# Improving trust in cloud computing

A framework that incorporates the factors
that influence trust in cloud services

**J. Heins**

**September 13, 2017**

“Vertrouwen komt te voet en gaat te paard”

– Prof. Dr. Ir. M. F. W. H. A. Janssen
during the green-light meeting

# Improving trust in cloud computing

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

**MASTER OF SCIENCE**

in **Complex Systems Engineering and Management**

Faculty of Technology, Policy and Management

by

Jacco Heins

Student number: 4155149

To be defended in public on September 27, 2017

## Graduation committee

|  |  |
|---|---|
| Chairperson | : Prof. Dr. Ir. M. F. W. H. A. Janssen, Section ICT |
| First Supervisor | : Dr. H. Asghari, Section Policy, Organisation, Law and Gaming |
| Second Supervisor | : Dr. M. E. Warnier, Section Systems Engineering |
| External Supervisor | : T. Hommel MSc, Accenture |

# Summary

In recent years, cloud computing has made its way into enterprise IT. With cloud computing services, the applications and data of your organisation are no longer deployed on your own servers, but on the servers of the cloud service provider. Consequently, when you walk into your office in the morning and start your computer, you have to trust, either consciously or unconsciously, the cloud service provider to give you access to the applications and data to perform your job. Currently, organisations are asking themselves the question: "do we trust this cloud computing service with this task?"

So, what precisely is "this task"? Cloud computing is an IT deployment model, based on virtualization, where resources, in terms of infrastructure, applications and data are deployed via the internet as a distributed service by one or several service providers. These services are scalable on demand and can be priced on a pay-per-use basis. Cloud computing can provide several benefits to organisations, such as such as scalability, ubiquitous network access, decreased effort in managing technology and cost savings. On the other hand, there are also numerous challenges and uncertainties that have to be overcome in order to reach the promised benefits. One of the key challenges of adopting cloud computing is related to trust. Trust is defined as: *an organisation's dynamic, calculated and dependent expectation of the other organisation's competence and goodwill*. Trust is necessary for effective collaboration between customers and providers and reducing transaction costs, however, in practice this trust is often lacking. From the scientific literature, it becomes clear that there is still a lot of ambiguity about trust in cloud services and that it is unclear which factors influence this trust. At least, there is no empirical research that aims to explain the factors that influence trust in a cloud service. Since cloud computing is subject to a lot of ambiguity and multiple perspectives exist, it is also expected there are multiple perspectives related to the factors that influence trust (i.e. a certain factor may be relevant for trusting a cloud service to one (sub)group, while this factor is irrelevant for another (sub)group). These perspectives are not yet defined in scientific literature. Additionally, no scientifically based design exists that aims to improve the trust of (potential) customers in a cloud service.

Based on these knowledge gaps, the following research question was defined: *"What are the factors that influence the trust of an organisation in a cloud service and what are the different perspectives and how can this trust be improved?"*

In order to answer this a design approach was established. First, an analysis of the concepts of cloud computing and trust, and the integration of those concepts in scientific literature is performed. From this analysis, a conceptual model is derived. This conceptual model is then evaluated with a Q-method study on the potential factors influencing trust in cloud services. The interpretation of the Q-method results reveals which factors influence the trust in a cloud service and the several (in this case three) perspectives related to this. Based on the perspectives, combined with an analysis of the customer's organizational configuration, an

artifact is designed which facilitates cloud brokers in improving the trust of the (potential) customers.

With this approach certain empirical findings were done. In general, it is perceived that the customer needs to perform certain actions before adopting a cloud service. The customer needs to make sure their organisation is ready and willing to make the change, as well as making sure that the cloud service they want to adopt is *secure* and provides *privacy* over their data. Having knowledge on the security and privacy of the cloud services increases trust. As all perspectives agree on the fact that also change from the customer is required, it can be concluded that organisational change is seen more as a condition that needs to be met in order to adopt cloud computing, than that it is seen as a factor influencing trust in a cloud service. Thus, the factor will be redefined to: *the willingness to change the organisation*. When an organisation is willing to change, adopting a cloud service is more easily trusted. Moreover, all perspectives seem to understand what a cloud service entails. A *transparent* cloud service gives the customer the trust in the provider's competence and goodwill.

Besides the general viewpoints, there are also viewpoints specific to the three perspectives. The first perspective is the perspective of the *techno-optimists.* In short, this group really sees cloud computing as the most important trend in enterprise IT. Because a cloud service can offer significant *technological advantages*, they are willing to trust it. But, a lack of *interoperability* is seen as an important issue: when it is not possible to change from one provider to another, trust in the cloud service will be limited. The second perspective is the perspective of the *responsibility-shifters*. In short, this group wants to make the provider *accountable* in case contingencies with the cloud service occur, preferably through the use of *contracts*. When a cloud service satisfies these conditions, they trust the cloud service. The third, and last perspective is the perspective of the *operational conservatives*. This group does not see cloud computing as an important trend or significant *technological advantage* and has its doubt with respect to the reliability; they prefer to keep things as they are. This perspective has a more negative viewpoint of cloud computing, but increasing the perception of the *technological advantage* and *reliability* will improve their trust in a cloud service.

Based on these findings, the OPF (Organisation, Perspective, Factor) Framework was designed. The OPF Framework provides cloud broker with a tool to improve the trust of (potential) customers in a cloud service. The implementation design that accompanies the framework, gives the cloud broker insight in when to approach which part of the organisation.

*So, in short, the answer to the main research question can be defined as:*

Trust in a cloud service is approached from three perspectives: techno-optimists, responsibility-shifters and operational conservatives. In general, all of these perspectives perceive security and transparency as factors that influence their trust in a cloud service. On top of that, techno-optimists perceive technological advantage and interoperability as important, responsibility-shifters perceive contracting and accountability as important and operational conservatives perceive reliability and (the lack of) technological advantage as important. The OPF Framework as proposed in this thesis uses these perspectives in combination with the different parts of the organisation: strategic apex, cloud service

management, operational IT department and cloud experts. By addressing the main concerns of the specific part of the organisation, in combination with the relevant perspective, it is possible to improve the trust of an organisation in a cloud service.

# Foreword & Acknowledgements

Before I started this thesis project, I expected it to be tough. And it was. All the years of studying and hard work had to be reflected into one final thesis: this document. During the study, things weren't always easy; as a matter of fact, there were moments that I gave up, only to grab myself together a few moments later and finish that project, paper or exam successfully. This exact same process has taken me through several stages of my thesis: get knocked down, but always get up. Along the way I always trusted myself. Trust is not only the topic of this thesis, it has also been the driving force during the development of it. Trusting yourself, that you are capable of doing it right, that is what keeps you going, also when things get rough. So that is what I did, I trusted myself.

During the process of writing this thesis, I have been supported by several people, whom I would like to thank now. First of all, my graduation committee. Thank you, Hadi, for being my first supervisor. You took this role after I got some setbacks in the formation of my committee and this helped me tremendously. I am thankful that you introduced me to Q-method, which was both for me and for the participants of my research a delightful way of gathering empirical data. Also, I am thankful for your critical feedback and guidance throughout the whole process of writing this thesis. Thank you, Martijn, for being my second supervisor. I am thankful that you made me look at problems from another perspective when I was stuck in my own thinking process. And lastly, thank you, Marijn, for being the chair of my graduation committee and ensuring the quality of this thesis.

I would also like to thank Accenture and all the people that helped me there. Thank you, Thomas, for being my supervisor. I am thankful that you got me in touch with relevant people for my research and provided me with problems and challenges you faced in practice during the cloud projects you and your team worked on. Thank you, Reihaneh, also for being my supervisor. I am thankful for the fact that you took your role as a buddy so seriously and extending it by being my second supervisor within Accenture. I am also thankful for your critical feedback and guidance in the planning of my thesis. And lastly, thank you, Bas, for giving me the opportunity to take a look at several clients and projects.

Also, a big 'thank you' to my parents, who supported me in every step I took. Thank you for providing me with the opportunity to study in Delft and Lund. My last thank you goes out to Mariana, who I met during the process of writing this thesis. You were able to take my thoughts off my thesis when this was needed and provided me with fresh energy to work even harder than I did before.

Yours sincerely,

Jacco Heins

# List of figures

# List of tables

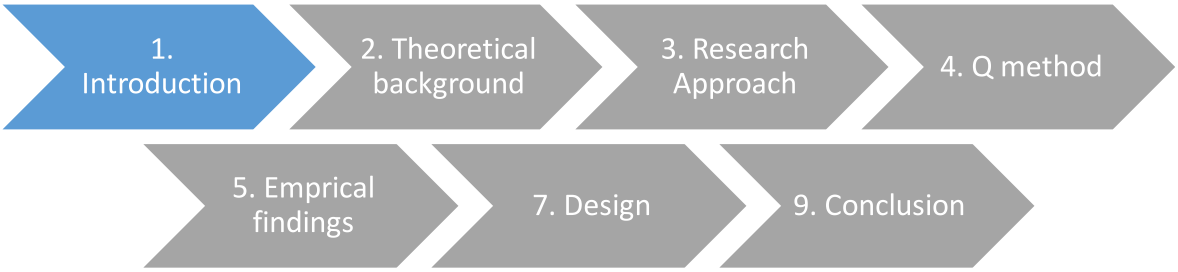
# Table of content

# Chapter 1 Introduction

This chapter will introduce the thesis. The introduction consists of the following:

- Problem definition
- Research objective
- Research question
- Relevance and contribution
- Scope
- Thesis outline
- Readers guide

This chapter will introduce this thesis by discussing the problem. This will be used as the basis for the research objective and research question. Also, the relevance and contribution, scope, thesis outline and readers guide will be introduced in this chapter.



# 1. Introduction

## 1.1. Problem definition

Cloud computing is becoming more and more a way for organisations to enhance next-generation digital business and provides agile, scalable and elastic solutions. Although cloud computing previously has been seen as a hype by some, it now has started to become clear that cloud computing solutions can exceed the capabilities of the traditional on-premise IT solutions (Gartner, 2017). This is also confirmed by the fact that many organisations are leaving the cloud experimentation phase behind and start seeking strategic partnerships with providers.

Cloud computing is an IT deployment model where resources such as infrastructure, applications and data are deployed through the internet as a distributed service by one or more providers (Leimeister, Riedl, Bohm, & Krcmar, 2010). The service is scalable on demand and can be priced on a pay-per-use basis. Virtualization technology is the enabling technology for cloud computing, making it possible for data centre providers to adjust their resources on demand and as a consequence utilise their hardware more efficiently (Leimeister et al., 2010).

Organisations that adopt cloud computing expect to get several benefits from it. The most commonly mentioned benefits are scalability, ubiquitous network access, cost savings and decreased effort in managing technology (Khajeh-hosseini, Greenwood, Smith, & Sommerville, 2012; Prasad & Green, 2015; C. Wang, Chow, Wang, Ren, & Lou, 2013). Virtualization technology and large datacentres make it possible for organisations to have scalable and ubiquitous network access. Moreover, because IT resources are used more efficiently through economies of scale, cost savings can be achieved. Lastly, because the service is now provided by the provider, less internal technological expertise over the IT resources is necessary, resulting in a decreased effort in managing technology.

Although cloud computing can offer various benefits, trust management still proves to be one of the key challenges in the adoption of cloud computing (Armbrust et al., 2010; Noor, Sheng, Zeadally, & Yu, 2013). While cloud services reduce the responsibility of the customer in terms of hardware and software management, it is likely that critical information and applications are moved outside the direct control of the customer (Uusitalo, Karppinen, Juhola, & Savola, 2010). Also, with the market growing at an increasing pace, reliably identifying a trustworthy provider becomes harder (Habib, Ries, & Mühlhäuser, 2010; Habib, Ries, Mühlhäuser, & Varikkattu, 2014). Additionally, trust leads to effective and ongoing collaboration, since it promotes continuous interaction and directs firms into investing in the collaboration (Rousseau, Sitkin, Burt, & Camerer, 1998). Lastly, research shows that an assurance of a higher degree of trust in a provider is required in order to attain efficient resource allocation and utilization (Abawajy, 2009), partly by allowing organisations to adopt less elaborate safeguards, thereby economizing on transaction costs (Chiles & McMackin, 1996).

For this reason, trust in cloud services has gained some attention from academia and businesses. Several scientific studies produced conceptual trust models for cloud computing, with some of the studies validating the conceptual models by literature research (Chu, Lai, & Lai, 2013; Lansing & Sunyaev, 2016; Uusitalo et al., 2010). However, empirical research on trust in a cloud service is fairly limited, hence it is still unclear which factors influence the trust in a cloud service. Moreover, within the field of cloud computing, there is a lot of ambiguity and uncertainty with respect to the actual realisation of the benefits and if cloud computing can overcome certain challenges. This ambiguity and uncertainty leads to multiple perspectives on different aspects of the cloud, with trust being one of them. It is not yet explicitly defined which perspectives on trust in a cloud service there are, and what the implications for its adoption are. Lastly, there is no scientifically based method or approach that aims to improve the trust of organisations in a cloud service.

### 1.1.1. Problem statement

Based on the problem definition, it can be concluded that cloud computing can offer various benefits for organisations, but that their lack of trust is preventing them to adopt it. Which factors influence the trust of organisations in a cloud service and what the different perspectives on this matter are, is yet unknown. A design that incorporates the different perspectives and the factors that influence the trust in a cloud service has to be developed, as it is currently missing.

Thus, the problem statement for this thesis can be defined as:

*Cloud computing has the potential to provide various benefits to organisations, but the lack of trust is still a key challenge that prevents the adoption of it. Knowledge on the perspectives on trust in a cloud service and the factors influencing the trust, is missing, as well as a design to improve this trust.*

### 1.1.2. Research gaps

The following knowledge gaps can be derived from the problem definition:

- It is unknown what the different perspectives on trust in cloud computing are
- There is no empirical research that explains what factors influence trust in cloud computing
- No scientifically based design exists that aims to improve the trust of (potential) customers in a cloud service

## 1.2. Research objective

In accordance with the problem definition, the objective of this thesis can be defined as:

*To define the relevant perspectives on trust in a cloud service based on the factors that influence trust and to design an artifact that facilitates in the improvement of this trust.*

The research objective consists of three interrelated components. Meaning that the perspectives will be based upon the factors that influence trust, while the design will be based upon the perspectives and the factors. So, in order to reach one objective, first another objective needs to be reached. The order in which the objectives are reached is as follows:

- Define factors influencing the trust in a cloud service

- Define perspectives on trust in a cloud service
- Design an artifact to facilitate the improvement of trust in a cloud service

## 1.3. Research question

The main research question of the proposed research will be as follows:

*"What are the factors that influence the trust of an organisation in a cloud service and what are the different perspectives and how can this trust be improved?"*

The sub questions that are related to this main research question are as follows:

1. What is the current state of trust in a cloud computing service? (Chapter 2)
2. How can the factors influencing trust in cloud computing services be analysed and structured? (Chapter 3 & 4)
3. Which factors influence the trust of an organisation in a cloud computing service? (Chapter 2 & 5)
    a. Which potential factors are found in the literature? (Chapter 2.4.2)
    b. What does a conceptual trust model that describes the potential factors influencing trust look like? (Chapter 2.4.3)
    c. What are the factors influencing trust in a cloud computing service according to empirical research? (Chapter 5)
4. What are the perspectives on trust in a cloud service? (Chapter 5)
5. What does a design look like that facilitates the improvement of trust, based on the perspectives? (Chapter 6)

## 1.4. Relevance and contribution

According to the definitions of Verschuren & Doorewaard (2010) the research as done in this thesis can be defined as practice-oriented. Within practice-oriented research, there are five possible steps in the so-called *intervention cycle*: problem analysis, diagnosis, design, intervention/change and evaluation. This intervention cycle is a model to solve practical problems, rather than a model to carry out empirical research. A practice-oriented research can contribute to any of these five steps. Based on the characteristics of the defined problem and objective of this research, it can be concluded that this research will mainly focus on the diagnosis, followed by a design.

The kind of diagnostic research that will be used in this thesis is the *opinion research*. Since trust is subjective, it is less important to gain objective knowledge about a problem than to learn more about the opinions shared by certain (sub)groups. For this type of research to be relevant and contribute to science and practice, a specifically defined group of people and their opinions need to be studied. Moreover, a clear scientific method needs to be used to analyse and interpret structures and patterns among the different opinions and perspectives in order for the results to be generalizable.

With respect to design research, Johannesson & Perjons (2014) extensively describe design science in their book *Introduction to Design Science*. Design science is intended to produce and communicate knowledge that is of general interest and is relevant for a global practice and for the research community. This is visualised in Figure 1.

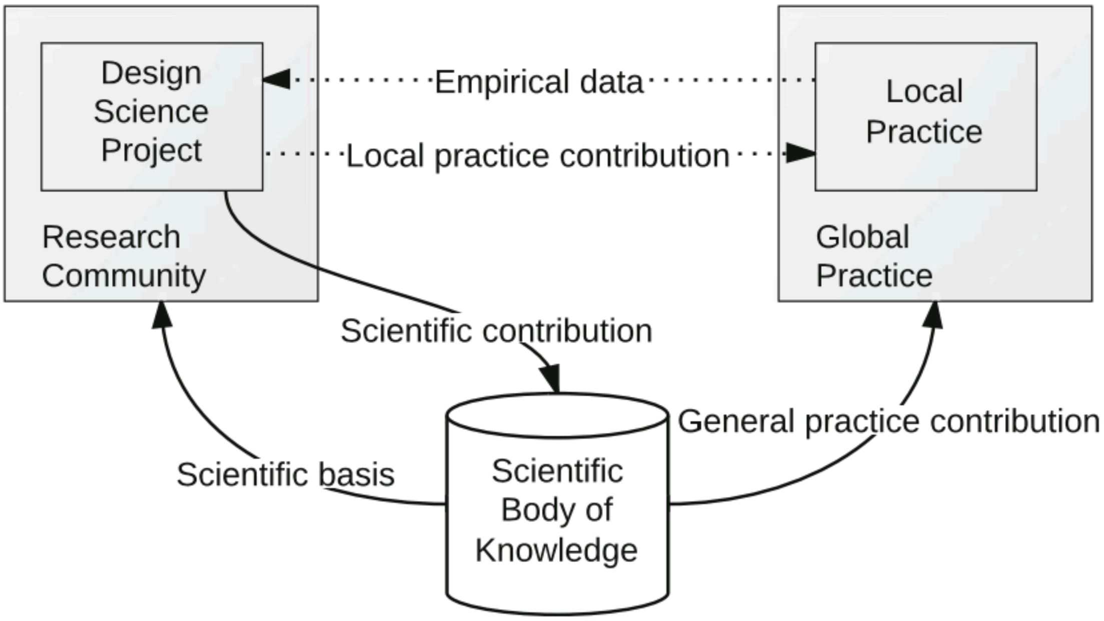


*Figure 1 Scientific and practical contribution as presented by Johannesson & Perjons (2014)*

### 1.4.1. Scientific contribution

In their research, Lansing & Sunyaev (2016) found that:

> *"Trust is an important facilitator for successful business relationships and an important technology adoption determinant. However, thus far trust has received little attention in the context of cloud computing, resulting in a lack of understanding of the dimensions of trust in cloud services and trust-building antecedents."*

The literature review that is done for this research confirms this finding. While Lansing & Sunyaev (2016) try to define factors influencing the trust in a cloud service through a literature study, empirical research is still lacking. Moreover, Chu et al. (2013) developed a conceptual trust model for cloud computing, including security, usability, reliability, auditability, interoperability, accountability and controllability with the aim to provide a basis for further (empirical) research. This thesis will contribute to the scientific body of knowledge by building upon existing conceptual trust models and literature researches with empirical research on the factors influencing trust in a cloud service.

To make sure the results of the diagnostic research, or more specifically opinion research, are generalizable, Q-method is used. Q-method is the combination of philosophy, concepts, data-gathering procedures, and statistical methods that provides a  thoroughly elaborated foundation for examining human subjectivity in a structured way (Brown, 2008). Additionally, the design will be done according to the theory of Johannesson & Perjons (2014) and in accordance with the principles of TIP (Bots & Daalen, 2012). A combination of the organisational configuration theory of Mintzberg (1989) and the empirical findings from the

Q-method will be used as input for the design. So, by basing all parts of the thesis on scientific theories and methods, the scientific value is secured.

### 1.4.2. Practical contribution

From interviews with practitioners in the field of cloud computing it becomes clear that there still is resistance from organisations to adopt cloud computing. Certainly, in the field of IT consultancy, where the consultancy company often advices organisations to adopt cloud computing and functions in the role of cloud broker, there is the perception that there is a lack of trust of their clients in cloud services. First, for a cloud broker it is valuable to get a better understanding on which factors are important for different organisations to trust a cloud service. This can help them in selecting the right cloud services to the right organisations. Besides, the design will help cloud brokers in addressing the right factor in the right way on the right moment. Key questions related to a certain factor and a certain part of the organisation will facilitate the cloud broker in improving the trust (see Chapter 6). Modelling the activities and decisions during a cloud adoption project and implementing the activity of improving trust there, provides cloud brokers with the knowledge on when to approach which part of the organisation.

## 1.5. Scope

This thesis will focus on the diagnosis and design steps of the *intervention cycle* as defined by Verschuren & Doorewaard (2010). Also to some extent the problem will be analysed, although this will not be the main contribution of this thesis. Intervention/change and evaluation will fall outside the scope of this thesis.

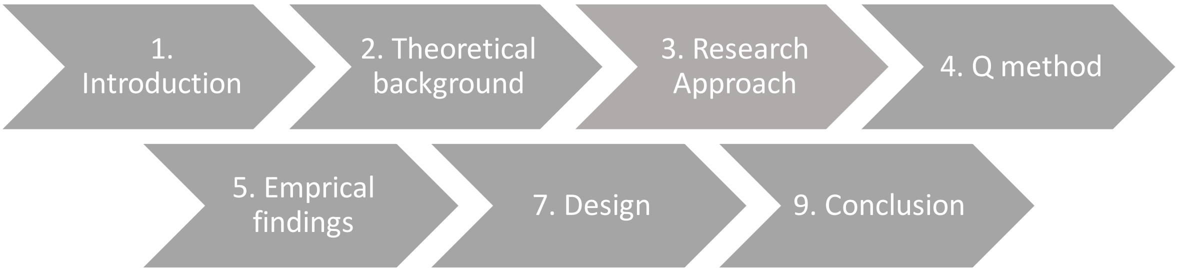
For the first part of the research, the diagnosis, several practitioners will be interviewed using the Q-method. The practitioners that are participating in this research fall within this scope:

1. Person has been involved in the assessment, migration or optimization of a cloud service
2. Person works in the technology, IT consultancy or retail sector
3. Person works for a large, private organisation
4. Person currently works in the Netherlands
5. Persons has either an IT or business role in the cloud project

Additionally, literature provides a lot of factors that potentially influence the trust in a cloud service. This thesis will not consider all of them, but only the ones that are most commonly found in the literature. These factors include: contracting, auditing, jurisdiction, interoperability, privacy, transparency, organisational change, financial costs, technological advantage, sustainability, security and reliability. All other potential factors fall outside the scope of this thesis. This means that factors related to the provider, such as reputation, brand, firm size, marketing, etcetera fall out of the scope of this research.

## 1.6. Thesis outline

The outline of the thesis will be as follows:



All chapters logically follow each other up, where conclusions from one chapter are used as a foundation for the next. For this reason, it is advised to read the chapters in the order as they are presented. The research itself is performed according to the structure as presented in the book of Verschuren & Doorewaard (2010) on *Designing a Research Project*. For readability purposes, it was chosen not to follow this structure for the thesis itself.

## 1.7. Readers guide

In order to keep this thesis readable, several terms will be shortened because they are used often. The following terms will be shortened:

*Table 1 Terms used in thesis*

| Complete term | Used in thesis |
|---|---|
| Public cloud | Cloud |
| Cloud computing service | Cloud service |
| Cloud service customer | Customer |
| Cloud service provider | Provider |

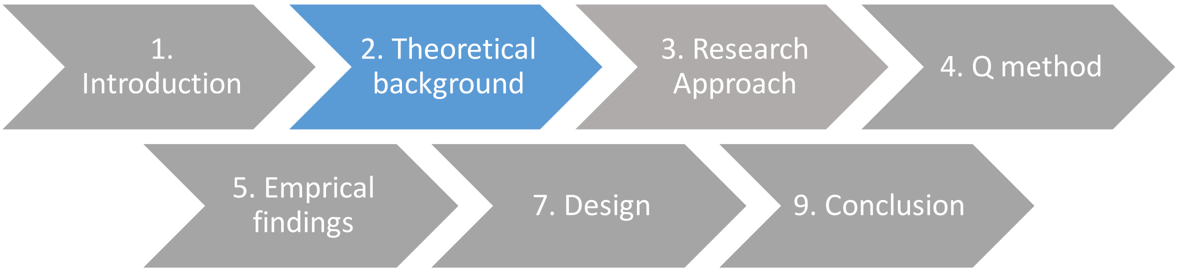
Note that the terms are not always shortened, because there may be cases where it is clearer to use the complete term. For example, in Chapter 2, the concept of cloud computing will be explained, so sometimes here terms will be used in full. After this chapter, the short version of the terms will be used.

# Chapter 2 Theoretical Background

In this chapter, the theoretical background will be elaborated upon. The theoretical background consists of the following:

- Cloud computing
- Trust
- Trust and Cloud
- Conceptual model
- Chapter conclusion

This chapter will serve as the theoretical foundation of this thesis. The scientific literature regarding cloud computing, trust and the combination of both concepts will be analysed and translated into a conceptual model. This conceptual model incorporates the factors that influence trust in a cloud service, according to the scientific literature. This model will be used as a guidance for the next chapters.



# 2. Theoretical background

## 2.1. Cloud computing

This section will discuss the general characteristics of cloud computing, cloud deployment models, cloud service models and the benefits and challenges of cloud computing.

### 2.1.1. General

To get a better understanding of cloud computing in general, it is relevant to look at the history of this concept. How did this concept grow into the multi-billion industry that it is now?

The rise of cloud computing finds it origin in the 1950's. Various users could access a central computer through simple terminals. The sole function of these terminals was to provide access to the mainframe. Buying and maintaining such a mainframe was expensive and thus it was not practical to have one mainframe for each employee, besides the fact that a typical user had no need for the large storage capacity and processing power a mainframe could provide. Hence, shared access to this single resource was the solution that was economically most profitable. (Neto, 2014)

The concept of the Virtual Machine (VM) took the shared access mainframe further into its development. Using virtualisation software, it was possible to run multiple operating systems at the same time in an isolated environment. This technology was one of the most important catalysts for cloud computing as we know it now.

With this development, telecommunication companies could leave their single dedicated point-to-point data connection offerings and switched to the new virtualised private network connections. This meant that instead of constructing more physical infrastructure to serve more users, the telecommunication companies were now able to provide shared access to the same physical infrastructure (Neto, 2014).

Other developments that facilitated the growth of cloud computing were the development of worldwide high-speed bandwidth and software interoperability standards. The timeline of the history of cloud computing can be found in Figure 2.

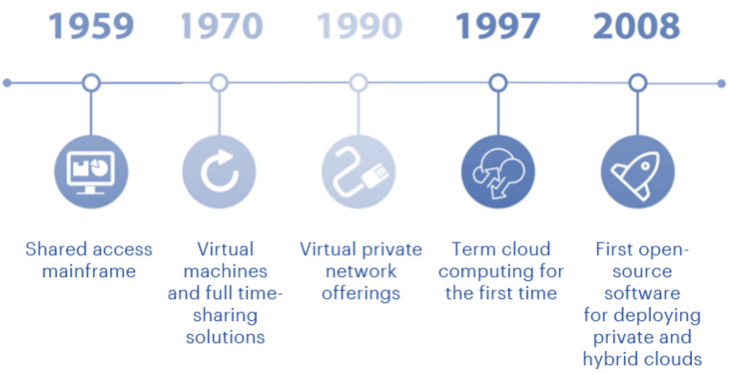

1959
1970
1990
1997
2008
Shared access mainframe
Virtual machines and full time-sharing solutions
Virtual private network offerings
Term cloud computing for the first time
First open-source software for deploying private and hybrid clouds

*Figure 2 History of Cloud Computing Timeline* (Kerridgecs, 2017)

In the scientific literature and in practice there are different definitions of cloud computing. The research of Leimeister et al. (2010) compiled definitions from a range of scientific articles and developed a definition that is supported by the vast majority of the literature:

> *"Cloud computing is an IT deployment model, based on virtualization, where resources, in terms of infrastructure, applications and data are deployed via the internet as a distributed service by one or several service providers. These services are scalable on demand and can be priced on a pay-per-use basis"* (Leimeister et al., 2010, pp. 4)

Compared to the traditional ways of providing computing resources, cloud computing includes three new aspects (Armbrust et al., 2010; Böhm, Leimeister, Riedl, & Krcmar, 2011):

1. Infinite computing capacity which is available on demand
2. No up-front costs related to IT resources for the cloud user
3. Short-term usage-based pricing

For the provision of computational resources to the users Virtual Machines (VM) are used. Virtualization technology is the enabling technology for cloud computing, making it possible for data centre providers to adjust their resources on demand and consequently utilise their hardware more efficiently (Leimeister et al., 2010). Virtualization refers to the creation of a virtual machine that acts as a real computer with an operating system, but of which the software is separated from the actual underlying hardware. This means several operating systems can run in parallel on a single CPU. This dramatically improves the efficiency and availability of resources of the data centres, since it is not relying on the old model of "one server, one application" which leads to underutilized resources.

### 2.1.2. Deployment models

In the literature, when the term cloud computing is used, it is often used to describe the public cloud. This thesis will also interpret cloud computing as public cloud (see Chapter 1.7). However, there are also other deployment models; private cloud and hybrid cloud. For the sake of completeness all three deployment models are shortly described here.

With public cloud, the infrastructure and computational resources are made available through the Internet by an external provider (Hsu, Ray, & Li-Hsieh, 2014). Consequently, customers don't need their own physical hardware, but instead buy the resources from the provider when necessary. This also indicates that maintenance and support for the IT is transferred from the customer to the provider. This automatically means the IT department of the customer will undergo a transition in their day-to-day tasks. Instead of managing the IT system, they now must take care of the technical and organisational connection to the provider (Javadi, Abawajy, & Buyya, 2012).

Private cloud is a deployment model where the computing environment is maintained exclusively for one organisation, and thus granting them greater control over their IT compared to the public cloud (Hsu et al., 2014). Consequently, the organisation still needs to have their own physical hardware. In private clouds organisations virtualize their IT, which leads to benefits like economies of scale, but without losing direct control of the IT infrastructure (Hofmann & Woods, 2010). Private clouds are small scale systems compared to public clouds and are usually managed by a single organisation (Javadi et al., 2012).

Hybrid clouds are the integration of services that are located on both public and private clouds. The idea of the hybrid cloud is for organisations to leverage the scalability and cost effectiveness of public clouds by only paying for the resources that they consume, while securing the levels of performance and control that are available in the private cloud (Javadi et al., 2012). The main issue of hybrid clouds is the integration of the private and public cloud (Javadi et al., 2012). The rise of new management technologies, such as cloud management platforms (CMPs), makes it possible to manage these complex environments using a single interface for provisioning and scaling (David, 2016).

So, the public cloud requires the organisation to give a lot of their control over IT to the provider, while the private cloud stays in the direct control of the organisation. This has large implications for the organisation and requires close cooperation with the provider. For this reason, public cloud is chosen as the deployment model for this research. So, when the term cloud computing or cloud service is mentioned, it refers the public cloud.

### 2.1.3. Service models

The different service models are presented in Figure 3. Each service model provides a different level of manageability and customization over the IT solution.

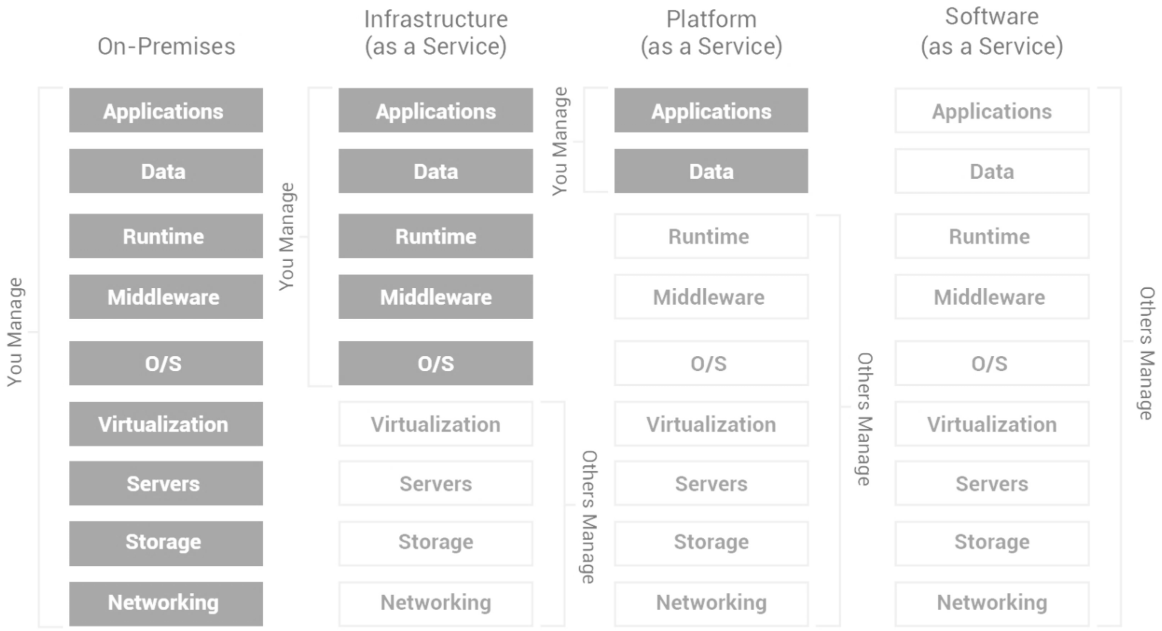


*Figure 3 Service Models for Cloud*

The service model where the organisation needs to manage everything themselves is the on-premise service model. Here all hardware and software are managed by the organisation itself. This means all the hardware is on-premise and all software runs on hardware that is located on-premise. When the servers are located on-premise, it automatically indicates that there is no public cloud involved. In the case when there is a virtualisation of the servers, one can speak of a private cloud. Without virtualization of the servers one can't speak of a cloud solution, but rather of a traditional IT solution. Business critical systems are mostly provided through the on-premise service model (Jamshidi, Ahmad, & Pahl, 2013). There are two reasons why these business-critical systems are provided through this service model: (1) the system consists of several legacy applications based on outdated information technology which makes it technically too hard to move them to the cloud, i.e. a lack of technological readiness (Oliveira et al, 2014) or (2) the transition to cloud computing implies too much risk and uncertainty combined with a lack of trust in the capabilities of the provider (e.g. Khajeh-hosseini et al., 2012; Oliveira et al., 2014; Venters & Whitley, 2012; Zissis & Lekkas, 2012).

The highest level of customization and management is offered by Infrastructure as a Service (IaaS). This service allows customers to architect the environment by configuring a virtual network, which is segmented from other networks and allow you to deploy compute, storage and other resources as you require (Keahey, Armstrong, Bresnahan, LaBissoniere, & Riteau, 2012). In addition, customers can configure the type of OS and applications that are needed. This service allows customers to take full advantage of the clouds automation, resiliency and other cloud infrastructure features. Although this offers the highest level of customization, the underlying infrastructure is still managed by the provider for maintenance purposes.

The main feature of IaaS is virtualisation, which can be defined as the ability to run different multiplexed operating systems on a single physical system that shares the underlying hardware resources (Abdelmaboud, Jawawi, Ghani, Elsafi, & Kitchenham, 2015).

Platform as a Service (PaaS) represents the service model that functions as the middle layer between IaaS and SaaS (Giessmann & Stanoevska-Slabeva, 2013). With PaaS, the underlying architecture, the host hardware, network components and the operation system are typically managed by the provider and taken care of from a maintenance and support perspective. This makes it a good deployment service for developers. Developers are then free to focus on developing new applications sitting on this platform.

Software as a Service (SaaS) allows for the delivery of an application that can be widely distributed and accessed. The application offered through SaaS is fully managed by the provider and can be accessed over the internet. There is no requirement to install any software on a local device to use it. They are often simple in their design and focus on ease-of-use to appeal a wide audience. This service model offers the least amount of customization. The capabilities of the customer in the technological domain are less important in the SaaS service model than in the IaaS and PaaS service models, as the provider gets more technological responsibility (Joha & Janssen, 2012).

So, the on-premise solution is not a form of public cloud, while IaaS, PaaS and SaaS are. As stated in the previous section, this thesis will focus on public cloud, thus for this reason the on-premise solution is not considered during the research. To get a better understanding of cloud computing in general, it is necessary take into account the IaaS, PaaS and SaaS service models together. So, no distinction between the service models will be made in this research.

### 2.1.4. Benefits and challenges

This section will address the benefits and challenges of cloud computing.

#### Benefits

Cloud computing (public cloud) has certain possible benefits for the customer, according to the scientific literature. Among these benefits are cost savings, scalability, decreased effort in managing technology, environmental benefits and ubiquitous network access (Khajeh-hosseini et al., 2012; Prasad & Green, 2015; C. Wang et al., 2013). There are more benefits of cloud computing, but these are the most common and relevant ones according to the literature.

Cost savings can be achieved because cloud computing works with a usage based pricing model. This means that the client only pays for the resources it uses. Before, organisations had to have server capacity equal to the maximum capacity to keep their services running all year through. This resulted in a lot of servers not being used throughout the rest of the year. These servers however, still required an initial capital investment and maintenance during its lifecycle. With cloud computing, the customer only pays for what they use. In other words, there is no server capacity leaved unused, which leads to less costs. Nevertheless, different services require different resources and deployment models. This means that the financial management process should define whether a certain service or resource can be deployed in the cloud more efficiently, and thus whether it really saves costs compared to the traditional model (Khajeh-hosseini et al., 2012; Mourad & Hussain, 2014).

Scalability is the ability to scale the server capacity up or down and is one of the most important drivers to move to the cloud (Jamshidi et al., 2013). When more capacity is needed, this can be manually or automatically scaled up to the amount that is necessary. The goal of cloud computing is to dynamically scale the resources with minimal interaction with the provider by using software API's depending on the customer's load (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2014). This scalability makes it possible for the cloud service customer to quickly respond to developments in the market and respond to *their* customer's needs. In this way, the cloud service customer can provide a higher quality of service to *their* customers.

When the responsibility over the IT resources is moved towards the provider, decreased effort in managing technology is needed from the customer's side. This means the customer doesn't need as much technological expertise resources anymore. However, instead of technical expertise, more expertise related to managing and coordinating the external relationships with the providers is necessary. Consequently, employees of the customer need to be re-educated, or replaced by more qualified persons.

As mentioned before, server capacity is used more efficient when organisations decide to move to the cloud. Instead of every organisation having its own servers, of which some are consuming energy but are not being used, the servers are centralized and used in a more efficient way. This means that less servers are consuming energy, which in turn is more sustainable. However, the datacentres where theses servers are centralized still consume large amounts of energy, leading to substantial $CO_2$ emissions. For example, in 2014, datacentres consumed 70 billion kWh of energy, which is equal to around 2% of the US total energy consumption (Zakarya & Gillam, 2017).

