



University of
Zurich^{UZH}

Effects of Legal and Regulative Constraints on Cloud and its Federated Environment

Sacha Uhlmann
Zürich, Switzerland
Student ID: 09-608-076

Supervisor: Radhika Garg, Patrick Poullie
Date of Submission: Thursday 10th September, 2015

Zusammenfassung

Cloud Computing ermöglicht es Unternehmen, Teile ihrer IT an Cloud-Anbieter auszulagern. Es befähigt Unternehmen, sich auf ihre Kernkompetenzen zu fokussieren und ihre Fixkosten für die IT zu reduzieren. Bei Cloud Computing werden IT-Dienstleistungen via Breitbandverbindung zur Verfügung gestellt. Unternehmen, welche sich überlegen, Cloud Computing einzuführen, müssen eine Reihe von Faktoren berücksichtigen. Diese Faktoren lassen sich in verschiedene Kategorien (technische, organisatorische, ökonomische und beziehungsspezifische) einteilen. Die gesetzlichen Rahmenbedingungen erhöhen die Komplexität weiter. Diese verschiedenen Faktoren und Gesetze können nicht isoliert betrachtet werden, da viele Abhängigkeiten bestehen und sie sich somit gegenseitig beeinflussen.

Einzelne Faktoren wurden bereits von verschiedenen Autoren analysiert. Der Fokus in den vorhandenen Veröffentlichungen liegt jedoch jeweils auf wenigen Faktoren. Auch die Beziehungen zwischen Faktoren wurde bis anhin nur teilweise analysiert. Gesetze und Regulationen wurden ebenfalls isoliert betrachtet, ohne die Konsequenzen ganzheitlich zu analysieren.

Um die Auswirkungen von Cloud-basierten Dienstleistungen ganzheitlich zu verstehen, müssen Unternehmen nicht nur die Vor- und Nachteile von Cloud Computing verstehen. Sie müssen auch die juristischen Gegebenheiten und Problemfelder berücksichtigen. Es muss erkannt werden, dass technische, organisatorische, ökonomische und beziehungs-spezifische Faktoren und juristische Problemstellungen nicht isoliert betrachtet werden dürfen. Die Auswirkungen von einzelnen Faktoren auf andere müssen beachtet werden, um die Risiken und Konsequenzen von Cloud Computing zu verstehen.

In dieser Bachelorarbeit werden die relevanten Anspruchsgruppen vorgestellt, technische, organisatorische, ökonomische und beziehungsspezifische Faktoren gesammelt, diskutiert, und eine XML-basierte Taxonomie wurde entwickelt. Weiterhin werden die Konsequenzen und Verantwortlichkeiten der einzelnen Akteure analysiert. Die gesetzlichen und regulativen Rahmenbedingungen werden, mit Fokus auf den EU und US-Raum, berücksichtigt. Die Beziehungen zwischen den einzelnen Faktoren sowie die daraus resultierenden Konsequenzen der gesetzlichen Rahmenbedingungen werden modelliert und untersucht. Mit zeitbasierten Diagrammen und Szenarien werden auch die Auswirkungen von Änderungen von Faktoren auf andere Faktoren aufgezeigt und die Gefahren für die Akteure diskutiert.

Es zeigt sich, dass viel interdisziplinäres Wissen erforderlich ist, um die Auswirkungen von Cloud Computing zu verstehen. Insbesondere Organisationen, welche sich überlegen, öffentliche oder Multi-Clouds zu nutzen, müssen sicherstellen, dass sie über das nötige

Wissen verfügen, um die Konsequenzen von Cloud Computing zu verstehen. Sie müssen neben den Auswirkungen auf die Organisation auch das juristische Umfeld, die zusätzlichen Problemstellungen in Cloud Federations und die Relevanz der Service Level Agreements kennen.

Abstract

Cloud computing has been on the rise for the last years. It opens new market opportunities, allows organizations to focus on their core competencies and to reduce capital expenditures by having IT services delivered via broadband network connection. Organizations envisioning adopting cloud computing have to consider many different factors, including technical, organizational, economical and relational ones. Legal and regulative constraints increase the complexity even further and can vary in different deployment models and service levels. The different factors, legal and regulative constraints, cannot be considered independently, as they are interconnected and influence each other.

Factors influencing cloud computing have been examined by various authors. However, previous work was focused on few factors. Interrelations have only been partly targeted in previous work, addressing few factors and interrelations. Legal issues arising in cloud computing have been discussed without addressing the consequences to other factors.

