes them use cloud computing in a smaller extent than they could have. On the contrary the expert mentioned that the cloud provider has more resources to spend on security and therefore likely has a high level of security in the cloud environment. This contradicts the believes of the organizations, but does highlight the importance of security. The trust in cloud computing and providers is not completely there, since it is a subjective matter for all of the organizations. I do believe that the introduction of dynamic certification and standards would improve this trust and also the security and trust in security of cloud computing and providers. With dynamic certification and standards the cloud providers have to be more transparent about the measures they are taking in order to guarantee a standard level of security. Also the providers have to prove on a regular basis how secure they are. The certification and standards also could have an effect on the reputation of the cloud provider and the trust paired with the reputation.

The compatibility of the cloud environment with the information systems of the organization is the only attribute that did not receive regular mention in the case studies. Two of the eight organizations mentioned that the cloud environment should be compatible with their own information system. The overall quality of cloud computing, divided in service quality and system quality, is also of great importance for organizations. The quality of the system should meet the quality of their own systems if not exceed this quality in order to adopt cloud computing. Organizations require great service quality with a 24/7 helpdesk from the cloud provider. Not being able to access the cloud environment for even a few hours can be devastating for an organization. Organizations also expect some personalized service of the cloud provider and not being just one of the hundred organizations that have employed their cloud computing service.

Looking at the attributes, no single attribute on its own can explain the trust and adoption of cloud computing. A trusted cloud provider may also not score on all of the attributes. Therefore a right balance between the different attributes is required for a cloud provider to ensure trust from organizations. This research shows that there is not one attribute or sample of attributes that explains the trust in all cases and that every organization and situation allows for a different combination of attributes.

In sum, to answer the main research question: *"What are the attributes of cloud computing for an organization to trust a cloud provider?"* remains a bit unclear. The research has shown that there is not one attribute or sample of attributes that explains the trust and adoption of cloud computing and that every organization and situation allows for a different combination of attributes. So there is no single answer to the main question but the research does show the importance of these attributes for organizations.

Appendix

Appendix A PRIMA interview questions

P	Primair proces
P1	Hoe ziet uw werkproces eruit? Maakt uw organisatie op dit moment al gebruik van cloud computing? Op hoeveel procent van uw werk zou het gebruik van cloud computing van toepassing zijn?
P2	In welke vorm maakt uw organisatie gebruik van cloud computing of zou uw organisatie gebruik willen maken van cloud computing?
P3	Wat vindt u belangrijk bij het gebruik maken van cloud computing?
P4	Welke risico's zouden er voor uw organisatie zijn bij het gebruik maken van cloud computing? En hoe hoog zijn deze risico's voor uw organisatie?
P5	Welke functies van cloud computing zijn voor uw organisatie het belangrijkste? Welke onderdelen van cloud computing zouden eventueel een bottleneck kunnen veroorzaken in uw processen?
P6	Welke onderdelen van cloud computing zou u verbetert willen zien (om gebruik te maken) van cloud computing?

R	Relevantie
R1	Wat ervaart u, als belangrijkste in uw dagelijkse werk als u kijkt naar de diensten die u verleent?
R2	Welke aspecten ervaart u als knelpunt of als problematisch?
R3	Op welke punten zou het inzetten van cloud computing voor u van belang kunnen zijn?
R4	Moet het systeem dat de cloud provider biedt makkelijk te integreren zijn in de systemen die uw eigen organisatie heeft? Is de mate waarin het systeem van de cloud provider geïntegreerd kan worden van belang bij het kiezen van een cloud provider?

I	Informatiebehoefte en informatiekwaliteit
I1	Wat is uw inschatting van de kwaliteit van cloud computing?
I2	Welke aspecten van het systeem zijn belangrijk voor u?
I3	Is de content in the cloud voor uw gevoel veilig? Biedt de cloud provider voldoende veiligheid voor uw content?