Lastly, cloud computing provides ubiquitous network access to the customer. Practically, there is no limit to the amount of computing power that the customer can consume.

In all those benefits, two major trends currently present in information technology can be found: (1) IT efficiency and (2) business agility (Breivold, 2015; Marston et al., 2014). Cloud computing can offer IT efficiency, *"whereby the power of modern computers is utilized more efficiently through highly scalable hardware and software resources"* (Marston et al., 2014, pp. 177). Furthermore, cloud computing provides opportunities for business agility *"whereby IT can be used as a competitive tool through rapid deployment, parallel batch processing, use of compute-intensive business analytics and mobile interactive applications that respond in real time to user requirements"* (Marston et al., 2014, pp. 177).

### Challenges

Although cloud computing has the potential to offer a lot of benefits, still a lot of ambiguity and uncertainty exist with respect to the actual realization of them (Khajeh-hosseini et al., 2012). There are several challenges organisations will have to face in order to move to the cloud, such as security, privacy, lock-in and interoperability, lack of standards, organisational change and return on investment (Oliveira et al., 2014; Radwan, Azer, & Abdelbaki, 2017; Yongsiriwit, 2016).

Security and privacy are still two of the most mentioned challenges of cloud computing (Müller, Ludwig, & Franczyk, 2017). When all the IT resources are on premise, the organisation has direct control over its security and privacy measures. When going to the cloud, the applications and data of the organisation are send to datacentres of often large providers. With a lot of sensitive information of a lot of different customers in those clouds, it is argued that these providers are a very desired target for hackers. Moreover, since the applications and data are now running and stored at the servers of the provider, it is easier for this provider to gain access to private information, resulting in privacy concerns. On the other hand, large organisations such as Amazon or Google, often have more expertise and resources for putting the right security and privacy measures in place than organisations that are smaller and/or don't have IT as their expertise.

Another challenge of cloud computing is related to interoperability. When an organisation makes the decision to move a certain service into the cloud, certain procedures, languages and rules need to be followed. This means that, when the customer wants to change the provider for this service, it needs to transform everything into the new procedures, languages and rules. Often this will result in projects that cost a lot of time and money. Moreover, this can also occur between the legacy system of the customer and the new cloud solution. Problems with interoperability are mainly caused by a lack of standard interfaces and API's, open standards for VM formats, service deployment interfaces and open formats for data interchange (Opara-Martins, Sahandi, & Tian, 2015).

Additionally, as mentioned previously, cost savings are a possible benefit of cloud computing. Nevertheless, with the new pay-as-you-go payment model, it is unclear upfront how much resources will be used and thus how much money it is going to cost. Because the whole model changes from capital expenditure (capex) to operational expenditure (opex) it is a challenge to predict the return on investment, or even if there will be a positive return on investment. A lot of the benefits of cloud computing are not easily made explicit in monetary value. This makes it even harder to say something about the return on investment.

Lastly, there is the challenge of trust. Although an accelerated adoption of cloud computing in the industry can be observed, trust management still proves to be one of the key challenges in the adoption of cloud computing (Armbrust et al., 2010; Noor et al., 2013). While cloud services reduce the responsibility of the customer in terms of hardware and software management, it is likely that critical information and applications are moved outside the direct control of the customer (Uusitalo et al., 2010). Also, with the market growing at an increasing pace, reliably identifying a trustworthy provider becomes harder (Habib et al., 2010, 2014). The concept of trust and how it is of importance for cloud computing will be further elaborated upon in the next sections of this chapter.

#### Perspectives

So, according to the literature there is a wide variety of both benefits and challenges. Those benefits and challenges are mainly found through theoretical studies and still a lot of ambiguity about the realization of the benefits and the impact of the challenges exists. Moreover, there are even aspects of cloud computing that are considered both a challenge and a benefit. One of those aspects is for example security, as stated earlier. This indicates that there are several perspectives on different aspects of cloud computing. Yet, for some aspects, such as security, these perspectives are specified. For other aspects, such as trust, this remains unknown in the scientific literature.

## 2.2. Trust

Trust is extensively covered in the scientific literature. The concept is used in different disciplines such as economics, psychology and sociology (Rousseau et al., 1998). Trust is seen as either calculative or institutional by economists, seen in accordance with personal attributes by psychologists and seen in the perspective of socially embedded properties of relationships by sociologists (Rousseau et al., 1998). These different viewpoints make it that there is no common understanding of trust. This section will elaborate on the definition and interpretation of trust, and how it will be used in this thesis.

### 2.2.1. Definition

There are many different definitions of trust, differing from discipline to discipline. The research of Blomqvist (1997) searched for the definition of trust in the disciplines of social psychology, philosophy, economics, contract law and marketing. This research concluded that it is not possible to construct a universal definition of trust, but rather constructed a working definition for business contexts. Here, trust is defined as:

> *"An actor's expectation of the other party's competence and goodwill"* (Blomqvist, 1997, pp. 283)

Besides this working definition for the business context, Blomqvist (1997) also found some general aspects that hold up for all disciplines:

- *Uncertainty and vulnerability* are necessary conditions for the existence of trust;
- Trust is always perceived in the eyes of the beholder, who makes a *subjective assessment* of the other party;
- Development of trust relationships occurs gradually and is the *outcome of a process*;
- Trust is a property of *collective units* rather than isolated individuals; thus, the focus should be on the relationship rather than the individual.

Since this definition is still very broad and general, the interpretation of trust for this thesis will be elaborated upon in the next section.

### 2.2.2. Interpretation of trust

There are a lot of aspects related to trust. These aspects can be interpreted in different ways for different purposes. How this thesis will interpret trust will be discussed here.

Part of the scientific psychology literature views trust as 'either/or', where one actor completely trusts or distrusts another actor, with the Prisoner's Dilemma game as one of the examples (Rousseau et al., 1998). However, there is enough comparative and historical evidence that suggests that trust changes over time; developing, building and declining of trust relationships (Rousseau et al., 1998). Thus, in this thesis trust between different actors is treated as a dynamic concept which can increase and decrease over time.

When taking the example of the Prisoner's Dilemma again, it can be argued that trust can be interpreted as a cause. When there is high trust between the two actors involved, it is likely they will cooperate and reach economic gains. In this case trust is conceptualized as the independent variable that influences the decision-making process. Moreover, Transaction Cost Economics (Williamson, 1981), describes that trust reduces opportunism between two transacting actors. On the other side, trust can be interpreted as the result of different factors. There are all kind of reasons why actors trust or distrust one another. This thesis will approach trust from this perspective, by trying to define which factors influence the trust in a cloud service.

In a buyer-seller relationship both interorganisational trust and interpersonal trust can influence the purchasing choice of the buyer (Doney & Cannon, 1997). Interorganisational trust is the trust in the seller-organisations, where interpersonal trust is the trust in the seller-salesperson. Most organisations are handled and managed by individual *boundary spanners*, individuals that are closely involved in the interorganisational relationship and interact with their counterpart at the other organisation to a great extent (Zaheer, McEvily, & Perrone, 1998). But, this is typically not the case for cloud services. Cloud services can be acquired through the internet, without any necessary intervention of a salesperson. Although, when a cloud broker or consultant is involved, interpersonal relationships exist with those actors. For this thesis, it is chosen not to study the social and relational characteristics of the provider of a cloud service, which can be either the cloud service provider, the broker or the consultant.

Instead it is chosen to study the technological and organisational aspects that may influence the trust of customers in a cloud service.

As mentioned earlier, trust develops gradually. Because of this, it can be divided into different stages: calculus-based trust, knowledge-based trust and identification-based trust (Lewicki & Bunker, 1996). With calculus-based trust, trust is gained by weighing the benefits of trust against the costs of violating this trust. Knowledge-based trust derives its trust from the history of interaction, which makes it possible to predict the other's behaviour. In identification-based trust the understanding of the desires and intentions of the other party plays an important role, where shared values help the process of trust development. This thesis will treat trust as calculus-based trust. Since organisations deciding on whether they should adopt cloud are in an early stage of the relationship with the provider, there is no history of interaction or a clear view on the desires and intentions of the provider.

Now, the definition of trust of Blomqvist (1997) can be adapted to represent how trust will be used in this thesis. For this thesis, trust can be defined as:

*An **organisation**'s **dynamic, calculated and dependent** expectation of the other **organisation**'s competence and goodwill*

### 2.2.3. Importance of trust

Now that it is clear what trust is, the next step is to identify why it is of importance for organisations. In general, trust is critical for partnership formation and to future successes of cooperation (Blomqvist, 1997). Earlier organisational trust studies have showed that trust is closely related to relationships and is crucial for sustaining one (Lewicki & Bunker, 1996; Qi & Chau, 2013). Also, trust is one of the key success factors in outsourced information systems (Qi & Chau, 2013). Several closely related aspects play an important role for making trust such an important aspect in relationships.

First, trust functions as a control mechanism. Instead of constructing detailed contracts and safeguarding devices, organisations have the option to trust each other. In this scenario, trust is used to have control over the outcome of the relationship. Second, trust is a reduction mechanism for transaction costs and uncertainty. As stated, no extensive contracting or safeguarding is required when there is sufficient trust between two parties. This means less resources are used for reducing opportunistic behaviour and uncertainty and thus reducing the transaction costs as such. In Chapter 2.3.1 the relevance of transaction costs will be elaborated upon more extensively. Lastly, trust leads to effective and ongoing collaboration, since it promotes ongoing interaction and directs firms into investing in the collaboration (Rousseau et al., 1998).

## 2.3. Cloud computing and trust

This section will combine the concepts of cloud computing and trust. With Transaction Cost Economics (TCE) the relevance of trust in a cloud service is explained. Also, prior work on trust in cloud computing will be discussed.

### 2.3.1. TCE, cloud computing and trust

Transaction Cost Economics (TCE) explains several decisions, which not only include buying and selling, but also day-to-day informal interactions. The choice to trust a cloud service can also be placed under these decisions. TCE provides a good basis in trying to predict the organisational implications of trusting and adopting a cloud service (Ross & Blumenstein, 2013).

Because of the ubiquitous nature of cloud services, the ability of organisations to gain competitive advantage by accessing new IT technologies is limited. Instead, the extent to how organisations plan and coordinate these cloud services into the overall business processes and outcomes can provide an advantage (Ross & Blumenstein, 2013). Trust can help in this regard by arguing that *"[…] trust's role in constraining opportunistic behaviour allows parties to adopt less elaborate safeguards, thereby economizing on transaction costs and, in turn, altering the choice of governance structure. In other words, the introduction of trust in the TCE model can alter the efficient boundaries of the firm"* (Chiles & McMackin, 1996, pp. 88)

According to Williamson (1981) there are five determinants of transaction costs: opportunism, frequency, asset specificity, uncertainty and bounded rationality. The relation of these determinants with the concept of trust in cloud services will now be discussed.

Opportunism can arise when, for example incomplete contracts exist (Yigitbasioglu, 2014). However, following the logic of TCE, contracts are always incomplete. This is because the transaction costs will be too high if all possible contingencies need to be specified in a contract, especially when high uncertainty exists. This means some form of trust between the two exchange partners need to exist. With legislation and SLA's not able to cover all possible contingencies possible when adopting a cloud service, there needs to be some form of trust between the customer and provider.

Asset specificity is the concept where an investment is done into a particular transaction which is not redeployable for another transaction. When an organisation moves their IT resources to the cloud, certain standards and procedures specific to the provider need to be adopted as well. This means that switching from one provider to another brings high transaction costs with it, which is also known as a vendor lock-in. So, in order to make this move, the organisation needs to be sure that the transaction costs are lower than the total profit. However, since there is no way of being sure, a certain degree of trust is required

A complex transaction with high degree of uncertainty will introduce an increasing number of contingencies. The more contingencies occur, the more difficult and costly to construct and enforce the contracts and thus the higher the transaction costs. In cloud services, many uncertainties exist, and trust can be a means to address this (Uusitalo et al., 2010). Uncertainty in cloud services exist of, for example, uncertainty on how providers ensure the security, privacy, integrity and confidentiality of the cloud service (Yigitbasioglu, Mackenzie, & Low, 2013).

When the rationality of an individual is limited by the cognitive limitations of their minds and the time available for making a decision, one can speak of bounded rationality. When making a decision about whether to adopt cloud computing, there are many aspects to consider, including the impacts of the decisions, which are normally very significant (H. Wang, 2016). This means that the rational to adopt a certain cloud service is always bounded, meaning that the rational that falls outside the bounds has to be trusted upon. Furthermore, bounded rationality also comes in play when drafting contracts. Because the rationality of both parties is bounded, it is not possible to include all possible contingencies into the contract, thus incomplete contracts occur (Chiles & McMackin, 1996).

Lastly, the greater the volumes of trade, the more likely the benefits of hierarchical governance exceed the costs. In other words, the higher the frequency, the higher the benefits when the transaction is performed within the company. This determinant does not have a direct link with trust and therefore is of no interest for this thesis.

### 2.3.2. Prior work

Both cloud computing and trust separately receive a lot of attention in the scientific literature. However, the both concepts combined aren't as commonly found. A closer look will be taken at the literature on the combination of these topics.

Uusitalo et al. (2010) did a literature study of trust and cloud services. The research concludes that the most important factors affecting perceived trust was brand, including aspects as reputation, image, history and name. Moreover, security, privacy, reliability and transparency were also found to be important factors. The research of Noor et al. (2013) focusses on the obstacles and solutions of trust management of services in cloud environments. Also, 30 trust management research prototypes found within the scientific literature are evaluated. All the prototypes evaluated are mainly focussed on technical and quantitative solutions. Lansing & Sunyaev (2016) developed a conceptual model that describes trust in cloud services. This conceptual model was evaluated based on scientific literature and functions as encouragement and foundation for other scholars to explore trust in cloud services. The main proposition of this article is that research on trust in cloud services needs to consider both the trust in the provider, as well as the trust in the cloud service artifact. Also, Chu et al. (2013) put effort in developing a conceptual trust model. This conceptual model contains several trust factors influencing the adoption of cloud-based interorganisational systems. However, this model is not validated and hence further research is required. Eldred, Adams, & Good (2015) focussed their research on the trust challenges in a high-performance cloud computing project, specific to the petrochemical industry. The research showed that politics, driven by trust, within an organisation have serious implications for the adoption of cloud computing. The research concluded that:

> *"[…] the evaluation and adoption of HPCC projects, with their considerable change to business practices, will likely involve more than technical performance and business improvements: it will also need to consider the wider political cloud and fault-lines of issues that would impact the acceptance from various stakeholders"(Eldred et al., 2015. pp. 1050)*

Chen & Nakayama (2016) researched the key factors that increase trust and the intention to adopt standard cloud-based applications, such as Google Docs. This research only includes SaaS, and is performed on students. Rahi, Bisui, & Misra (2017) took the Semiconductor sector in India as the scope for their research on the moderating effect of trust on the adoption of cloud-based services, while using the TOE framework. This study looks at trust as the moderating factor for technology, organisation and environment related success factors. In other words, a trust as a cause, rather than an effect.  Finally, there are several mathematical trust models, where trust is calculated and seen as a quantifiable concept. This approach is taken by amongst others Manuel (2015), Habib et al. (2014) and Firdhous et al. (2011).

So, this literature study shows that there is no empirical research on the factors influencing trust in a cloud service. Moreover, there is no scientifically based design that aims to improve trust in a cloud service.

## 2.4. Conceptual framework

Now that it is clear what cloud computing is, what trust is, how trust is relevant for cloud computing and what research is already done on this topic, it is time to start working towards the empirical research of this thesis. In order to research the factors influencing trust in a cloud service, it is of importance to develop a conceptual model.

A conceptual model is an important tool for the theoretical underpinning of the research. The conceptual model includes a set of assumed relationships between the concepts that are being researched. The purpose of a conceptual model is to: (1) demarcate the research subject and (2) to formulate the assumed relationships between the concepts clearly and to link the research to the existing literature.

The conceptual model will be constructed based on the design theory of (Verschuren & Doorewaard, 2010). The following steps will be taken:

- Determine the dependent variable Y that needs a causal explanation or needs improvement
- Determine which core concepts are the independent variables
- Carry out a literature study to determine the variables there are within each of the core concepts and select which variables are within the scope of the research and which are not
- Formulate the assumed causal relationships between the variables

The problem statement for this thesis describes that: *Cloud computing has the potential to provide various benefits to organisations, but the lack of trust is still a key challenge that prevents the adoption of it. Knowledge on the perspectives on trust in a cloud service and the factors influencing the trust, is missing, as well as a design to improve this trust.* This means that the *trust in cloud services* is the dependent variable here.

### 2.4.1. Core concepts

From the problem definition, several core concepts are derived as being the independent variables influencing trust in a cloud service.

- Compliance
- Control
- Costs

- Benefits
- Capability

Compliance refers to complying to the formal institutions that must be considered when adopting cloud computing. This includes international and national legislation, but also the contract with other organisations need to be considered. Deploying applications in datacentres of another organisation, possibly in another jurisdiction, has implications for the compliance of the customer. Also, there is the question of who the owner of the data is: the customer or the provider? Thus, uncertainty about whether or not the organisation complies to all relevant institutions when cloud computing is adopted may have an influence on the trust in cloud services.

Control refers to the power to influence or direct the course of events. When adopting a cloud service, the customer loses control over the hardware and, in the case of SaaS, software. This means that the customer has no power to influence the course of events related to those resources, but is dependent on the provider for this. So, when a cloud services requires a customer to give up a lot of its control, it is harder to trust because it requires more competence of the provider. For example, when giving up control over a small, simple task, it is easier to trust somebody else with it than it is when you need to give up control over a large, complex task. Thus, the more control a customer loses, the less it will trust a cloud service.

Costs are related to the costs of change. Changing a part of the organisation always comes with certain costs. Adopting cloud computing will require some initial resources that need to be invested before benefits can be gained. Although there is no upfront capital expenditure with cloud computing, the actual assessment, preparation and migration of data and applications and finally the operationalisation and optimization of the cloud service will require some dedicated resources. With calculus-based trust, trust is gained by weighing the benefits of trust against the costs of violating this trust (Lewicki & Bunker, 1996). When adopting a cloud services brings large costs with it, the cost of violating the trust will also be high, because a lot of resources were already dedicated to the project.

Benefits refer to the benefits that can be gained from adopting a cloud service. Amongst these benefits are scalability, decreased effort in managing technology, environmental benefits and ubiquitous network access. As the benefits increase, it becomes more valuable to have trust in the cloud service, according to the concept of calculus-based trust. So, as benefits increase, trust may also increase.

Capability relates to the actual ability of the service to perform. One of the most important reasons to adopt cloud computing is because it provides the organisations with more capabilities. Cloud computing can be used as a strategic means to reach certain business objectives. Moreover, the providers are specialised in IT, while the customer might have no expertise within this field at all. This makes the provider more capable in operating and maintaining the IT resources.

### 2.4.2. Potential factors influencing trust

A literature analysis has been done to define several potential factors influencing trust (i.e. independent variables for the conceptual model). These are represented in Table 2 and will be further elaborated upon in this section. More independent variables could be chosen that would also fit the core concepts. However, based on what was most commonly found, it was decided to scope the research around the independent variables as presented in Table 2.

*Table 2 Core concept and independent variable of trust in a cloud service*

| Core concept | Independent variable |
|---|---|
| Compliance | Contracting |
| | Auditing |
| | Jurisdiction |
| Control | Interoperability |
| | Privacy |
| | Transparency |
| Costs | Organisational change |
| | Financial costs |
| Benefits | Technological advantage |
| | Sustainability |
| Capability | Security |
| | Reliability |

#### Contracting

Contracts will set terms and conditions for the relationship between the customer and the provider. In the case of cloud computing, contracts are often in the form of Service Level Agreements (SLA's). SLA's can be defined as the explicit statement of obligations and expectations that exist in the business relationship between a service customer and a service provider (Wu & Buyya, 2010). SLA's typically consist of the following components (Wu & Buyya, 2010):

- Purpose: the objectives of the SLA
- Restrictions: the required actions that need to be taken to reach requested level of service.
- Validity period: the working time period of the SLA.
- Scope: the services that will be delivered to the customer, and services that will not be delivired to the customer
- Parties: all organizations and individuals that are involved and their roles (e.g. provider and consumer).
- Service-level objectives (SLO): levels of services which both parties agree on, such as availability, performance, and reliability.
- Penalties: penalties will occur when the delivered service does not achieve the SLO's
- Optional services: services that are not obligatory but might be required.
- Administration: the organisational responsibilities for the processes that are used to guarantee the achievement of SLO's.

When these components are put on paper, it provides both parties a legal mechanism to punish opportunistic behaviour. It is clear what is expected from the provider, and when they do not fulfill these expectations it is clear what the penalties will be. Violation of the contract however, will undeniably decrease the trust in the other party (Hani, Paputungan, & Hassan, 2015). Good contract management is a way of ensuring high levels of trust between a customer and a provider (Hani et al., 2015). Hence, contracting, when done adequately, has a positive effect on trust in a cloud service. Thus, the following hypothesis can be defined:

*A1. There is a positive effect of 'contracting' on 'trust in cloud service'*

### Auditing

Auditing is the process of the systematic examination of books, accounts, statutory records, documents and vouchers of an organization to ensure how far the financial and non-financial statements present a true and fair view of the reality. Auditing has the potential to ensure data integrity and secure the customers' computation resources. A third-party auditor (TPA), who has expertise and capabilities the customer lacks, is and independent party that performs this task of auditing. The TPA checks the integrity of all data on behalf of the user. This provides the user with an easier and affordable way of ensuring that they receive the cloud service they require (C. Wang et al., 2013).

Auditing provides the customer with the certainty that the provider conforms to certain standards and regulations. This makes the cloud service in itself more trustworthy. So having a fair and unprejudiced auditing process, together with the preservation of the customers computational resources, can lead to a higher standard for trust in the cloud services (Razaque & Rizvi, 2017). Thus, the following hypothesis can be defined:

*A2. There is a positive effect of 'auditing' on 'trust in cloud service'*

### Jurisdiction

In certain jurisdictions, governments can be intrusive under the local law or under accepted local practices. Providers may be required to disclose information to their own governments, as for example can be enforced through the Patriot Act in the United States (Yigitbasioglu, 2014). The disclosure of this information is then outside the control of the customer; however, they are still hold responsible for its privacy. The disclosure of private information, for which the customer is responsible, can be in conflict with the legislation in their own jurisdiction. This can result in large fines and severe reputational setback (Yigitbasioglu, 2014).

So, when data and applications are moved to the cloud, there is the chance that they are stored and ran on servers outside of the country where the customer is located. Since the legislation related to (private) data storage differs from jurisdiction to jurisdiction, more uncertainty about whether the customer complies to the legislation will arise when data and applications reside in another jurisdiction. Thus, the following hypothesis can be defined:

*A3. There is a negative effect of 'use of datacentres in intrusive jurisdiction' on 'trust in cloud service'*

### Interoperability

Interoperability is the ability of an IT system to exchange information with other IT systems and use this information (Yongsiriwit, 2016). For cloud services specifically, this means that a customer must have the ability to switch their cloud resources from one provider to another, the ability to use multiple providers that are communicating with each other and the ability to use the public cloud together with a private cloud. However, vendor lock-in is seen as one of the biggest barriers for cloud adoption (Opara-Martins et al., 2015). Vendor lock-in refers to the problem where customers are dependent on a single provider and there is no easy way of moving to another provider, without high costs, legal issues or technical incompatibilities (Opara-Martins et al., 2015). This vendor lock-in is a result of the differences between the individual providers, offering services with non-compatible underlying technologies and standards (Opara-Martins et al., 2015).

Already many cloud resource management standards have been developed to tackle this issue (Yongsiriwit, 2016). These standards are developed by separate companies. Consequently, these standards may not be simply interoperable because of their heterogeneous schema and vocabulary (Yongsiriwit, 2016).

So, when an organisation decides to adopt a cloud service from a specific provider, it will need to conform to the IT standards and procedures of that specific cloud service. However, when trust is violated, the customer might decide it wants to switch of provider. When the interoperability of the cloud services are high, costs related to this change are relatively lower, meaning that the costs related to the violation of trust are also relatively low. Thus, the following hypothesis can be defined:

*B1. There is a positive effect of 'interoperability' on 'trust in cloud service'*

### Privacy

There is not one general definition for privacy. However, it is known that the concept of privacy encompasses, among other things, freedom of thought, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches (Solove & Washington, 2008). When organisations adopt cloud computing, private data is stored on servers that are not under the physical possession of the organisation itself. Hence, the concepts as stated above can easily been harmed. The provider faces threats with respect to outages and security breaches, possibly putting the privacy of the data at risk (C. Wang et al., 2013). Moreover, providers might have reasons to behave unfaithfully towards the stored data, such as erasing data that is not or barely accessed for financial reasons or hide data loss incidents to maintain their reputation (C. Wang et al., 2013). Also, the data that is deployed on the servers of the provider can give the provider a competitive advantage when they access them.

To protect privacy in the cloud, several laws and regulations exist. For the EU, the protection of data as a fundamental right is defined in the provisions of Article 8 of the EU Charter, titled "Protection of personal data" (Katulic & Vojkovic, 2016, pp. 1447):

1. *"Everyone has the right to the protection of personal data concerning him or her.*

2. *Such data must be processed fairly for the specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access to data which has been collected concerning him or her, and the right to have it rectified. "*
3. *Compliance with these rules shall be subject to control by an independent authority."*

Through this directive, the data protection standards prohibit that personal data is transferred to countries that do not comply with the EU standards of data protection (Katulic & Vojkovic, 2016). In order to allow the export of European personal data to the US, a framework of cooperation between the US and the EU concerning the collection, storing, analysis and use of European citizens personal data under certain conditions was developed (Katulic & Vojkovic, 2016). However, recent cases of illegal access and interception of personal data shows that the current legal frameworks are somewhat outdated (Katulic & Vojkovic, 2016). Hence, while legislation gives some form of protection against the violation of privacy of the data, storing data in the cloud still includes a risk.

When private sensitive data is stored in the cloud, the customer requires some kind of privacy over this data. Since the data can contain valuable information about the organisation itself or their clients, privacy is an important requirement. When the provider is able to offer privacy, the data can only be accessed by the people that are supossed to. Having the right privacy measures will ensure that even the provider can't freely read the data that they store. This gives the customer the expectation of the competence and goodwill with respect to the privacy of their data. Thus, the following hypothesis can be defined:

*B2. There is a positive effect of 'privacy' on 'trust in cloud service'*

### Accountability

Accountability can be defined as "*the obligation and/or willingness to demonstrate and take responsibility for the performance in light of the agreed-upon expectations* (Chu et al., 2013, pp. 2).". Accountability can be achieved through public and private accountability: public accountability is derived from the interaction between providers and regulatory bodies, while private accountability is derived from the interaction between providers and customers (Pearson & Charlesworth, 2009). Private accountability is premised on contract law, technological processes and practical internal compliance requirements (Pearson & Charlesworth, 2009). The objective of accountability is to reduce the risk of disproportionate harm to the customer, which will lead to a higher level of trust in the provider (Ko, Lee, & Pearson, 2011; Pearson & Charlesworth, 2009). Thus, the following hypothesis can be defined:

*B2. There is a positive effect of 'accountability on 'trust in cloud service'*

### Transparency

When customers move to the cloud, their applications and data are deployed on servers of the provider. Because of the distributed and non-transparent nature of cloud computing, customers feel that they lose control over the data and on how to access it (Habib et al., 2014). Transparency is required for obtaining information about other factors influencing trust, as for example privacy and security. For the customer to make a good assessment on the security and privacy of a cloud service it needs to have access to information on these matters. When the provider is not transparent about these things, it's hard for the customer to evaluate the competence and goodwill of the provider.

Moreover , cloud computing provides the opportunity to pay-as-you-go. This means that the customer only pays for what it uses. Consequently, it is of great importance to know what resources are used for what purpose. If the customer only receives a bill at the end of the month, it is unclear how the provider came to this amount. When the provider is able to substantiate all expenses and elaborate on the usage of the customer, the customer can check this with their own numbers. When the numbers add up, it shows the provider provides the right service for the right price.

So, when the provider is transparent about its service, it's possible for the customer to evaluate the competence and goodwill of the provider, hence also to form expectations of it: trust it or not. Thus, the following hypothesis can be defined:

*B4. There is a positive effect of 'transparency' on 'trust in cloud service'*

### Organisational change

When adopting cloud computing, serious changes in the organisation need to be considered. This doesn't only apply to the IT department, but also to other parts of the organisation. There will be changes for enterprise IT, business unit IT, business unit operations and business unit management (Rajendran, 2013). This means also the way people do their day-to-day tasks changes. When more computing power is required, employees may need to manually set up and activate the servers themselves (although there are technical means that can automate this process). There are examples where employees afterwards forgot to scale down their computing capacity which led to huge amounts of unnecessary costs. When a cloud service requires a lot of organisational change, the costs related to a potential violiation of the trust is high, in terms of time, effort and money. A cloud service tends to be trusted easier when the need for organisational change is limited. Thus, the following hypothesis can be defined:

*C1. There is a negative effect of 'organisational change' on 'trust in cloud service'*

### Financial costs

Financial costs refer to the actual money that it will cost the organisation to adopt cloud computing. A lot of costs are hidden and not directly visible for the organisation. If adopting cloud computing comes with too much costs, it is likely that the organisation won't trust that the cloud service will be beneficial for them. As earlier mentioned, calculus-based trust is gained by weighing the benefits of trust against the costs of violating this trust (Lewicki & Bunker, 1996). When trust is violated, and the customer wants to pull out of the agreement, the money that was invested into this particular cloud service will disappear into thin air. Meaning that, if the customer needs to put a lot of money into migrating and operating the cloud, trust will be less. Thus, the following hypothesis can be defined:

*C2. There is a negative effect of 'financial costs' on 'trust in cloud service'*

### Technological advantage

The technological advantages are related to the technological benefits, as stated in Chapter 2.1.1, that can be gained from adopting cloud computing. This includes amongst others:

scalability, ubiquitous network access and remote access to resources. For example, a retail company with high peak in demand during Christmas may have a considerable technological advantage from a cloud service with good scalability performances.

When there are clear technological advantages to be gained from adopting cloud computing, an organisation has more benefit from trusting a cloud service. This is in line with the principle of calculus-based trust, where trust is gained by weighing the benefits of trust against the costs of violating this trust (Lewicki & Bunker, 1996). So, by getting a clear technological advantage from adopting cloud computing, one side of that equation increases: the benefits. In other words, trust is gained more easily. Thus, the following hypothesis can be defined:

*D1. There is a positive effect of 'competitive advantage' on 'trust in cloud service'*

### Sustainability

In 2015, across the whole world almost 416.2 terawatt hours of energy was consumed by datacenters which is higher that the total consumption of the United Kingdom (Zakarya & Gillam, 2017). This shows energy consumption and sustainbility, also in the sector of cloud computing, are important factors to take into consideration.

Besides that sustainability serves a public goal, it can also serve a more strategic goal. Sustainability can improve the image and brand of the company. Since data centres use a large amount of energy, selecting a sustainable cloud service can have a positive impact on the environment, but maybe even more on the public opinion. This benefit gives an organisation an incentive to trust a sustainable provider. Thus, the following hypothesis can be defined:

*D2. There is a positive effect of 'sustainability' on 'trust in cloud service'*

### Security

In traditional IT architectures, security policies address constraints on functions and flow among them and constraints on access by external systems, programs or people (Zissis & Lekkas, 2012). In the cloud, the control over security is delegated to the provider owning the IT infrastructure. This means that the provider must enforce the security policies that would normally be done by the customer itself.

Security in general consists of three pillars: confidentiality, integrity and availability. Cloud computing proposes certain challenges for each of these aspects. In short, confidentiality can be defined as the characteristic where only the authorized parties or systems have the ability to access protected data (Zissis & Lekkas, 2012). The threat of a breach in the confidentiality of the system increases in the cloud, because more parties, devices and applications are involved, hence leading to more points of access. Moreover, transferring the control of the data to the provider increases the threat of compromised data. Integrity refers to protecting assets, which include data, software and hardware, from being modified by unauthorized parties or in unauthorized ways. By doing this, higher confidence in the data can be achieved because it ensures that valuable data and services are not abused or stolen (Zissis & Lekkas, 2012). Availability means that the system is accessible and usable on demand by authorized entities. This includes that the system should be able to perform operations even when some authorities misbehave or when there is the possibility of a security breach (Zissis & Lekkas, 2012).

Cloud computing on itself, already provides certain security benefits due to its architecture and characteristics, such as centralization of security, redundancy, high availability and data and process segmentation. However, additional measures, such as authentication, authorisation, encryption and segregation of data, are needed to prevent the compromising of confidentiality, integrity and availability. In order for cloud computing to be an effective and secure technology solution, the security should be guided by the ISO 7438-2 standard (Radwan et al., 2017).

Since the control over security is being transferred partially to the provider, a certain degree of trust is needed to adopt a certain cloud service. Complete assurance with respect to the security is not possible, and hence the customer must trust in the capabilities of the provider to secure its resources. The other way around, when there is a clear indication of good security measures taken by the provider, it is more likely that the customer will trust the cloud service. Thus, the following hypothesis can be defined.

*E1. There is a positive effect of 'security' on 'trust in cloud service'*

### Reliability

Reliability refers to the ability of a system to perform its required functions for a specified period of time, under certain conditions (Manuel, 2015). Cloud computing has the potential to increase the reliability of the IT system, because the provider develops expertise in managing, running and maintaining the IT resources (Yigitbasioglu et al., 2013). Thus, reliability is put forward as one of the key selling points for cloud computing. However, outages are still recorded, as for example the outage of Amazon Web Service, where certain cloud services in the Northern Virginia Region were unavailable for several hours (Amazon, 2017). When mission critical applications are being operated in the cloud, this can lead to large (financial) problems for organisations.

Additionally, the geographic location of the servers where applications and data are stored has certain implications for the cloud service as such. First, the further away the datacentre is located the higher the latency (Paraiso, Merle, & Seinturier, 2016). Second, characteristics of the geographic locations, such as having a high probability/occurrence of high-impact environmental risks (e.g. floods, tornadoes, earthquakes, hurricanes) or low technical maturity in the infrastructure (e.g. power grid, type of fibre) can hamper the continuity of the cloud service.

Providers inform their customers on their reliability by providing numbers on the availability. Most service providers offer 99.99% or even higher availability of their servers (Habib et al., 2010). When the provider is not able to deliver this amount of availability, it must pay a fine to the customer. However, the possibility exists anticipates on these fines so that it can offer a higher availability then where the infrastructure is designed for (Hofmann & Woods, 2010).

So, although providers may offer the availability a customer requires, there are no guarantees that the provider can actually provide it. This means the customer needs to trust the provider in its ability to reach the required availability. And the other way around, when there is historical evidence of high availability and thus reliability, it is more likely that the customer will trust the cloud service. Thus, the following hypothesis can be defined.

*E2. There is a positive effect of 'reliability' on 'trust in cloud service'*

### 2.4.3. Conceptual framework

The previous steps result in a conceptual model as shown in Figure 4. The conceptual model includes the hypothesis as described in the previous section.

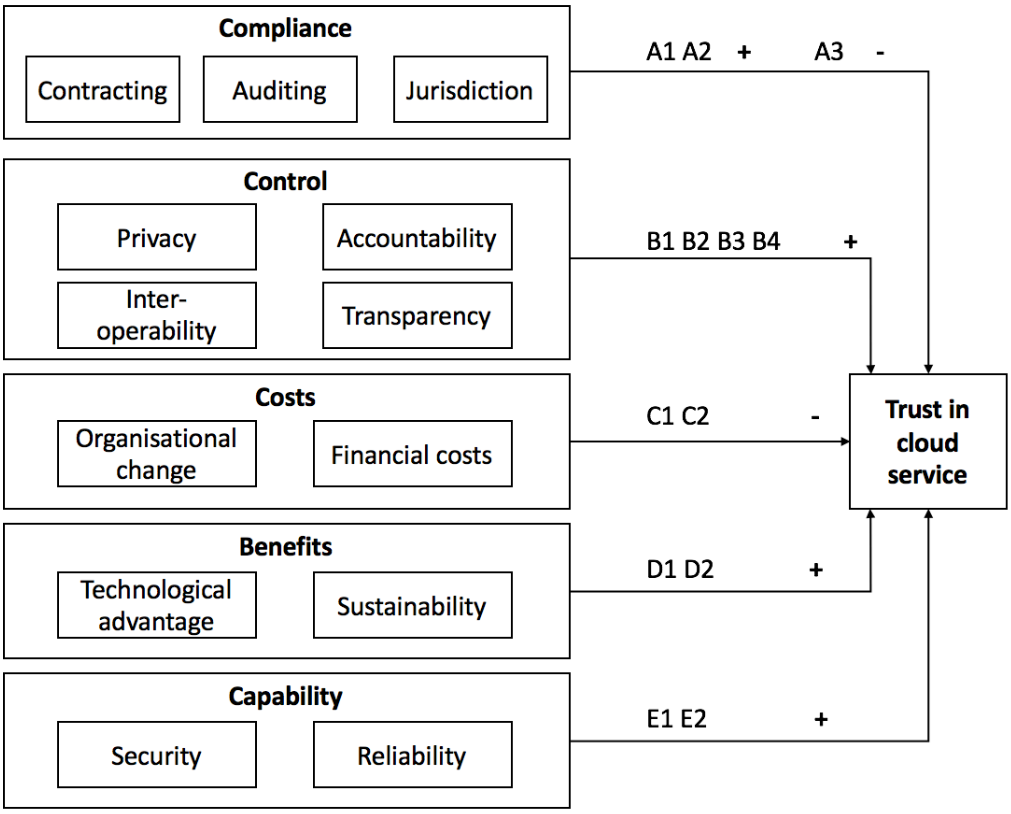


*Figure 4 Conceptual framework*

## 2.5. Chapter conclusion

The rise of the internet and the emergence of virtualisation technology made it possible that cloud computing became the multi-billions industry that it is now. With cloud computing being one of the most important trends in IT at this moment, it is logical that there is a lot of scientific literature on this matter. However, there is still a lot of ambiguity and uncertainty surrounding the subject. There is unclarity if cloud computing can really achieve the benefits that are expected from it and whether certain challenges can be overcome. With this ambiguity, it is logical there are different perspectives on cloud computing. While some aspects of cloud computing receive a lot of attention, there is not yet a clear definition of the perspectives on trust in a cloud service.

Trust is a concept that is extensively covered in scientific literature, since it is relevant for many disciplines. This means that there is no universal definition for trust. For this research, trust will be defined as *an organisation's dynamic, calculated and dependent expectation of the other organisation's competence and goodwill.* When adopting a cloud service the customer needs to expect certain competence and goodwill from the provider. In other words, there needs to be a certain amount of trust between both parties before the choice is made to adopt a cloud service. So, trust is an important facilitator for relationships and a critical success factor for cooperation. Transaction Cost Economics confirms this importance of trust when adopting cloud computing: more trust in a cloud service reduces the transaction costs, because less measures to deal with opportunistic behaviour and uncertainty need to be taken.

Although there is a clear importance of trust in cloud computing, there isn't yet an *empirical* research that studies the factors influencing trust in cloud computing services. By combining the relevant literature on trust in cloud computing, a conceptual model was drafted that includes the potential factors influencing the trust in a cloud service. This conceptual model will be used as a guide in the next Chapters.