To fully understand the consequences of adopting cloud-based services, organizations must not only understand benefits and drawbacks of cloud computing. They must also consider legal and regulative issues. They have to understand that factors influencing cloud-based computing, including legal issues, cannot be considered independently, but that they are interconnected. Furthermore, the different deployment and service models must be considered, as the consequences of cloud computing differ with them.

This thesis aims to increase the understanding of consequences cloud-based computing introduces in organizations. To do this, different stakeholders and their interactions, deployment and service models are introduced. Technical, organizational, economical and relational factors are collected, discussed and a XML taxonomy is developed. The liabilities and consequences for the different stakeholders are explored. The legal and regulative constraints are considered, with the focus on EU and US legislation. Interrelations between factors as well as the consequences of legislation and regulation are modeled and analyzed. Time-based graphs and scenarios are further used to visualize and explore consequences of changes in factors on other factors, and risks for stakeholders are discussed.

It is shown that adopting cloud-based services requires a lot of expertise in many fields. Especially organizations considering the adoption of public, federated or multi-clouds must ensure to acquire the expertise to fully understand the consequences of cloud computing. They must not only consider the consequences on their organization, but also understand the legal and regulative environment, the special implications in cloud federations and the importance of the service level agreements.

Acknowledgments

I would like to thank Prof. D. Burkhard Stiller and the Communication Systems Research Group for providing the opportunity to write this thesis. I would also like to thank Patrick Poullie for co-supervising this thesis.

Special thanks to my supervisor Radhika Garg. Without all her effort, the highly appreciated feedback and discussions, this thesis would not have been completed.

Contents

Zusammenfassung	i
Abstract	iii
Acknowledgments	v
1 Introduction	1
1.1 Motivation	2
1.2 Description of Work	2
1.3 Thesis Outline	3
2 Related Work	5
3 Cloud Computing - Terminology and Stakeholders	9
3.1 Cloud Computing Definition	9
3.2 Cloud Service Models	10
3.2.1 Software as a Service - SaaS	10
3.2.2 Platform as a Service - PaaS	10
3.2.3 Infrastructure as a Service - IaaS	11
3.2.4 Everything as a Service - XaaS	11
3.3 Cloud Deployment Models	11
3.3.1 Public Cloud	12
3.3.2 Private Cloud	12
3.3.3 Community Cloud	12

3.3.4	Hybrid Cloud	13
3.3.5	Multiple Clouds	13
3.3.6	Intercloud	14
3.4	Stakeholders	14
3.4.1	Cloud Consumers	14
3.4.2	Cloud Providers	15
3.4.3	Cloud Brokers	15
3.4.4	Regulators	15
3.5	Interrelations between Stakeholders	15
4	Factors that Influence Cloud Adoption	17
4.1	Technical Factors	23
4.2	Economical Factors	40
4.3	Organizational Factors	47
4.4	Relational Factors	52
5	Legal and Regulative Constraints	55
5.1	Privacy and Data Protection	55
5.1.1	Core Principles of OECD Privacy Guidelines	56
5.1.2	EU Data Protection Directive and General Data Protection Regulation	57
5.1.3	Selected Changes in the EU GDPR Draft	59
5.1.4	US and the Safe Harbor Agreement	60
5.2	Competition Laws	61
5.3	Contracts and Service Level Agreements	62
5.4	Other Legislation and Industry Specific Regulations	63
5.4.1	Copyright	64
5.4.2	Ecological Legislation	64
5.4.3	Industry Specific Regulations	64

5.5	Cloud Specific Issues	65
5.5.1	Outsourcing	65
5.5.2	Location and Cross-Border Data Flow	65
5.5.3	Subcontract Offerings	66
5.5.4	Standard Offerings, Terms of Usage and Service Level Agreements .	67
5.6	Legislative Implications in Cloud Federation Scenarios	67
5.6.1	Roles according EU DPD in Cloud Federation Scenarios	67
5.6.2	Location and Applicable Jurisdiction in Cloud Federation Scenarios	69
6	Interrelations within Factors that Affect Cloud Computing	71
6.1	Interrelations Affecting Availability	71
6.2	Interrelations Affecting Backups	72
6.3	Interrelations Affecting Business Flexibility and Agility	73
6.4	Interrelations Affecting CAPEX	74
6.5	Interrelations Affecting Collaboration	75
6.6	Interrelations Affecting Control	75
6.7	Interrelations Affecting Cost Flexibility	76
6.8	Interrelations Affecting Marginal Cost and Profit	77
6.9	Interrelations Affecting OPEX	78
6.10	Interrelations Affecting Organizational Compatibility	79
6.11	Interrelations Affecting Migration	79
6.12	Interrelations Affecting Legal and Regulative Compliance	80
6.13	Interrelations Affecting Software Assurance	81
6.14	Interrelations Affecting QoS	82
6.15	Interrelations Affecting Return on Investment	82
6.16	Interrelations Affecting Trust towards the CSP	83
6.17	Interrelations Affecting Usability	84
6.18	Interrelations Affecting Vendor Lock-In	85