M	Mensen en middelen
M1	Is de service van de cloud provider belangrijk voor uw organisatie? Is het belangrijk dat een helpdesk snel op u (en uw organisatie) reageert?
M2	Krijgt u voldoende support van de cloud provider?
M3	Wordt er vanuit uw organisatie voldoende ondersteuning geboden om vernieuwingen op het gebied van ICT door te voeren? Zoals cloud computing invoeren.
M5	Is de ICT ondersteuning van voldoende niveau om de kwaliteit te kunnen garanderen?

A	Attitude
A1	Hoe staat u tegenover ICT vernieuwingen in het algemeen?
A2	Ervaart u belemmeringen bij het doorvoeren van vernieuwingen?
A3	Voelt u (en uw organisatie) de druk om cloud computing toe te passen?
A4	Wat verstaat u onder vertrouwen?
A5	Heeft u zelf vertrouwen in cloud computing en cloud providers? En zou u cloud providers met uw informatie vertrouwen?
A6	Is cloud computing volgens u (en uw organisatie) betrouwbaar? Biedt het voldoende privacy?

Appendix B Expert interview questions

- Hoe zit uw werkproces eruit? Maakt uw eigen organisatie op dit moment gebruik van cloud computing? Zo ja, in welke vormen maakt het gebruik van cloud computing en op hoeveel procent van uw werk is dit van toepassing?
- Wat is uw ervaring met cloud computing?
- Welke functies van cloud computing zijn volgens u belangrijk? Wat is voor u het belangrijkste bij het gebruik maken van cloud computing?
- Welke onderdelen van cloud computing kunnen eventueel een bottleneck veroorzaken?
- Welke risico's hangen aan het gebruik maken van cloud computing en zijn de risico's hiervan voor elke organisatie even groot?
- Welke onderdelen van cloud computing zou u in de toekomst graag verbetert willen zien?
- Moet het systeem dat de cloud provider biedt makkelijk te integreren zijn in de systemen die uw eigen organisatie heeft? Is de mate waarin het systeem van de cloud provider geïntegreerd kan worden van belang bij het kiezen van een cloud provider?
- Wat is uw inschatting van de huidige kwaliteit van cloud computing?
- In hoeverre is de service van een cloud provider belangrijk?
- Krijgt uw eigen organisatie voldoende support van de cloud provider?
- Hoe kijkt u tegen het certificeren van cloud providers aan? Heeft het voor u en uw organisatie een toegevoegde waarde als cloud providers een certificaat hebben of een bepaalde standaard hanteren?
- Hoe staat u zelf tegenover vernieuwingen in het algemeen? Bent u iemand die graag meegaat met de nieuwe trends en doet u dat ook met uw organisatie? Of voelt u belemmeringen bij het doorvoeren van nieuwe trends binnen uw organisatie of in het algemeen?
- Wat verstaat u onder vertrouwen hebben in een cloud provider en cloud computing?
- In welke mate heeft u vertrouwen in cloud computing voor u zelf en voor uw organisatie?
- Is cloud computing volgens u betrouwbaar en biedt het organisaties voldoende privacy en veiligheid?

References

Adams, D. A., R. R. Nelson, P. A. Todd. 1992. Perceived usefulness, ease of use, and usage of information technology: A replication. MIS Quart. 16(2) 227–250.

Arias-Cabarcos, P., Almenárez-Mendoza, F., Marín-López, A., Díaz-Sánchez, D., & Sánchez-Guerrero, R. (2012). A metric-based approach to assess risk for "on cloud" federated identity management. *Journal of Network and Systems Management*, *20*(4), 513-533.

Armbrust, M., Fox, O., Griffith, R., Joseph, A. D., Katz, Y., Konwinski, A., ... & Zaharia, M. (2009). M.: Above the clouds: a Berkeley view of cloud computing.

Arpaci, I. (2016). Understanding and predicting students' intention to use mobile cloud storage services. *Computers in Human Behavior*, *58*, 150-157.

Artz, D., & Gil, Y. (2007). A survey of trust in computer science and the semantic web. *Web Semantics: Science, Services and Agents on the World Wide Web*, *5*(2), 58-71.

Bigley, G. A., & Pearce, J. L. (1998). Straining for shared meaning in organization science: Problems of trust and distrust. *Academy of management review*, *23*(3), 405-421.