The following knowledge gaps were found:

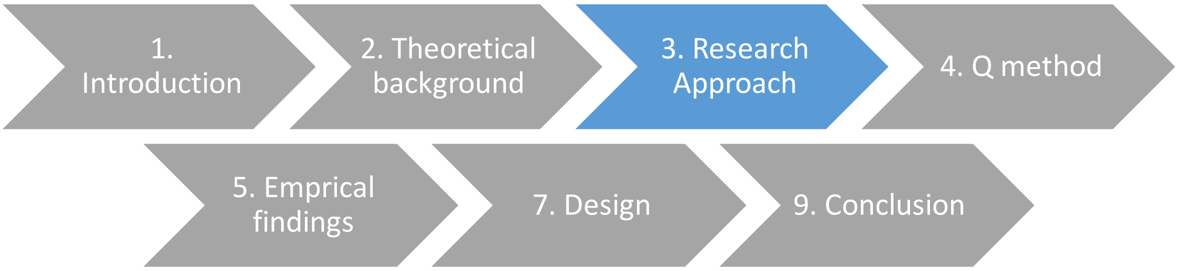
- It is unknown what the different perspectives on trust in cloud computing are
- There is no empirical research that explains what factors influence trust in cloud computing
- No scientifically based design exists that aims to improve the trust of (potential) customers in a cloud service

# Chapter 3 Research approach

In this chapter, the research approach will be elaborated upon. The research approach consists of the following:

- Research Framework
- Research strategy
- Data collection and analysis
- Limitations
- Chapter conclusion

The previous chapter has shown the relevance and importance of trust when organisations are looking to adopt cloud computing. Moreover, certain knowledge gaps in the scientific literature have been identified. This research approach will describe how this research will fill those knowledge gaps and contribute to the scientific literature. This research approach combines the theories on design science of Johannesson & Perjons (2014) and Verschuren & Doorewaard (2010).



# 3. Research approach

## 3.1. Research framework

A research framework will guide the research process and prescribes the appropriate steps that should be taken to reach the research objective. A research framework *"[...] shows clearly how the different phases of the research are interconnected, and how the one step implies the other. In short, the research framework represents the internal logic of a research project"* (Verschuren & Doorewaard, 2010, pp. 65).

In order to define the research framework, a step-by-step approach based on the approach of Verschuren & Doorewaard (2010, pp. 83) will be used. The following steps will be taken:

1. Characterise *the objective* of the research project.
2. Determine the *object* or objects of the research project
3. Define the *nature* of the research perspective.
4. Determine the *sources* of the research perspective.
5. Develop a *schematic presentation* of the research framework by using the principle of confrontation.
6. *Formulate* the research framework in the form of an elaborate argument.

### Objective

The research objective, as stated in Chapter 1.2, is:

*To define the relevant perspectives on trust in a cloud service based on the factors that influence trust and to design an artifact that facilitates in the improvement of this trust.*

### Object of research

The research objects in this research are the perspectives on trust in cloud services of practitioners that worked on the assessment, implementation or optimization of a cloud service for a large organisation, specifically in the sectors of technology, retail and consultancy in the Netherlands.

### Nature of research

The nature of the research is design-oriented research. The research will define a practical plan to reach certain structural and policy-induced solutions (Verschuren & Doorewaard, 2010). More specifically, the research will design an artifact that includes policy recommendations for cloud brokers to address the different perspectives on trust in cloud services.

### Sources of research

In Chapter 2, the concepts of cloud computing and trust were studied separately to get a wider understanding of both concepts and the challenges they individually bring to this thesis. Then the concepts were brought together by introducing the factors that influence trust in cloud computing according to the scientific literature. These factors were then combined into a conceptual model.

The conceptual model will be used as the input for the Q-method. The statements that will be used for this Q-method will be based on the conceptual model and will all fit within a one of the independent variables (the factors). This Q-method will then result in different perspectives on trust in cloud services.

For the design phase, the theory on organizational configuration by Mintzberg (1989) will be used to structure the parts of the organisation.

### Schematic representation

The schematic representation of the research framework is presented below in Figure 5.

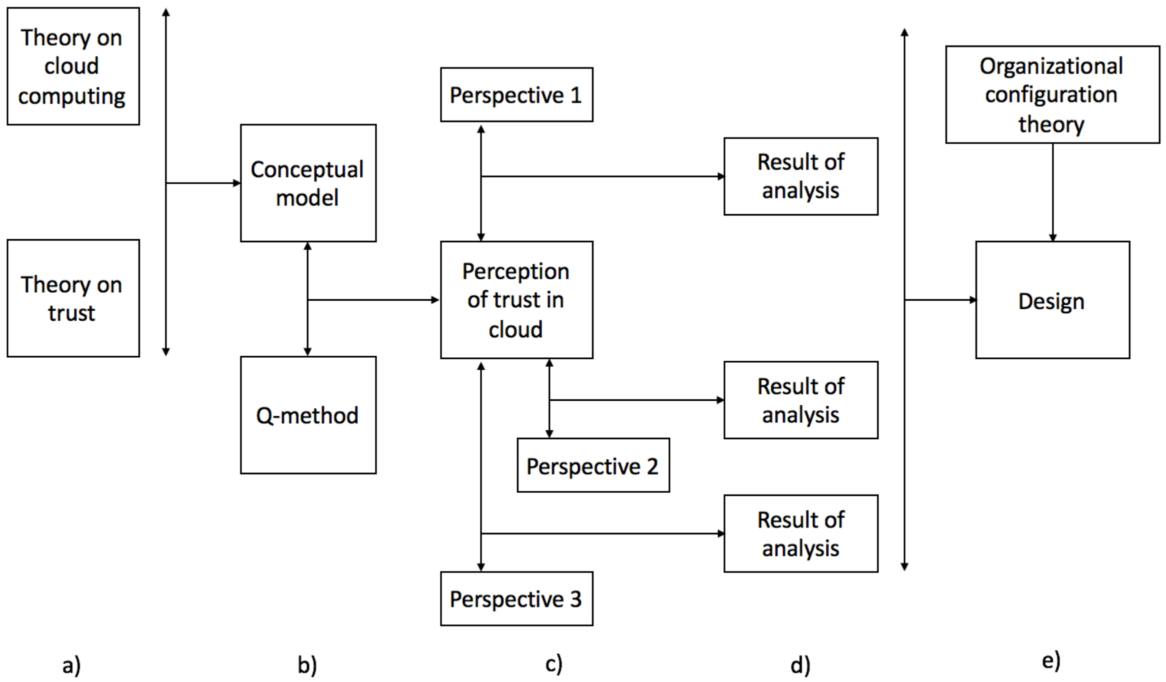


*Figure 5 Schematic representation of research framework*

### Formulation

(a) An analysis of the concepts of cloud computing and trust, and the integration of those concepts in scientific literature will be performed. (b) From this analysis, a conceptual model will be developed, which will be evaluated with a Q-method study on the potential factors influencing trust in cloud services. (c) The Q-method reveals the perception of the participants regarding trust in cloud computing. From this perception, it is possible to define several (in this case three) perspectives. (d) This will then give a result of analysis: which factors influencing the trust in a cloud service are important to all perspectives, and which factors are important to the specific perspective. (e) Based on the perspectives, combined with an analysis of the customer's organizational configuration, a design will be developed which facilitates the provider of a cloud service in improving the trust.

## 3.2. Research strategy

Research strategy can be defined as:

> *"[...] the coherent body of decisions concerning the way in which the researcher is going to carry out the research. We refer especially to gathering relevant material and processing this material into valid answers to the research questions."* (Verschuren & Doorewaard, 2010)

For this research, the *mixed methods* approach is taken. This means that a combination of methods and strategies is used in order to view the same phenomenon from different perspectives (Johannesson & Perjons, 2014). Moreover, the *mixed methods* approach makes use of a combination of quantitative and qualitative research (Ramlo, S., & Newman, 2011). Making use of the *mixed methods* approach is helpful for validating the findings (Johannesson & Perjons, 2014).

Since trust is a concept that is dependent on the context it is used in, a merely quantitative research is not desirable. Moreover, trust is about the perception of persons, a subjective matter. Although it is not possible to prove subjective matters, it is possible to show structure and form in them. This is possible with Q-method. This can be seen as a mixture between surveys and case studies. It is not just qualitative or quantitative; the method is actually qualiquantological (Watts & Stenner, 2005), a combination of both qualitative (Q-sorts) and quantitative (factor analysis) research (Ramlo, S., & Newman, 2011). Not being one or the other has led to various objections and misunderstandings by scientific researches (Watts & Stenner, 2005). However, Stenner & Rogers (2004) show in their study that qualiquantology (Q-method) is an excellent, if not the best, way of investigating contextualised social emotions; which trust is.

Data is also collected through document analysis. Potential factors influencing the trust in cloud services are defined based on the scientific literature. This provides a theoretical perspective, next to the more practical, observational perspective that will be gained by the Q-method. The data collection will be further discussed in the next section.

## 3.3. Data collection and analysis

Data will be collected through a document analysis and Q-method. The document analysis is performed to define the statements necessary for the Q-method and to develop the conceptual model that describes the potential factors influencing trust in cloud services. The Q-method is used to get data on the importance of the factors influencing trust in cloud services and to define several perspectives.

### 3.3.1. Document analysis

Document analysis, where documents are the main source of data, takes a shorter period of time and takes less effort than what would be the case with surveys or interviews (Johannesson & Perjons, 2014). The document analysis can be found in **steps a) and b)** of the research framework and is for the most part described in Chapter 2. The document analysis is performed to collect:

1. Potential factors influencing trust in cloud services, which will function as a basis for the conceptual model.

2. Opinions on these factors, which will function as a basis for the concourse used in the Q-method.

To develop a conceptual model that describes the potential factors influencing trust in cloud services, insight into prior scientific research is necessary. In the scientific literature, there are already both validated and invalidated conceptual models that can function as a basis for the conceptual model of this study (Alhamad, Dillon, & Chang, 2010; Chu et al., 2013; Lansing & Sunyaev, 2016; Uusitalo et al., 2010). Integrating all relevant research on this topic into one conceptual model provides a more holistic view on the matter.

Moreover, during the document analysis all kinds of sources are used to define the statements that will be used during in the Q-method. Because the statements need to represent all relevant opinions in the field, not only scientific literature is considered. Also, blogs, forums, white papers, etcetera are analysed during this phase of the research.

The document analysis will provide an answer to the following research questions:

- What is the current state of trust in a cloud computing service? (Chapter 2.1-2.3)
- Which factors influence the trust in a cloud computing service? (Chapter 2 & 5)
    - Which potential factors are found in the literature? (Chapter 2.4.2)
    - What does a conceptual trust model that describes the potential factors influencing trust look like? (Chapter 2.4.3)

### 3.3.2. Q-method

Q-method is the combination of philosophy, concepts, data-gathering procedures, and statistical methods that provides a thoroughly elaborated foundation for examining human subjectivity in a structured way (Brown, 2008). The Q-method can be found in **step b)** of the research framework and in Chapter 4 of this document.

Q-method is primarily an explorative technique, that can bring some coherence to research questions with many complex and socially contested answers (Watts & Stenner, 2005). Consequently, this method will not be able to prove the hypotheses defined in Chapter 5. However, it will provide structure, form and importance to the opinions related to these hypotheses by creating several common perspectives on trust in cloud services. Knowing which of the hypotheses are supported by which perspectives can then function as the input for the design phase.

So why use Q-method? Also, other research methods, such as case studies or textual analysis (i.e. narrative analysis) can provide insight in the factors that influence trust in a cloud service. So, in order to ensure Q-method is the right method for the proposed research, it is important to distinguish the advantages or complementarity of Q-method in relation to other research methods. Q-method can actually also be applied in case studies. However, Watts & Stenner (2005) state the following about using Q-method in case studies:

> *"In this guise, Q methodology ordinarily adopts a multiple-participant format and is most often deployed in order to explore (and to make sense of) highly complex and socially contested concepts and subject matters from the point of view of the group of participants involved. […]*

> *It does not do this in a thematic fashion, nor does it focus on the viewpoints of specific individuals. It should be no surprise, therefore, to find that this typical form of Q methodology disappoints when themes and/or individuals are the primary research targets."*(Watts & Stenner, 2005, pp. 70)

For this research, the themes are the primary research target: the factors influencing the trust in a cloud service. Instead of using those themes as a starting point during the analysis, it is the objective to define them during the research. This means that case studies, where highly complex and socially contested concepts and subject matters from the point of view of the group of participants involved are explored, are not suitable for this research objective.

With respect to textual analysis, and narrative analysis specifically, Q-method differs in three ways (Watts & Stenner, 2005). First, the participants are required to engage with the task of relating with a set of prepared items, instead of defining its own discourse. Second, narratives have a beginning, middle and end, while Q-method makes a "snapshot" and tries to position the structures, functions and implications of this temporary state. Third, narrative analysis focusses on specific individuals, while Q-method focusses on the wide range of perspectives among groups of participants. By scoping the research around the group and their shared viewpoints, Q-method provides an ideal complement to qualitative approaches which highlight the individual (Watts & Stenner, 2005).

The application and analysis of the Q-method will be elaborated upon in Chapter 4. The Q-method will provide an answer to the following research questions:

- Which factors influence the trust in a cloud computing service? (Chapter 2 & 5)
    - What are the factors influencing trust in a cloud computing service according to empirical research? (Chapter 5)
- How can the factors influencing trust in cloud computing services be analysed and structured? (Chapter 4)
- What are the perspectives on trust in a cloud service? (Chapter 5)

### 3.3.3. Interpretation of results

The interpretation of the results can be found in step **c) and d)** of the research framework. The interpretation will be done based on both the quantitative and qualitative data that is gathered in the previous parts of the research.

The analysis of the Q-sorts results in correlations between the different participants and between the different factors, loadings of the participants to each factor*, and factor scores for all statements. This is all quantitative data that needs to be interpreted. The interpretation of these results will be done in accordance with the output from the interviews that are held during and after the Q-sorting. This provides more context to the reasons of why a certain statement is agreed or disagreed with. The interpretation of the results of the Q-method is a somewhat explorative process. To provide a certain consistency in the interpretation of the results, a method was developed that uses the factor scores on each statement as input. This method consists of the following steps:

- For each statement, the average factor score is calculated;

The statements with the highest average factor score are agreed upon strongly by the complete participant group, while the statements with the lowest average factor scores are strongly disagreed upon by the complete participant group. This information is the input for defining the similarities between the different perspectives.

- For each statement, the *difference score* is calculated;

The difference score is the absolute difference between the factor score of a statement with the average factor score of this statement. The higher this difference score on a certain statement for a certain factor[*], the stronger the opinion on this statement differs from the other perspectives. In other words, when there is a high difference score on a certain statement, this statement represents the perspective that belongs to this factor[*].

- The *difference scores* of each factor are plotted in a histogram;

Every statement will have a difference score, and thus the amount of difference scores is equal to the amount of statements. The difference scores are plotted in a histogram, with the difference score on the x-axis and the amount of difference scores that fall within a certain interval on the y-axis. The intervals need to be chosen in such a way that gaps between the intervals occur. These gaps are used to identify the cut-off points that decide whether the statements are still representative for the factor[*]. For example, when three statements respectively have a difference score of 0,20; 0,25 and 0,30 (scenario 1), it is hard to argue that the statements with a difference score of 0,25 and 0,30 need to be used for the interpretation of the factor[*] and not 0,20. With intervals of 0,05 these values would be clustered together in a histogram (see Figure 6). However, when the difference scores would be 0,10; 0,25 and 0,30 (scenario 2) it would make sense to make a cut-off point at 0,25 and not include 0,10. In a histogram with intervals of 0,05 only the statements with a difference score of 0,25 and 0,30 will be clustered together, showing a gap between them and the statement with a difference score of 0,10 (see Figure 6). So, a histogram with the right interval size can quickly and methodically show logical cut-off points for the amount of statements that will be representative for a certain factor[*].

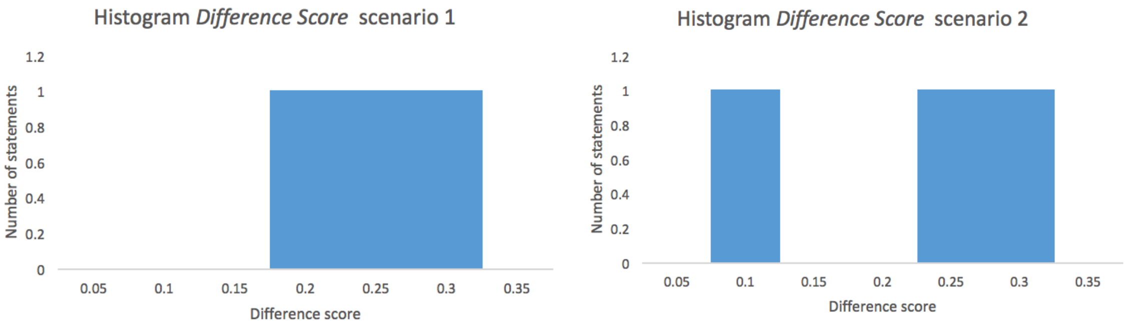


*Figure 6 Histogram of scenario 1 & 2*

[*] Factor that is the result of the factor analysis, not to be confused with 'factors' influencing the trust in a cloud service

- Based on the cut-off point that is established in step 3, the statements that represent the perspective of this factor* are defined;

This final step will provide the statements that can be used to interpret the perspective of the factor*. After this there will be spoken of a perspective, rather than a factor*.

The perspectives that are then found through the analysis of the data are a function of the participants themselves. This means that there isn't an observer bias, as for example happens when categories or perspectives are formed based a large volume of interview transcripts that are qualitatively analysed. With Q-method the perspectives are grounded in more than a conceptual sense: *"They are wholly naturalistic inasmuch as they are inextricably tied to and emerge from the concrete operations of the participants."*(Brown, 2008, pp. 701)

## 3.4. Design approach

Step e) of the research framework deals with the design phase of the research. Since the design will aim to improve the trust of an organisation in a cloud service, it is relevant to have more insight in the organisational configuration of such an organisation. Hence, a combination of the organisational configuration theory of Mintzberg (1989) and the empirical findings from the Q-method will be used as input for the design.

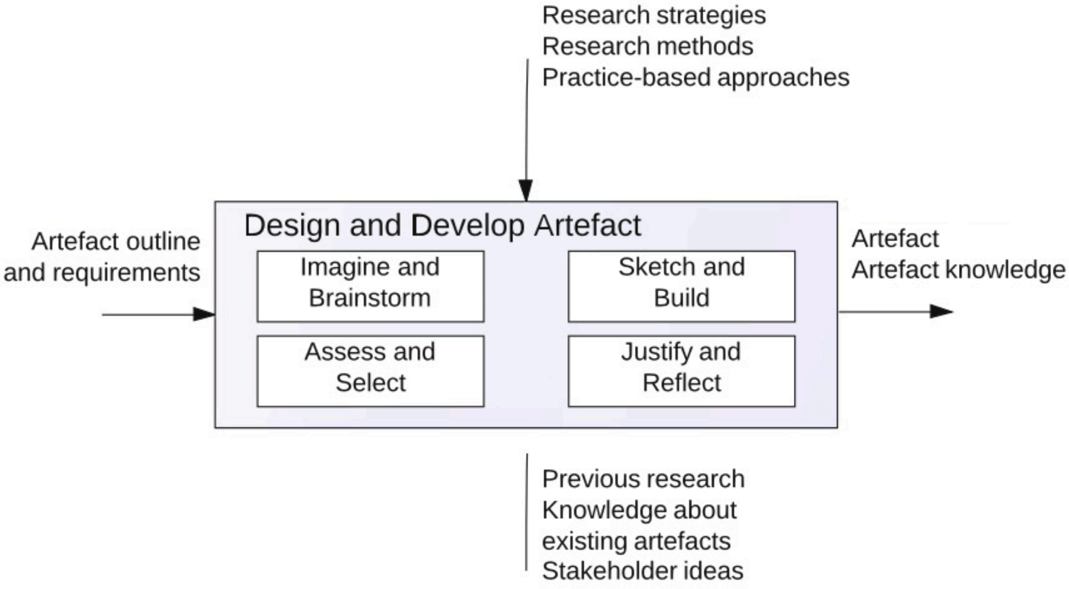


*Figure 7 Design and develop artifact (Johannesson & Perjons, 2014)*

The design itself will be done according to the theory of Johannesson & Perjons (2014) (see Figure 7) and in accordance with the principles of TIP (Bots & Daalen, 2012), taking into account the technological, institutional and process aspects in the design. The activities, inputs, outputs, controls and mechanisms/resources will be modelled with the IDEF0 method.

The design will answer the following research question:

1. What does a design look like that facilitates the improvement of trust, based on the perspectives? (Chapter 6)

## 3.5. Limitations

Although the collection of data has been described extensively and the gathering of the data will be done carefully, still issues related to the data may arise.

One of the biggest issues with using documents for data collection is the assessment of their credibility: determining the authenticity, correctness and whether they are free from bias (Johannesson & Perjons, 2014).

With Q-method, all that can really be said is that the participants expressed their viewpoint at that time, through sorting a specific set of statements. So, this leaves open the possibility that individuals may change their minds over time, making the results of this Q-method less relevant. However, it can be expected that shared viewpoints show a certain degree of consistency over time (Watts & Stenner, 2005). Moreover, this means that the Q-method will result in '*subjectively expressed, socially organized semantic patterns*', rather than scientific prove that certain causal relationships as presented in a conceptual model exist in reality.

Additionally, when performing the Q-sorting, both the method and the instructions need to be explained to the participants, because most of them are unfamiliar with it. Validity can therefore be affected when the participant's lack of comprehension leads to misunderstandings. This will even more so be the case when the Q-sorting is not done face to face, but rather through an online tool. Although instructions may be structured and a step-by-step process has to be followed, there is no possibility for the participants to ask questions when anything is unclear. Furthermore, when the Q-sorting is done through an online tool, the context of their sorting will be unclear, since the opportunity to explain their reasoning is limited in this tool. A (video)call can only solve this problem until a certain extent.

## 3.6. Chapter conclusion

This chapter elaborated on the research approach by explaining what steps will be taken in order to get the answers to the research gaps that were found in Chapter 2. The approach combines document analysis, Q-method and design science into one framework. The document analysis will answer the following research questions:

- What is the current state of trust in a cloud computing service? (Chapter 2.1-2.3)
- Which factors influence the trust in a cloud computing service? (Chapter 2.4)
    - Which potential factors are found in the literature? (Chapter 2.4.2)
    - What does a conceptual trust model that describes the potential factors influencing trust look like? (Chapter 2.4.3)

Q-method will be used to answer the following research questions:

1. How can the factors influencing trust in cloud computing services be analysed and structured? (Chapter 4)
2. What are the perspectives on trust in a cloud service? (Chapter 5)

By using the outcomes from the Q-method and the organizational configuration theory a design will be made. This design will be done according to the theory of Johannesson & Perjons (2014) and will answer the following research questions:

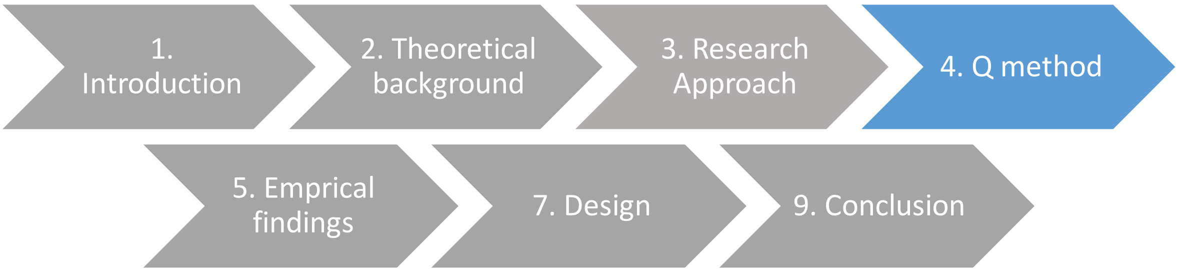
2. What does a design look like that facilitates the improvement of trust, based on the perspectives? (Chapter 6)

# Chapter 4 Q-method

Q-method provides the basis for studying subjectivity in a systematic way. This means only subjective opinions are used in Q-method. Although it is not possible to prove them, this method makes it possible to show structure and form in them. This means Q-method can reveal and describe both divergent views as consensus in a group. The Q-method is a complete methodology, involving technique (sorting), method (factor analysis), philosophy and ontology and was created by William Stephenson (1902-1989) (ISSSS, 2017). The research question for this Q-method study is defined as: "*Which factors influence trust in a cloud service*". The Q-method consists of the following:

- Concourse
- Q-sample
- P-sample
- Q-sort
- Analysis and results
- Limitations
- Chapter conclusion

This chapter will use the conceptual model as described in the previous chapter as guidance for establishing statements in the concourse and determining the final Q-sample. This ensures the scientific degree of this study. The outcome of this chapter will consist of the data that will be used to identify the different perspectives related to the factors influencing trust in a cloud service, which will be done in the next chapter.



# 4. Q-method

## 4.1. Concourse

The concourse is a list of approximately 120 statements related to the potential factors influencing trust in a cloud service. This complete list can be found in Appendix B.

A concourse refers to the incoherent batch of beliefs and perspectives and is the foundation of the Q-method. Concourse is a more general term than discourse, which implies a special case with coherency and a linear story. This is not the case with a concourse, since it refers to all opinions and perspectives that exist about a certain topic. Statements in the concourse are limitless and subjective, because it is about opinions, rather than facts. The statements can be gathered from all kinds of sources.

During the document analysis, all kinds of sources are used to define the statements that will be used for the concourse. Because the statements need to represent all relevant opinions in the field, not only scientific literature will be considered. Also, blogs, forums, white papers, etc. are analysed during this phase of the research. When the concourse is saturated with all relevant opinions, the concourse is considered complete.

The statements are found by using the following keywords or combinations of them: cloud computing, trust, (inter)organisational trust, contracting, auditing, security, privacy, reliability, transparency, interoperability, organisational change, costs, sustainability, accountability and technological advantage. Most of these keywords were established during the initial document analysis for potential factors influencing trust in cloud services in Chapter 2.4.2. These keywords were then used to get the complete perspective on this specific potential factor in order to achieve a saturated concourse.

## 4.2. Q-sample

The complete concourse is too large for a participant to analyse, and thus the concourse is represented by a Q-sample of forty statements. These statements should be structured in terms of a conceptual model (Brown, 2008). This conceptual model is defined in Chapter 2.4. The statements are structured according to the potential factors influencing trust, which are the independent variables in the conceptual model. The complete Q-sample, together with the argumentation for the statements can be found in Appendix E.

## 4.3. P-sample

The P-sample is a representative sample from the complete relevant group of people that are researched. The selection of the people that will participate in the Q-method study defines the scope of the research, but also limits the outcomes to the group of people they represent. Within the P-sample it is important to have as much diversity as possible, so that all relevant perspectives are represented in the study (Brown, 1993). This representativeness is desired above all else. This also means that without a clear scope, perspectives can be endless and representativeness will be limited. For Q-method a small number of participants is needed, usually between twenty and forty (Watts & Stenner, 2005). For this study 25 people are willing to participate. Several conditions are used for scoping the P-sample:

6. Person is/was involved in the assessment, migration or optimization of a cloud service
7. Person works in the technology, IT consultancy or retail sector
8. Person works for a large, private organisation
9. Person currently works in the Netherlands
10. Persons has either an IT or business role in the cloud project

This means only persons that work or worked on a cloud project in a business or IT role for a large, private organisation in the technology, IT consultancy or retail sector in the Netherlands are approached. More information regarding the roles and education within the P-sort can be found in Figure 8. This figure also shows information about the cloud computing deployment and service models that the participants worked with. To keep the study scoped, only persons in business or IT roles were invited to participate. This resulted in 1/3th being business and 2/3th being IT in the P-sample. With cloud being primarily an IT solution, this distribution makes sense as a representation of the complete group. Additionally, most participants were involved in public cloud (84%) and private cloud (68%) projects, as well as all three service models (IaaS 68%, PaaS 76% and SaaS 76%). Furthermore, participants were mostly involved during the assessment (72%) or migration (92%) phase of cloud adoption. This means that only the hybrid cloud as deployment model and optimization as maturity level are represented less in the P-sample. Since the study is related to the *adoption* of *public* cloud services, this seems logical, and thus the low numbers are representative for the complete group that the P-sample represents.

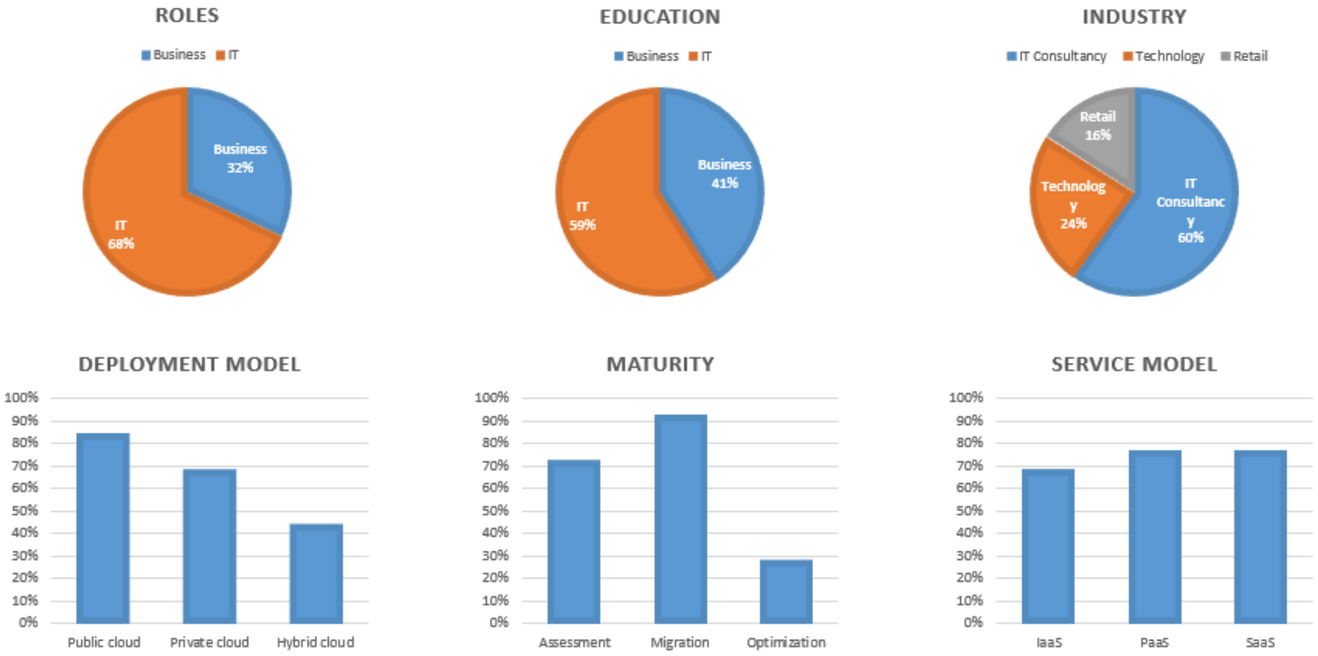


*Figure 8 Background information about the P-sort*

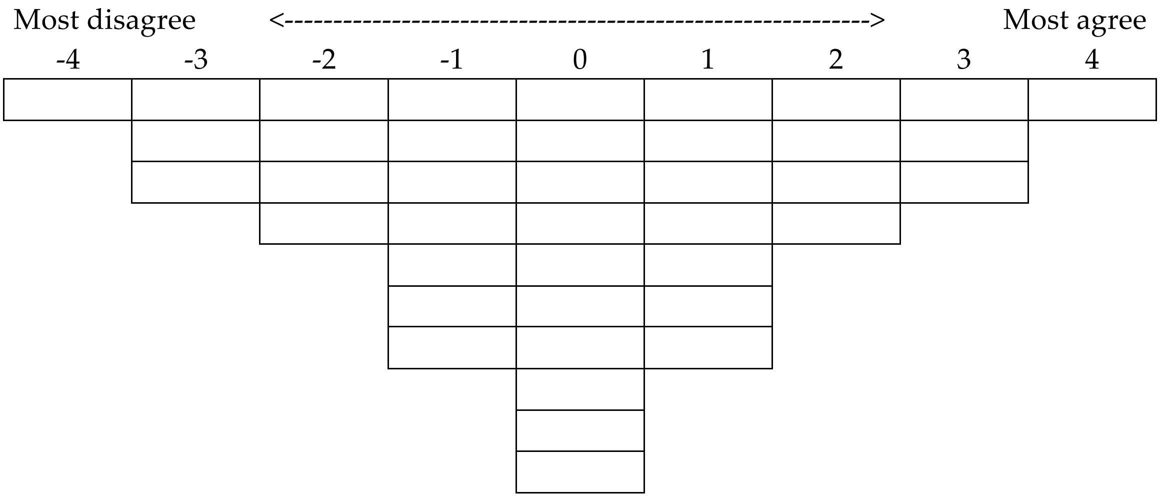
So, based on the previous findings, it can be said that the P-sample is representative for the relevant group of people that fit within the scope. Categories based on respondent characteristics are of little interest and are normally not used for further analyses (Watts & Stenner, 2005). However, background information can be valuable to provide some context to the findings. It might for example be valuable for the interpretation to see whether a perspective consists mainly of participants with an IT or business background.

## 4.4. Q-sort

During the Q-sort phase of the Q-method, the participant is required to rank the statements. As the statements are a matter of subjectivity, the ranking will represent the subjective perspective of the participant. The quantification of the qualitative perspectives constitutes the focal observation of the Q-sorting (Brown, 1993). Validation doesn't need to be considered, since the Q-sort represents the participants personal point of view, for which external criteria are not important (Brown, 1993). A Q-sort can never be wrong or right.

The Q-sort produces a set of scores, ranging from -4 to 4 as can be seen in figure 9, where every cell represents one statement. In total there are 40 cells, that corresponds to the amount of statements in the Q-sample. Participants are required to follow the distribution as presented in the figure. This forces the participant into carefully prioritizing the statements. The Q-sort reflects each participant's personal view and is statistically correlated with the other participants, where the magnitude of correlation corresponds with the degree of similarity in the different perspectives. (Brown, 1993)

*Figure 9 Q-sort distribution*



The Q-sorting itself is ideally done face-to-face. In this way, the participant can explain their choices and motivations for putting the statements in a certain distribution. Before the actual Q-sorting commences, the participant is asked to fill in a small form asking about some background questions related to their education, their role in cloud computing projects, their organisation and their experience with different aspects of cloud computing. This form can be found in Appendix C. Both the interview part of Q-method and the background information about the participant tell something about the context of the Q-sort, which is useful during the analysis of the results.

The Q-sort starts with the participant sorting the statements in three piles: agree, neutral and disagree. This helps the participant during the process of putting the statements in the required distribution. When the participants completed sorting the 40 statements into the three piles, the participant starts with putting the statements from the ‘agree pile’ into the right part of the distribution, where the far-right statements represent the statements the participant agrees most with. Then the same is done with the statements from the ‘disagree pile’, but then for the left side of the distribution. Finally, the statements from the ‘neutral pile’ fill the gap in the middle. The more elaborate instructions that were presented to the participant can be found in Appendix D. The sessions took about thirty minutes to an hour.

Five participants were not able to perform the Q-sort face-to-face. For those participants, an online tool was setup. This tool was created by Stephen Jeffares[1]. The tool provides clear instructions and leads the participant through the Q-sorting in a step-by-step process. Moreover, the participants are asked to give their motivation for the statement they agree most and disagreed most with and there is an option to provide additional comments.

## 4.5. Analysis and results

The Q data will be analysed using the dedicated software package PQMethod that was developed by Peter Schmolk[2]. Using this software, different factors can be defined. In this section, the term ‘factor’ refers to the unobserved variable that is defined by observed, correlated variables. If all participants were to sort the statements in approximately the same order, the correlations would be high, which would result in only one factor. On the other hand, if all participant’s view would be completely different from each other, correlation would be very low, which would result in one factor for every participant. However, usually, between two and five factors will result from the analysis, depending on the segmentation of the participants. Each factor will represent a perspective that is held in common by a certain subset of the participants. When a Q-sort ‘loads high’ on a certain factor, it means there is a high correlation between the Q-sort and the factor. (Brown, 1993)

The PQMethod software provides several possibilities for analysing the data. First, PQMethod provides Centroid factor analysis and Principal Components factor analysis as methods for doing the factor analysis. Factor analysis is used to describe variability among correlated variables, in this case the Q-sorts, in terms of a lower number of unobserved variables, called factors. With respect to the choice between the two abovementioned methods for doing this factor analysis, there seems little reason to prefer one factor analysis option over another (Watts & Stenner, 2005). Since the Centroid factor analysis is the method of choice for Stephenson (Stephenson, 1952), this method is chosen. For the factor analysis initially seven factors will be extracted, since this is advised by (Schmolk, 2014). It would make no sense

[1] https://jeffar.es/poetq/

[2] http://schmolck.userweb.mwn.de/qmethod/downpqwin.htm

selecting less than seven, because upon rotation of the factors, one can choose how many unrotated factors to use.

When the factor analysis is done, the factors need to be rotated. Rotation is done in order to make the output more understandable. Through rotation, a pattern of loadings where each item loads strongly on only one of the factors, and much weaker on the other factors is sought. In PQMethod, this procedure can be done by hand, or through the varimax procedure. The varimax procedure offers a simple and reliable way of rotating the factors (Watts & Stenner, 2005), hence this method is chosen.

Next, it has to be decided which factors will be selected for interpretation. It is common practice that only the factors with an eigenvalue of more than 1.00 are selected (Watts & Stenner, 2005). However, it is also known that a factor with an eigenvalue of more than 1.00 is extracted from random data, because random patterns can always be detected (Watts & Stenner, 2005).

The analysis of the Q-sorts for this study gave the following eigenvalues:

| Factor | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Eigenvalue | 8.1958 | 1.6656 | 0.1279 | 1.3598 | 0.1647 | 1.0930 | 0.0878 |

This suggests that the factors 1, 2, 4 and 6 are selected for interpretation, since they all have an eigenvalue above 1.00. However, during the interpretation of the factors, there was no coherent pattern to be found in factor 6 (see Appendix **Error! Reference source not found.**, Table 30 for factor scores of all four factors with an eigenvalue of more than 1). For this reason, factor 6 will be excluded from further interpretation and analysis.