7	Consequences of Changes in Cloud Computing	87
7.1	Time-Based Graphs Explained	88
7.2	Changes in Trends of Backup on Cost	90
7.3	Changes in Trends of Complexity on Usability	91
7.4	Changes in Trends of Cost on QoS	92
7.5	Changes in Trends of Network Quality on Availability	93
7.6	Changes in Trends of Organizational Compatibility on Migration Time . .	94
7.7	Changes in Trends of Scalability on Business Flexibility	96
7.8	Changes in Trends of Security Configuration and Maintenance on Legal and Regulative Compliance	97
7.9	Changes in Trends of Size of Organization on Marginal Cost	98
7.10	Changes in Trends of Software Assurance on Trust	99
7.11	Changes in Trends of Standards on Vendor Lock-In	101
7.12	Changes in Trends of Traceability and Auditability on Legal and Regulative Compliance	103
7.13	Changes in Trends of Utility Based Computing on Cost Flexibility	104
8	Summary, Conclusion and Future Work	107
8.1	Conclusion	107
8.2	Future Work	108
	Bibliography	109
	Abbreviations	115
	List of Figures	116
	List of Tables	118
	A Factor Index	121
	B XML Taxonomy	123
	C Contents of the CD	127

Chapter 1

Introduction

Cloud computing (CC) offers flexible access to computational infrastructure and resources operated at a remote source [1]. CC has been on the rise for the last years. Google, Microsoft and Amazon are just few examples of companies who offer cloud-based services. Services offered via the cloud range from applications to infrastructure. CC opens new market opportunities, allows organizations to focus on their core competencies and to reduce capital expenditures by having IT services delivered via broadband network connection. While cloud-based services bring many advantages to organizations adopting it, it also introduces risks.

Organizations envisioning adopting cloud-based computing have to consider a multitude of factors. These factors can be assigned to different fields, such as technical, organizational, economical and relational. Legal and regulative constraints increase the complexity further and vary depending on the location of the different stakeholders. Different deployment models and service levels can lead to a variety of important considerations. All these factors including legal and regulative constraints cannot be considered by themselves. They are interconnected and influence each other.

Factors influencing CC have been examined by various authors. However, the focus of previous work was based on few factors. Interrelations have only been partly targeted in previous work, focusing on few factors and interrelations. Legal issues arising in cloud computing have been discussed without addressing the consequences to other factors. To fully understand the impact of cloud-based computing, the consequences of interrelations and the risks of changes within factors cannot be neglected. They must be carefully studied.

1.1 Motivation

The decision to outsource IT services, to what extent and how should not be taken lightly. It can have extensive consequences on an organization. To understand the consequences, it is important to gain a better understanding of CC and the legal and regulatory framework. To achieve this it is not enough to understand benefits and drawbacks of CC without considering the applicable legislation carefully. Organizations have to realize that factors influencing cloud-based computing, including legal issues, cannot be considered independently, but that they are interconnected.

Organizations that want to benefit from CC, do not only have to choose from a variety of cloud providers, but also from a range of service and deployment models. These service and deployment models introduce differing advantages, disadvantages and legal issues that have to be considered. In addition, cloud federations increase the complexity even further.

It is the motivation of this thesis, to help decision makers in organizations considering CC adoption to gain a better understanding for CC and its consequences. It aims to increase the understanding of factors to be considered, the legal and regulative constraints, the interrelations between factors and legislation, and how changes in factors can have consequences on other factors.

1.2 Description of Work

This thesis aims to increase the global understanding of consequences in an organization by adopting cloud-based services. To achieve this, the different stakeholders and their interactions as well as deployment and service models are introduced.

To increase the global understanding of CC, technical, organizational, economical and relational factors are collected, discussed and broken down into sub-factors. These factors are used to develop an XML taxonomy. The liabilities and consequences for stakeholders are explored and discussed for the various factors in different deployment and service models. The XML taxonomy and the complete overview of all factors considered, including an index where they are discussed, is to be found in Appendix A and Appendix B.

The legal and regulative constraints are considered, with the focus on EU and US legislation. Interrelations between factors as well as the consequences of legislation and regulation are modeled and analyzed.

Finally, relations between factors and influences of legislation are explored further using time-based graphs and scenarios. The consequences and impact of changes in factors on other factors are visualized and discussed. Risks for stakeholders arising from changes are explored.