Burda, D., & Teuteberg, F. (2014). The role of trust and risk perceptions in cloud archiving—Results from an empirical study. *The Journal of High Technology Management Research*, *25*(2), 172-187.

Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on* (Vol. 1, pp. 647-651). IEEE.

Chin, W.W., A. Gopal. 1993. An examination of the relative importance of four belief constructs on the GSS adoption decision: A comparison of four methods. Proc. 26th Hawaii Internat. Conf. System Sci. 548–557

Chin, W.W., P. A. Todd. 1995. On the use, usefulness, and ease of use of structural equation modelling in MIS research: A note of caution. MIS Quart. 19(2) 237–246.

Clarke, G. (2009). Microsoft Azure cloud suffers first crash. The Register, March 16. Retrieved from: http://www.theregister.co.uk/ 2009/03/16/azure_cloud_crash/

Creeger, M., 2009. CTO Roundtable: Cloud Computing. Communications of the ACM, 52(8), pp.50-56.

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (Doctoral dissertation, Massachusetts Institute of Technology).

Davis, F. D. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quart. 13(3) 319–339.

Davis, F.D., R. P. Bagozzi, P. R. Warshaw. 1989. User acceptance of computer technology: A comparison of two theoretical models. Management Sci. 35(8) 982–1002.

Davis, F.D. 1993. User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. Internat. J. Man-Machine Stud. 38(3) 475–487.

Davis, F.D., V. Venkatesh. 1996. A critical assessment of potential measurement biases in the technology acceptance model: Three experiments. Internat. J. Human-Comput. Stud. 45(1) 19–45.

de Hert, P., Papakonstantinou, V., & Kamara, I. (2016). The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection. *Computer Law & Security Review*, *32*(1), 16-30.

Depietro, R., Wiarda, E., & Fleischer, M. (1990). The context for change: Organization, technology and environment. *The processes of technological innovation*, *199*(0), 151-175.

Firdhous, M., Ghazali, O., & Hassan, S. (2011, December). A trust computing mechanism for cloud computing. In *Kaleidoscope 2011: The Fully Networked Human?-Innovations for Future Networks and Services (K-2011), Proceedings of ITU* (pp. 1-7). IEEE.

Gefen, D., D. W. Straub. 1997. Gender differences in the perception and use of e-mail: An extension to the technology acceptance model. MIS Quart. 21(4) 389–400.

Harauz, J., Kaufman, L.M, Potter, B. (2009). Data security in the world of cloud computing. *Co-published by the IEEE Computer And reliability Societies*, 61-64.

Harris, S., 2002. CISSP All-in-one Certification Exam Guide. McGraw-Hill/Osborne, New York, USA.

Hendrickson, A. R., P. D. Massey, T. P. Cronan. 1993. On the test retest reliability of perceived usefulness and perceived ease of use scales. MIS Quart. 17(2) 227–230.

Huang, J., & Nicol, D. M. (2013). Trust mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *2*(1), 1.

Igbaria, M., A. Chakrabarti., N. Zinatelli, P. Cragg, A. L. M. Cavaye. 1997. Personal computing acceptance factors in small firms: A structural equation model. MIS Quart. 21(3) 279–305.

Jansen, W. & Grance, T., 2011. Guidelines on Security and Privacy in Public Cloud Computing. Special Publication. Gaithersburg: U.S. Department of Commerce National Institute of Standards and Technology.

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security*, *20*(5), 332-349.

Jarvenpaa, S., Tractinsky, N., Saarinen, L. (1999). Consumer Trust in an Internet Store: A Cross-Cultural Validation. Journal of Computer Mediated Communication, 5(2), December, 1-37.

Kim, S., & Yoon, A. (2012). Do I trust Google? An exploration of how people form trust in cloud computing. *Proceedings of the American Society for Information Science and Technology*, *49*(1), 1-3.

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, *37*(4), 372-386.

Kuyoro, S., Ibikunle, F., & Awodele, O. (2011). Cloud computing security issues and challenges. *International Journal of Computer Networks*, *3*(5).