*Table 3 Loadings of Q-sorts on the different factors*

| | Factor | | |
|---|---|---|---|
| **Q-sort** | **1** | **2** | **3** |
| 1 | -0,0542 | 0,2229 | **0,5744** |
| 2 | **0,6364** | 0,175 | 0,199 |
| 3 | 0,0691 | **0,54** | 0,3371 |
| 4 | **0,5571** | 0,0927 | 0,4465 |
| 5 | **0,532** | 0,1521 | 0,4364 |
| 6 | 0,3472 | **0,5878** | 0,2969 |
| 7 | 0,2114 | 0,071 | **0,5123** |
| 8 | 0,0938 | 0,4378 | **0,0654** |
| 9 | 0,4228 | **0,6632** | -0,108 |
| 10 | **0,6007** | 0,2733 | 0,288 |
| 11 | **0,5047** | 0,0687 | -0,0036 |
| 12 | **0,4512** | 0,1881 | -0,0606 |
| 13 | 0,2007 | **0,5445** | 0,4027 |
| 14 | **0,7705** | 0,2238 | 0,0737 |
| 15 | **0,4988** | 0,4194 | 0,2478 |
| 16 | 0,1269 | **0,7063** | -0,0226 |
| 17 | 0,4127 | 0,3521 | 0,4395 |
| 18 | 0,4247 | 0,2806 | **0,5795** |
| 19 | **0,7981** | 0,0624 | 0,2591 |
| 20 | 0,1947 | 0,4427 | **0,4935** |
| 21 | 0,1644 | -0,1171 | **0,5598** |
| 22 | 0,3881 | 0,2367 | 0,3008 |
| 23 | -0,0101 | 0,3435 | 0,3657 |
| 24 | **0,6294** | 0,1097 | 0,365 |
| 25 | **0,6252** | 0,0698 | 0,1093 |

In Table 3 the loadings of the Q-sorts on the different factors is presented (here the factors are renamed as factor 1, 2 and 3). Q-sorts are only being used in the interpretation of the results when their loading is significant. As a rule of thumb, when a Q-sort loads higher than $1/\sqrt{N} \times 2.5$ (where N is the number of participants) it is considered significant (Brown, 1993). With 25 participants, this results in a threshold of 0,5. However, to maximize the number of relevant participants, the threshold can be set so that there are as much single loadings as possible. Single loading means that a Q-sort only significantly loads on one of the factors. If a Q-sort loads significantly on multiple factors, the Q-sort is not representative for a single factor and thus can't be used during further analysis. When the threshold is set at 0,45 the maximum number of Q-sorts present a single loading. For this reason, this threshold will be used. The loadings that are marked bold in the table, are significant and only have a single loading. This means Q-sort 17, 22 and 23 do not have a single loading and consequently are not taken into consideration during further analysis.

## 4.6. Limitations

The limitations of Q-method itself are already discussed in Chapter 3.5. This section will elaborate on the limitations of the actual application of Q-method for this specific research.

All participants were from large organisations in the IT consultancy, retail or technology sector. Making the results of the study only generalizable for large organisations in these sectors. Further research should be done for other sectors, such as banking and government and also for smaller organisations, such as for SME's and start-ups.

## 4.7. Chapter conclusion

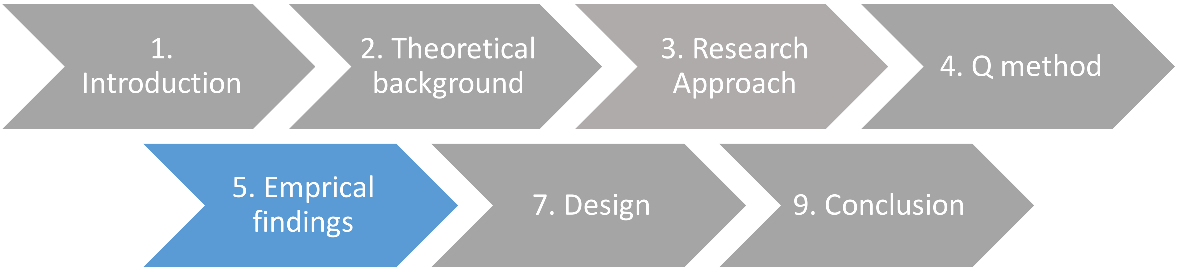
From the Q-method, that was held among 25 participants, it can be concluded that the three factors found during the analysis represent three perspectives on trust in a cloud service. The combinations of the perspectives and the factors scores on the statements will be used in the next chapter to define the perspectives. Also, some information on the P-sort will be used in order to provide more context to the perspectives.

# Chapter 5 Empirical Findings

In this chapter, the research findings will be elaborated upon. The research findings consist of the following:

- General findings
- Defining the perspectives
- Limitations
- Chapter conclusion

This chapter will discuss the empirical findings that were acquired from the Q-method. The data from the correlation and factor analysis that was performed in the previous chapter will be interpreted. This will show which factors influence the trust in a cloud service in general. Also, it becomes possible to identify which statements and factors are important for the different perspectives. These perspectives and the factors influencing trust in a cloud service will be used as input in the next chapter: design.



# 5. Empirical findings

## 5.1. General findings

Although Q-method can be used to find different perspectives on a certain topic, it also provides the possibility to find similarities among the perspectives. First, the correlation matrix between the perspectives shows the degree of similarity between the perspectives. These correlations can be found in Table 4.

*Table 4 Correlation matrix between factor scores*

| Perspective | 1 | 2 | 3 |
|---|---|---|---|
| 1 | 1,0000 | 0,4755 | 0,5198 |
| 2 | 0,4755 | 1,0000 | 0,5031 |
| 3 | 0,5198 | 0,5021 | 1,0000 |

The correlation between the factors are approximately 0,5 for all perspectives. This indicates that there are clear similarities between the perspectives. What these similarities are, will be discussed in this section.  First, an analysis will be done on the statements that all perspectives strongly agree with. Then, an analysis will be done on the statements that all perspectives strongly disagree with. This is done by looking at the average factor scores. If all perspectives agree strongly with a statement, the factor score of each individual perspective is high for this statement, meaning the average factor score will also be high. The same applies to when the perspectives strongly disagree with a statement, but then the average factor score is low (close to zero).

### 5.1.1. Actions of the customer

The results of the analysis to determine the highest average factor scores can be found in Table 5. These are the statements all perspectives agree on strongly. In general, the participants most strongly agreed with the fact that adopting cloud computing will require a change in the organisation’s culture. One of the participants stated in the interviews for example that:

> *“The most important is to achieve an attitude that users always use the cloud storage facility instead of a local server. This is even more important when using a SaaS solution.”*

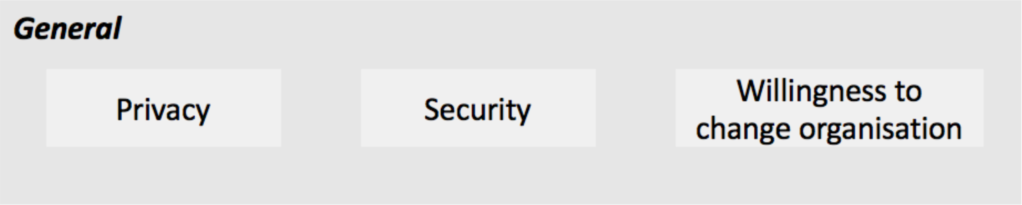
This means that the participants perceive cloud computing as an impactful measure, influencing the entire organisation. This indicates that the participants expect actions from the customer too. Customers can not just left click a couple of times, provide their credit card information and start using the cloud service. There actually needs to be a change from within the organisation too. This view is supported by other statements all perspectives strongly agree on. Namely, when adopting a cloud service, the participants expect the customer to take actions in the forms of (1) encrypting sensitive data before storing it in the cloud, (2) asking the provider about backup retention strategies, encryption, data disposal procedures and business continuity and (3) define communication processes capable of quickly and effectively notifying data owners about any potential breach in security. As can be seen, these actions are mostly related to security. Following the line of argumentation that customers need to perform actions themselves too, it can be concluded that organisational change is more seen as a condition that needs to be met by the customer, than that it is a factor that influences the trust in a cloud service. Hence, organisational change will be redefined to: willingness to change the organisation. This factor then has a positive influence on trust: the more an organisation is willing to change, the more it will trust a cloud service.

Additionally, ranked as number two, participants strongly agree with the statement that providers should not use the data that is entrusted to them inappropriately. This once more underlines the importance of privacy for the customer.

*Table 5 Statements all perspectives* ***agree*** *on*

| Rank | Statement | Independent variable |
|---|---|---|
| 1 | Adopting cloud computing will require a change in the organisation’s culture | Organisational change |
| 2 | It is important that CSPs do not use the data that is entrusted to them inappropriately | Privacy |
| 3 | In the case of highly sensitive data, it's important to encrypt it before storing it in the cloud | Security |
| 4 | Providers should be asked about their backup and retention strategies, encryption, data disposal procedures, and business continuity in the contract. | Security |
| 5 | Users of cloud computing services should have communication processes capable of quickly and effectively notifying data owners about any potential breach in security | Organisational change |

So, according to the interpretation of the statements all perspectives agree strongly with, these three factors influencing trust in a cloud service are the important to all perspectives:



The main conclusion of the analysis and interpretation of these statements is the fact that it is perceived important that also the customer performs certain actions before adopting a cloud service. The customer needs to make sure their organisation is ready and willing to make the change, as well as making sure that the cloud service they want to adopt is secure and provides privacy over their data.

### 5.1.2. Public cloud is secure and understood

The results of the analysis to determine the lowest average factor scores can be found in Table 6. These are the statements all perspectives disagree on strongly. In general, the participants most strongly disagreed with the fact that the cloud is a black box into which the enterprise dumps its applications, data workloads and processes. This indicates that in general, customers understand what the cloud is and how it works. Although, it has to be noted that the word "dump" is rather strong, which may have led to people disagreeing more with that word than with the actual statement. Interestingly enough, one of the participants agreed with this statement most strongly out of all statements. His argumentation was:

> *"That's where the business value is. The cloud is not a goal in itself, the goal is to have an appliance that you plug into and that works, anywhere, always."*

So, although the participants in general know what the cloud is and how it handles their data and application, there are also people that seem to think that this is not necessary at all: you just plug it in and it works, without having to know how it works. The fact that the participants think to know what the cloud is and how it works, is somewhat confirmed by the fact they also strongly disagree with the statement that the anonymous and on-demand nature of the cost of consumption of cloud usage makes it difficult for business to evaluate and incorporate it into their business plans. This means that they know what they need from the cloud and what this is going to cost them. It shows a certain understanding of the cloud. Moreover, it indicates that there are apparently no problems for the participants to change their IT costs from capital expenditure (capex) to operational expenditure (opex).

Additionally, participants don't think shared access to CPU and storage can allow other people or an attacker to view other's data or even take on another person's identity. This fundamental part of the cloud technology is not considered as a security issue.

Lastly, participants disagree on the fact that a local or private server should be used instead of a public cloud. Even for the mission-critical information, the cloud should be used. As one of the participants stated:

> *"You should adopt cloud computing or you should not do it. It makes no sense to only go partly into the cloud, that limits the value you get from it."*

Thus, among the participants, there is a tendency to trust the public cloud over any other deployment model.

*Table 6 Statements all perspectives* ***disagree*** *on*

| Rank | Statement | Independent variable |
|---|---|---|
| 1 | The cloud is a black box into which the enterprise dumps its applications, data, workloads and processes | Transparency |
| 2 | Because there is shared access to CPU and storage, a simple flaw can allow other people or an attacker to view other's data or even take on another person's identity | Security |
| 3 | Private clouds are preferred over public clouds | n.a. |
| 4 | The anonymous and the on-demand nature of the cost of consumption of cloud usage makes it difficult for business to evaluate and incorporate it into their business plans | Organisational change |
| 5 | At least the mission-critical information should be backed up on a local server | Reliability |

So, according to the interpretation of the statements all perspectives disagree strongly with, these two factors influencing trust in a cloud service are the important to all perspectives:

The main conclusion of the analysis and interpretation of these statements is the fact that the public cloud is understood and secure, and in general preferred over other deployment models.

## 5.2. Defining the perspectives

In order to define the different perspectives, the differences between the factors need to be studied. One way of doing this is by putting all the factor scores together into an *average factor score* and then comparing the factor score of each factor with this average. Table 7 presents an example of how this is done:

*Table 7 Example for interpretation of perspectives*

| Statement | F1 | F2 | F3 | Average score | Difference score F1 |
|---|---|---|---|---|---|
| Cloud computing is the most important trend in enterprise IT | 1,18 | -0,41 | -1,64 | -0,29 | 1,47 |

As can be seen, there is a significant difference between the three factors. Having a positive factor score, means that perspective 1 (F1) agrees with the statement. Having a negative factor score means that perspective 2 (F2) and perspective 3 (F3) disagree with the statement. Since perspective 3 has a bigger negative value than perspective 2, it means that they disagree stronger with this statement. The average factor score of the three perspectives combined is -*0,29*. The difference of the own factor score with the average factor score (now to be called *difference score*) of perspective 1 on this statement is then *1,47*. When this is done with all statements, a ranking can be made that shows which statements differ most from the average. The statements that differ most from the average will then be seen as the statements that are representative for this specific perspective. However, when this ranking is made, it is important to individually interpret the results. In the example as provided above it can be seen that perspective 1 really agrees, perspective 2 is somewhat indifferent about the subject and perspective 3 really disagrees with it. It can also be the case that one perspective really agrees with a statement and that the other two perspectives are fairly indifferent about the matter. The difference scores are relative to each other, and are no absolute independent indication of the viewpoint of a certain perspective. So, individual interpretation is still necessary.

Then, when the ranking is known, an approach to decide which statements are still important to the specific perspective and which ones are not. In other words, it has to be decided what the threshold is for the statements to still be representative for this perspective. This will be done by first plotting a histogram of the *difference score* of the individual perspectives. When statements have approximately the same *difference score*, it is hard to argue that one is really more representative for the perspective than the other. To show 'gaps' in the difference scores a histogram is plotted. When there is a gap between clusters of statements, it means that there is an arguable difference in the representativeness of the statement. Hence, these statements will be interpreted in the process of defining a coherent perspective a more elaborate explanation of this method is provided in Chapter 3.3.3.

### 5.2.1. Perspective 1: Techno-Optimists

The histogram of this perspective is presented in Figure 10. The histogram clearly shows a gap, resulting in three statements to seem most representative for this perspective.

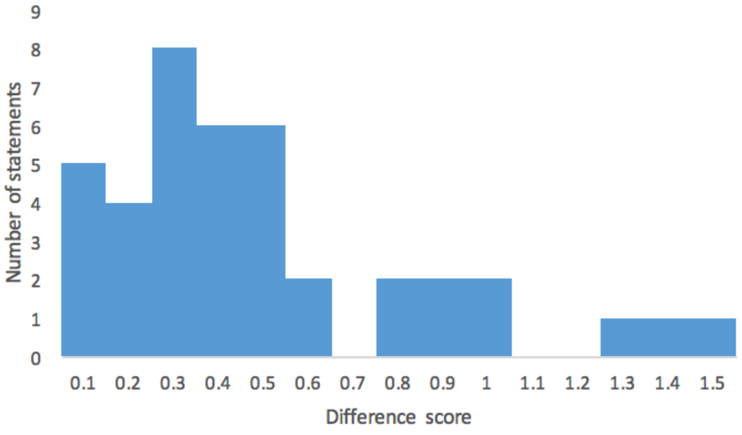


*Figure 10 Histogram of the Difference Scores of Perspective 1*

The three statements that are most representative are presented in Table 8. This perspective sees cloud computing as the most important trend and is thus positive about the technology behind it. People in this perspective gain trust from the benefits, and specifically the technological advantage that it provides. One of the participants stated that:

> *"Cloud is assumed. It is not a question of "if", but "when". It is expected that by 2019, more than 90% of all companies will be using public cloud and that the total earnings in cloud computing worldwide will increase from $40 billion in 2016 to $170 billion in 2026"*[3]

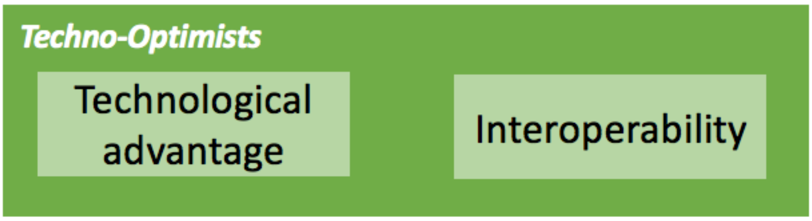
Moreover, the use of multiple providers is considered as important. This indicates that, although the technology is believed to be trustworthy, it is still important to limit the dependency on the provider. On the other hand, it shows that participants in this perspective expect a certain degree of interoperability in order to trust a cloud service. Otherwise, it would not be possible to effectively integrate the cloud services of the different providers. Lastly, this perspective does not seem to think the lack of control over IT is the biggest challenge. So, although some of the control will be out of their hands, this perspective seems to be okay with it and trust on the cloud service technology to provide what is necessary.

*Table 8 Statements representative for Perspective 1: Techno-Optimists*

| Rank | Statement | Independent variable | Agree/ Disagree |
|---|---|---|---|
| 1 | Cloud computing is the most important trend in enterprise IT | Technological advantage | Agree |
| 2 | Organisations should use more than one provider | Interoperability | Agree |
| 3 | Lack of control over IT is the biggest challenge | Accountability | Disagree |

In Appendix E more information about the participants within this perspective can be found. This information can provide some more context to the interpretation of the statements. The main conclusion that can be made from this information is the fact that compared to the complete group of participants, this group has relatively more people from the technology sector. This confirms the view that this perspective really values the technological advantages when assessing their trust in a cloud service.

Thus, because of their positive attitude towards technology, this perspective is defined as the *techno-optimists*. The following two factors are the most representative for the *techno-optimists*:



[3] Accenture estimates

### 5.2.2. Perspective 2: Responsibility-Shifters

The histogram of this perspective is presented in Figure 11 Histogram of the Difference Scores of Perspective 2. The histogram clearly shows two gaps, resulting in one statement being most representative for this perspective. However, since there is another isolated cluster with statements, these will also be taken into account.

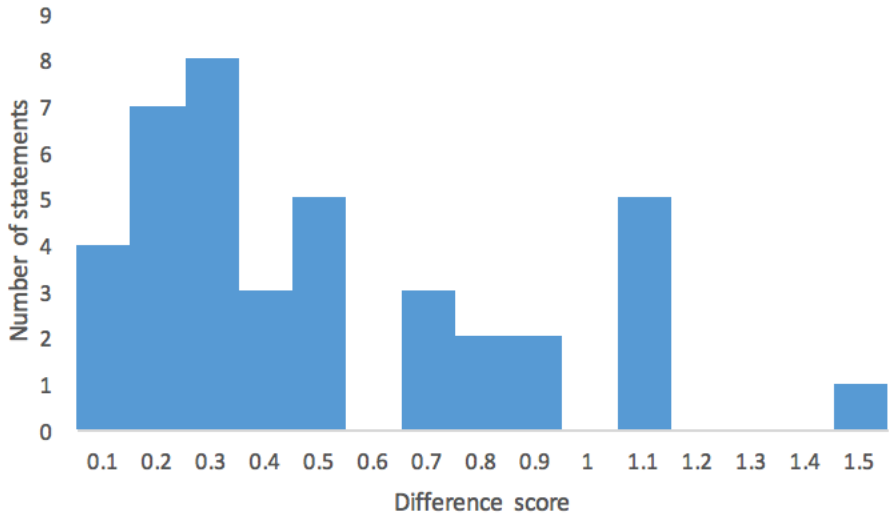


*Figure 11 Histogram of the Difference Scores of Perspective 2*

The statement that is most representative for perspective two can be found in Table 10 Statements less representative for Perspective 2: Responsibility-Shifters. From this, it becomes clear that the participants in this perspective do not want to have the responsibility over the security of the cloud service. In their opinion security is included in the service that they buy and as long as the provider takes this responsibility they trust it. Although there is a clear preference in this perspective to shift the responsibility towards the provider, it needs to be said that the high *difference score* is mostly because of the fact that the other two perspectives really disagree with it. Hence, the other statements with a relative high *difference score* will also be analysed.

*Table 9 Statements representative for Perspective 2: Responsibility-Shifters*

| Rank | Statement | Independent variable | Agree/ Disagree |
|---|---|---|---|
| 1 | Security of IT is the responsibility of the provider | Accountability | Agree |

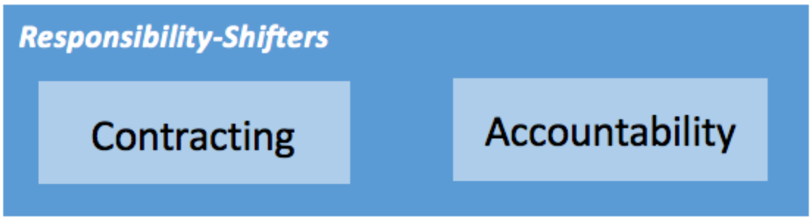
There is a cluster of five statements in the histogram that are less important than the first statement, but are still clearly more important than the rest of all statement. These statements are presented in Table 10. These statements show that this perspective really puts their trust into contracts. As long as everything is specified in a contract, they trust it. This is closely related to the principle of responsibility, since contracts are the actual formalization of the distribution of responsibilities. Moreover, the responsibility-shifters do not really care about whether the service delivered is the same as the service promised, since they do not see the urgency for auditing. So, as long as the provider takes responsibility and this is all formalized in contracts, the participants in this perspective trust the cloud service.

*Table 10 Statements less representative for Perspective 2: Responsibility-Shifters*

| Rank | Statement | Independent variable | Agree/ Disagree |
|---|---|---|---|
| 2 | SLA's are sufficient to protect against costs related to downtime | Contracting | Agree |
| 3 | The service-level agreements (SLAs) of the provider are adequate to guarantee the availability and scalability | Contracting | Agree |
| 4 | It is hard to switch from one service provider to another | Interoperability | Disagree |
| 5 | Cloud services need to be audited by an independent third party | Auditing | Disagree |
| 6 | Standard vendor contracts do not come close to best practices for meeting customer data security needs | Contracting | Disagree |

In Appendix E more information about the participants within this perspective can be found. This information can provide some more context to the interpretation of the statements. From this, it can be concluded that this perspective includes significantly more participants from the IT consultancy sector. However, this does not show a direct and clear link towards the statements representative for this perspective.

Thus, because this perspective mainly focusses on shifting the responsibilities towards the provider, it is defined as the *responsibility-shifters*. The following two factors are the most representative for the *responsibility-shifters*:



### 5.2.3. Perspective 3: Operational-Conservatives

The histogram of this perspective is presented in Figure 12. The histogram clearly shows one gap, resulting in two statements being most representative for this perspective

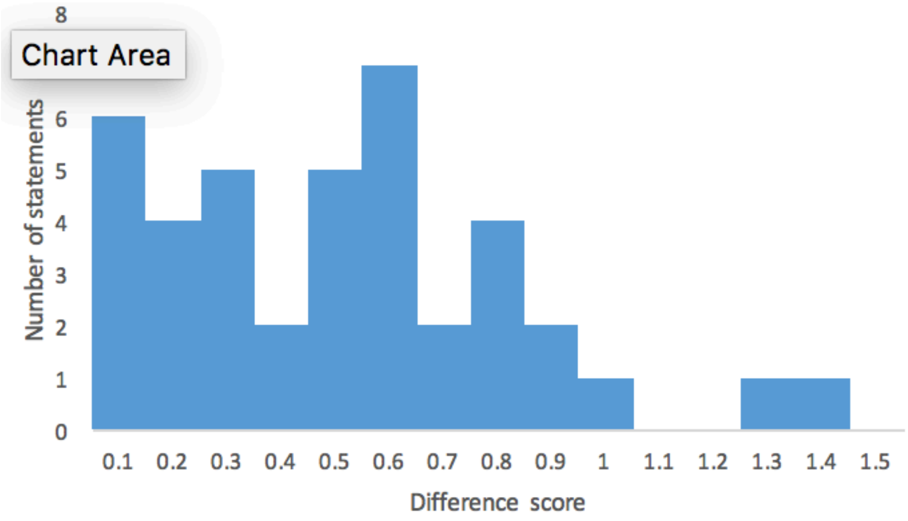


*Figure 12 Histogram of the Difference Scores of Perspective 3*

The statements that are most representative for perspective two can be found in Table 11. According to the operational-conservatives cloud computing is not the most important trend in enterprise IT. This can be because they think cloud computing is just not important, or that there are other more important trends. Either way, they do have no trust in cloud computing to offer significant IT advantages. Moreover, it seems that participants in this perspective have no problems with transparency, because there is no unclarity for them with respect to who the actual owner of the data.

*Table 11 Statements related to Perspective 3: Operational-Conservatives*

| Rank | Statement | Independent variable | Agree/ Disagree |
|---|---|---|---|
| 1 | Cloud computing is the most important trend in enterprise IT | Technological advantage | Disagree |
| 2 | Unclarity about who is the actual owner of the data is a problem that arises with cloud computing | Transparency | Disagree |

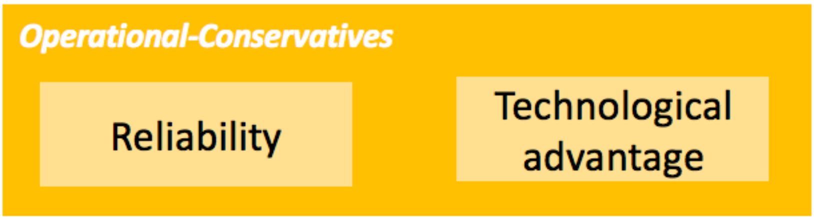
Since these two statements together are a little too limited to describe the complete perspective, also the statements with a *difference score* from 0,70 and higher will be taken into account. Although those statements are not directly really representative for the perspective, they can offer more insight about the context of the two statements that are considered being representative for the perspective. From the statements with a score of 0,70 of higher, it becomes clear that there is no trust in the interoperability (lack of standards) of the technology, no trust in the reliability the provider promises and no trust in the fact that the cloud is secure. In general, this can be taken together into the view that this perspective is not trusting cloud services because it can influence their day-to-day work. According to this perspective, everything goes fine as it is, and changing it by adopting a cloud services only brings risks with it. One of the participants belonging to this perspective stated that:

> *"How well designed the cloud offering is, outages are a fact of life, and you should be able to deal with them. The architecture of your business applications should take these risks into account, and mitigate them appropriately"*

This statement clearly shows a lack of trust because of the reliability of cloud services.

In Appendix E more information about the participants within this perspective can be found. This information can provide some more context to the interpretation of the statements. Where the other two perspectives consequently consisted of mostly participants from the technology and IT consultancy sector, this perspective has relatively more people from the retail sector. This means that this sector is more focussed on making actual products and thus operations are crucial and IT is really just a facilitator. This strokes with the earlier findings, where cloud computing is really not seen as an important trend and the most important thing is that people can just perform their day-to-day job without any disruptions because of changes in IT.

Thus, as this perspective really values operations and prefers to stick to the situation as-is, this perspective is defined as the *operational-conservatives*. The following two factors are the most representative for perspective 3:



Operational-Conservatives

Reliability

Technological advantage

## 5.3. Limitations

Although the Q-method was performed carefully, there still are some limitations with regard to the findings.

As also stated Chapter 3.5, Q-method will result in '*subjectively expressed, socially organized semantic patterns*', rather than scientific prove that certain causal relationships as presented in a conceptual model exist in reality. This means that the results as presented above should be interpreted as subjectively expressed, socially organized semantic patterns. In other words, the three perspectives that were found are the patterns in the viewpoint of the people related to the factors that influence the trust in a cloud service.

It also needs to be stated that it became clear during the Q-sorting that the statements that represented the concepts of security and privacy were often combined by participants; no clear distinction existed in their minds and the interpretation of those two factors mostly corresponded with the factor security. This meant that it is also hard to separate these concepts in the interpretation, because in the heads of the people they have overlapping definitions. It is most likely that this mix up of factors is the result of too vaguely defined statements.

## 5.4. Chapter conclusion

When the similarities and differences of the different perspectives are combined, the conceptual model as defined in Chapter 2.4 can be adapted to represent the results of the Q-method. This conceptual model is presented in Figure 13 Conceptual model of factors influencing trust according to Q-method study.

In general, it is perceived that the customer needs to perform certain actions before adopting a cloud service. The customer needs to make sure their organisation is ready and willing to make the change, as well as making sure that the cloud service they want to adopt is *secure* and provides *privacy* over their data. Having knowledge on the security and privacy of the cloud services increases trust. As all perspectives agree on the fact that also change from the customer is required, it can be concluded that organisational change is seen more as a condition that needs to be met in order to adopt cloud computing, than that it is seen as a factor influencing trust in a cloud service. Thus, the factor will be redefined to: *the willingness to change the organisation*. When an organisation is willing to change, adopting a cloud service is more easily trusted. Moreover, all perspectives seem to understand what a cloud service entails. A *transparent* cloud service gives the customer the trust in the provider's competence and goodwill.

Besides the general viewpoints, there are also viewpoints specific to the three perspectives. The first perspective is the perspective of the *techno-optimists*. In short, this group really sees cloud computing as the most important trend in enterprise IT. Because a cloud service can offer significant *technological advantages*, they are willing to trust it. But, a lack of *interoperability* is seen as an important issue: when it is not possible to change from one provider to another, trust in the cloud service will be limited. The second perspective is the perspective of the *responsibility-shifters*. In short, this group wants to make the provider *accountable* in case contingencies with the cloud service occur, preferably through the use of *contracts*. When a cloud service satisfies these conditions, they trust the cloud service. The third, and last perspective is the perspective of the *operational conservatives*. This group does not see cloud computing as an important trend or significant *technological advantage* and has its doubt with respect to the reliability; they prefer to keep things as they are. This perspective has a more negative viewpoint of cloud computing, but increasing the perception of the *technological advantage* and *reliability* will improve their trust in a cloud service.

This means that some factors from the initial conceptual model are not included. These are the factors jurisdiction, auditing, financial costs and sustainability. These factors do not play a role in the trust of customers in a cloud service.

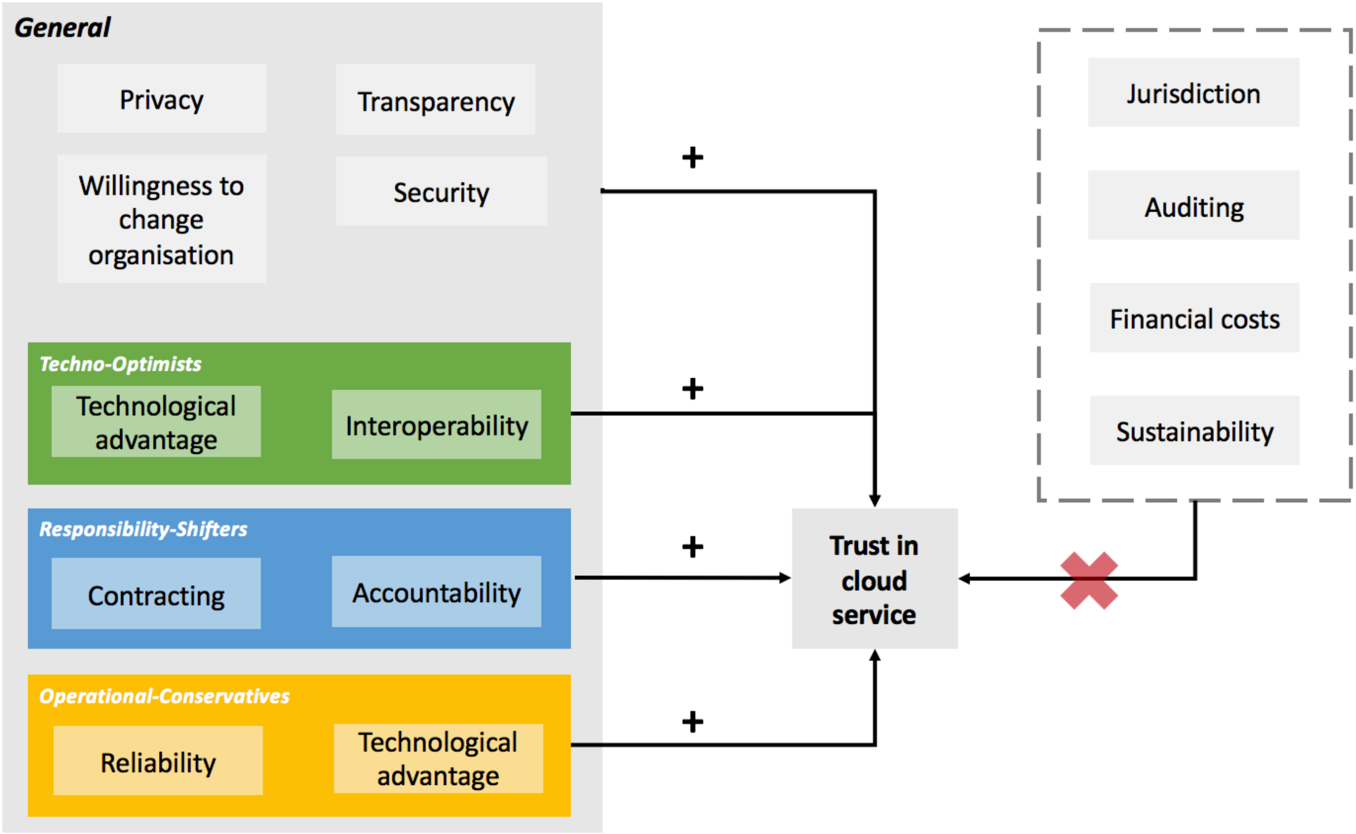


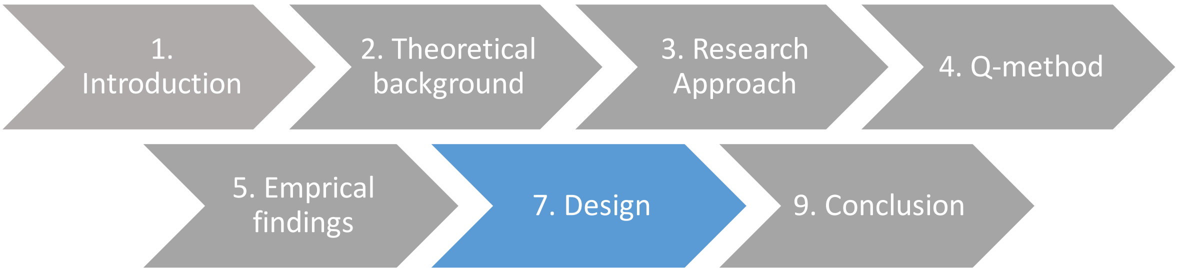
*Figure 13 Conceptual model of factors influencing trust according to Q-method study*

# Chapter 6 Design

In this chapter, the design will be elaborated upon. The design consists of the following:

- Design approach
- Definition of functional requirements
- Design space
- OPF Framework
- Implementation design
- Limitations
- Chapter conclusion

This chapter will use the empirical findings from the previous chapter to design an artifact that can improve the trust of (potential) cloud service customers. This will be done by creating a design space by defining the functional requirements. Then the components of the design space are the basis for the artifact that is designed: the OPF Framework, where OPF stands for **o**rganisation, **p**erspective and **f**actor. When this framework should be used during the adoption process, will then be discussed in the implementation design.



# 6. Design

## 6.1. Design approach

To come up with a design that contributes to solving the research problem, a design approach will be defined. This approach will guide the design of the artifact by specifying how the empirical findings from Chapter 5 can be translated into an artifact. The objective of this design is defined as: *to facilitate a cloud broker in the improvement of trust of a (potential) customer in a cloud service.*

Improving the trust of a customer in a provider can be initiated from both sides. Internally, a part of the customer's organisation can try to improve the trust in a cloud service by trying to improve trust in other parts of the organisation. Externally, the provider of the cloud service can try to improve trust. As can be seen in the actor analysis in Appendix A, there are two providers of cloud services: (1) cloud service providers and (2) cloud brokers. Cloud brokers have close contact with the customer and have the ability to integrate and customize cloud services according to the wishes of the customer. Furthermore, they gain direct benefits from an increased trust in a cloud service, because they are the once that can perform the migration and operation of the cloud service. These characteristics make the cloud broker the logical actor to improve the trust of a customer in a cloud service.

For the design of the artifact, the principles of TIP are be followed. This means that technological, institutional and process aspects will be taken into account in the design. The problem however, is that the concept of process is rather fluid and ambiguous, because it is a product of the technological artifact and context it is placed in (Bots & Daalen, 2012). Therefore, an artifact is designed that shapes this process, rather than that the process itself is designed. This leaves the T and I components for the design of the artifact.

While technical structures (being a subset of physical/material structures) shape physical processes, institutional structures (being a subset of social/psychological structures) shape decision-making processes (Bots & Daalen, 2012). When adopting cloud computing, both of those structures are relevant. However, this thesis is scoped around (the factors influencing) the trust of a customer in a cloud service. Since trust is a social concept, the artifact entails an institutional structure. Consequently, no physical artifact is designed.

This institutional framework includes both technical and institutional aspects in order to shape the process to improve trust in a cloud service. For this framework, first the requirements will be defined to function as input (see Figure 14). These requirements reflect the desires of the actor for whom it is designed, to ensure that there is actual value to be gained from the design.

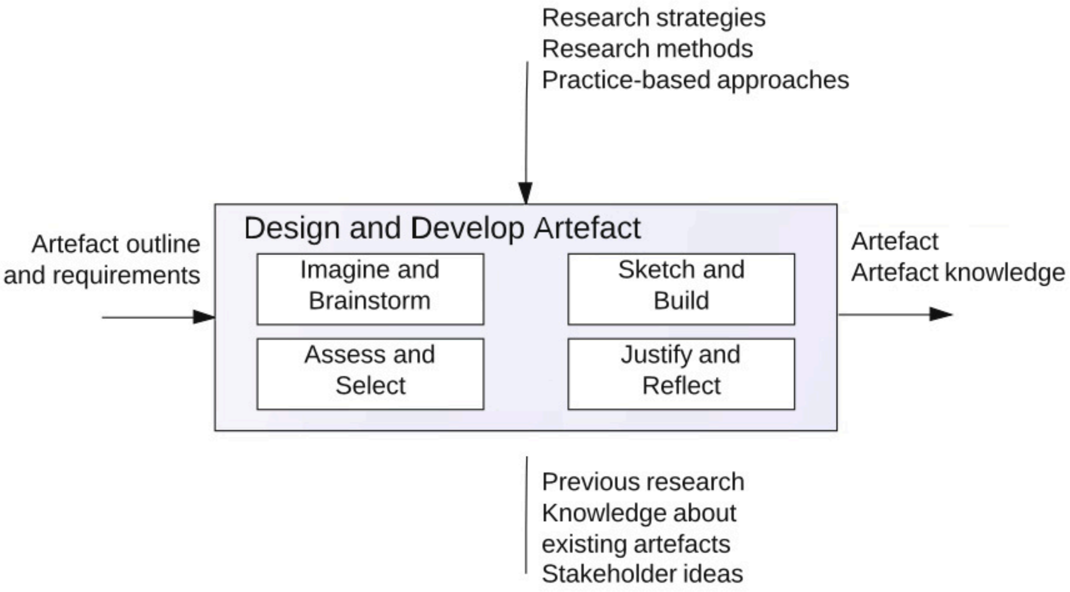


*Figure 14 Design and develop artifact (Johannesson & Perjons, 2014)*

Besides the requirements, also the results of the Q-method (research method) and the document analysis (previous research) will be used as input, as can be seen in Figure 14. This will be done in accordance with the theory on design science of Johannesson & Perjons (2014).

## 6.2. Definition of functional requirements

To design an artifact that effectively addresses the research problem, functional requirements are established. This section will address the following question:

> *"What artifact can be a solution for the explicated problem and which requirements on this artifact are important for the stakeholders?"*(Johannesson & Perjons, 2014, pp. 103)

So, before establishing the requirements, it is first important to define what the definition of requirement is and what the problem is for which requirements are established.