1.3 Thesis Outline

This thesis is structured as follows: Chapter 2 provides information on the related work regarding factors, interrelations and the legal and regulative constraints in CC. Then, in Chapter 3, CC, the stakeholders and their incentives, deployment and service models are introduced and the terminology used in this thesis defined. Chapter 4 and Chapter 5 provide an overview of the technical, organizational, economical, relational factors and the legal and regulative constraints that have to be considered. The legal and regulative constraints focus on the EU and the US. The next chapter, Chapter 6, shows and discusses interrelations between factors and the influences of legal and regulative constraints. In Chapter 7, time-based graphs and scenarios are used to explore consequences of relations between factors further. The effects of changes in factors on other factors and risks for stakeholders are discussed. The last chapter summarizes the findings, draws conclusions and explores options for further work.

Chapter 2

Related Work

The related work of this thesis can be grouped into the following categories:

- Factors that influence cloud adoption (group 1)
- Interrelations and influences between factors (group 2)
- Legal and regulative constraints in the context of CC and the legal implications of cloud federations (group 3)

Factors influencing Cloud Adoption

Factors influencing cloud adoption are identified and explored by several authors. [23] analyzes success factors for deploying CC and the importance of relational, technical and managerial factors for cloud adoption success. It concludes that trust, managerial capability, and technical capability all significantly influence cloud deployment performance.

[11] applies the Technology-Organization-Environment (TOE) framework towards CC adoption and considers factors from these three domains. It concludes, that the perceived advantage of CC, management support and high competition intensity are positively associated with the decision to adopt CC.

[36], [47] and [44] also consider CC from a TOE perspective, exploring different technological, organizational and environmental factors. While all this work builds on the TOE framework, the factors identified and explored differ. Findings include that cloud adoption is positively influenced by collaboration, size of an organization and technical advantages of CC, such as scalability. Organizations with low IT requirements are less likely to adopt cloud-based computing.

[48] carries out an empirical analysis for factors that are affecting CC adoption, including factors that are considered advantageous (*e.g.* scalability, flexibility) and disadvantageous (*e.g.* loss of control, lack of standard). It concludes that the study evinces that there are overall net benefits in adopting CC.

[59] applies the Diffusion of Innovation (DoI) theory and Technology Acceptance Model (TAM) toward cloud adoption. It focuses on compatibility, relative advantage, complexity, image, security and trust. [24] explores factors which benefit cloud adoption or rise concerns, and includes legal issues. It concludes that understanding the benefits is crucial for cloud adoption, and that different deployment models have to be considered.

[7] discusses the top ten obstacles and opportunities for CC. It concludes that CC will grow and acknowledges the importance of scalability.

Other related work focuses on few factors, analyzing them in depth or comparing them to other technologies. [31] compares CC, grid and cluster computing. While doing so, it identifies several advantages and disadvantages of CC. The identified advantages of CC include shared resources, utility based computing and cost savings, while disadvantages include reliability, required network quality and the non-interoperability.

[8] discusses fault tolerance challenges, used techniques and implementation in CC. [61] focuses on security and privacy challenges in CC. It concludes that CC is still in its “infancy”, and that further development of the security and privacy landscape has a major impact on widespread CC adoption. [52] explores portability and interoperability issues in cloud-based computing, also exploring the requirements for multiple clouds.

[25] applies a SWOT (Strength, Weakness, Opportunity, Threat) analysis on CC for Small and Medium Enterprises (SME), focusing on key drivers and inhibitors of CC. It concludes, that CC allows SMEs to benefit from reduced costs, faster updates and scalability but that security is a major concern.

[56] introduces the Service Measurement Index (SMI) by the Cloud Service Measurement Initiative Consortium (CSMIC). The SMI is a hierarchical framework, grouping factors influencing cloud-based computing into seven characteristics with three or more attributes for all the characteristics. The framework aims to help decision makers with an objective measure of cloud services that is easy to use and can manage the performance. The seven groups of the framework include accountability, agility, assurance, financial, performance, security and privacy, and usability. Compared to the SMI framework, this thesis groups factors into four different fields (technological, economical, organizational and relational) and considers more factors.

[55] introduces the Multiple Attribute Decision Methodology for Adoption of Clouds (MADMAC). It discusses factors which influence cloud adoption, but the focus lies on the Decision Support System (DSS). It focuses on different factors in CC and acknowledges the importance of trade-offs between these factors.

[22] focuses on quality of service (QoS) and introduces a framework to rank services based QoS attributes. It is built upon the previously discussed SMI framework.

All of the above work introduces relevant factors, and is considered as group 1 of related work.