Landeweerd, M., Spil, T., & Klein, R. (2013). The Success of Google Search, the Failure of Google Health and the Future of Google Plus. In*International Working Conference on Transfer and Diffusion of IT* (pp. 221-239). Springer Berlin Heidelberg.

Lee, G.-G., & Lin, H.-F. (2005). Customer perceptions of e-service quality in online shopping. International Journal of Retail & Distribution Management, Vol. 33, No. 2, 161-176.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social forces*, *63*(4), 967-985.

Lian, J. W. (2015). Critical factors for cloud based e-invoice service adoption in Taiwan: An empirical study. *International Journal of Information Management*,*35*(1), 98-109.

Lin, C., & Varadharajan, V. (2007, April). A hybrid trust model for enhancing security in distributed systems. In *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on* (pp. 35-42). IEEE.

Lins, S., Grochol, P., Schneider, S., & Sunyaev, A. (2016). Dynamic Certification of Cloud Services: Trust, but Verify!. *IEEE Security & Privacy*, *14*(2), 66-71.

Lonescu, D. (2009). Microsoft red-faced after massive sidekick data loss. PC World, October 12. Retrieved from: http://www.pcwo- rld.com/ article/173470/

Mackay, M., Baker, T., & Al-Yasiri, A. (2012). Security-oriented cloud computing platform for critical infrastructures. *Computer Law & Security Review*, *28*(6), 679-686.

Marcella, A. J. (1999). *Establishing trust in virtual markets*. Institute of Internal Auditors.

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

Mathieson, K. 1991. Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior. Inform. Systems Res. 2(3) 173–191.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, *20*(3), 709-734.

McLarnon, B., Robinson, P., Milligan, P., & Sage, P. (2014). An Iterative Approach to Trustable Systems Management Automation and Fault Handling.*Journal of Network and Systems Management*, *22*(3), 366-395. McCarthy, J., 1999. MIT Centennial Speech. In Abelson, H., ed. Architects of the Information Society, Thirty-Five Years of the Laboratory for Computer Science at MIT., 1999. The MIT Press.

McLarnon, B., Robinson, P., Milligan, P., & Sage, P. (2014). An Iterative Approach to Trustable Systems Management Automation and Fault Handling.*Journal of Network and Systems Management*, *22*(3), 366-395.

Meixner, F., & Buettner, R. (2012). Trust as an Integral Part for Success of Cloud Computing. In *ICIW 2012: 7th International Conference on Internet and Web Applications and Services*.

Mell, P. and Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology, October 7. Available from: http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

Messerschmidt, C. M., & Hinz, O. (2013). Explaining the adoption of grid computing: An integrated institutional theory and organizational capability approach. *The Journal of Strategic Information Systems*, *22*(2), 137-156.

Mohammed, D. (2011). Security in cloud computing: an analysis of key drivers and constraints. *Information Security Journal: A Global Perspective*, *20*(3), 123-127.

Morales-Sandoval, M., Vega-Castillo, A. K., & Diaz-Perez, A. (2014). A secure scheme for storage, retrieval, and sharing of digital documents in cloud computing using attribute-based encryption on mobile devices. *Information Security Journal: A Global Perspective*, *23*(1-2), 22-31.

Oxford English Dictionary, The Compact Edition. (1971). New York: Oxford University Press.

Parker, D. (2010). Our excessively simplistic information security model and how to fix it. *ISSA Journal*, 12-21.

Parkhill, Douglas F. *The Challenge of the Computer Utility*. Massachusetts: Addison-Wesley Publishing Company, 1966. 3. Print.

Pearson, S. (2013). Privacy, security and trust in cloud computing. In *Privacy and Security for Cloud Computing* (pp. 3-42). Springer London.

Rangasamy, K., & Somasundaram, T. S. (2016). Trust Enabled CARE Resource Broker. In *Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC–16')* (pp. 13-32). Springer International Publishing.

Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in close relationships. *Journal of personality and social psychology*, *49*(1), 95.

Rogers, E. (1983). *Diffusion of Innovation* (3rd Edition ed.). New York: Free Press.

Rogers, E. M. (1962). *Diffusion of Innovations* (1st ed.). New York: Free Press.