A requirement is a property of an artifact that is perceived as desirable by actors. It is used to guide the design of the artifact. Requirements can be split up in both functional and non-functional requirements. The functional requirements refer to the functions of the artifact and are dependent on the problem and needs of the actors. The non-functional requirements are non-functional and encompass desires with respect to structure and environment of the artifact. It is chosen not to include the non-functional requirements, since the desires and the environment of the artifact will depend on the actual application in practice of the artifact.

As stated in the problem definition in Chapter 1.1, an accelerated adoption of cloud computing in the industry can be observed, mainly because it can offer a wide variety of benefits. Nevertheless, trust management still proves to be one of the key challenges in the adoption of cloud computing. Also, with the market growing at an increasing pace, reliably identifying a trustworthy provider becomes harder. Research shows however, that an assurance of a higher degree of trust in a provider is required in order to attain efficient resource allocation and utilization and reach successful business outcomes. So, in order to adopt cloud computing and acquire its benefits, trust of the (potential) customer in a cloud service has to improve. The designed artifact should contribute to the solution of this problem.

With the empirical findings from Chapter 5 and the actor analysis in Appendix A, it becomes possible to define the requirements for an artifact that facilitates the cloud broker in improving the trust of the customer in a cloud service.

### 6.2.1. Requirement 1: Parts of the organisation

As can be seen in Appendix A, there are several parts of the customer's organisation relevant during the adoption of a cloud service. It is apparent that the customer has different parts within the organisation that are relevant during the cloud service adoption process. Hence, in order to increase the trust of an organisation in a cloud service, the different parts of the organisation need to be addressed. So, the root cause for this requirement can be defined as: there are different parts of the organisation involved when adopting a cloud service. Based on this finding, the following requirement is established:

> Requirement 1: The *framework* must enable the identification of the different **parts of the** customer's **organisation** and take their concerns and interest into account

### 6.2.2. Requirement 2: Perspectives

From the interpretation of the Q-method in Chapter 5.2 it became clear that there are several perspectives on trust in cloud services. Since the design aims to improve the trust in cloud services, the framework must include these perspectives in order to do so. So, the root cause for this requirement can be defined as: there are different perspectives on trust in a cloud service. Based on this finding, the following requirement is established:

> Requirement 2: The *framework* must enable the identification of the different **perspectives** among the relevant actors

### 6.2.3. Requirement 3: Factors

What also became clear from the interpretation of the Q-method in Chapter 5.2 is that there are general factors that influence the trust in a cloud service as well as factors that specifically relate to a perspective. In order to address the trust in a cloud service in general, all relevant factors need to be taken into consideration in the framework. Meaning that both the general factors and the factors specific to the perspectives that are present in an organisation need to be taken into consideration. So, the root cause for this requirement can be defined as: the different perspectives have different factors influencing trust in a cloud service. Based on this finding, the following requirement is established.

> Requirement 3: The *framework* must facilitate in addressing the relevant **factors** influencing trust in a cloud service

## 6.3. Design space

With the requirements established in the previous section, it is now a matter of defining how those requirements can be met in an artifact. One way of ensuring the requirements are adequately addressed in the framework is by translating them directly into a component of the design. Consequently, the design space of the framework that is to be designed can be defined as follows:

*Table 12 Design space*

| Requirement | Requirement 1 | Requirement 2 | Requirement 3 |
|---|---|---|---|
| | Parts of the organisation | Perspectives | Factors |
| Question | Which parts of the customer's organisation are directly involved during the adoption of a cloud service? | Which perspectives on trust in cloud services are there among the relevant actors? | What are the most important factors influencing the trust in cloud services for this organisation? |
| Function | Extract and analyse different parts of the organisation to better address the different perspectives within the organisation and their corresponding interests and needs | Determining which perspectives on trust in a cloud service there are and what these perspectives look like in accordance with the different parts of the organisation | Determining which factors are most important, both in general and specifically for the relevant perspective(s), and define what the implications are for each part of the organisation |
| Foundation | Organisational configurations theory (Mintzberg, 1989)(Appendix A) | Q-method | Q-method |
| Output | Internal involved actors and their corresponding interests | Perspective on trust in a cloud service for each part of the organisation | Factors influencing trust that are most important based on the perspectives among the actors |

Each requirement in the design space will function as a component of the design. These components will now be further elaborated upon.

### 6.3.1. Organisational component

The organisational component of the framework needs to assure the relevant parts of the organisation are involved. The framework needs to able to extract and analyse different parts of the organisation to better address the different perspectives within the organisation and their corresponding interests and needs. As a theoretical foundation, the organisational configuration theory of Mintzberg (1989) is used.

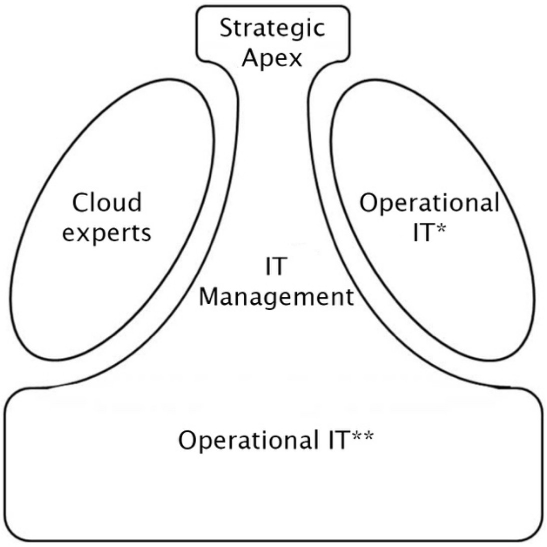


*Figure 15 Different parts of a customer organisation*

This theory divides an organisation in the strategic apex, middle line, core of operation, support staff and techno-structure. The strategic apex is highest in the hierarchy and will make the final decision whether to adopt cloud computing or not. Underneath their command, we find IT service management representing the middle line. IT service management is most likely in charge of the choice of which specific cloud service will be selected. Moreover, they coordinate and supervise the operational IT department, who are concerned with the day-to-day organisational IT tasks. Depending on the type of company, the operational IT department can be in the operating core or in the support staff. This depends on the core product or service that the organisation provides to its customers. When this is an IT service, the operational IT department** is part of the operating core, if not, the operational IT department* is part of the support staff. Lastly, the cloud expert team will analyse, design and plan for the potential cloud service adoption. The different parts of the customer organisation are schematically represented in Figure 15. A more elaborate analysis of the actors, including the different parts of a customer organisation can be found in Appendix A.

The output of the organisational component will consist of the following parts of the customer's organisation and their corresponding interests:

*Table 13 Parts of the organisation of a customer*

| *Actor* | *Objective* | *Function* |
|---|---|---|
| *Strategic Apex* | To ensure that the organization effectively serves its mission, and that it serves the needs of the people who control or have power over it | 1. Direct supervision (authorization of major decisions made by employees, resource allocation)<br>2. Managing the relationship with its environment (develop high level contacts, reaching major agreements with outside parties) |

| | | |
|---|---|---|
| | | 3. Development of the organisation’s strategy (maintain a pace of change that is responsive to the environment without being disruptive to the organization) |
| *IT Service Management (middle line)* | To ensure that the unit effectively serves its mission, and that it serves the needs of the people who control or have power over it | 4. Collect feedback information on the performance of its own unit and communicate it to the persons higher up the hierarchy (vertical coordination)<br>5. Coordinate with other managers (horizontal coordination)<br>6. Formulate strategy for own unit |
| *Operational IT Department (support staff or core of operation)* | To provide support to the organisation outside the direct work flow | 7. Provide the complete organisation with the required IT resources (hardware and software)<br>8. Maintain software and hardware<br>9. Provide IT support |
| *Cloud Experts (techno-structure)* | To adapt the organisation in order to meet environmental change | 10. Assess possibilities for adopting cloud computing<br>11. Migrate applications to the cloud<br>12. Standardize work processes in the cloud and transfer them to Operational IT Department |

### 6.3.2. Perspective component

The perspective component should facilitate in determining which perspectives on trust in a cloud service there are and what these perspectives look like in accordance with the different parts of the organisation. This will be done by presenting the three perspectives that were found through the use of the Q method and the interpretation of these results in Chapter 5.

The first perspective is the perspective of the *techno-optimists*. In short, this group really sees cloud computing as the most important trend in enterprise IT and for this reason trusts cloud services.  The second perspective is the perspective of the *responsibility-shifters*. In short, this group wants to shift all responsibilities towards the provider, preferably through the use of contracts. When this is possible, they trust the cloud service. The third, and last perspective is the perspective of the *operational conservatives*. This group does not see cloud computing as an important trend and has its doubt with respect to the reliability; they prefer to keep things as they are.

### 6.3.3. Factor component

In the factor component of the design, it should be determined which factors are most important, both in general and specifically for the relevant perspective(s), and define what the implications are for each part of the organisation.

For each part of the organisation, the general factors influencing trust in a cloud service are applicable, irrespectively their perspective. These general factors were defined as: security, privacy, transparency and the willingness to change the organisation. It became clear that participants were unable to make the distinction between the concepts of security and privacy using the statements in the Q-sort. For this reason, this is combined into the factor security in this design. Moreover, the factor willingness to change the organisation is more a characteristic of the customer itself and can't directly be changed by the cloud broker. So, in general, whatever the perspective of the part of the organisation is, these factors need to be addressed:

- Security
- Transparency

Then, depending on the perspective of each part of the organisation, other factors also need to be addressed. For the techno-optimists these are:

- Technological advantage
- Interoperability

For the responsibility-shifters these are:

- Contracting
- Accountability

And lastly, for the operational-conservatives these are:

- Technological advantage
- Reliability

Depending on the perspectives that are dominant in the different parts of the organisation, different factors need to be addressed. But also depending on the part of the organisation, the factors need to be addressed differently. The strategic apex will focus more on the strategic aspect of the factor, while the operational IT department will focus on the operational aspect of the factor, while IT service management and the cloud experts may focus on completely different other things. For example, the strategic apex may view interoperability as an issue because of vendor-lock in, while the operational IT department has to be worried about the interoperability between the on-premise applications and the applications in the cloud. Each combination of part of the organisation and perspective requires different issues related to trust to address. These trust issues can be presented in the form of key questions, that the customer wants to be answered in order to trust the cloud service. When a cloud service clearly provides answers and solutions to these key questions, trust will be improved.

## 6.4. OPF Framework

With the three components described in the previous section, the complete design can be defined. The framework will be called the OPF Framework, where OPF stands for *Organisation, Perspective and Factor*. The complete framework can be found in Appendix H. The separate table represents a different part of the organisation, while every colour represents a different perspective; grey for the general perspective, green for the techno-optimists, blue for the responsibility-shifters and yellow for the operational-conservatives. The key questions in the tables were derived from interviews and through reasoning in accordance with the organizational configuration theory in combination with the statements that represent the different perspectives.

The OPF Framework will be demonstrated by using a fictional organisation. This organisation has the following perspectives among the different parts of the organisation:

| | |
|---|---|
| • Strategic apex: | Techno-Optimists |
| • IT service management: | Responsibility-Shifters |
| • Operational IT: | Operational-Conservatives |
| • Cloud experts: | Techno-Optimists |

The OPF Framework for this organisation will look as follows:

*Table 14 Demonstration of OPF Framework*

| **Part of the organisation** | **Perspective** | **Perspective factors** | **General factors** |
|---|---|---|---|
| *Strategic Apex* | Techno-Optimist | Technological Advantage | Security |
| | | Interoperability | Transparency |
| *IT service management* | Responsibility-Shifters | Contracting | Security |
| | | Accountability | Transparency |
| *Operational IT department* | Operational-Conservatives | Technological Advantage | Security |
| | | Reliability | Transparency |
| *Cloud experts* | Techno-Optimist | Technological Advantage | Security |
| | | Interoperability | Transparency |

Each factor will have its own key questions per part of the organisation. This for example means that the key questions of technological advantage are different for the strategic apex and operational IT. For example, the for strategic apex, some of the key questions on technological advantage are:

1. Is cloud computing the right response to our changing environment or will it be disruptive for our organisation?
2. Should we allocate our IT resources outside of the organisation?
3. Does cloud computing really provide the benefits that are promised (on the long term)?

While for the operational IT department, key questions are:

- What hardware and software will still be necessary when cloud computing is adopted?
- What applications are capable to be moved into the cloud and have benefits from this?
- Will cloud computing provide benefits for our day-to-day tasks?

Thus, every combination of a perspective (and the factors related to it) and a part of the organisation, will result in different key questions. All these combinations and the key questions can be found in Appendix H in the complete OPF Framework.

## 6.5. Implementation design

The framework facilitates the improvement of trust of the customer in a cloud service. The actor that uses this framework is the cloud broker. Adopting cloud computing is a process that normally is done in several steps. It is important to define at which stages of this adoption the framework should be used in order to improve the trust of the specific actor. The three general activities that are important for cloud adoption are the following:

- Define strategy
- Assess applications and cloud services
- Migrate and deploy target applications

The A1 scheme of the IDEF0 model in Appendix I shows these three activities and how they are related to each other, together with the relevant inputs, outputs, controls and mechanisms/resources. Each of the separate activities will be discussed in this section.

### 6.5.1. Function A1: Define strategy

The first activity is the definition of the strategy. The strategic apex defines it core strategy that applies to the organisation as a whole. From this, the IT service management derives it specific cloud service. In order to increase the adoption of cloud services, the trust in cloud computing should be improved before those strategies are made. The activities, inputs, outputs, controls and mechanisms/resources related to this are presented in Figure 16.

This means that the strategic apex should be approached by the cloud broker in a process to improve trust, using the OPF Framework, before the core strategy is defined. In practice, organisations already have their core strategies defined and will not change it often, if they do it at all. However, when cloud computing does not fit into the core strategy of an organisation, cloud adoption will surely not be adopted. If this is the case because cloud services are not trusted by the strategic apex, the only way to realise cloud adoption for this organisation is to improve this trust. Although it should not be the focus of cloud brokers to convince organisations with a core strategy that is not in line with cloud computing, it is of importance to identify this has an impact on cloud adoption. If the core strategy is in line with cloud computing but does not specifically mention it, then there are better changes for the cloud broker to improve the trust in cloud services and realise the adoption of cloud computing.

IT service management needs to be included in the process of improving trust after the core strategy is defined, but before the cloud strategy is defined. Logically, only when the core strategy allows for cloud services to be adopted this is relevant, otherwise the cloud broker should go back to try to improve the trust of the strategic apex to change this core strategy. The extent to which cloud computing is adopted will mainly be decided by the IT service management. They will make decisions about for example the service model: Infrastructure as a Service, Platform as a Service or Software as a Service. Also, the amount of cloud services, the amount of cloud services and the amount of applications that will be moved to the cloud will be decided by the IT service management. In order to get high adoption rates for the organisation, trust in the cloud services should be high. So, before this cloud strategy is defined, the cloud broker should approach the IT service management in a process to improve trust while using the OPF Framework.

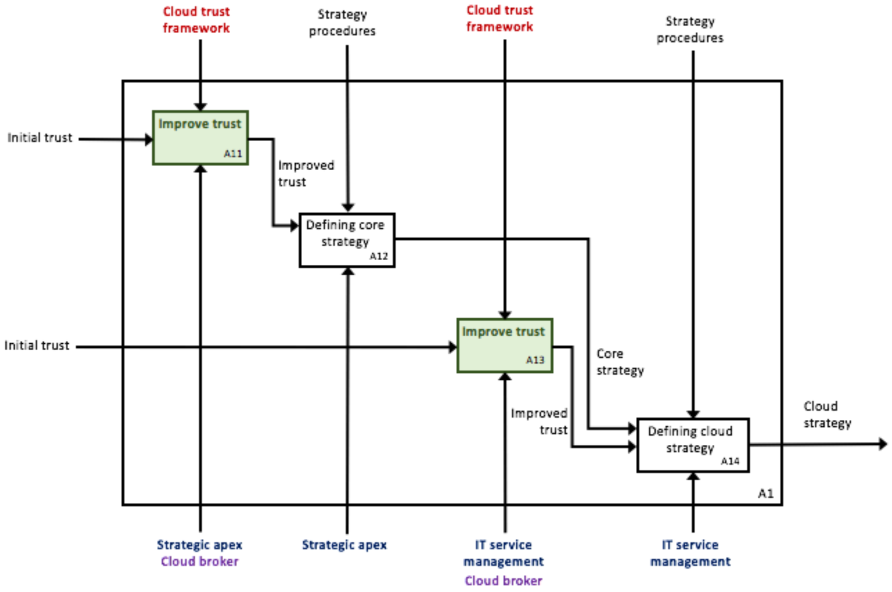


*Figure 16 IDEF0 model: A1 Define strategy*

### 6.5.2. Function A2: Assess applications & cloud services

The second activity is the assessment of applications and cloud services. Here it is assessed whether it is technically possible to move certain applications to the cloud and which cloud services are most fit for such an application. Even when an application can be moved to the cloud based on its technical characteristics, it is still the question whether it is profitable to do. So, for the relevant target applications, the business case will be defined that will show whether it is profitable to move the application to the cloud or not. When this is the case, a roadmap that will guide the migration of the application to the cloud will be defined. The activities, inputs, outputs, controls and mechanisms/resources related to this are presented in Figure 17.

This activity will mostly be performed by the cloud experts. In most large cloud projects the cloud broker is part of the cloud expert team, meaning that improving the trust in this stage should be easier than during the strategy defining activity. During all stages of assessing the applications and cloud services, it is important that there is trust of the cloud experts in cloud services. When this is not the case, the assessment is a more likely to be negative for most of the applications. On the other hand, when the trust in the cloud services is high, applications are more likely to be positively assessed for moving to the cloud. Thus, before the assessment starts, the cloud experts should be involved in the process of improving the trust in cloud services, while using the OPF Trust Framework.

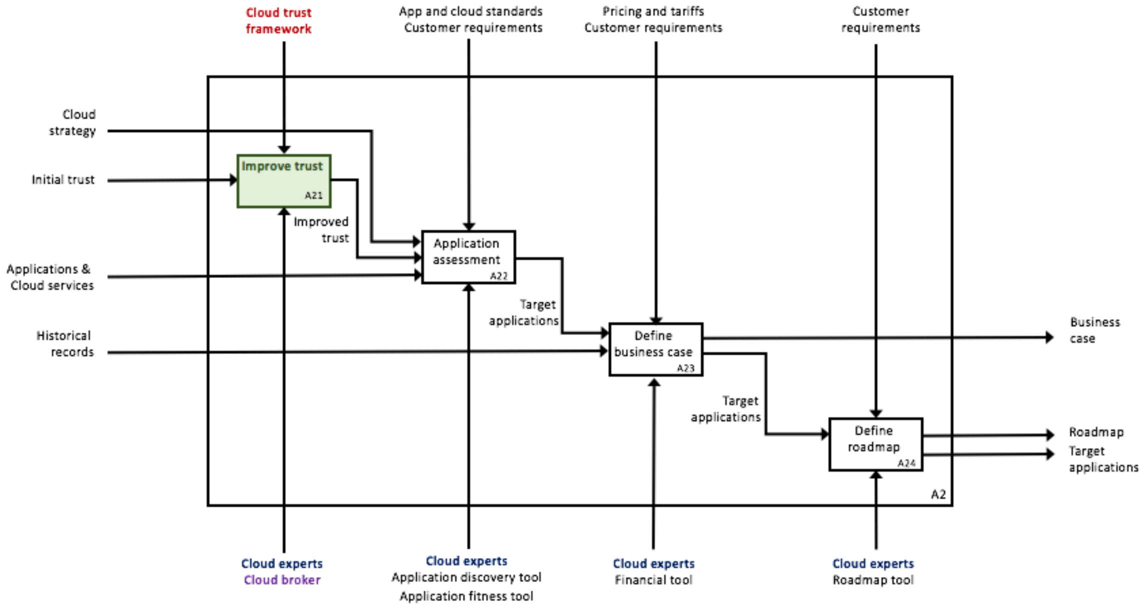


*Figure 17 IDEF0 model: A2 Assess applications & cloud services*

### 6.5.3. Function A3: Migrate and deploy target applications

The last activity is the migration and deployment of the target applications to the cloud. Here, the target application is migrated to the cloud. Then this application is tested and validated to make sure it works as it is supposed to work. When all test results are positive the application can be really deployed in the cloud. After this is done, the organisation completely adopted the cloud service. The activities, inputs, outputs, controls and mechanisms/resources related to this are presented in Figure 18.

This activity is done with the combined efforts of the cloud experts and operational IT. When this stage is reached, there is no real influence on the actual adoption of the cloud services anymore. This is only the execution and thus trust of the operational IT department is not that important for the adoption. However, when trust is low, cooperation will be low and transaction costs are generally low. This can impact the speed and costs of the adoption. Thus, before the operational IT department gets involved in the adoption process it is important to improve the trust in cloud services. So, before the applications are actually migrated, the operational IT department should be involved in a process to improve their trust in cloud service, while using the OPF Framework.

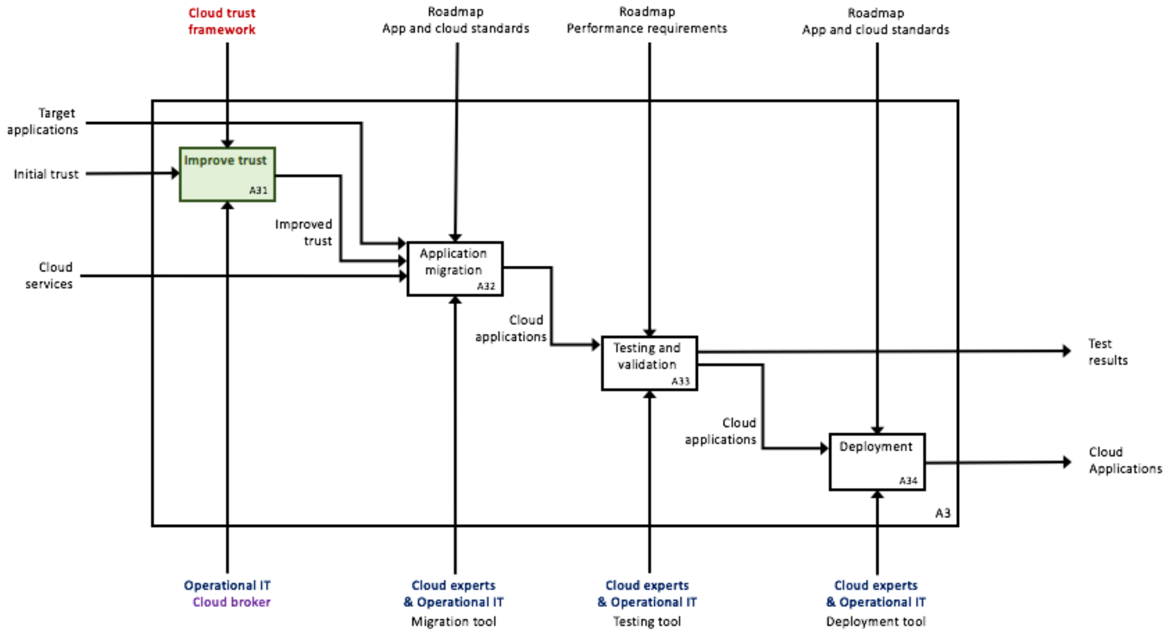


*Figure 18 IDEF0 model: A3 Migrate and deploy target applications*

## 6.6. Limitations

The design aims to facilitate in the improvement of trust in a cloud service. This means that it is not a step-by-step plan that guarantees improvement of trust. The OPF Framework describes key concerns that are likely to arise in different parts of the organisation of a (potential) customers when they are looking at trust in a cloud service from a certain perspective. These key concerns are an indication of the concerns they most likely will have, but that does not mean no other concerns exist. Consequently, cloud brokers can use this framework as a basis during cloud adoption projects, rather than as a complete tool to improve trust. So, they will need to extend it with their own findings relevant for their field of work for it to be useful.

It also has to be stated that trust is not something that is improved instantly by this design. Trust is hard to gain, but easy to lose. So, although the implementation design describes that the cloud broker should initiate the interaction with the different parts of the organisation before they get involved in the cloud adoption process, it doesn't mean this process stops when the adoption process is started. Improving trust is an ongoing process, and the OPF framework will only be effective when it is used before, but certainly also during the cloud adoption process.

## 6.7. Chapter conclusion

The OPF Framework as presented in this chapter provides cloud broker with a tool to improve the trust of (potential) customers in a cloud service. The implementation design gives the cloud broker insight in when to approach which part of the organisation.

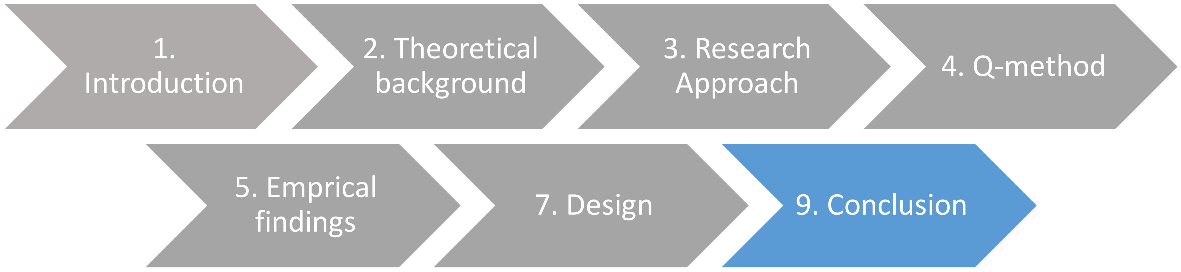
Although the design provides the possibility to improve the trust of the strategic apex and the operational IT department, it seems that improving the trust of the IT service management and the cloud experts is most effective. These are the actors that make the crucial decisions with respect to cloud computing. The strategic apex makes decisions concerning the core strategy, and is not directly concerned with cloud computing, while the operational IT department just needs to follow the directions they get from the IT service management. So, improving their trust in a cloud service is less effective than improving the trust of IT service management and the cloud experts.

# Chapter 7 Conclusion

In this chapter, the conclusions of this thesis will be elaborated upon. The conclusion consists of the following:

- Conclusion
- Discussion

The main conclusions of this thesis will be discussed first. After that, the conclusions will be discussed by reflecting on the scientific and practical relevance, the limitations of the research and the directions for future research.



# 7. Conclusion

## 7.1. Conclusion

In the first Chapter, the main research question of the proposed research was defined as:

*"What are the factors that influence the trust of an organisation in a cloud service and what are the different perspectives and how can this trust be improved?"*

To answer this main research question, several sub questions were defined. By answering all of these sub question, it is possible to establish an answer to the main research question.

- **What is the current state of trust in a cloud computing service? (Chapter 2.1-2.3)**

Cloud computing can provide a variety of benefits for organisations, such as scalability, ubiquitous network access, decreased effort in managing technology and cost savings. On the other hand, there are also numerous challenges and uncertainties that have to be overcome in order to reach the promised benefits. One of the key challenges of adopting cloud computing is related to trust. Trust is defined as: *an organisation's dynamic, calculated and dependent expectation of the other organisation's competence and goodwill*. Trust is necessary for effective collaboration between customers and providers and reducing transaction costs, however, in practice this trust is often lacking. From the scientific literature, it becomes clear that there is still a lot of ambiguity about trust in cloud services and that it is unclear which factors influence this trust. At least, there is no empirical research that aims to explain the factors that influence trust in a cloud service. Since cloud computing is subject to a lot of ambiguity and multiple perspectives exist, it is also expected there are multiple perspectives related to the factors that influence trust (i.e. a certain factor may be relevant for trusting a cloud service to one (sub)group, while this factor is irrelevant for another (sub)group). These perspectives are not yet defined in scientific literature. Additionally, no scientifically based design exists that aims to improve the trust of (potential) customers in a cloud service.

- **How can the factors influencing trust in cloud computing services be analysed and structured? (Chapter 3 & 4)**

According to scientific literature there is a large number of factors that influence trust. The scientific literature provides the input for the conceptual model that describes the factors influencing trust in a cloud service. This conceptual model is used as a guide for performing the empirical research. The research method to perform this empirical research is Q-method. Q-method is primarily an explorative technique, that can bring some coherence to research questions with many complex and socially contested answers. In this case it can provide some structure and patterns in the opinions and perspectives of practitioners on the factors influencing trust in a cloud service. This Q-method is done with 25 participants from the IT consultancy, retail and technology sectors. The outcomes of the statistical analysis of the Q-method consist of a number of factors, in this case three, that represent the perspectives on trust in a cloud service. Each perspective is represented by the statements it strongly agrees and disagrees with, relative to the other perspectives. These statements in their turn represent the different factors. This results in factors that are relevant for all perspectives, factors that are specifically relevant to one or two perspectives and factors that are irrelevant for all perspectives.

- **Which factors influence the trust in a cloud computing service? (Chapter 2 & 5)**

**1.1. Which potential factors are found in the literature? (Chapter 2.4.2)**

According to the scientific literature the following factors influence the trust in a cloud computing service: contracting, auditing, jurisdiction, privacy, accountability, interoperability, transparency, organisational change, financial costs, technological advantage, sustainability, security and reliability. Here jurisdiction relates to whether a cloud service makes use of datacentres in jurisdictions that can be intrusive under local law or common practices. Accountability relates to the degree the provider is willing to be responsible for any problems or damages related to the cloud service. Organisational change relates to the amount of organisational change that is required to adopt cloud computing: the more organisational change is required, the less trust in a cloud service. All other factors are self-explanatory.

**1.2. What does a conceptual trust model that describes the potential factors influencing trust look like? (Chapter 2.4.3)**

The conceptual model that describes the potential factors influencing trust is defined as follows:

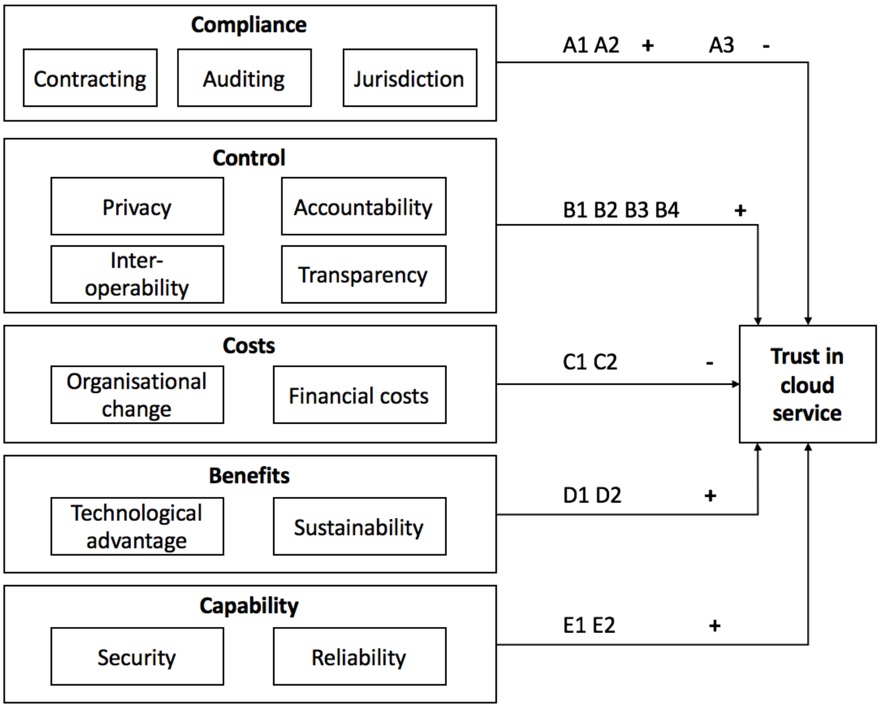


*Figure 19 Conceptual trust model*

This means all factors except *jurisdiction*, *organisational change* and *financial costs* have a positive influence on the trust in a cloud service.

### 1.3. What are the factors influencing trust in a cloud computing service according to empirical research? (Chapter 5)

The Q-method shows that there are several factors that are relevant for all perspectives. In general, it is perceived that the customer needs to perform certain actions before adopting a cloud service. The customer needs to make sure their organisation is ready and willing to make the change, as well as making sure that the cloud service they want to adopt is *secure* and provides *privacy* over their data. Having knowledge on the security and privacy of the cloud services increases trust. As all perspectives agree on the fact that also change from the customer is required, it can be concluded that organisational change is seen more as a condition that needs to be met in order to adopt cloud computing, than that it is seen as a factor influencing trust in a cloud service. Thus, the factor will be redefined to: *the willingness to change the organisation*. When an organisation is willing to change, adopting a cloud service is more easily trusted. Moreover, all perspectives seem to understand what a cloud service entails. A *transparent* cloud service gives the customer the trust in the provider's competence and goodwill.

The factors technological advantage, interoperability, contracting, accountability and reliability were the factors that are relevant for one (or two) of the perspectives.

This means that jurisdiction, auditing, financial costs and sustainability are not relevant factors that influence the trust in a cloud service. The complete overview of the factors influencing trust can be found in Figure 20. Here also the perspectives are included, which will be addressed in the answer to the next sub question.

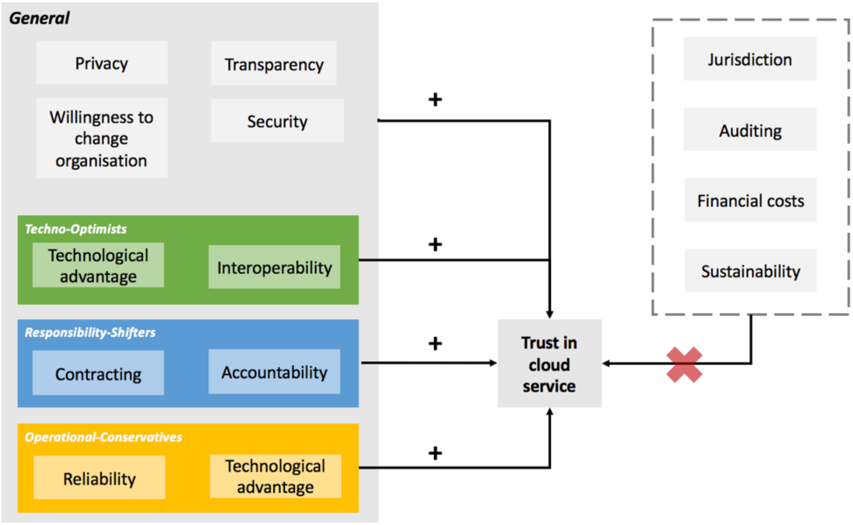


*Figure 20 Factors influencing trust in a cloud service according to empirical research*

- **What are the perspectives on trust in a cloud service? (Chapter 5)**

As a result of the Q-method, three perspectives on trust in a cloud service were found. The first perspective is the perspective of the *techno-optimists.* In short, this group really sees cloud computing as the most important trend in enterprise IT. Because a cloud service can offer significant *technological advantages*, they are willing to trust it. But, a lack of *interoperability* is seen as an important issue: when it is not possible to change from one provider to another, trust in the cloud service will be limited. The second perspective is the perspective of the *responsibility-shifters*. In short, this group wants to make the provider *accountable* in case contingencies with the cloud service occur, preferably through the use of *contracts*. When a cloud service satisfies these conditions, they trust the cloud service. The third, and last perspective is the perspective of the *operational conservatives*. This group does not see cloud computing as an important trend or significant *technological advantage* and has its doubt with respect to the reliability; they prefer to keep things as they are. This perspective has a more negative viewpoint of cloud computing, but increasing the perception of the *technological advantage* and *reliability* will improve their trust in a cloud service. The perspectives are also included in Figure 20.

- **What does a design look like that facilitates the improvement of trust, based on the perspectives? (Chapter 6)**

The artifact that is designed is a framework, called the OPF Trust Cloud Framework, accompanied with an implementation design. Three functional requirements are defined that the design needs to fulfil:

Requirement 1: The *framework* must enable the identification of the different **parts of the** customer **organisation** and take their concerns and interest into account

Requirement 2: The *framework* must enable the identification of the different **perspectives** among the relevant actors

Requirement 3: The *framework* must facilitate the prioritization of the **factors** influencing trust according to the distribution of perspectives among the different actors

These three requirements are translated into components for the actual design, to ensure that they are adequately addressed. This means that the parts of the organisation, the perspectives and the factors are the components of the framework. The combination of the parts of the organisation with the perspectives require a different focus for the cloud broker in order to improve trust. This focus is made specific by defining key questions. These are the key questions that the part of the organisation, when looking at trust in cloud from a specific perspective, wants to see answered before it trusts a cloud service and is willing to adopt it. The implementation design describes when these key questions need to be answered by the cloud broker. In general, before any decisions are done or activities are started by a certain part of the organisation, the cloud broker should engage with them in a process to improve the trust in a cloud service. The cloud broker uses the OPF Framework as a tool to support the activity of improving the trust.

- **Main research question: what are the factors that influence the trust of an organisation in a cloud service and what are the different perspectives and how can this trust be improved?**

The answers to the sub questions as defined previously, function as the components towards defining an answer to the main research question. In order to effectively address the main research question, a better understanding of the concepts of cloud computing and trust, and how the combination of those concepts can be researched is required. For the context of this research, trust is defined as an organisation's dynamic, calculated and dependent expectation of the other organisation's competence and goodwill. By using Q-method as research method, it is possible to establish structure and patterns in the opinions and perspectives of practitioners on the factors influencing trust in a cloud service. The Q-method research found there are different kind of factors that influence trust of an organisation in a cloud service. There are factors that are shared among all people in an organisation. And there are factors that are only relevant to certain perspectives that exist within an organisation.

The general factors, relevant for all people, are security (which includes privacy), transparency and willingness to change the organisation. The factors that are only relevant to a certain perspective are technological advantage and interoperability for techno-optimists, contracting and accountability for responsibility-shifters and reliability and (the lack of) technological advantage for operational-conservatives.

Trust in a cloud service can be improved by a cloud broker by addressing the main concerns of the different parts of the organisation (i.e. strategic apex, cloud service management, operational IT department and cloud experts) of a (potential) cloud service customer. These main concerns are different for each perspective. Process-wise, this needs to be done before the different parts of the organisation fulfil their part in the cloud adoption process. With four parts of the organisation, that can have three different perspectives, an organisation has 64 potential ways of being structured. Designing an artifact that guides each of these structures would be too much and unnecessary. So, the OPF framework has been designed that provides the main concerns for each part of the organisation for each perspective. This way the cloud broker can specify these according to the organisation they are dealing with, and extend it where possible and necessary. Addressing these concerns should improve the trust of that organisation in the cloud service.

*In short, the answer to the main research question can be defined as:*

Trust in a cloud service is approached from three perspectives in practice: techno-optimists, responsibility-shifters and operational conservatives. In general, all of these perspectives perceive security and transparency as factors that influence their trust in a cloud service. On top of that, techno-optimists perceive technological advantage and interoperability as important, responsibility-shifters perceive contracting and accountability as important and operational conservatives perceive reliability and (the lack of) technological advantage as important. The OPF Framework as proposed in this thesis uses these perspectives in combination with the different parts of the organisation: strategic apex, cloud service management, operational IT department and cloud experts. By addressing the main concerns of the specific part of the organisation, in combination with the relevant perspective, it is possible to improve the trust of an organisation in a cloud service.

## 7.2. Discussion

This section will reflect on this thesis, by discussing the scientific relevance, practical relevance, limitations and directions for future research.