Interrelations between Factors

[21] introduces a comprehensive list of technical, economical and organizational factors that influence CC adoption. While some previous work has recognized that factors can be interrelated (*e.g.* [55], [24]), they neither discuss nor visualize such interrelations. [21] stresses the importance of interrelations and several are discussed.

Group 2 only contains [21], as it does not only acknowledge interrelations, but also discusses some. Group 2 does not explore interrelations in the same depth as this thesis, nor are the influences of changes of one factor on other factors considered.

The related work in group 1 and 2 were used as starting point for the created XML taxonomy. Group 2 has also been used for an initial set of interrelations between factors.

Legal and Regulative Constraints and Implications of Cloud Federations

The third group is previous work on legal and regulative issues. As the implications of cloud federations are also based on legal and regulative issues, this contains both the general legal issues, and the cloud federation issues. Some of the related work in group 1 and 2 have included legal and regulations as factors to be considered (*e.g.* [24], [21]), but not to the required depth needed for this thesis.

[9] introduces an in-depth analysis of legal and regulative aspects to be considered in CC. It includes a SWOT analysis of CC in general, the applicable regulations and cloud specific issues with a focus on Germany and the EU, and how to design legally compatible cloud systems.

The other related work in the third group is focused on specific legal issues. [13] and [4] focus on data protection issues in CC. [4] compares the different legislations and regulations that affect privacy and their influence on CC. It concludes that more awareness regarding privacy issues in CC is required. [13] focuses on the OECD core principles of data protection and explores the consequential issues with CC. [32] focuses on contracts and service level agreements and concludes, that SMEs may lack the negotiation power to decrease risks introduced with CC.

[33] explores the legal issues regarding applicable roles and jurisdiction in CC federation scenarios. It concludes that data protection in cloud federations is more complex than in other cloud deployment models, and every case needs to be carefully analyzed.

[12] introduces the main differences between the currently applicable legislation in the EU and the one that should replace it in the near future. Other areas include cross border data flow issues [58], regulations that are sector specific [28], anti-trust [66] and security [30].

While all this work is in depth, direct consequences on other factors in CC are not considered. The related work from group 3 and the corresponding legislative text is used to identify the legal and regulative constraints.

Overview of Related Work and Identified Gaps

The following table provides an overview of how existing work is related to this thesis:

	Group 1	Group 2	Group 3	this Thesis
Factors influencing CC Adoption	yes	yes	partly	yes
Legal and Regulative Constraints	partly	partly	yes	yes
Implications of Cloud Federations	no	no	yes	yes
Interrelations between Factors, Legal and Regulative Constraints	no	yes	no	yes
Consequences and Risks of Changes in Interrelated Factors	no	no	no	yes

Table 2.1: Related Work

In the existing work several gaps have been identified, mainly in the consequences of legal and regulative constraints, and in the interrelations between factors. This thesis aims to fill these gaps by:

- Introducing a comprehensive list of factors influencing CC adoption, grouped into four different categories, describing each and discussing potential issues with these factors for different stakeholders
- The influence of legal and regulative constraints on CC
- A visualization and an in-depth discussion of interrelated factors and legal and regulative constraints
- The consequences of changes in one factor on others using time based graphs
- The risks introduced by the consequences of changes

Chapter 3

Cloud Computing - Terminology and Stakeholders

3.1 Cloud Computing Definition

CC is a technology model in which resources, such as software, processing power and storage are delivered over the Internet [26]. The National Institute of Standards and Technology (NIST) defines CC as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.* networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [41]. The offerings from cloud providers can vary considerably and can be split into different service models, which will be discussed in Sector 3.2.

The essential characteristics of CC include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [41].

- **On-demand self-service** allows consumers to increase computing capabilities without “human interaction with the service providers”.
- **Broad network access** is about the way the services are accessed. The services are accessed via a network, usually the Internet.
- **Resource pooling** refers, from a provider’s perspective, to the fact that “resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumers demand”.
- **Rapid elasticity** is about scalability, either inward or outward, often automatically to match demand.
- **Measured service** is about optimizing resources and control using an appropriate type of abstraction for the service. Depending on the service, the measured resource could be storage, processing, bandwidth etc. This allows both the cloud consumer

and the cloud provider transparency in the sense that it can be monitored, controlled, and reported.

In CC, consumers often only pay for the resources they need, removing the need for huge up front investments and allowing to scale the cloud solution to match the growth of the company. However, this is highly dependent on the deployment models, which will be discussed in Chapter 3.3. CC also allows for cloud consumers to access services where they have no previous operational knowledge [3]. Furthermore, it increases flexibility and minimizes the technical expertise required in the consumers organization, as the provider is responsible for the infrastructure [47].