Rogers, E. M. (1983). *Diffusion of innovations* (3rd ed.). New York: Free Press.

Rogers, E. M. (1995). *Diffusion of Innovations* (4th ed.). New York: Free Press.

Rogers, E. M. (2003). *Diffusion of Innovations* (5th ed.). New York: Free Press.

Rogers, E. M. (2003). *Diffusion of Innovations*. New York: Free Press.

Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering*,*39*(1), 47-54.

Sabahi, F. (2011). Cloud Computing Security Threats and Responses. In: *IEEE 3rd International Conference on Communication Software and Networks*. 245–249.

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, *63*(9), 1278-1308.

Segars, A. H., V. Grover. 1993. Re-examining perceived ease of use and usefulness: A confirmatory factor analysis. MIS Quart. 17(4) 517–525

Sharma, S. K., Al-Badi, A. H., Govindaluri, S. M., & Al-Kharusi, M. H. (2016). Predicting motivators of cloud computing adoption: A developing country perspective. *Computers in Human Behavior*, *62*, 61-69.

Spil, T. A., Schuring, R. W., & Michel-Verkerke, M. B. (2004). Electronic prescription system: do the professionals USE IT? Int. J. Healthcare Technology Management, Vol. 6, No. 1 , 32-55.

Spil, T. A., Michel-Verkerke, M. B. (2012). De waarde van informatie in de gezondheidswereld, Eburon, Delft

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.

Subramanian, G. H. 1994. A replication of perceived usefulness and perceived ease of use measurement. Decision Sci. 25(5/6) 863– 874.

Sunyaev, A., & Schneider, S. (2013). Cloud services certification. *Communications of the ACM*, *56*(2), 33-36.

Szajna, B. 1994. Software evaluation and choice: Predictive validation of the technology acceptance instrument. MIS Quart. 18(3) 319–324.

Szajna, B. 1996. Empirical evaluation of the revised technology acceptance model. Management Sci. 42(1) 85–92.

Taylor, S., P. A. Todd. 1995. Understanding information technology usage: A test of competing models. Inform. Systems Res. 6(2) 144–176.

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *Processes of technological innovation*. Lexington Books.

Uusitalo, I., Karppinen, K., Juhola, A., & Savola, R. (2010, November). Trust and cloud services-an interview study. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on* (pp. 712-720). IEEE.

Venkatesh, V. 1999. Creating favorable user perceptions: Exploring the role of intrinsic motivation. MIS Quart. 23(2) 239–260.

Venkatesh, V. A. (2000). A theoretical extension of the Technoly Acceptance Model: Four longitudal field studies. Management Science, Vol. 46, No. 2, 186-204.

Venkatesh, V., F. D. Davis. 1996. A model of the antecedents of perceived ease of use: Development and test. Decision Sci. 27(3) 451–481.

Venkatesh, V., M. G. Morris. 2000. Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and user behavior. MIS Quart. 24 115–139.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, Vol. 27, No. 3, 425- 478.

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in human behavior*, *21*(1), 105-125.

Weber, T. (2011). Cloud computing: How to get your business ready. Retrieved from /http://www.bbc.co.uk/news/business-12779201S.

Weis, J., & Alves-Foss, J. (2011). Securing database as a service: Issues and compromises. *IEEE Security & Privacy*, *9*(6), 49-55.

Wheeler, E. (2011). *Security risk management: Building an information security risk management program from the Ground Up*. Elsevier.

Whitman, M. E., & Mattord, H. J. (2012). *Hands-on information security lab manual*. Cengage Learning.

Yigitbasioglu, O. (2014). Modelling the intention to adopt cloud computing services: a transaction cost theory perspective. *Australasian Journal of Information Systems*, *18*(3).

Zaheer, A., McEvily, B., & Perrone, V. (1998). Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. *Organization science*, *9*(2), 141-159.

Zargari, S. A., & Smith, A. (2014). Policing as a Service in the Cloud.*Information Security Journal: A Global Perspective*, *23*(4-6), 148-158.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, *1*(1), 7-18.

Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010, November). Security and privacy in cloud computing: A survey. In *Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on* (pp. 105-112). IEEE.