### 7.2.1. Scientific relevance

The literature review that is done for this research confirms that trust is an important facilitator for successful business relationships and an important technology adoption determinant, but that trust has received little attention in the context of cloud computing, which results in a lack of understanding of the factors influencing the trust in a cloud service. While there is research that tries to define factors influencing the trust in a cloud service through literature studies, empirical research still is lacking. Moreover, conceptual trust model for cloud computing were developed, including security, usability, reliability, auditability, interoperability, accountability and controllability with the aim to provide a basis for further (empirical) research. This thesis contributes to the scientific body of knowledge by building upon existing conceptual trust models and literature researches with empirical research on the factors influencing trust in a cloud service.

To make sure the results of the diagnostic research, or more specifically opinion research, are generalizable, Q-method is used. Q-method is the combination of philosophy, concepts, data-gathering procedures, and statistical methods that provides a thoroughly elaborated foundation for examining human subjectivity in a structured way (Brown, 2008). Additionally, the design will be done according to the theory of Johannesson & Perjons (2014) and in accordance with the principles of TIP (Bots & Daalen, 2012). A combination of the organisational configuration theory of Mintzberg (1989) and the empirical findings from the Q-method will be used as input for the design. So, by basing all parts of the thesis on scientific theories and methods, the scientific value is secured.

### 7.2.2. Practical relevance

From interviews with practitioners in the field of cloud computing it becomes clear that there still is resistance from organisations to adopt cloud computing. Certainly, in the field of IT consultancy (where the consultancy company often advices organisations to adopt cloud computing and functions in the role of cloud broker) there is the perception that a lack of trust in cloud services exists.

First, for a cloud broker it is valuable to get a better understanding on which factors are important for different organisations in order to trust a cloud service. This can help them in selecting the right cloud services to the right organisations.

Moreover, the design will help cloud brokers in addressing the right factor in the right way on the right moment. Key questions related to a certain factor and a certain part of the organisation will facilitate the cloud broker in improving the trust.

Additionally, modelling the activities and decisions during a cloud adoption project and implementing the activity of improving trust there, provides cloud brokers with the knowledge on when to approach which part of the organisation.

### 7.2.3. Reflection and limitations

The reflection on this research can be categorised into four categories: research approach, research execution, research design and wider implications.

### Research approach

With Q-method, the Q-sort of the participants only reflects their opinions at that specific moment. So, this leaves open the possibility that individuals may change their minds over time, making the results of this Q-method less relevant. Moreover, Q-method will result in *subjectively expressed, socially organized semantic patterns*, rather than scientific prove that certain causal relationships as presented in a conceptual model exist in reality.

Additionally, when performing the Q-sorting, both the method and the instructions need to be explained to the participants, because most of them are unfamiliar with it. Validity can therefore be affected when the participant's lack of comprehension leads to misunderstandings. This will even more so be the case when the Q-sorting is not done face to face, but rather through an online tool. This done with five participants. Although instructions may be structured and a step-by-step process has to be followed, there is no possibility for the participants to ask questions when anything is unclear. Furthermore, when the Q-sorting is done through an online tool, the context of their sorting will be unclear, since the opportunity to explain their reasoning is limited in this tool.

### Research execution

The concourse was established by only using online sources, such as blogs, whitepapers and scientific articles. However, getting opinions directly from people in the field through interviews may have given other perspectives and making the concourse more complete and representative.

During the Q-sorting it became clear that the statements that represented the concepts of security and privacy were often combined by participants; no clear distinction existed in their minds and the interpretation of those two factors mostly corresponded with the factor security. This meant that it is also hard to separate these concepts in the interpretation, because in the heads of the people they have overlapping definitions. It is most likely that this mix up of factors is the result of too vaguely defined statements. Additionally, the perspective of the *operational-conservatives* is not as clearly distinguishable from the statements as the other two. It mostly seems that they just have the opposite opinion from the other two perspectives on their most important statements.

### Research design

The design aims to facilitate in the improvement of trust in a cloud service. This means that it is not a step-by-step plan that guarantees improvement of trust. The OPF Framework only describes some key questions that different parts of the organisation of a (potential) customers may have when they are looking at trust in a cloud service from a certain perspective. These key questions are just an indication of the concerns they most likely will have, but that does not mean no other concerns exist. Consequently, cloud brokers can use this framework as a basis during cloud adoption projects, rather than as a complete tool to improve trust. So, they will need to extend it with their own findings relevant for their field of work for it to be useful.

Reflecting on the design, it also has to be said that trust is not something that is improved instantly. Trust is hard to gain, but easy to lose. So, although the implementation design describes that the cloud broker should initiate the interaction with the different parts of the organisation before they get involved in the cloud adoption process, it doesn't mean this process stops when the adoption process is started. Improving trust is an ongoing process, and the OPF framework will only be effective when it is used before, but certainly also during the cloud adoption process.

Besides, the research design has not been applied in a real-life case yet. Applying it in practice can result in discussions about the viability of the design and issues related to the implementation of it before and during the cloud adoption process.

#### Wider implications

For this research, a specific scope was set in order to keep the research doable and generalizable within certain boundaries (e.g. large organisations, cloud computing, etc.). However, the findings from this thesis can also have wider implications outside of the boundaries of the scope.

First of all, the research had its boundaries around public cloud. However, to a certain extent, the findings of this research can also be translated to the private cloud. The biggest difference between the public and private cloud is the fact that there is no external cloud service provider in the private cloud service model. This means that the perspectives of the techno-optimists and operational-conservatives would still be valid, since the technology and implications for day-to-day work will be the same. However, the responsibility-shifters would be in a different situation. Since responsibility and accountability cannot be shifted towards an external party, it is less likely that they will trust a cloud service. So, responsibility-shifters will still be relevant, but their role in the adoption of public cloud will be different.

The same comparison can be done for IT outsourcing in general. Here, there is an external service provider, and thus the role of the responsibility-shifters will stay the same: as long as the service provider takes all responsibility and accountability, responsibility-shifters are fine with trusting the outsourcing. Instead, IT outsourcing can exist of many different information technologies, which will influence the role that techno-optimists and operational-conservatives will have. The more advanced and promising the technology, the more techno-optimists will trust an outsourced technology. On the other hand, the more implications an outsourced technology has on the day-to-day activities, the less likely the operational-conservatives are to trust it.

### 7.2.4. Directions for future research

#### Validation

Within practice-oriented research, there are five possible steps in the so-called *intervention cycle*: problem analysis, diagnosis, design, intervention/change and evaluation. This intervention cycle is a model to solve practical problems, rather than a model to carry out empirical research. A practice-oriented research can contribute to any of these five. Based on the characteristics of the defined problem and objective of this research, this research mainly focused on the diagnosis, followed up by some design. As a consequence, the intervention/change and evaluation steps are still open for research. As a first logical step, the findings and the design should be validated.

First, future research can focus on the validation of the findings. This can be done by performing a survey or expert validation. With a survey, it is possible to validate certain aspects of the findings of the Q-method. It is for example, possible to set up questions concerning the factors influencing the trust in a cloud service. When the outcomes of this survey are comparable with the ones received from the Q-method, the findings are valid. The survey can also provide additional insights in the findings gained from the Q-method. While Q-method provides the perspectives, it is not defined what the distribution of those perspectives is. The Q-method only gives all the relevant perspectives that exist, but does not say anything about how common those perspectives are. Thus, surveys may provide more insight in this. Additionally, expert validation can be used to validate the findings. When experts can recognise and confirm the findings of this research, the findings can be considered valid. Since cloud brokers (e.g. Accenture) work in different projects and with different organisations, it is likely that the employees of the cloud broker have experienced different point of views with regard to trust in cloud services. Thus, using those people as the experts during the expert validation would be a logical start. From there on, different organisations that did or did not adopt cloud computing should be approached in order to also validate the findings with experience from cloud service customers themselves.

After the findings are validated, the design should be validated. To do this, a pilot can be set up in which a cloud brokers makes use of the OPF framework during the (potential) adoption of a cloud service. Since the framework does not require large structural changes in the process, but rather just adds a step before any action is taken by the relevant parts of the organisation, the consequences will be minor when it turns out the framework fails. Thus, the framework can be used without large risks. When the pilot is finished, certain lessons will be learned. These lessons should be applied when redesigning the framework. This process can be repeated until the framework is complete, usable and effective for the cloud broker to improve trust of (potential) cloud service customers in a cloud service.

### Expanding or narrowing the scope

Additionally, the research as performed in this thesis has a specific scope. Expanding this scope can provide new insights and contribute to the body of scientific knowledge. Future research can focus on other sectors, such as for example banking and government. Moreover, instead of taking large organisations as the subject of research, SME's and start-ups can be researched. Lastly, it was chosen to research twelve potential factors influencing trust in a cloud service. However, literature provided a lot more options. Instead of looking at the characteristics of the cloud service, it is also possible to look at the characteristics of the provider. Hence, researching factors such as brand, reputation, firm size, marketing, etcetera.

Moreover, future research can also narrow down the scope. It was chosen for this research not to make a distinction between the different deployment models (IaaS, PaaS and SaaS). However, it is possible that there are relevant differences between the deployment models if it comes to trusting a certain cloud service. Future research can focus on mapping these differences.

### Process design

Lastly, this research lacks a process design. Several moments of intervention were established with the help of the IDEF0 model, however, how the actual process of improving trust should be performed falls outside the scope of the design. Future research can establish a process design that helps cloud brokers in the actual process of improving the trust of the (potential) customer.

# 8. References

Abawajy, J. (2009). Determining service trustworthiness in intercloud computing environments. *I-SPAN 2009 - The 10th International Symposium on Pervasive Systems, Algorithms, and Networks*, 784–788. http://doi.org/10.1109/I-SPAN.2009.155

Abdelmaboud, A., Jawawi, D. N. A., Ghani, I., Elsafi, A., & Kitchenham, B. (2015). Quality of service approaches in cloud computing: A systematic mapping study. *Journal of Systems and Software*, *101*, 159–179. http://doi.org/10.1016/j.jss.2014.12.015

Alhamad, M., Dillon, T., & Chang, E. (2010). Conceptual SLA framework for cloud computing. *4th IEEE International Conference on Digital Ecosystems and Technologies - Conference Proceedings of IEEE-DEST 2010, DEST 2010*, 606–610. http://doi.org/10.1109/DEST.2010.5610586

Amazon. (2017). Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … Stoica, I. (2010). A View of Cloud Computing. *Communication of the ACM*, *53*(4), 50–58.

Blomqvist, K. (1997). The many faces of trust. *Scandinavian Journal of Management*, *13*(3), 271–286. http://doi.org/10.1016/S0956-5221(97)84644-1

Böhm, M., Leimeister, S., Riedl, C., & Krcmar, H. (2011). Cloud Computing – Outsourcing 2.0 or a new Business Model for IT Provisioning? *Application Management*, 3–29. http://doi.org/10.1007/978-3-8349-6492-2

Bots, P. W. G., & Daalen, C. van. (2012). Designing socio-technical systems: Structures and processes, (June), 18–20. Retrieved from http://www.cesun2012.tudelft.nl/images/e/e9/Bots.pdf

Breivold, H. P. (2015). Architecting for the Cloud : A Systematic Review. In *Proceedings - 17th IEEE International Conference on Computational Science and Engineering* (pp. 312–318). http://doi.org/10.1109/CSE.2014.85

Brown, S. R. (1993). A primer on Q methodology. *Operant Subjectivity*, *16*(3/4), 91–138. http://doi.org/10.1177/104973239600600408

Brown, S. R. (2008). Document analysis. In *The Sage Encyclopedia of Qualitative Research Methods* (pp. 699–702). http://doi.org/10.4135/9781412963909

Chambers, D. (2010). Windows Azure: Using Windows Azure's Service Bus to Solve Data Security Issues, (July). Retrieved from http://archive.org/stream/windowsazureusin00cham/windowsazureusin00cham_djvu.txt

Chen, C. C., & Nakayama, M. (2016). Key factors increasing the trust and intention to adopt standard cloud-based applications. *International Journal of Information Systems and Change Management*, *8*(2), 144–159. http://doi.org/10.1504/IJISCM.2016.079566

Chiles, T. H., & McMackin, J. F. (1996). Integrating variable risk preferences, trust, and transaction cost economics. *Acadamy of Management Review*, *21*(1), 73–99.

Chu, R., Lai, I. K. W., & Lai, D. C. F. (2013). Trust factors influencing the adoption of cloud-based interorganizational systems: A conceptual model. *Engineering, Management Science and Innovation (ICEMSI), 2013 International Conference on*, 1–3. http://doi.org/10.1109/ICEMSI.2013.6914006

David, S. (2016). Emerging Hybrid Cloud Patterns.

Doney, M., & Cannon, J. P. (1997). Trust Examination of the Nature of in Buyer-Seller Relationship for assistance. *Journal of Marketing*, *61*(2), 35–51.

Eldred, M., Adams, C., & Good, A. (2015). Trust challenges in a high performance cloud computing project. *Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom, 2015–Febru*(February), 1045–1050. http://doi.org/10.1109/CloudCom.2014.21

Firdhous, M., Ghazali, O., Hassan, S., & Member, S. (2011). A Trust Computing Mechanism for Cloud Computing with Multilevel Thresholding. *Architecture*, 457–461.

Gartner. (2017). *Top Strategic Predictions for 2017 and Beyond: Surviving the Storm-Winds of Digital Disruption.*

Giessmann, A., & Stanoevska-Slabeva, K. (2013). Business Models of Platform as a Service (PaaS) Providers: Current State and Future Directions. *Journal of Information Technology Theory and Application*, *13*(4), 31–55. Retrieved from http://aisel.aisnet.org/jitta/vol13/iss4/4/

Habib, S. M., Ries, S., & Mühlhäuser, M. (2010). Cloud computing landscape and research challenges regarding trust and reputation. *Proceedings - Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing in Conjunction with the UIC 2010 and ATC 2010 Conferences, UIC-ATC 2010*, 410–415. http://doi.org/10.1109/UIC-ATC.2010.48

Habib, S. M., Ries, S., Mühlhäuser, M., & Varikkattu, P. (2014). Towards a trust management system for cloud computing marketplaces: using CAIQ as a trust information source. *SECURITY AND COMMUNICATION NETWORKS*, *7*, 2185–2200.

Hani, A. F. M., Paputungan, I. V., & Hassan, M. F. (2015). Renegotiation in Service Level Agreement Management for a Cloud-Based System. *ACM Computing Surveys*, *47*(3), 1–21. http://doi.org/10.1145/2716319

Hofmann, P., & Woods, D. (2010). Cloud computing: The limits of public clouds for business applications. *IEEE Internet Computing*, *14*(6), 90–93. http://doi.org/10.1109/MIC.2010.136

Hsu, P., Ray, S., & Li-Hsieh, Y.-Y. (2014). Examining cloud computing adoption intention , pricing mechanism , and deployment model. *International Journal of Information Management*, *34*(4), 474–488. http://doi.org/10.1016/j.ijinfomgt.2014.04.006

ISSSS. (2017). Q-methodology. Retrieved March 31, 2017, from https://qmethod.org/

Jamshidi, P., Ahmad, A., & Pahl, C. (2013). Cloud Migration Research: A Systematic Review. *IEEE Transactions on Cloud Computing*, *1*(2), 142–157. http://doi.org/10.1109/TCC.2013.10

Javadi, B., Abawajy, J., & Buyya, R. (2012). Failure-aware resource provisioning for hybrid Cloud infrastructure. *J. Parallel Distrib. Comput.*, *72*(10), 1318–1331. http://doi.org/10.1016/j.jpdc.2012.06.012

Joha, A., & Janssen, M. (2012). Transformation to Cloud Services Sourcing : Required IT Governance Capabilities. *ICST Transactions on E-Business*, *12*(7–9), 1–12. http://doi.org/10.4108/eb.2012.07-09.e4

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science. Springer International Publishing Switzerland*. http://doi.org/10.1007/978-3-319-10632-8

Katulic, T., & Vojkovic, G. (2016). From safe harbour to European data protection reform. *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2016 - Proceedings*, 1447–1451. http://doi.org/10.1109/MIPRO.2016.7522367

Keahey, K., Armstrong, P., Bresnahan, J., LaBissoniere, D., & Riteau, P. (2012). Infrastructure outsourcing in multi-cloud environment. *Proceedings of the 2012 Workshop on Cloud Services, Federation, and the 8th Open Cirrus Summit*, 33. http://doi.org/10.1145/2378975.2378984

Kerridgecs. (2017). History of Cloud Computing Timeline. Retrieved July 17, 2017, from https://cdn2.hubspot.net/hubfs/620276/History_of_Cloud_Computing_Timeline.pdf?t=1488486871142

Khajeh-hosseini, A., Greenwood, D., Smith, J. W., & Sommerville, I. (2012). The Cloud Adoption Toolkit :

supporting cloud adoption decisions in the enterprise. *Software - Practice and Experience*, *42*(4), 447–465. http://doi.org/10.1002/spe

Ko, R. K. L., Lee, B. S., & Pearson, S. (2011). Towards Achieving Accountability, Auditability and Trust in Cloud Computing, 432–444. http://doi.org/10.1007/978-3-642-22726-4_45

Lansing, J., & Sunyaev, A. (2016). Trust in Cloud Computing: Conceptual Typology and Trust-Building Antecedents. *ACM SIGMIS Database*, *47*(2), 58–96. http://doi.org/10.1145/2963175.2963179

Leimeister, S., Riedl, C., Bohm, M., & Krcmar, H. (2010). The Business Perspective of Cloud Computing, Actors, Roles, and Value Networks.

Lewicki, R. J., & Bunker, B. B. (1996). Developing and Maintaining Trust in Work Relationships. *Trust in Organizations: Frontiers of Theory and Research*, (November), 114–139. http://doi.org/10.4135/9781452243610.n7

Manuel, P. (2015). A trust model of cloud computing based on Quality of Service. *Annals of Operations Research*, *233*(1), 281–292. http://doi.org/10.1007/s10479-013-1380-x

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2014). Cloud computing — The business perspective ☆. *Decision Support Systems*, *51*(1), 176–189. http://doi.org/10.1016/j.dss.2010.12.006

Mintzberg, H. (1989). The structuring of organizations. *Readings in Strategic Management*, 322–352. http://doi.org/10.1007/978-1-349-20317-8_23

Mourad, M. B. Al, & Hussain, M. (2014). The Impact of Cloud Computing on ITIL Service Strategy Processes. *International Journal of Computer and Communication Engineering*, *3*(5), 367–371. http://doi.org/10.7763/IJCCE.2014.V3.351

Müller, A., Ludwig, A., & Franczyk, B. (2017). Data security in decentralized cloud systems – system comparison, requirements analysis and organizational levels. *Journal of Cloud Computing*, *6*(1), 15. http://doi.org/10.1186/s13677-017-0082-3

Neto, M. D. (2014). A brief history of cloud computing. Retrieved September 2, 2017, from https://www.ibm.com/blogs/cloud-computing/2014/03/a-brief-history-of-cloud-computing-3/

Noor, T. H., Sheng, Q. Z., Zeadally, S., & Yu, J. (2013). Trust management of services in cloud environments: Obstacles and solutions. *ACM Computing Surveys*, *46*(1), 1–30. http://doi.org/10.1145/2522968.2522980

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Information & Management Assessing the determinants of cloud computing adoption : An analysis of the manufacturing and services sectors. *Information & Management*, *51*(5), 497–510. http://doi.org/10.1016/j.im.2014.03.006

Opara-Martins, J., Sahandi, R., & Tian, F. (2015). Critical review of vendor lock-in and its impact on adoption of cloud computing. *International Conference on Information Society, I-Society 2014*, 92–97. http://doi.org/10.1109/i-Society.2014.7009018

Paraiso, F., Merle, P., & Seinturier, L. (2016). soCloud: a service-oriented component-based PaaS for managing portability, provisioning, elasticity, and high availability across multiple clouds. *Computing*, *98*(5), 539–565. http://doi.org/10.1007/s00607-014-0421-x

Pearson, S., & Charlesworth, A. (2009). Accountability as a Way Forward for Privacy Protection in the Cloud Abstract : Accountability as a Way Forward for Privacy Protection in the Cloud, (December), 131–144. http://doi.org/10.1007/978-3-642-10665-1

Plummer, D. (2012). The Business Landscape of Cloud Computing. *Gartner*, 1–41.

Prasad, A., & Green, P. (2015). Governing cloud computing services : Reconsideration of IT governance structures. *International Journal of Accounting Information Systems*, *19*, 45–58. http://doi.org/10.1016/j.accinf.2015.11.004

Qi, C., & Chau, P. Y. K. (2013). Investigating the roles of interpersonal and interorganizational trust in IT outsourcing success. *Information Technology & People*, *26*(2), 120–145. http://doi.org/10.1108/ITP-09-2012-0088

Radwan, T., Azer, M. A., & Abdelbaki, N. (2017). Cloud computing security: challenges and future trends. *International Journal of Computer Applications in Technology*, *55*(2), 158. http://doi.org/10.1504/IJCAT.2017.082865

Rahi, S. B., Bisui, S., & Misra, S. C. (2017). Identifying the moderating effect of trust on the adoption of cloud-based services. *International Journal of Communication Systems*, *30*(11), 1–19. http://doi.org/10.1002/dac.3253

Rajendran, S. (2013). Organizational Challenges in Cloud Adoption and Enablers of Cloud Transition Program. *Mit*, *145*(January), 1–49. http://doi.org/10.1136/emj.2010.096966

Ramlo, S., & Newman, I. (2011). Q Methodology and Its Position in the Mixed-Methods Continuum. Operant Subjectivity: *The International Journal of Q Methodology*, *34*(3), 173–192.

Razaque, A., & Rizvi, S. S. (2017). Privacy preserving model : a new scheme for auditing cloud stakeholders, 1–17. http://doi.org/10.1186/s13677-017-0076-1

Ross, P., & Blumenstein, M. (2013). Cloud computing: the nexus of strategy and technology. *Journal of Business Strategy*, *34*(4), 39–47. http://doi.org/10.1108/JBS-10-2012-0061

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393–404. http://doi.org/10.5465/AMR.1998.926617

Schmolk, P. (2014). PQMethod Manual.

Solove, D. J., & Washington, G. (2008). *Understanding Privacy*.

Stenner, P., & Rogers, R. S. (2004). Q Methodology and qualiquantology: the example of discriminating between emotions. *Mixing Methods in Psychology. The Integration of Qualitative and Quantitative Methods in Theory and Practice*, (February), 101–117. http://doi.org/10.4324/9780203645727

Stephenson, W. (1952). Some observations on Q technique. *Psychological Bulletin*, *49*(4), 483–498. http://doi.org/10.1037/h0057171

Uusitalo, I., Karppinen, K., Juhola, A., & Savola, R. (2010). Trust and cloud services - An interview study. *Proceedings - 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010*, 712–720. http://doi.org/10.1109/CloudCom.2010.41

Venters, W., & Whitley, E. (2012). A Critical Review of Cloud Computing : Researching Desires and Realities A Critical Review of Cloud Computing : Researching Desires and Realities. *Journal of Information Technology*, *27*(3), 179–197. http://doi.org/10.1057/jit.2012.17

Verschuren, P., & Doorewaard, H. (2010). *Designing a Research Project* (2nd ed.). The Hague: Eleven International Publishing.

Wang, C., Chow, S. S. M., Wang, Q., Ren, K., & Lou, W. (2013). Privacy-Preserving Public Auditing for Secure Cloud Storage. *IEEE Transactions On Computers*, *62*(2), 362–375.

Wang, H. (2016). Decision Models for Cloud Computing. *Grid, Cloud, & Cluster Computing*, 28–32.

Watts, S., & Stenner, P. (2005). Doing Q methodology: theory, method and interpretation. *Qualitative Research in Psychology*, *2*(1), 67–91. http://doi.org/10.1191/1478088705qp022oa

Williamson, O. E. (1981). The Economics of Organization: The Transaction Cost Approach. *American Journal of Sociology*. http://doi.org/10.1086/227496

Wu, L., & Buyya, R. (2010). Service level agreement (SLA) in utility computing systems. *arXiv Preprint* *arXiv:1010.2881*, 27. http://doi.org/10.4018/978-1-60960-794-4.ch001

Yigitbasioglu, O. (2014). Modelling the Intention to Adopt Cloud Computing Services: A Transaction Costs Theory Perspective. *Australasian Journal of Information Systems*, *18*(3), 331–345.

Yigitbasioglu, O., Mackenzie, K., & Low, R. (2013). Cloud Computing: How does it differ from IT outsourcing and what are the implications for practice and research? *The International Journal of Digital Accounting Research*, *13*(April), 99–121. http://doi.org/10.4192/1577-8517-v13

Yongsiriwit, K. (2016). A Semantic Framework Supporting Cloud Resource Descriptions Interoperability. http://doi.org/10.1109/CLOUD.2016.81

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. http://doi.org/10.2307/2640350

Zakarya, M., & Gillam, L. (2017). Energy Efficient Computing, Clusters, Grids and Clouds: A Taxonomy and Survey. *Sustainable Computing: Informatics and Systems*, *14*, 13–33. http://doi.org/10.1016/j.suscom.2017.03.002

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. http://doi.org/10.1016/j.future.2010.12.006

# 9. Appendix

## A. Actor analysis

To get a better understanding of the relevant actors and their roles and interest during the adoption of a cloud service, an actor analysis is performed. This analysis can be found in Figure 21.

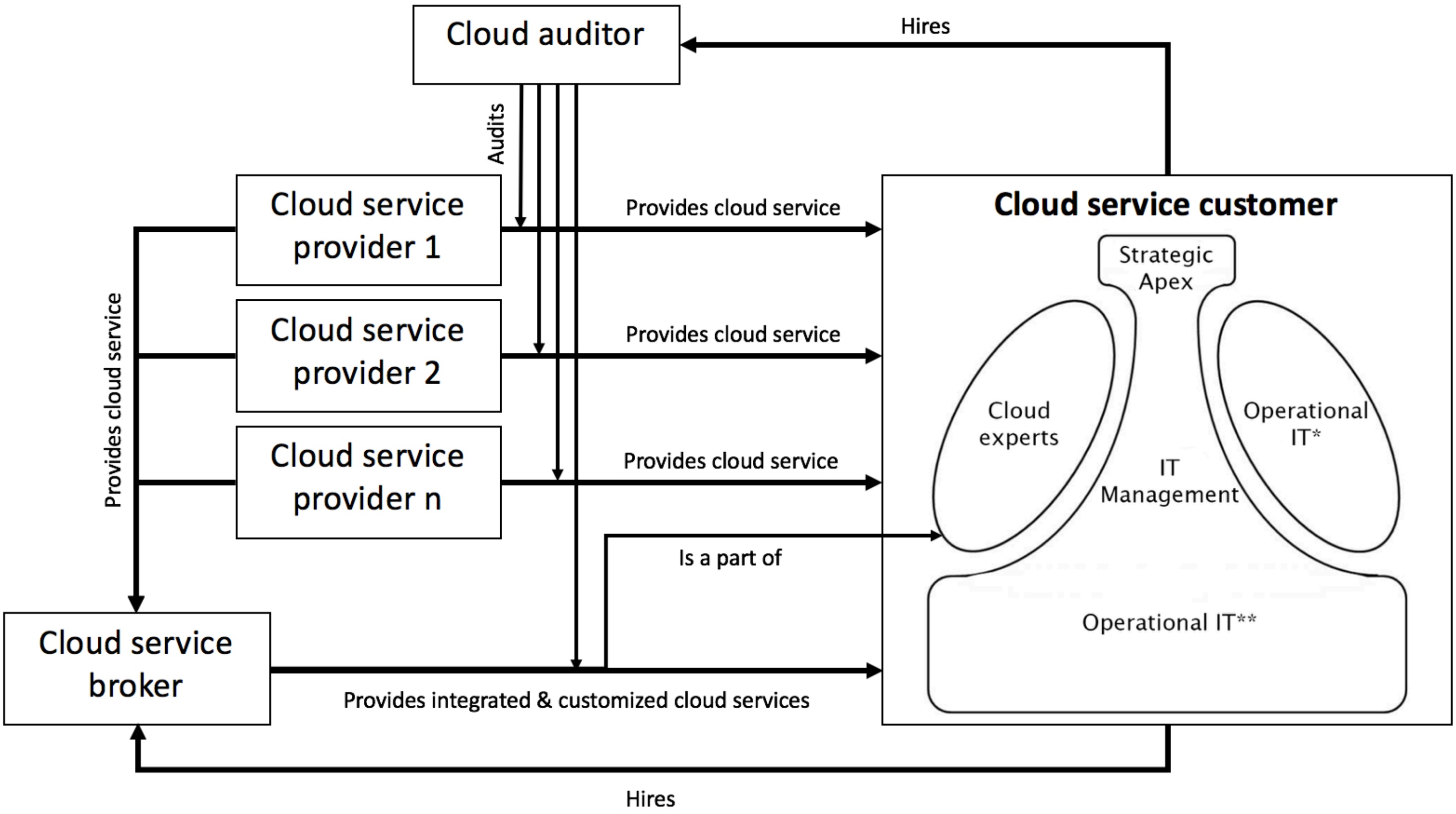


Figure 21 Visual representation of actor analysis

When a cloud service is adopted, mainly four actors are involved. There are potentially many other actors involved such as for example governments, financers, legislators, etc. but those actors fall outside the scope of this thesis.

First of all, there is the customer. This is the actor that will consume and pay the cloud service. The provider exists of several parts. These parts of the organisation are structured according to the organisational configurations theory of (Mintzberg, 1989). This theory describes an organisation that consist of a *core of operation*, who do the basic work of producing the products and services and an administrative part of managers who coordinate their work. Management occurs at both the *middle line*, as well as at the top of the hierarchy; the *strategic apex*. Furthermore, there is a *techno-structure*, where analysts standardize and analyse to help the organisation adapt to its environment. Lastly, the support staff supports the functioning of the operating core indirectly, so outside the normal flow of operating work.

Strategic apex is highest in the hierarchy and will make the final decision whether to adopt cloud computing or not. Underneath their command, we find IT service management. IT service management is most likely in charge of the choice of which specific cloud service will be selected. Moreover, they coordinate and supervise the operational IT department, who are concerned with the day-to-day organisational IT tasks. Depending on the type of company, the operational IT department can be in the operating core or in the support staff. This depends on the core product or service that the organisation provides to its customers. When this is an IT service, the operational IT department** is part of the operating core, if not, the operational IT department* is part of the support staff. Lastly, the cloud expert team will analyse, design and plan for the potential cloud service adoption. The power, objective and function of each of these parts of the organisation can be found in Table 15.

Second, there are the providers. They are the actors that design and develop the cloud services. There are several large providers such as Amazon[4], Google[5] and Microsoft[6]. But, there are also smaller organisations that offer cloud services. Also, organisations with their own private datacentres look for opportunities for providing their excess computational power to other organisations. However, for this thesis, no distinction will be made between the types of providers.

Third, there are the cloud service brokers. Cloud service brokers can make it less expensive, easier, safer and more productive for customers to navigate, integrate, consume and extend cloud services (Plummer, 2012). This is particularly the case when customers make use of multiple and diverse cloud services. Cloud service brokers can be seen as a specialized form of the provider, offering a new service by integrating pre-existing cloud services to the customers. For this reason, they are both the customer (from the perspective of the provider) and a provider (from the perspective of the customer) (Leimeister et al., 2010).

Last, there are the cloud auditors. Customers can delegate the inspection of a cloud service to a third-party: the cloud auditor. In that case, the customer, the provider and the cloud auditor would negotiate a trilateral agreement where the provider agrees to inspections of the cloud auditor, which they then report to the customer (Plummer, 2012).

[4] https://aws.amazon.com/

[5] https://cloud.google.com

[6] https://azure.microsoft.com

*Table 15 Parts of the organisation of a customer based on* Mintzberg (1989)

| *Actor* | *Power* | *Objective* | *Function* |
|---|---|---|---|
| *Strategic Apex* | High | To ensure that the organization effectively serves its mission, and that it serves the needs of the people who control or have power over it | 1. Direct supervision (authorization of major decisions made by employees, resource allocation)<br>2. Managing the relationship with its environment (develop high level contacts, reaching major agreements with outside parties)<br>3. Development of the organisation's strategy (maintain a pace of change that is responsive to the environment without being disruptive to the organization) |
| *IT Service Management (middle line)* | High | To ensure that the unit effectively serves its mission, and that it serves the needs of the people who control or have power over it | 1. Collect feedback information on the performance of its own unit and communicate it to the persons higher up the hierarchy (vertical coordination)<br>2. Coordinate with other managers (horizontal coordination)<br>3. Formulate strategy for own unit |
| *Operational IT Department (support staff or core of operation)* | Low | To provide support to the organisation outside the direct work flow | 1. Provide the complete organisation with the required IT resources (hardware and software)<br>2. Maintain software and hardware<br>3. Provide IT support |
| *Cloud Experts (techno-structure)* | Medium | To adapt the organisation in order to meet environmental change | 1. Assess possibilities for adopting cloud computing<br>2. Migrate applications to the cloud<br>3. Standardize work processes in the cloud and transfer them to Operational IT Department |

## B. Concourse

The concourse is compiled from all kinds of sources, including from talks with practitioners. Therefore, not all statements are accompanied with a source, because they are opinions of people who were engaged with face-to-face or are considered as such general statements that no reference is necessary.

1. Cloud computing is the most hyped trend in enterprise IT
2. Cloud computing is the most important trend in enterprise IT
3. The adoption of cloud computing is more than just a shift in technology
4. In the future, everything will be in the cloud
5. Cloud computing is a form of IT outsourcing (Yigitbasioglu, 2014)
6. Cloud computing is a risk
7. Adopting cloud computing requires a change in the organisation’s culture
8. Private clouds are preferred over public clouds
9. Jobs will be lost when a move towards the cloud is made
10. Providers attempt to limit your ability to negotiate SLAs
11. IT has struggled to align the vision and promise of cloud computing[7]
12. For cloud adoption to succeed, an approach is needed that aligns strategy with a pragmatic approach to implementation, measured against business and organizational outcomes[8]
13. Cloud computing is adopted because we think it enhances innovation
14. Cloud computing has positive environmental impacts due to its carbon abatement potential
15. Lack of control over IT is the biggest challenge
16. Providers do not use the data that is entrusted to them inappropriately
17. Providers build in privacy and data protection principles into their services
18. Sensitive private information may not be stored on a public cloud
19. Users of cloud computing services should have communication processes capable of quickly and effectively notifying data owners about any potential breach in security[9]
20. In the case of highly sensitive data, it's important to encrypt it before storing it in the cloud[10]
21. Particularly in a model like clouds, organisations should care about the service provider’s authentication systems that grant access to data[11]
22. Data and applications in the cloud cannot be accessed by unauthorized individuals or parties

[7] https://www.networkworld.com/article/2364273/cloud-computing/aligning-cloud-vision-with-adoption.html

[8] https://www.networkworld.com/article/2364273/cloud-computing/aligning-cloud-vision-with-adoption.html

[9] https://www.computerworld.com/article/2859496/do-you-know-the-laws-that-govern-personal-information-in-the-cloud.html

[10] https://www.networkworld.com/article/2686975/public-cloud/cloud-failures-will-happen-are-you-ready.html

[11] http://www.enterprisefeatures.com/common-threats-cloud-computing-security/

23. Data in the cloud is (should be) destroyed when it is no longer needed
24. Security is not only the responsibility of the provider
25. Standard vendor contracts do not come close to best practices for meeting customer data security needs[12]
26. The ease with which cloud-computing services can be acquired by a business process owner (often the only thing needed is a credit card) can result in traditional IT and procurement controls being bypassed[13]
27. Security should result from a cycle, no static security
28. Security should be incorporated as an essential element of information systems and networks
29. It is important that providers allow client-auditing of their security offerings
30. Giving more attention for specifying human resource requirements, since security can also be compromised by malicious insiders
31. Providers should not use third party providers to deliver the cloud service
32. The security of the provider itself is important for the overall security of the cloud service
33. As data is the pedestal for providing Cloud Computing services, trusted data integrity is a fundamental task
34. There is a big risk data will be lost because of a technical failure
35. The provider can compensate for any failure
36. A cloud outage would be a big problem for the organisation
37. 99,999% (five nines) reliability is necessary
38. Outages in the cloud are always a possibility and thus the customer should have procedures in place to migrate this risk
39. It's not desirable that all applications are moved to the cloud
40. A cloud disaster recovery plan is absolutely necessary
41. SLA's are sufficient to protect against costs related to downtime
42. Back up at least your mission-critical information to a local server[14]
43. If your business cannot afford to go offline for a short period, you might want to consider a business interruption insurance[15]
44. Resources should be available at all the time to the authorised person
45. Clouds that limit visibility result in significant operational and financial issues (e.g. performance problems, challenges reporting to management, and unexpected bills)[16]

[12] https://www.computerworld.com/article/2483868/cloud-computing/nasa-s-cloud-audit-holds-value-for-all.html

[13] https://www.computerworld.com/article/2483868/cloud-computing/nasa-s-cloud-audit-holds-value-for-all.html

[14] https://www.networkworld.com/article/2686975/public-cloud/cloud-failures-will-happen-are-you-ready.html

[15] https://www.networkworld.com/article/2686975/public-cloud/cloud-failures-will-happen-are-you-ready.html

[16] http://www.businesscloudnews.com/2015/08/24/businesses-are-ready-for-cloud-but-lack-of-transparency-is-limiting-its-usefulness/

46. On-demand access to necessary reports to make compliance and audit processes easier are necessary[17]
47. providers need to simplify the process for ensuring advanced security and compliance in the cloud[18]
48. Customers can use data to make better purchasing decisions[19]
49. The agreements made in the Service Level Agreements are clear
50. Compliance reporting, breach notification and transparency into provider processes and procedures are important for presenting secure cloud
51. Providers should be asked about their backup and retention strategies, encryption, data disposal procedures, and business continuity in the contract.
52. The cloud is a black box into which the enterprise dumps its applications, data, workloads and processes[20]
53. Once a specific provider is chosen it is hard to switch
54. There should be standards for cloud services to increase interoperability
55. The absence of interoperability has become a barrier to adoption
56. Organisations want the freedom to switch between providers
57. Organisations should use more than one provider
58. It's a good thing cloud computing is centralized around three big players (Amazon, Google and Microsoft)
59. The public cloud should be combined with a private cloud
60. It's a problem that many providers prohibit or otherwise restrict access to data or the ability to transfer data between cloud environments
61. The limitation to transfer data from one cloud service to another is a legal issue rather than a technical issue
62. Latency is minimised because servers are hosted as close as possible
63. The location of the cloud is irrelevant
64. Because of the location of the datacentre cases will be adjudicated in favourable jurisdictions
65. Governments can be intrusive under the local law or under accepted local practices
66. Resources should be spread across multiple zones
67. IT should know the specifics of what's where
68. The provider should not use datacentres in regions prone to natural disasters
69. The provider should not use datacentres in regions with low technical maturity (e.g. power grid maturity, type of fibre)
70. Cloud services need to be audited by an independent third party

[17] http://www.businesscloudnews.com/2015/08/24/businesses-are-ready-for-cloud-but-lack-of-transparency-is-limiting-its-usefulness/

[18] http://www.businesscloudnews.com/2015/08/24/businesses-are-ready-for-cloud-but-lack-of-transparency-is-limiting-its-usefulness/

[19] http://www.businesscloudnews.com/2015/08/24/businesses-are-ready-for-cloud-but-lack-of-transparency-is-limiting-its-usefulness/

[20] https://www.networkworld.com/article/2364273/cloud-computing/aligning-cloud-vision-with-adoption.html

71. It is clear which aspects of the cloud service need to be audited
72. Big challenged is that cloud security auditors must be familiar with cloud computing terminology and have a working knowledge of a cloud system's constitution and delivery method[21]
73. Auditing in the cloud is more difficult because the security-relevant data is harder to obtain as provider, rather than CSUs, control most of the data[22]
74. Understanding of organisational functions allows the establishment of the scope of the auditing process by identifying and mapping IT infrastructure to those functions to provide the best suited controls for them[23]
75. The use of a third-party auditor (TPA) is recommended for performing the auditing
76. Auditing by a third- party could help in improving the QoS provided by cloud-based platforms and resources (Razaque & Rizvi, 2017)
77. A malicious TPA is a big threat (Razaque & Rizvi, 2017)
78. To circumvent potential financial losses or insider threats, a strict check and balance process over the TPA performance should exist (Razaque & Rizvi, 2017)
79. Cloud services provide enough computing capacity
80. Capacity management isn't necessary anymore when moving to cloud computing
81. Purchased cloud capacity can exceed the capabilities of the own IT infrastructure
82. While cloud computing offers unprecedented flexibility, it is extremely important to analyse your usage and plan accordingly
83. In the cloud the same maximum capacity is necessary as in the traditional IT solution
84. A part of the cloud capacity that is bought is not used
85. Cloud computing saves money
86. It is clear how the costs for the cloud service are calculated
87. Operating expenses are preferred over capital expenses
88. The cloud services are easy to use
89. Support service should be available 24/7
90. The certification programs for cloud computing are adequate
91. Hackers pose a serious threat when moving to the cloud
92. A public cloud is not a relevant solution to our organisation
93. A private cloud is not a relevant solution to our organisation
94. It is difficult to assess the costs involved due to the on-demand nature of the services[24]
95. The service-level agreements (SLAs) of the provider are not adequate to guarantee the availability and scalability[25]

[21] https://www.infoq.com/articles/cloud-security-auditing-challenges-and-emerging-approaches

[22] https://www.infoq.com/articles/cloud-security-auditing-challenges-and-emerging-approaches

[23] http://www.bcs.org/content/conWebDoc/56520

[24] https://cloudtweaks.com/2012/08/top-five-challenges-of-cloud-computing/

[25] https://cloudtweaks.com/2012/08/top-five-challenges-of-cloud-computing/

96. Our organisation has the leverage and capabilities to migrate in and out of the cloud and switching providers whenever they want[26]
97. It is vital to have plans to supervise usage, SLAs, performance, robustness, and business dependency of these services.[27]
98. We want a provider that has the financial resources to invest in all security technologies as they evolve
99. Companies that are investing in cloud solutions should also determine that their users receive effective preparation to apply the technology across the organization
100. You need to understand the duration of the subscription, and understand what the cost profile looks like long-term beyond the initial contract
101. Data security becomes an even trickier concept when companies have cloud-based systems and do business across borders.
102. The IT department and legal department need to be aligned when companies with cloud-based systems do business in different jurisdictions
103. A vulnerability assessment on the provider's overall security measures against external attacks is an effective way of ensuring that data on the cloud is adequately protected[28]
104. Even as much as most providers have stringent security measures, cyber-attacks are always looming[29]
105. When the service provider decides to shut down the business or a choice is made to terminate contract with the provider, it is a huge challenge to get back all data without it being shared or used by third parties.[30]
106. The cloud computing company's disaster recovery capabilities to a great extent determines the user's disaster recovery measures[31]
107. Because there is shared access to CPU and storage, a simple flaw can allow other people or an attacker to view other's data or even take on other's people's identity[32]
108. For big enterprises centred on mission-critical IT support systems, the use of cloud computing services can be a challenge in terms of cost[33]
109. Data may be stored across multiple data centres in an effort to improve reliability, increase performance, and provide redundancies. This geographic dispersion may make it more difficult to ascertain legal jurisdiction if disputes arise (Chambers, 2010)
110. Unclarity about who is the actual owner of the data is a problem that arises with cloud computing (Chambers, 2010)

[26] https://cloudtweaks.com/2012/08/top-five-challenges-of-cloud-computing/
[27] https://cloudtweaks.com/2012/08/top-five-challenges-of-cloud-computing/
[28] https://www.stacktunnel.com/critical-risks-and-challenges-cloud-computing.html
[29] https://www.stacktunnel.com/critical-risks-and-challenges-cloud-computing.html
[30] https://www.stacktunnel.com/critical-risks-and-challenges-cloud-computing.html
[31] https://www.stacktunnel.com/critical-risks-and-challenges-cloud-computing.html
[32] https://www.stacktunnel.com/critical-risks-and-challenges-cloud-computing.html
[33] https://www.stacktunnel.com/critical-risks-and-challenges-cloud-computing.html

111. Sustainability is one of the reasons why cloud computing should be adopted, because the more efficient usage of IT hardware reduces energy consumption (Chambers, 2010)

112. organizations need a set of capabilities that are essential when effectively implementing and managing cloud services, including demand management, relationship management, data security management, application lifecycle management, risk and compliance management (Chambers, 2010)

113. the anonymous nature of the cost of consumption of cloud usage makes it difficult for business to evaluate and incorporate it into their business plans (Chambers, 2010)

## C. Form with background question

This questionnaire will address the viewpoint of the interviewee on trust in cloud computing. First some contextual questions will be asked in which the interviewee provides information about their background and current organisation. Then the interviewee will continue to the Q-sort, where 40 statements need to be reviewed from their personal view. The complete questionnaire will take approximately 30-45 minutes.