In comparison to grid computing, users neither do have to change their working environments, nor do they have to learn new commands to access the service [3]. CC is also considered more simple than grid computing [67], as it requires less expertise from the user and therefore is available to more users.

3.2 Cloud Service Models

While CC services were initially split into three different service layers, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), there exist many more services as of today which are delivered via cloud [21], “literally everything” [26]. In the following section not only the three original services are introduced, but also several others, which are often combined as Everything as a Service (XaaS).

3.2.1 Software as a Service - SaaS

A software distribution model, where the software can be accessed via various devices, running on a cloud infrastructure. The underlying cloud infrastructure and software are managed and controlled by the service provider [41]. SaaS allows consumers a simple access to software with typically very little administration effort, but introduces issues such as dependency on network connection, latency and lock-in effect. An example for SaaS is Google Apps for Work¹.

3.2.2 Platform as a Service - PaaS

PaaS allows users to deploy, manage and run their own application on the cloud. As in SaaS, the underlying infrastructure is managed by the cloud provider, but the consumer has control over the application and the settings. [41] An example for PaaS is Microsoft Azure Cloud Services².

¹<https://www.google.com/work/apps/>

²<http://azure.microsoft.com/en-us/services/cloud-services/>

3.2.3 Infrastructure as a Service - IaaS

In IaaS, the consumer still does not manage the underlying cloud infrastructure, but can provision fundamental computing resources, such as processing, storage, and networks to deploy any software. Therefore, the consumer has a lot more control over operating systems and applications. [41] An example for IaaS are virtual machines in Microsoft Azure³.

3.2.4 Everything as a Service - XaaS

In cloud everything is treated as a service [69], which is referred to as XaaS. XaaS includes a variety of services, such as:

- **Communication as a Service - CaaS:** Enterprise communication systems, this can include VoIP, IM, and video conference services.
- **Desktop as a Service - DaaS:** A service model where virtual desktops are hosted in the cloud. VMWare offers DaaS as Horizon Air Desktop⁴.
- **Databases as a service - DBaaS:** Includes the storage and management of structured in the cloud. One example for DBaaS is Oracle Cloud⁵.
- **Monitoring as a Service - MaaS:** Cloud monitoring functionalities for other cloud services and applications, allows to monitor and track the dynamic infrastructure. An example for MaaS is DataDogHQ⁶.
- **Security as a Service - SECaaS:** Everything security related as a service, typically includes anti-virus, intrusion detection, security event management etc. McAfee Security-as-a-Service⁷ is one of the current SECaaS providers.
- **Storage as a Service - STaaS:** Storage space in the cloud, allowing portable access. Examples include Google Drive⁸ and Microsoft OneDrive⁹.

3.3 Cloud Deployment Models

Not only the service models can differ, but “clouds” can also be deployed in different models. This section introduces these different cloud deployment models. The importance of factors and legal aspects can vary in different deployment models, therefore it is essential to distinguish and understand the differences between them. The differences between the

³<http://azure.microsoft.com/en-us/services/virtual-machines/>

⁴<http://www.vmware.com/cloud-services/desktop/horizon-air-desktop>

⁵<https://cloud.oracle.com/database>

⁶<https://www.datadoghq.com/>

⁷<http://www.mcafee.com/us/products/security-as-a-service/index.aspx>

⁸<https://www.google.com/drive/>

⁹<https://onedrive.live.com/>

scenarios will be discussed in ownership, control, security and privacy concerns as well as for the initial costs for the user of the cloud.

	Public C.	Private C.	Community C.	Hybrid C.	Multi C.
Ownership	Third Party	Depends	Depends	Depends	Depends
Control	Low	High	Medium	Medium	Depends
Security and Privacy Concerns	High	Low	Medium	Medium	Depends
Required Initial Investment	Low	High	Medium	Medium	Depends

Table 3.1: Overview Cloud Deployment Models from Cloud Consumers' Perspective

3.3.1 Public Cloud

Public clouds are open for the use of general public and multi-tenant capable. They are owned and controlled by the cloud owner, which can be a private business, the government, or an academic institution [41]. Public clouds introduce higher risks regarding to security and privacy, but require less expertise due to reduced difficulty and financial investment as other cloud deployment models.

3.3.2 Private Cloud

The services and infrastructure of a private cloud are for exclusive use of one organization. The cloud can be owned, operated and managed by the organization itself or by a third party which sells it as a service to the organization [41]. As private clouds are for exclusive use of one company, they rise less security and privacy concerns. [29] compare private clouds to the intranet, where only members of the users organization has access to the service. Private clouds require large initial investments.

3.3.3 Community Cloud

Community clouds are clouds which are for a specific group of customers/organizations. These organizations usually share similar requirements towards the cloud, such as security, compliance level, and availability. The cloud can either be owned and controlled by the group, by a specific member or a group of members, or by a third party [41]. Community clouds are often used when several organizations are working on joint projects. Costs can be split between the different community members, therefore community clouds are more expensive than public clouds, but cheaper than private clouds. Security and privacy concerns are lower than in public clouds, as only members of the community can access the cloud.

3.3.4 Hybrid Cloud

Hybrid clouds are compositions of two or more clouds, which communicate with each other using open or proprietary standards to allow data and application portability [41]. Within this thesis, a hybrid cloud defines a cloud which is composed of private and public clouds. Other cloud compositions will be discussed in the next section. Hybrid clouds allow to have more sensitive information in the private part, but still benefit from a public cloud, where it is possible. As only a part of the infrastructure is hosted privately, the costs range between a public and private cloud. As sensitive data can be kept on the private cloud within the hybrid cloud, security and privacy concerns are lower than in pure public clouds.

3.3.5 Multiple Clouds

Hybrid clouds are not the only clouds composed of more than one cloud. To distinguish federated clouds from other multiple clouds, both the terms are introduced. The usage of the term multi-cloud is not consistent in the existing literature. In this thesis, the approach of [19] and [53] is followed and it is distinguished between the terms multi-cloud and federated cloud.

Multi-Cloud

A multi-cloud is a cloud that is formed by two or more independent cloud services. For the consumer, it is clear that there are several cloud providers and the consumer is aware of them. Unlike the federated cloud environment, it is the consumer's responsibility to set-up contracts with the involved cloud providers, unlike in federated clouds, where the consumers would typically have a contract with a broker [19], [53]. A hybrid cloud is therefore a special case of a multi-cloud. multi-clouds can include privately and publicly owned and controlled clouds. Costs, security and privacy concerns highly depend on the case, but are typically in between private and public clouds.

Federated Cloud

As in multi-cloud, the cloud federation is a composition of several clouds. As “a next step of evolution” in CC, cloud federation allows cooperating providers to fulfill the requests of another cloud provider [65]. [35] introduce cloud federations to further increase flexibility, interoperability and to counter vendor lock-in effects. However, unlike in the multi-cloud scenario, the consumer is not aware that there are several different cloud providers in the background. The cloud provider, or broker (see Section 3.4), whom the consumer has a contract with, is responsible for guaranteeing the agreed upon Service Level Agreements (SLA, further discussed in Section 4.4.3 and Section 5.3) [53]. As with multi-clouds, costs, security and privacy depend on the concrete case, but are typically in between private and public clouds.

3.3.6 Intercloud

The term intercloud refers to the “cloud of clouds”. While multiple clouds are interconnected, the vision of intercloud is that it “will have the dimensions of one machine comprised of all servers on the planet” [10]. As the intercloud is still a vision, it is not further discussed regarding to costs, privacy and security concerns and is not included in the overview table.

3.4 Stakeholders

In the following section the different stakeholders and their role in CC are introduced. To understand the factors and interrelations that will be discussed in Chapter 4 it is important to know the different roles and their motivation.