*Personal Background*

- Which of these categories best describes your role in cloud computing projects?

IT / Business / Security / Legal / Other

- Which of these categories best describes the area of your education?

IT / Business / Security / Legal / Other

*Organisation's Background*

- What is the industry your organisation is in?

…………………………………………………………………………………………………………

- What is the sector your organisation is in?

Public / Private / Not for profit / Other

*Cloud computing*

- What is the maturity of the cloud computing solution(s) you were involved with?

Assessment / Migration / Optimization / None / Other

- What service model is used in the cloud computing solution(s) you were involved with?

Infrastructure as a Service / Platform as a Service / Software as a Service / None / Other

- What deployment model is used in the cloud computing solution(s) you were involved with?

Public cloud / Private cloud / Hybrid cloud / None / Other

## D. Instructions for Q-sort

During this part of the questionnaire 40 statements on cloud computing will be presented to the interviewee. Based on these 40 statements the interviewee will provide their perspective on the topic of cloud computing. The statements need to be evaluated from the personal view of the interviewee. The interview will consist of the follow steps:

1. The interviewee sorts the 40 statements into three separate groups
   a. Agree; these are the statements the interviewee agrees with
   b. Neutral; these are the statements that the interviewee has no opinion on or are unclear
   c. Disagree; these are the statements the interviewee disagrees with
2. The interviewee takes the pile with the statements that he or she agrees with and places them into the distribution as presented below, where each box represents a statement. Starting from the right-hand side with the statements the interviewee agrees most with, towards the centre until no cards are left.
3. The interviewee takes the pile with the statements that he or she disagrees with and does the same thing as with the statements he or she disagreed with, only this time starting from the left-hand side.
4. The interviewee takes the rest of the cards and places them in between the cards that were placed during the previous steps
5. The interviewee reviews whether the distribution of the statements still matches their personal view, and adjusts it when this is not the case.
6. The interviewee is asked to provide some more information around the chosen distribution of statements
   a. Was anything unclear?
   b. Was anything missing?
   c. Did you doubt about certain choices or statements?
   d. Does the distribution represent your own personal view?

Most disagree <-----------------------------------------------------> Most agree

| -4 | -3 | -2 | -1 | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|---|---|
| □ | □ | □ | □ | □ | □ | □ | □ | □ |
|  | □ | □ | □ | □ | □ | □ | □ |  |
|  | □ | □ | □ | □ | □ | □ | □ |  |
|  |  | □ | □ | □ | □ | □ |  |  |
|  |  |  | □ | □ | □ |  |  |  |
|  |  |  | □ | □ | □ |  |  |  |
|  |  |  | □ | □ | □ |  |  |  |
|  |  |  |  | □ |  |  |  |  |
|  |  |  |  | □ |  |  |  |  |
|  |  |  |  | □ |  |  |  |  |

## E. Q-sample

### a. Capability

#### Security

To represent security as a potential factor influencing the trust in cloud services, the following statements are taken into the Q-sample:

*Table 16 Statements on security*

| | |
|---|---|
| 1 | Cyber-attacks can be prevented by stringent security measures |
| 2 | Because there is shared access to CPU and storage, a simple flaw can allow other people or an attacker to view other's data or even take on other people's identity |
| 3 | In the case of highly sensitive data, it's important to encrypt it before storing it in the cloud |
| 6 | Providers should be asked about their backup and retention strategies, encryption, data disposal procedures, and business continuity in the contract. |
| 38 | The provider should have clear human resource requirements in order to prevent security breaches by malicious insiders |

#### Reliability

To represent reliability as a potential factor influencing the trust in cloud services, the following statements are taken into the Q-sample:

*Table 17 Statements on reliability*

| | |
|---|---|
| 8 | Outages in the cloud are always a possibility and thus the customer should have procedures in place to mitigate this risk |
| 9 | Resources should be spread across multiple zones |
| 10 | The provider should not use datacentres in regions prone to natural disasters |
| 11 | The provider should not use datacentres in regions with low technological maturity (e.g. power grid maturity, type of fibre) |
| 12 | At least the mission-critical information should be backed up on a local server |

#### Other

| | |
|---|---|
| 7 | Private clouds are preferred over public clouds |

### b. Benefits

#### Technological advantage

To represent technological advantage as a potential factor influencing the trust in cloud services, the following statements are taken into the Q-sample:

*Table 18 Statements on technological advantage*

| | |
|---|---|
| 13 | Cloud computing is the most important trend in enterprise IT |
| 14 | Cloud computing is adopted because we think it enhances innovation |

### Sustainability

To represent sustainability as a potential factor influencing the trust in cloud services, the following statement is taken into the Q-sample:

*Table 19 Statement on sustainability*

| | |
|---|---|
| 16 | Sustainability is one of the reasons why cloud computing should be adopted, because the more efficient usage of IT hardware reduces energy consumption |

## c. Costs

### Organisational change

To represent organisational change as a potential factor influencing the trust in cloud services, the following statements are taken into the Q-sample:

*Table 20 Statements on organisational change*

| | |
|---|---|
| 17 | Adopting cloud computing will require a change in the organisation's culture |
| 18 | Users of cloud computing services should have communication processes capable of quickly and effectively notifying data owners about any potential breach in security |
| 19 | The ease with which cloud-computing services can be acquired by individuals in the organisation (often the only thing needed is a credit card) can result in traditional IT and procurement controls being bypassed |
| 15 | The anonymous and the on-demand nature of the cost of consumption of cloud usage makes it difficult for business to evaluate and incorporate it into their business plans |

### Financial costs

To represent financial costs as a potential factor influencing the trust in cloud services, the following statements are taken into the Q-sample:

*Table 21 Statements on financial costs*

| | |
|---|---|
| 20 | You need to understand the duration of the subscription, and understand what the cost profile looks like long-term beyond the initial contract |

## d. Compliance

### Jurisdiction

To represent jurisdiction as a potential factor influencing the trust in cloud services, the following statements are taken into the Q-sample:

*Table 22 Statements on jurisdiction*

| | |
|---|---|
| 26 | It is a problem when governments can be intrusive under the local law or under accepted local practices |

| | |
|---|---|
| 27 | IT should know the specifics of what data is stored where |

### Auditing

To represent auditing as a potential factor influencing the trust in cloud services, the following statements are taken into the Q-sample:

*Table 23 Statements on auditing*

| | |
|---|---|
| 28 | It is important that providers allow client-auditing of their security offerings |
| 29 | Cloud services need to be audited by an independent third party |
| 25 | To circumvent potential financial losses or insider threats, a strict check and balance process over the third-party auditor's performance should exist |

### Contracting

To represent contracting as a potential factor influencing the trust in cloud services, the following statements are taken into the Q-sample:

*Table 24 Statements on contracting*

| | |
|---|---|
| 30 | The service-level agreements (SLAs) of the provider are adequate to guarantee the availability and scalability |
| 31 | Standard vendor contracts do not come close to best practices for meeting customer data security needs |
| 22 | SLA's are sufficient to protect against costs related to downtime |

## e. Control

### Accountability

To represent responsibility as a potential factor influencing the trust in cloud services, the following statements are taken into the Q-sample:

| | |
|---|---|
| 32 | Lack of control over IT is the biggest challenge |
| 5 | Security of IT is the responsibility of the provider |
| 21 | The provider should be able to compensate for all damages done in the case of any failure |

### Interoperability

To represent interoperability as a potential factor influencing the trust in cloud services, the following statements are taken into the Q-sample:

*Table 25 Statements on interoperability*

| | |
|---|---|
| 33 | It is hard to switch from one service provider to another |
| 34 | There are enough standards in order to provide interoperability between cloud services |
| 35 | Organisations should use more than one provider |

### Privacy

To represent privacy as a potential factor influencing the trust in cloud services, the following statements are taken into the Q-sample:

*Table 26 Statements on privacy*

| | |
|---|---|
| 36 | It is important that providers do not use the data that is entrusted to them inappropriately |
| 37 | Resources should be available at all time to the authorised person |
| 4 | Sensitive private information should not be stored on a public cloud |

### Transparency

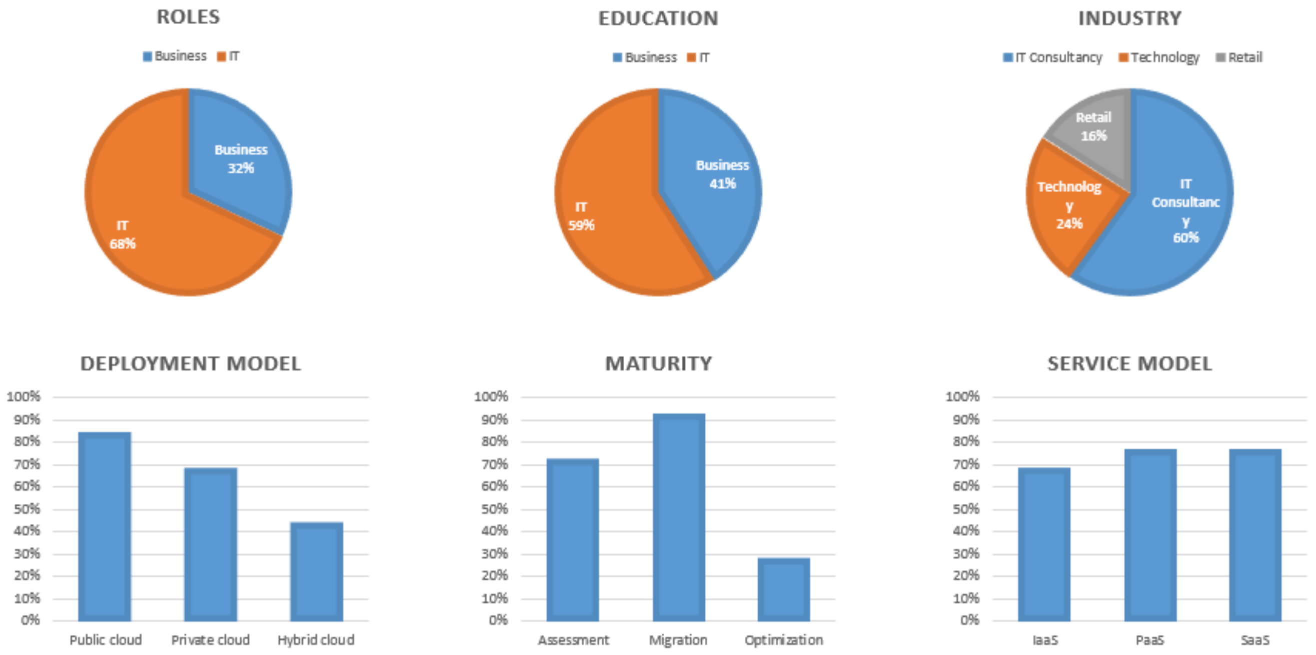
To represent transparency as a factor influencing the trust in cloud services, the following statements are taken into the Q-sample:

*Table 27 Statements on transparency*

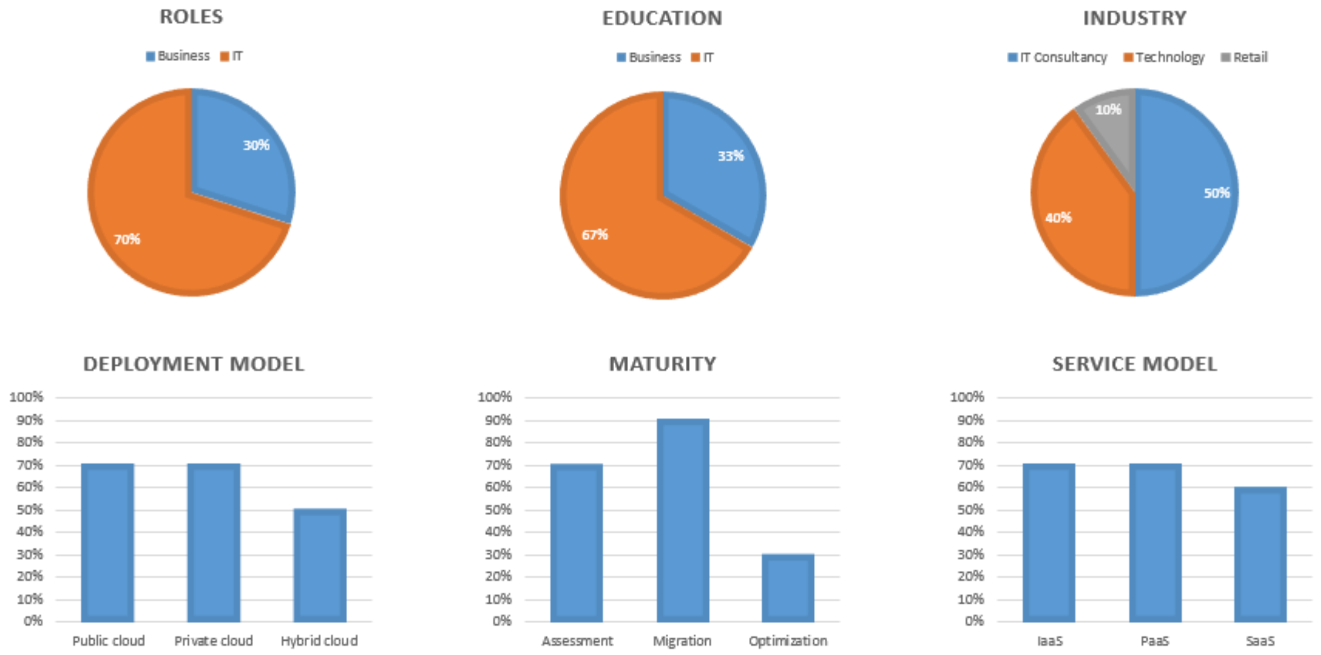
| | |
|---|---|
| 39 | Unclarity about who is the actual owner of the data is a problem that arises with cloud computing |
| 40 | The cloud is a black box into which the enterprise dumps its applications, data, workloads and processes |
| | Information on cloud computing usage should be provided by the provider, in order for the customer to make better purchasing decisions |
| 23 | Clouds that limit visibility result in significant operational and financial issues (e.g. performance problems, challenges reporting to management, and unexpected bills) |

## F. P-Sort

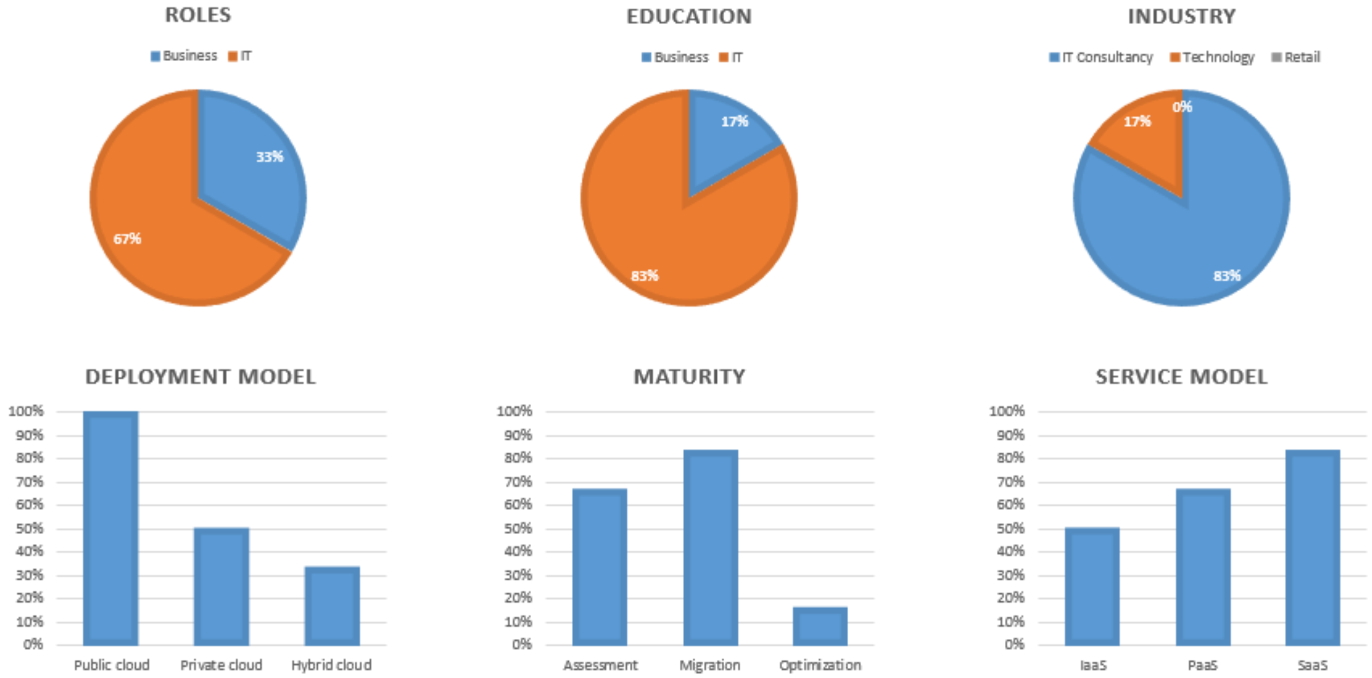
### a. Complete P-Sort



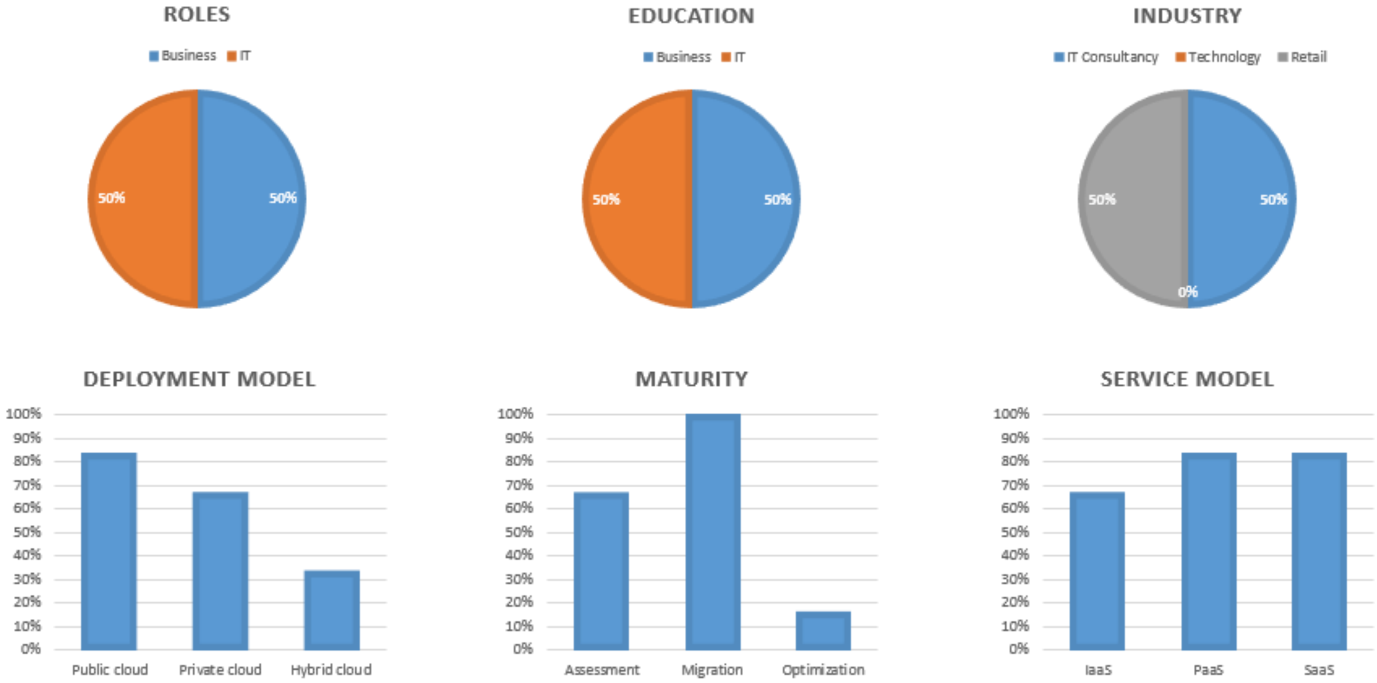
### b. Perspective 1: Trust through Benefits



## c. Perspective 2: Trust through Institutions



## d. Perspective 3: Trust through Resources



## G. PQMethod results

### a. Factor scores

*Table 28 Factor scores with 3 factors*

| | | Factors | | | | | |
|---|---|---|---|---|---|---|---|
| | | 1 | | 2 | | 3 | |
| **No.** | **Statement** | **Score** | **Rank** | **Score** | **Rank** | **Score** | **Rank** |
| 1 | Adopting cloud computing will require a change in the organisation's culture | 1,95 | 1 | 2,41 | 1 | 1,37 | 4 |
| 2 | Cloud computing is the most important trend in enterprise IT | 1,18 | 3 | -0,41 | 28 | -1,64 | 38 |
| 3 | Private clouds are preferred over public clouds | -1,6 | 35 | -1,32 | 35 | -0,83 | 31 |
| 4 | Cloud computing is adopted because we think it enhances innovation | 0,99 | 6 | -0,04 | 22 | -0,33 | 24 |
| 5 | Lack of control over IT is the biggest challenge | -1,68 | 39 | -0,09 | 23 | 0,49 | 13 |
| 6 | The anonymous and the on-demand nature of the cost of consumption of cloud usage makes it difficult for business to evaluate and incorporate it into their business plans | -0,63 | 29 | -1,28 | 34 | -1,45 | 37 |
| 7 | The service-level agreements (SLAs) of the provider are adequate to guarantee the availability and scalability | -0,56 | 28 | 0,8 | 11 | -1,02 | 33 |
| 8 | You need to understand the duration of the subscription, and understand what the cost profile looks like long-term beyond the initial contract | 0,79 | 10 | -0,25 | 26 | 1,2 | 5 |
| 9 | Cyber attacks can be prevented by stringent security measures | -0,72 | 31 | 0,38 | 14 | -0,44 | 27 |
| 10 | Because there is shared access to CPU and storage, a simple flaw can allow other people or an attacker to view others data or even take on other people's identity | -1,6 | 37 | -1,56 | 37 | -0,51 | 29 |
| 11 | Unclarity about who is the actual owner of the data is a problem that arises with cloud computing | -0,04 | 23 | -0,32 | 27 | -2,03 | 40 |
| 12 | Sustainability is one of the reasons why cloud computing should be adopted, because the more efficient usage of IT hardware reduces energy consumption | 0,32 | 18 | 0,26 | 17 | -0,46 | 28 |
| 13 | It is important that CSPs do not use the data that is entrusted to them inappropriately | 1,63 | 2 | 1,3 | 4 | 1,71 | 2 |
| 14 | In the case of highly sensitive data, it's important to encrypt it before storing it in the cloud | 0,71 | 13 | 1,32 | 3 | 1,86 | 1 |
| 15 | Sensitive private information should not be stored on a public cloud | -1,03 | 33 | -1,15 | 33 | -0,43 | 26 |
| 16 | Users of cloud computing services should have communication processes capable of quickly and effectively notifying data owners about any potential breach in security | 0,82 | 9 | 1,18 | 5 | 0,92 | 9 |
| 17 | Security of IT is the responsibility of the provider | -1,64 | 38 | 0,77 | 12 | -1,3 | 35 |
| 18 | Standard vendor contracts do not come close to best practices for meeting customer data security needs | -0,06 | 24 | -1,37 | 36 | 0,34 | 19 |
| 19 | The ease with which cloud-computing services can be acquired by individuals in the organisation (often the only thing needed is a credit card) can result in traditional IT and procurement controls being bypassed | 0,06 | 20 | 0,15 | 20 | 0,67 | 11 |
| 20 | It is important that CSPs allow client-auditing of their security offerings | 0,19 | 19 | -0,12 | 24 | 0,43 | 18 |
| 21 | The provider should have clear human resource requirements in order to prevent security breaches by malicious insiders | 0,05 | 21 | 0,83 | 10 | 0,67 | 10 |
| 22 | Resources should be available at all time to the authorised person | 0,52 | 15 | 0,43 | 13 | 0,54 | 12 |
| 23 | The provider should be able to compensate for all damages done in the case of any failure | -1,6 | 36 | -0,59 | 30 | 0,12 | 21 |
| 24 | SLA's are sufficient to protect against costs related to downtime | -1,72 | 40 | 0,22 | 18 | -1,05 | 34 |
| 25 | Outages in the cloud are always a possibility and thus the customer should have procedures in place to mitigate this risk | 1,14 | 4 | 1 | 7 | 0,46 | 15 |
| 26 | At least the mission-critical information should be backed up on a local server | -0,93 | 32 | -0,7 | 31 | -1,02 | 32 |
| 27 | Clouds that limit visibility result in significant operational and financial issues (e.g. performance problems, challenges reporting to management, and unexpected bills) | -0,03 | 22 | -0,92 | 32 | 0,47 | 14 |
| 28 | Information on cloud computing usage should be provided by the provider, in order for the customer to make better purchasing decisions | 0,94 | 8 | 0,05 | 21 | 0,44 | 17 |
| 29 | Providers should be asked about their backup and retention strategies, encryption, data disposal procedures, and business continuity in the contract. | 0,67 | 14 | 1,39 | 2 | 1,45 | 3 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 30 | The cloud is a black box into which the enterprise dumps its applications, data, workloads and processes | -1,39 | 34 | -1,92 | 40 | -1,65 | 39 |
| 31 | It is hard to switch from one service provider to another | -0,17 | 25 | -1,69 | 39 | -0,07 | 22 |
| 32 | There are enough standards in order to provide interoperability between cloud services | 0,43 | 17 | 0,85 | 8 | -0,66 | 30 |
| 33 | Organisations should use more than one provider | 0,5 | 16 | -1,57 | 38 | -1,42 | 36 |
| 34 | It is a problem when governments can be intrusive under the local law or under accepted local practices | 0,77 | 11 | -0,14 | 25 | 0,97 | 7 |
| 35 | Resources should be spread across multiple zones | 0,76 | 12 | 0,83 | 9 | -0,39 | 25 |
| 36 | IT should know the specifics of what data is stored where | 0,97 | 7 | 0,27 | 16 | 0,95 | 8 |
| 37 | The provider should not use datacentres in regions prone to natural disasters | -0,66 | 30 | 1,04 | 6 | 0,24 | 20 |
| 38 | The provider should not use datacentres in regions with low technological maturity (e.g. power grid maturity, type of fiber) | -0,18 | 26 | 0,16 | 19 | -0,1 | 23 |
| 39 | Cloud services need to be audited by an independent third party | 1,03 | 5 | -0,52 | 29 | 1,06 | 6 |
| 40 | To circumvent potential financial losses or insider threats, a strict check and balance process over the third party auditor's performance should exist | -0,19 | 27 | 0,31 | 15 | 0,45 | 16 |

*Table 29 Factor scores with 4 factors*

| | | Factors | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 1 | | 2 | | 3 | | 4 | |
| No. | Statement | Score | Rank | Score | Rank | Score | Rank | Score | Rank |
| 1 | Adopting cloud computing will require a change in the organisation’s culture | 1,84 | 1 | 2,38 | 1 | 1,86 | 1 | 2,48 | 1 |
| 2 | Cloud computing is the most important trend in enterprise IT | 1,15 | 5 | 0,15 | 20 | -1,9 | 40 | 0,29 | 15 |
| 3 | Private clouds are preferred over public clouds | -1,44 | 35 | -0,81 | 33 | -0,89 | 33 | -0,96 | 34 |
| 4 | Cloud computing is adopted because we think it enhances innovation | 1,24 | 3 | 0,6 | 8 | -0,44 | 24 | -0,9 | 32 |
| 5 | Lack of control over IT is the biggest challenge | -1,74 | 38 | -0,41 | 30 | 0,86 | 10 | 0,32 | 13 |
| 6 | The anonymous and the on-demand nature of the cost of consumption of cloud usage makes it difficult for business to evaluate and incorporate it into their business plans | -0,67 | 29 | -1,31 | 36 | -1,47 | 38 | -0,58 | 28 |
| 7 | The service-level agreements (SLAs) of the provider are adequate to guarantee the availability and scalability | -0,67 | 30 | 1,72 | 3 | -0,82 | 32 | -0,85 | 31 |
| 8 | You need to understand the duration of the subscription, and understand what the cost profile looks like long-term beyond the initial contract | 0,83 | 11 | 0,5 | 12 | 1,21 | 7 | -0,25 | 26 |
| 9 | Cyber attacks can be prevented by stringent security measures | -0,71 | 31 | 0,25 | 18 | -0,8 | 31 | 0,78 | 9 |
| 10 | Because there is shared access to CPU and storage, a simple flaw can allow other people or an attacker to view others data or even take on other people’s identity | -1,46 | 36 | -1,97 | 39 | -0,58 | 29 | -1,08 | 36 |
| 11 | Unclarity about who is the actual owner of the data is a problem that arises with cloud computing | -0,13 | 24 | -0,5 | 32 | -1,73 | 39 | 0,08 | 18 |
| 12 | Sustainability is one of the reasons why cloud computing should be adopted, because the more efficient usage of IT hardware reduces energy consumption | 0,32 | 18 | 0,41 | 14 | 0,35 | 17 | -0,94 | 33 |
| 13 | It is important that CSPs do not use the data that is entrusted to them inappropriately | 1,83 | 2 | 0,66 | 7 | 1,41 | 4 | 1,77 | 2 |
| 14 | In the case of highly sensitive data, it's important to encrypt it before storing it in the cloud | 0,58 | 13 | 0,56 | 11 | 1,48 | 3 | 1,45 | 4 |
| 15 | Sensitive private information should not be stored on a public cloud | -0,77 | 32 | -1,06 | 35 | -0,7 | 30 | -1,77 | 39 |
| 16 | Users of cloud computing services should have communication processes capable of quickly and effectively notifying data owners about any potential breach in security | 0,84 | 10 | 0,41 | 14 | 1 | 8 | 1,4 | 5 |
| 17 | Security of IT is the responsibility of the provider | -1,78 | 39 | 0,91 | 6 | -0,5 | 27 | -0,08 | 22 |
| 18 | Standard vendor contracts do not come close to best practices for meeting customer data security needs | -0,06 | 23 | -1,97 | 39 | 0,24 | 19 | -0,63 | 30 |
| 19 | The ease with which cloud-computing services can be acquired by individuals in the organisation (often the only thing needed is a credit card) can result in traditional IT and procurement controls being bypassed | 0,16 | 19 | -0,31 | 27 | 0,52 | 13 | 1,07 | 6 |
| 20 | It is important that CSPs allow client-auditing of their security offerings | 0,09 | 20 | 0 | 24 | -0,1 | 22 | 0,06 | 19 |
| 21 | The provider should have clear human resource requirements in order to prevent security breaches by malicious insiders | 0,03 | 21 | 0,15 | 20 | 0,72 | 11 | 0,91 | 8 |
| 22 | Resources should be available at all time to the authorised person | 0,49 | 16 | 0 | 24 | 0,44 | 14 | 0,17 | 17 |
| 23 | The provider should be able to compensate for all damages done in the case of any failure | -1,62 | 37 | -0,5 | 32 | 0,41 | 16 | -1,1 | 37 |
| 24 | SLA’s are sufficient to protect against costs related to downtime | -1,85 | 40 | -0,15 | 26 | -1,39 | 36 | -0,11 | 23 |
| 25 | Outages in the cloud are always a possibility and thus the customer should have procedures in place to mitigate this risk | 1,21 | 4 | 1,06 | 4 | -0,36 | 23 | 1,48 | 3 |
| 26 | At least the mission-critical information should be backed up on a local server | -0,82 | 33 | -0,97 | 34 | -1,42 | 37 | -1,02 | 35 |
| 27 | Clouds that limit visibility result in significant operational and financial issues (e.g. performance problems, challenges reporting to management, and unexpected bills) | 0,01 | 22 | -0,41 | 30 | 0,42 | 15 | -0,08 | 21 |
| 28 | Information on cloud computing usage should be provided by the provider, in order for the customer to make better purchasing decisions | 0,96 | 6 | -0,1 | 25 | 0,14 | 20 | 0,05 | 20 |
| 29 | Providers should be asked about their backup and retention strategies, encryption, data disposal procedures, and business continuity in the contract. | 0,52 | 14 | 0,97 | 5 | 1,28 | 6 | 0,7 | 10 |
| 30 | The cloud is a black box into which the enterprise dumps its applications, data, workloads and processes | -1,29 | 34 | -0,41 | 30 | -1,14 | 34 | -2,4 | 40 |
| 31 | It is hard to switch from one service provider to another | -0,37 | 27 | -2,38 | 40 | -0,44 | 25 | -0,51 | 27 |
| 32 | There are enough standards in order to provide interoperability between cloud services | 0,5 | 15 | 1,97 | 2 | -0,56 | 28 | 0,57 | 11 |
| 33 | Organisations should use more than one provider | 0,44 | 17 | -1,41 | 37 | -1,21 | 35 | -1,24 | 38 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 34 | It is a problem when governments can be intrusive under the local law or under accepted local practices | 0,94 | 7 | 0 | 24 | 1,53 | 2 | -0,58 | 29 |
| 35 | Resources should be spread across multiple zones | 0,74 | 12 | 0,25 | 18 | -0,46 | 26 | 0,92 | 7 |
| 36 | IT should know the specifics of what data is stored where | 0,84 | 9 | 0,35 | 15 | 0,63 | 12 | 0,44 | 12 |
| 37 | The provider should not use datacentres in regions prone to natural disasters | -0,61 | 28 | 0,56 | 11 | 0,32 | 18 | 0,3 | 14 |
| 38 | The provider should not use datacentres in regions with low technological maturity (e.g. power grid maturity, type of fiber) | -0,2 | 25 | 0,56 | 11 | -0,07 | 21 | -0,17 | 24 |
| 39 | Cloud services need to be audited by an independent third party | 0,86 | 8 | 0 | 24 | 1,31 | 5 | -0,17 | 25 |
| 40 | To circumvent potential financial losses or insider threats, a strict check and balance process over the third party auditor's performance should exist | -0,22 | 26 | 0,25 | 18 | 0,86 | 9 | 0,18 | 16 |

The analysis of the first three factors is done in the main text, because they are relevant for this research. The analysis of the fourth factor will be described here, because it does not provide a relevant, coherent perspective, but rather a perspective based on randomness.

When the *difference between the average factor score and the score of the fourth factor* (= *difference score)* is analysed, the following four statements are found to be defining the fourth perspective:

*Table 30 Statements relevant for the fourth (irrelevant) factor*

| Rank | Statement | Agree/ Disagree |
|---|---|---|
| 1 | The cloud is a black box into which the enterprise dumps its applications, data, workloads and processes | Disagree |
| 2 | It is a problem when governments can be intrusive under the local law or under accepted local practices | Agree |
| 3 | Cloud computing is adopted because we think it enhances innovation | Agree |
| 4 | Sustainability is one of the reasons why cloud computing should be adopted, because the more efficient usage of IT hardware reduces energy consumption | Agree |

From this, it is not possible to find a coherent pattern to form a perspective. Furthermore, mostly, these statements have a high *difference score* not because they strongly agree or disagree with these statements, but because they are just neutral about the statements, while the other perspectives have stronger opinions on them. This also indicates that there is no relevant perspective to be found in the fourth factor.

## b. Distinguishing statements

For the thesis, it was chosen to analyse the data of the Q-method by using a self-made approach. However, also PQMethod provides interpretation of the data by describing the distinguishing statements. These are presented here.

*Table 31 Distinguising statements for factor 1*

| Statements | Q-SV | Z-SCR | Q-SV2 | Z-SCR3 | Q-SV4 | Z-SCR5 |
|---|---|---|---|---|---|---|
| **Cloud computing is the most important trend in enterprise IT** | 3 | 1.18* | -1 | -0,41 | -3 | -1,64 |
| Cloud computing is adopted because we think it enhances innovation | 2 | 0.99* | 0 | -0,04 | 0 | -0,33 |
| Information on cloud computing usage should be provided by the cloud provider, in order for the customer to make better purchasing decisions | 2 | 0,94 | 0 | 0,05 | 0 | 0,44 |
| In the case of highly sensitive data, it's important to encrypt it before storing it in the cloud | 1 | 0,71 | 3 | 1,32 | 4 | 1,86 |
| Providers should be asked about their backup and retention strategies, encryption, data disposal procedures, and business continuity in the contract. | 1 | 0.67* | 3 | 1,39 | 3 | 1,45 |
| **Organisations should use more than one cloud service provider** | 0 | 0.50* | -3 | -1,57 | -2 | -1,42 |
| The cloud service provider should have clear human resource requirements in order to prevent security breaches by malicious insiders | 0 | 0,05 | 1 | 0,83 | 1 | 0,67 |
| To circumvent potential financial losses or insider threats, a strict check and balance process over the third-party auditor's performance should exist | -1 | -0,19 | 1 | 0,31 | 0 | 0,45 |
| The anonymous and the on-demand nature of the cost of consumption of cloud usage makes it difficult for business to evaluate and incorporate it into their business plans | -1 | -0,63 | -2 | -1,28 | -3 | -1,45 |
| The provider should not use datacentres in regions prone to natural disasters | -1 | -0.66* | 2 | 1,04 | 0 | 0,24 |
| The cloud service provider should be able to compensate for all damages done in the case of any failure | -2 | -1.60* | -1 | -0,59 | 0 | 0,12 |
| **Lack of control over IT is the biggest challenge** | -3 | -1.68* | 0 | -0,09 | 1 | 0,49 |
| SLA's are sufficient to protect against costs related to downtime | -4 | -1.72* | 0 | 0,22 | -2 | -1,05 |

*Table 32 Distinguising statements for factor 2*

| Statements | Q-SV | Z-SCR | Q-SV2 | Z-SCR3 | Q-SV4 | Z-SCR5 |
|---|---|---|---|---|---|---|
| The provider should not use datacentres in regions prone to natural disasters | -1 | -0,66 | 2 | 1.04* | 0 | 0,24 |
| **The service-level agreements (SLAs) of the provider are adequate to guarantee the availability and scalability** | -1 | -0,56 | 1 | 0.80* | -2 | -1,02 |
| **Security of IT is the responsibility of the cloud service provider** | -3 | -1,64 | 1 | 0.77* | -2 | -1,3 |
| Cyber-attacks can be prevented by stringent security measures | -1 | -0,72 | 1 | 0.38* | -1 | -0,44 |
| IT should know the specifics of what data is stored where | 2 | 0,97 | 0 | 0,27 | 2 | 0,95 |
| **SLA's are sufficient to protect against costs related to downtime** | -4 | -1,72 | 0 | 0.22* | -2 | -1,05 |
| Lack of control over IT is the biggest challenge | -3 | -1,68 | 0 | -0,09 | 1 | 0,49 |
| It is a problem when governments can be intrusive under the local law or under accepted local practices | 1 | 0,77 | 0 | -0.14* | 2 | 0,97 |
| You need to understand the duration of the subscription, and understand what the cost profile looks like long-term beyond the initial contract | 1 | 0,79 | -1 | -0.25* | 2 | 1,2 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Cloud computing is the most important trend in enterprise IT | 3 | 1,18 | -1 | -0.41* | -3 | -1,64 |
| **Cloud services need to be audited by an independent third party** | 2 | 1,03 | -1 | -0.52* | 2 | 1,06 |
| The cloud service provider should be able to compensate for all damages done in the case of any failure | -2 | -1,6 | -1 | -0,59 | 0 | 0,12 |
| Clouds that limit visibility result in significant operational and financial issues (e.g. performance problems, challenges reporting to management, and unexpected bills) | 0 | -0,03 | -1 | -0.92* | 1 | 0,47 |
| **Standard vendor contracts do not come close to best practices for meeting customer data security needs** | 0 | -0,06 | -2 | -1.37* | 0 | 0,34 |
| **It is hard to switch from one service provider to another** | 0 | -0,17 | -3 | -1.69* | 0 | -0,07 |

*Table 33 Distinguishing statements for factor 3*

| Statements | Q-SV | Z-SCR | Q-SV2 | Z-SCR3 | Q-SV4 | Z-SCR5 |
|---|---|---|---|---|---|---|
| Adopting cloud computing will require a change in the organisation’s culture | 4 | 1,95 | 4 | 2,41 | 3 | 1,37 |
| Lack of control over IT is the biggest challenge | -3 | -1,68 | 0 | -0,09 | 1 | 0,49 |
| The provider should not use datacentres in regions prone to natural disasters | -1 | -0,66 | 2 | 1,04 | 0 | 0.24* |
| The cloud service provider should be able to compensate for all damages done in the case of any failure | -2 | -1,6 | -1 | -0,59 | 0 | 0,12 |
| Resources should be spread across multiple zones | 1 | 0,76 | 1 | 0,83 | 0 | -0.39* |
| Sensitive private information should not be stored on a public cloud | -2 | -1,03 | -2 | -1,15 | -1 | -0,43 |
| Sustainability is one of the reasons why cloud computing should be adopted, because the more efficient usage of IT hardware reduces energy consumption | 0 | 0,32 | 0 | 0,26 | -1 | -0,46 |
| Because there is shared access to CPU and storage, a simple flaw can allow other people or an attacker to view others data or even take on other people’s identity | -3 | -1,6 | -3 | -1,56 | -1 | -0.51* |
| There are enough standards in order to provide interoperability between cloud services | 0 | 0,43 | 2 | 0,85 | -1 | -0.66* |
| SLA’s are sufficient to protect against costs related to downtime | -4 | -1,72 | 0 | 0,22 | -2 | -1.05* |
| **Cloud computing is the most important trend in enterprise IT** | 3 | 1,18 | -1 | -0,41 | -3 | -1.64* |
| **Unclarity about who is the actual owner of the data is a problem that arises with cloud computing** | 0 | -0,04 | -1 | -0,32 | -4 | -2.03* |

The statements in bold, are the statements that are also found as being representative for the perspectives according to the approach taken in the main text of this thesis. No statement from there is not included in the distinguishing statements as presented here, meaning that these results confirm the findings in the main text. Furthermore, the additional statements that are found to be representative for a perspective through this analysis mostly add to or don’t change the perspectives as found in the main text.

## H. Trust Framework

*Table 34 Perspectives, factors and key questions for the strategic apex*

| *Part of the organisation* | *Perspective* | *Factor* | *Key question(s)* |
|---|---|---|---|
| *Strategic Apex* | Techno-Optimists | Technological advantage | Is cloud computing the right response to our changing environment or will it be disruptive for our organisation?<br>Should we allocate our IT resources outside of the organisation?<br>Does cloud computing really provide the benefits that are promised (on the long term)? |
| | | Interoperability | When a certain cloud service is adopted can we still switch of provider when we need to be responsive to our environment?<br>How many different providers should we use in order to reduce dependency, while at the same time maintain interoperability? |
| | Responsibility-Shifters | Contracting | Can we draft contracts to effectively manage the relationship with a provider?<br>Are contracts sufficient to protect our mission against failures or opportunistic behaviour from the provider? |
| | | Accountability | To what degree is the provider able to take over responsibility over our IT?<br>Can the provider compensate for the damages that are done by their mistake? |
| | Operational-Conservatives | Technological advantage | Is cloud computing the right response to our changing environment or will it be disruptive for our organisation?<br>Should we allocate our IT resources outside of the organisation?<br>Does cloud computing really provide the benefits that are promised (on the long term)? |
| | | Reliability | Is the provider a reliable stakeholder to have in our business environment?<br>Can we rely on cloud computing to effectively serve our mission, or at least facilitate reaching it? |
| | General | Security | Are critical parts of the organisation still secure when cloud computing is adopted?<br>Does the provider or another party get access to sensitive private information? |
| | | Transparency | Is it still possible to monitor my organisation and keep effective supervision over other parts of the organisation? |

*Table 35 Perspectives, factors and key questions for IT service management*

| Part of the organisation | Perspective | Factor | Key question(s) |
|---|---|---|---|
| IT Service Management | Techno-Optimists | Technological advantage | Is this cloud service the right response to implement the strategy that is imposed by the strategic apex?<br>What applications are capable to be moved into the cloud and have benefits from this? |
| | | Interoperability | Is this cloud service interoperable with the on-premise solutions and other cloud services? |
| | Responsibility-Shifters | Contracting | Are standard SLA's adequate to guarantee the right quality of service and protect against costs related to downtime? |
| | | Accountability | What are the implications of adopting this cloud service for the people under our supervision (Operational IT)?<br>What are the implications of adopting this cloud service for other units?<br>Who is responsible for the connection between the organisation and the provider? |
| | Operational-Conservatives | Technological advantage | Is this cloud service the right response to implement the strategy that is imposed by the strategic apex?<br>What applications are capable to be moved into the cloud and have benefits from this? |
| | | Reliability | Can we rely on cloud computing to effectively serve our unit's mission, or at least facilitate reaching it?<br>What are the back-up and retention strategies of this cloud service? |
| | General | Security | What are the encryption and data disposal procedures of this cloud service?<br>Are critical parts of IT still secure when this cloud service is adopted? |
| | | Transparency | Is it still possible to collect feedback information on the performance of the unit and communicate it to the persons higher up the hierarchy (vertical coordination)? |

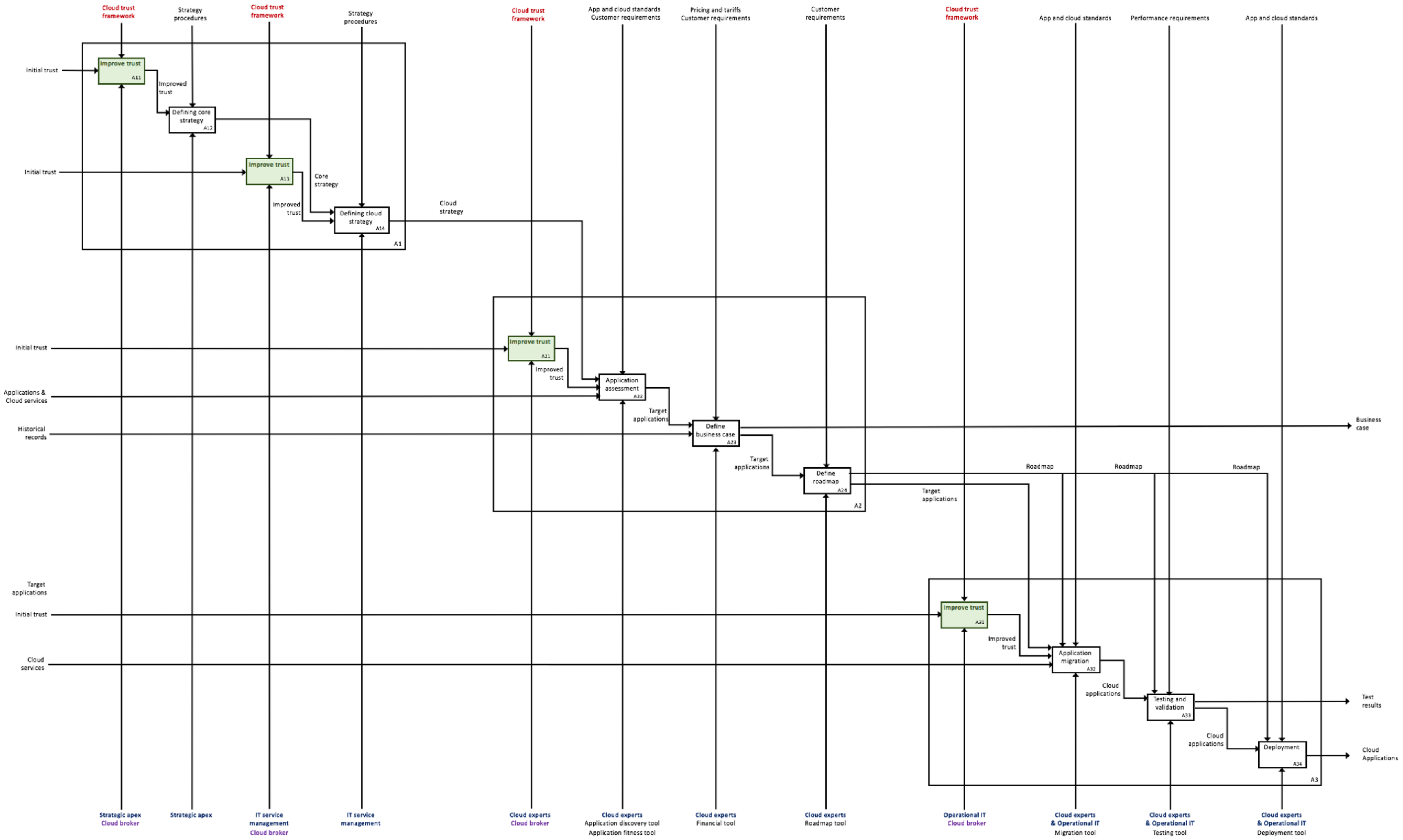
*Table 36 Perspectives, factors and key questions for operational IT*

| ***Part of the organisation*** | ***Perspective*** | ***Factor*** | ***Key question(s)*** |
|---|---|---|---|
| *Operational IT* | Techno-Optimists | Technological advantage | What hardware and software will still be necessary when cloud computing is adopted?<br>What applications are capable to be moved into the cloud and have benefits from this?<br>Will cloud computing provide benefits for our day-to-day tasks? |
| | | Interoperability | Is this cloud service interoperable with the on-premise solutions that are currently running on our servers? |
| | Responsibility-Shifters | Contracting | What are the operational requirements that are covered in the SLA's and which ones should be added? |
| | | Accountability | Which of our tasks can we put in the responsibility of the provider?<br>Who will be responsible for the (technological) connection between the organisation and the provider? |
| | Operational-Conservatives | Technological advantage | What hardware and software will still be necessary when cloud computing is adopted?<br>What applications are capable to be moved into the cloud and have benefits from this?<br>Will cloud computing provide benefits for our day-to-day tasks? |
| | | Reliability | Will adopting this cloud service lead to disturbance in the day-to-day jobs?<br>What are the back-up and retention strategies of this cloud service? |
| | General | Security | What are the encryption and data disposal procedures of this cloud service?<br>Where do the security measures of the provider end and where do ours start? |
| | | Transparency | Is there still insight in the usage of IT resources to effectively provide all parts of the organisation with the right resources and support? |

*Table 37 Perspectives, factors and key questions for the cloud experts*

| ***Part of the organisation*** | ***Perspective*** | ***Factor*** | ***Key question(s)*** |
|---|---|---|---|
| *Cloud Experts* | Techno-Optimists | Technological advantage | What are the benefits of cloud computing for this organisation as a whole?<br>What applications are capable to be moved into the cloud and have benefits from this? |
| | | Interoperability | How can multiple cloud services be integrated with the on-premise solutions and each other? |
| | Responsibility-Shifters | Contracting | How are the expectations towards the provider reflected in the Service Level Agreements? |
| | | Accountability | Which aspects will be taken over by the provider and which will stay inside the organisation?<br>Who will be responsible for the actual migration? |
| | Operational-Conservatives | Technological advantage | What are the benefits of cloud computing for this organisation as a whole?<br>What applications are capable to be moved into the cloud and have benefits from this? |
| | | Reliability | Is the cloud service able to provide the required up-time and reflect their numbers on reliability reality? |
| | General | Security | What are the security offerings of the provider and do they adequately handle our security concerns?<br>Where do the security measures of the provider end and where do ours start? |
| | | Transparency | What are the reporting procedures of the provider? |

# I. IDEF0 – A1 Scheme



# J. Scientific article

*Starts on next page*

# Trust in cloud computing

## a Q-method study to research the factors influencing trust in a cloud service

## Summary

One of the key challenges of adopting cloud computing is related to trust. Trust is necessary for effective collaboration between customers and providers and reducing transaction costs, however, in practice this trust is often lacking. From the scientific literature, it becomes clear that there is still a lot of ambiguity about trust in cloud services and that it is unclear which factors influence this trust. Hence, the research question is defined as: *which factors influence the trust of an organisation in a cloud service?* In order to answer this, first, an analysis of the concepts of cloud computing and trust, and the integration of those concepts in scientific literature is performed. From this analysis, a conceptual model is derived. This conceptual model is then evaluated with a Q-method study on the potential factors influencing trust in cloud services. In general, security, privacy, transparency and the willingness to change the organisation are found to be important factors. Besides the general viewpoints, there are also viewpoints specific to the three perspectives. Techno-optimist perceive technological advantage and interoperability as important, responsibility-shifters perceive contracting and accountability as important and the operational-conservatives perceive technological advantage and reliability as important.

Jacco Heins
4155149

Scientific Article for Master Thesis
Complex Systems Engineering and Management
TU Delft

## Introduction

Recent predictions show that cloud computing will become a multi-billion-dollar industry in the upcoming years and that there is an upward trend in cloud adoption (Gartner, 2017; Prasad & Green, 2015; Venters & Whitley, 2012). This upward trend is expected because cloud computing has the potential to provide a wide range of benefits. Among these benefits are cost savings, scalability, better alignment of technology, decreased effort in managing technology, environmental benefits, ubiquitous network access, location independent resource pooling, usage-based pricing and reliability (Khajeh-hosseini et al., 2012; Prasad & Green, 2015; C. Wang et al., 2013).

Although cloud computing can provide numerous benefits, there is still ambiguity and uncertainty with respect to the actual realization of these promised benefits (Khajeh-hosseini et al., 2012). There are several challenges organisations will have to face in order to move to the cloud, such as security, data ownership, lock-in and interoperability, lack of standards, enterprise support and service maturity, loss of data and return on investment (Oliveira et al., 2014; Radwan et al., 2017; Yongsiriwit, 2016). Although a lot of challenges are related to technology, the biggest one is related to attitude rather than technology (Marston et al., 2014). The largest organisational challenge is with respect to trust

(Alhamad et al., 2010; Lansing & Sunyaev, 2016; Noor et al., 2013).

While cloud services reduce the responsibility of the customer in terms of hardware and software management, it is likely that critical information and applications are moved outside the direct control of the customer (Uusitalo et al., 2010). Also, with the market growing at an increasing pace, reliably identifying a trustworthy provider becomes harder (Habib et al., 2010, 2014). Additionally, trust leads to effective and ongoing collaboration, since it promotes continuous interaction and directs firms into investing in the collaboration (Rousseau et al., 1998). Lastly, research shows that an assurance of a higher degree of trust in a provider is required in order to attain efficient resource allocation and utilization (Abawajy, 2009), partly by allowing organisations to adopt less elaborate safeguards, thereby economizing on transaction costs (Chiles & McMackin, 1996).

For this reason, trust in cloud services has gained some attention from academia and businesses. Several scientific studies produced conceptual trust models for cloud computing, with some of the studies validating the conceptual models by literature research (Chu et al., 2013; Lansing & Sunyaev, 2016; Uusitalo et al., 2010). However, empirical research on trust in a cloud service is fairly limited, hence it is still unclear which factors influence the trust in a cloud service. This results in the following research question: *which factors influence the trust of an organisation in a cloud service and what are the perspectives on this?*

To answer this question, the research method Q-method is used. Q-method is primarily an explorative technique, that can bring some coherence to research questions with many complex and socially contested answers. In this case it can provide some structure and patterns in the opinions and perspectives of practitioners on the factors influencing trust in a cloud service.

# Theoretical Background

The scientific literature regarding cloud computing, trust and the combination of both concepts will be analysed and translated into a conceptual model. This conceptual model incorporates the factors that influence trust in a cloud service. This model will be used as a guidance for the next chapters.

## Cloud computing

In the literature and industry there are different definitions of cloud computing. The research of Leimeister et al. (2010) compiled definitions from a range of scientific articles and developed a definition that is supported by the vast majority of the literature:

> *"Cloud computing is an IT deployment model, based on virtualization, where resources, in terms of infrastructure, applications and data are deployed via the internet as a distributed service by one or several service providers. These services are scalable on demand and can be priced on a pay-per-use basis"* (Leimeister et al., 2010, pp. 4)

Cloud computing has three deployment models: public cloud, private cloud and hybrid cloud. With public cloud, the infrastructure and computational resources are made available through the Internet by an external provider (Hsu et al., 2014). Private cloud is a deployment model where the computing environment is maintained exclusively for one organisation, and thus granting them greater control over their IT compared to the public cloud (Hsu et al., 2014). Hybrid clouds are the integration of services that are located on both public and private clouds. Thus, the public cloud requires the organisation to give a lot of their control over IT to the provider, while the private cloud stays in the direct control of the organisation. This has large implications for the organisation and requires close cooperation with the provider. For this reason, public cloud is chosen as the deployment model for this research. So, when the term cloud computing or cloud service is mentioned, it refers the public cloud.

## Trust

There is no universal definition of trust. For this reason, a general definition of trust will be taken and adapted to reflect trust as it will be used in this article. Blomqvist (1997) developed the following working definition of trust for business contexts:

> *"An actor's expectation of the other party's competence and goodwill"* (Blomqvist, 1997, pp. 283)

First, there is enough comparative and historical evidence that suggests that trust changes over time; developing, building and declining of trust relationships (Rousseau et al., 1998). Thus, trust is dynamic. Second, this research aims to uncover the factors that influence the trust of an organisation in a cloud service. In other words, trust is a dependent variable in this article. Third, for this research, it is chosen not to study the social and relational characteristics of the provider of a cloud service, which can be either the cloud service provider, the broker or the consultant. Instead it is chosen to study the technological and organisational aspects that may influence the trust of customers in a cloud service. Thus, trust is interorganisational. Last, trust can be divided into different stages: calculus-based trust, knowledge-based trust and identification-based trust (Lewicki & Bunker, 1996). With calculus-based trust, trust is gained by weighing the benefits of trust against the costs of violating this trust. Knowledge-based trust derives its trust from the history of interaction, which makes it possible to predict the other's behaviour. In identification-based trust the understanding of the desires and intentions of the other party plays an important role, where shared values help the process of trust development. This article will interpret trust as calculus-based trust. Since organisations deciding on whether they should adopt a cloud service are in an early stage of the relationship with the provider, there is no history of interaction or a clear view on the desires and intentions of the provider. Thus, trust is mainly calculus-based.

So, the definition of trust as it is being used in this article is: *An **organisation**'s **dynamic, calculated and dependent** expectation of the other **organisation**'s competence and goodwill*

## Conceptual trust model

According to existing (non-empirical) scientific literature there are several factors that influence the trust in a cloud service (Alhamad et al., 2010; Chu et al., 2013; Lansing & Sunyaev, 2016; Uusitalo et al., 2010). A number of these are represented in Table 1. More independent variables could be chosen that would also fit the core concepts. However, based on what was most commonly found, it was decided to scope the research around the independent variables as presented in Table 1.

*Table 1 Core concept and independent variable of trust in a cloud service*

| Core concept | Independent variable |
|---|---|
| Compliance | Contracting |
| | Auditing |
| | Jurisdiction |
| Control | Interoperability |
| | Privacy |
| | Transparency |
| Costs | Organisational change |
| | Financial costs |
| Benefits | Technological advantage |
| | Sustainability |
| Capability | Security |
| | Reliability |

This results in the following conceptual model:

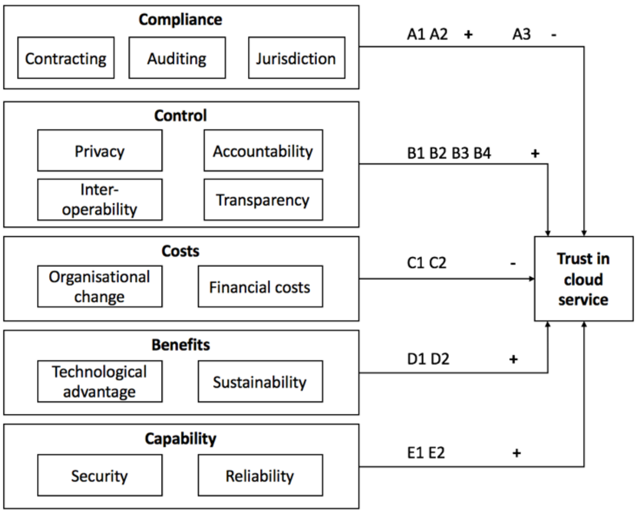


*Figure 1 Conceptual framework*

## Research Approach

Data will be collected through a document analysis and Q-method. The document analysis is performed to define the statements necessary for the Q-method and to develop the conceptual model that describes the potential factors influencing trust in cloud services, which is discussed in the previous chapter. The Q-method is used to get data on the importance of the factors influencing trust in cloud services.

Q-method provides the basis for studying subjectivity in a systematic way. This means only subjective opinions are used in Q. Although it is not possible to prove them, this method makes it possible to show structure and form in them. This means Q can reveal and describe both divergent views as consensus in a group. The Q-method is a complete methodology, involving technique (sorting), method (factor analysis), philosophy and ontology and was created by William Stephenson (1902-1989) (ISSSS, 2017).

First, a concourse is developed. A concourse refers to the incoherent batch of beliefs and perspectives and is the foundation of the Q-method. The goal of the concourse is to be as representative as possible. In other words, all opinions and perspectives that exist on the topic should be reflected in the concourse. From this concourse, forty statements are derived that are representative for the complete concourse, because the complete concourse would be too large for a participant to analyse. These statements are all categorised according to the independent variables in the conceptual model as presented in Figure 1.

The P-sample is a representative sample from the complete relevant group of people that are researched. The selection of the people that will participate in the Q-method study defines the scope of the research, but also limits the outcomes to the group of people they represent. For Q-method a small number of participants is needed, usually between twenty and forty (Watts & Stenner, 2005). For this study 25 people were willing to participate. Several conditions were used for scoping the P-sample:

1. Person is/was involved in the assessment, migration or optimization of a cloud service
2. Person works in the technology, IT consultancy or retail sector
3. Person works for a large, private organisation
4. Person currently works in the Netherlands
5. Persons has either an IT or business role in the cloud project

During the Q-sort phase of the Q-method, the participant is required rank the statements. The Q-sort produces a set of scores, ranging from -4 to 4 as can be seen in Figure , where every cell represents one statement. In total there are 40 cells, which corresponds to the amount of statements that will be presented. Participants are required to follow the distributed as presented in Figure 2. This forces the participant into carefully prioritizing the statements. The Q-sort reflects each participant’s personal view and is statistically correlated with the other participants, where the magnitude of correlation corresponds with the degree of similarity in the different perspectives. (Brown, 1993)

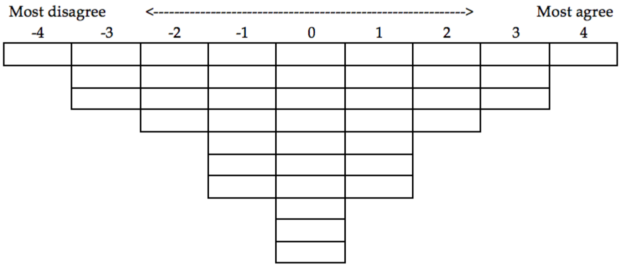


*Figure 2 Q-sort distribution*

The Q data is analysed using the dedicated software package PQMethod that was developed by Peter Schmolk. With the use of this software, a Centroid Factor Analysis is performed, after which the factors are rotated with the varimax procedure. The results of this statistical analysis will be addressed in the next Chapter.

## Limitations

With Q-method, the Q-sort of the participants only reflects their opinions at that specific moment. So, this leaves open the possibility that individuals may change their minds over time, making the results of this Q-method less relevant. Moreover, Q-method will result in *subjectively expressed, socially organized semantic patterns*, rather than scientific prove that certain causal relationships as presented in a conceptual model exist in reality.

Additionally, when performing the Q-sorting, both the method and the instructions need to be explained to the participants, because most of them are unfamiliar with it. Validity can therefore be affected when the participant's lack of comprehension leads to misunderstandings. This will even more so be the case when the Q-sorting is not done face to face, but rather through an online tool. This was done five times. Although instructions may be structured and a step-by-step process has to be followed, there is no possibility for the participants to ask questions when anything is unclear. Furthermore, when the Q-sorting is done through an online tool, the context of their sorting will be unclear, since the opportunity to explain their reasoning is limited in this tool.

## Empirical Findings

With the Q-method, it is possible to get an understanding of the importance of the different factors influencing trust. Moreover, different perspectives, that represent a smaller (sub)group, can be defined. This means that there are factors that are important to everybody, and factors that are important only to a certain perspective.

The Q-method shows that there are several factors that are relevant for all perspectives. In general, it is perceived that the customer needs to perform certain actions before adopting a cloud service. The customer needs to make sure their organisation is ready and willing to make the change, as well as making sure that the cloud service they want to adopt is *secure* and provides *privacy* over their data. Having knowledge on the security and privacy of the cloud services increases trust. As all perspectives agree on the fact that also change from the customer is required, it can be concluded that organisational change is seen more as a condition that needs to be met in order to adopt cloud computing, than that it is seen as a factor influencing trust in a cloud service. Thus, the factor will be redefined to: *the willingness to change the organisation*. When an organisation is willing to change, adopting a cloud service is more easily trusted. Moreover, all perspectives seem to understand what a cloud service entails. A *transparent* cloud service gives the customer the trust in the provider's competence and goodwill.

Additionally, three perspectives on trust in a cloud service were found. The first perspective is the perspective of the *techno-optimists.* In short, this group really sees cloud computing as the most important trend in enterprise IT. Because a cloud service can offer significant *technological advantages*, they are willing to trust it. But, a lack of *interoperability* is seen as an important issue: when it is not possible to change from one provider to another, trust in the cloud service will be limited. The second perspective is the perspective of the *responsibility-shifters*. In short, this group wants to make the provider *accountable* in case contingencies with the cloud service occur, preferably through the use of *contracts*. When a cloud service satisfies these conditions, they trust the cloud service. The third, and last perspective is the perspective of the *operational-conservatives*. This group does not see cloud computing as an important trend or significant *technological advantage* and has its doubt with respect to the reliability; they prefer to keep things as they are. This perspective has a more negative viewpoint of cloud computing, but increasing the perception of the *technological advantage* and *reliability* will improve their trust in a cloud service

This means that jurisdiction, auditing, financial costs and sustainability are not relevant factors that influence the trust in a cloud service.

## Conclusion and Future Research

The research question was defined as: *which factors influence the trust of an organisation in a cloud service and what are the perspectives on this?* The previously described research found an answer to this question, which can be defined as:

Trust in a cloud service is approached from three perspectives in practice: techno-optimists, responsibility-shifters and operational conservatives. In general, all of these perspectives perceive security and transparency as factors that influence their trust in a cloud service. On top of that, techno-optimists perceive technological advantage and interoperability as important, responsibility-shifters perceive contracting and accountability as important and operational conservatives perceive reliability and (the lack of) technological advantage as important.

Future research should focus on the validation and expanding of the findings. This can be done by performing a survey or expert validation. With a survey, it is possible to validate certain aspects of the findings of the Q-method. It is for example, possible to set up questions concerning the factors influencing the trust in a cloud service. When the outcomes of this survey are comparable with the ones received from the Q-method, the findings are valid. The survey can also provide additional insights in the findings gained from the Q-method. While Q-method provides the perspectives, it is not defined what the distribution of those perspectives is. The Q-method only gives all the relevant perspectives that exist, but does not say anything about how common those perspectives are. Thus, surveys may provide more insight in this. Additionally, expert validation can be used to validate the findings. When experts can recognise and confirm the findings of this research, the findings can be considered valid. Since cloud brokers (e.g. Accenture) work in different projects and with different organisations, it is likely that the employees of the cloud broker have experienced different point of views with regard to trust in cloud services. Thus, using those people as the experts during the expert validation would be a logical start. From there on, different organisations that did or did not adopt cloud computing should be approached in order to also validate the findings with experience from cloud service customers themselves.

## References

Abawajy, J., 2009. Determining service trustworthiness in intercloud computing environments. *I-SPAN 2009 - The 10th International Symposium on Pervasive Systems, Algorithms, and Networks*, pp.784–788.

Alhamad, M., Dillon, T. & Chang, E., 2010. Conceptual SLA framework for cloud computing. *4th IEEE International Conference on Digital Ecosystems and Technologies - Conference Proceedings of IEEE-DEST 2010, DEST 2010*, pp.606–610.

Blomqvist, K., 1997. The many faces of trust. *Scandinavian Journal of Management*, 13(3), pp.271–286.

Brown, S.R., 1993. A primer on Q methodology. *Operant subjectivity*, 16(3/4), pp.91–138.

Chiles, T.H. & McMackin, J.F., 1996. Integrating variable risk preferences, trust, and transaction cost economics. *Acadamy of Management Review*, 21(1), pp.73–99.

Chu, R., Lai, I.K.W. & Lai, D.C.F., 2013. Trust factors influencing the adoption of cloud-based interorganizational systems: A conceptual model. *Engineering, Management Science and Innovation (ICEMSI), 2013 International Conference on*, pp.1–3.

Gartner, 2017. *Top Strategic Predictions for 2017 and Beyond: Surviving the Storm-Winds of Digital Disruption*,

Habib, S.M. et al., 2014. Towards a trust management system for cloud computing marketplaces: using CAIQ as a trust information source. *SECURITY AND COMMUNICATION NETWORKS*, 7, pp.2185–2200.

Habib, S.M., Ries, S. & Mühlhäuser, M., 2010. Cloud computing landscape and research challenges regarding trust and reputation. *Proceedings - Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing in Conjunction with the UIC 2010 and ATC 2010 Conferences, UIC-ATC 2010*, pp.410–415.

Hsu, P., Ray, S. & Li-Hsieh, Y.-Y., 2014. Examining cloud computing adoption intention , pricing mechanism , and deployment model. *International Journal of Information Management*, 34(4), pp.474–488. Available at: http://dx.doi.org/10.1016/j.ijinfomgt.2014.04.006.

ISSSS, 2017. Q-methodology. Available at: https://qmethod.org/ [Accessed March 31, 2017].

Khajeh-hosseini, A. et al., 2012. The Cloud Adoption Toolkit : supporting cloud adoption decisions in the enterprise. *Software - Practice and Experience*, 42(4), pp.447–465.

Lansing, J. & Sunyaev, A., 2016. Trust in Cloud Computing: Conceptual Typology and Trust-Building Antecedents. *ACM SIGMIS Database*, 47(2), pp.58–96.

Leimeister, S. et al., 2010. The Business Perspective of Cloud Computing, Actors, Roles, and Value Networks.

Lewicki, R.J. & Bunker, B.B., 1996. Developing and Maintaining Trust in Work Relationships. *Trust in Organizations: Frontiers of Theory and Research*, (November), pp.114–139. Available at: https://books.google.com/books?hl=en&lr=&id=t6glCgAAQBAJ&oi=fnd&pg=PA114&dq=lewicki+bunker&ots=19Jm-Z18Ie&sig=XcnRF3K1Q2pHIapzCJtUXI5wdE0%5Cnhttp://sk.sagepub.com/books/trust-in-organizations/n7.xml.

Marston, S. et al., 2014. Cloud computing — The business perspective ☆. *Decision Support Systems*, 51(1), pp.176–189. Available at: http://dx.doi.org/10.1016/j.dss.2010.12.006.

Noor, T.H. et al., 2013. Trust management of services in cloud environments: Obstacles and solutions. *ACM Computing Surveys*, 46(1), pp.1–30. Available at: http://dl.acm.org/citation.cfm?doid=2522968.2522980.

Oliveira, T., Thomas, M. & Espadanal, M., 2014. Information & Management Assessing the determinants of cloud computing adoption : An analysis of the manufacturing and services sectors. *Information & Management*, 51(5), pp.497–510. Available at: http://dx.doi.org/10.1016/j.im.2014.03.006.

Prasad, A. & Green, P., 2015. Governing cloud computing services : Reconsideration of IT governance structures. *International Journal of Accounting Information Systems*, 19, pp.45–58. Available at: http://dx.doi.org/10.1016/j.accinf.2015.11.004 .

Radwan, T., Azer, M.A. & Abdelbaki, N., 2017. Cloud computing security: challenges and future trends. *International Journal of Computer Applications in Technology*, 55(2), p.158. Available at: http://www.inderscience.com/link.php?id=82865.

Rousseau, D.M. et al., 1998. Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3), pp.393–404.

Uusitalo, I. et al., 2010. Trust and cloud services - An interview study. *Proceedings - 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010*, pp.712–720.

Venters, W. & Whitley, E., 2012. A Critical Review of Cloud Computing : Researching Desires and Realities A Critical Review of Cloud Computing : Researching Desires and Realities. *Journal of Information Technology*, 27(3), pp.179–197.

Wang, C. et al., 2013. Privacy-Preserving Public Auditing for Secure Cloud Storage. *IEEE Transactions On Computers*, 62(2), pp.362–375.

Watts, S. & Stenner, P., 2005. Doing Q methodology: theory, method and interpretation. *Qualitative Research in Psychology*, 2(1), pp.67–91. Available at: http://www.tandfonline.com/doi/abs/10.1191/1478088705qp022oa.

Yongsiriwit, K., 2016. A Semantic Framework Supporting Cloud Resource Descriptions Interoperability.