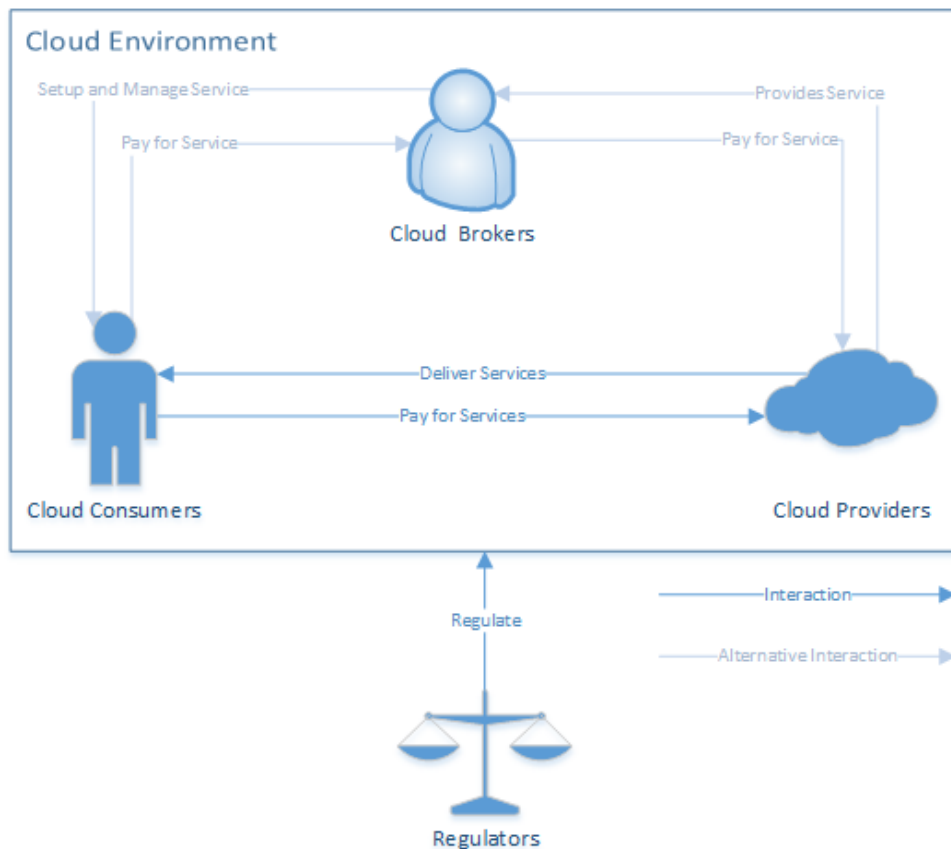


Figure 3.1: Overview of Stakeholders and their Interactions

3.4.1 Cloud Consumers

Cloud Consumers, or Cloud Service Consumers (CSC), are the subscribers of a cloud service. They can be end-users, or use the cloud service to support their customers with a

product. They pay a fee to use the service of the cloud providers. From an organizational perspective, the main motivation to use cloud providers is the promise of scalability and resource availability while being able to reduce IT capital and operational cost, since neither the equipment must be maintained nor the expertise kept in-house. It allows organizations to have access to technologies and take advantage of expertise that they might not be able to afford otherwise [38], [23], [63].

3.4.2 Cloud Providers

Cloud providers, or Cloud Service Providers (CSP), operate and own the cloud systems to deliver them as services. They are responsible for any maintenance and update of hardware and software used in their cloud. Furthermore, they are responsible for pricing of the cloud service and the corresponding SLAs. Their motivation is to sell their services to the CSCs, which can include software, platform, infrastructure or any other service model [38].

3.4.3 Cloud Brokers

Cloud brokers, or cloud service brokers (CSB), act as an intermediary between CSCs and CSPs. CSCs can contact CSBs instead of directly approaching CSPs, if the direct integration is too complex [2]. The CSB can act as enabler that provides additional services such as “facilitate the delivery, adoption and use of cloud computing” [38]. An enabler is usually expected to build and often maintain the hybrid cloud system. As [38] states, enablers are often necessary as CSPs “lack the core competencies of interacting with customers and actual implementation” and expects that the importance of a CSBs’ role continues to rise.

3.4.4 Regulators

[25] defines regulators as “international entities that permeate across the other stakeholders”. While all previous stakeholders are part of the value chain, the regulator’s role pervades across the value chain [38]. The role and effects of the regulators are further defined and discussed in Chapter 5.

3.5 Interrelations between Stakeholders

Graph 3.1 shows the different interactions between the stakeholders. While the regulators act from outside, setting the legislative framework, all the other stakeholders directly interact with one another. The CSC uses the services of the CSP, and typically pays for the provided service. The CSP is responsible to provide the service to the consumer. In public cloud services, especially in SaaS scenarios, the CSP often has an alternative

business model than being payed by the CSC (*e.g.* gmail, ad based business model). The CSB is not involved in all scenarios. Instead of directly contacting cloud providers, the CSC might use a CSB in between. The CSB might only act as consultant and support the CSC in choosing an appropriate CSP, or resells the offers from one or multiple CSPs.

Chapter 4

Factors that Influence Cloud Adoption

The decision to adopt CC and evaluating CSPs is highly dependent on many factors, which can act as motivators or barriers in cloud adoption [47]. It is important to understand these factors and how they differ for the various deployment and service models, to make sure the chosen cloud-based solution fits the requirements [21]. In this chapter, these factors are introduced and discussed. These factors often influence each other. They are also influenced by legal and regulative constraints introduced in the next chapter. The interrelation within these factors and the influences from regulation is discussed in Chapter 6. These constraints directly influence the relation networks within factors, which can be mutually dependent or result in trade-offs that should be considered [20].

The factors have been collected and categorized. Where reasonable, the factors have been broken down further. An XML taxonomy was developed to structure the factors (Appendix B). While several authors have discussed factors that influence cloud adoption, most have focused on a few and discussed them in depth, neglecting interrelations or only discussing the interrelations between few factors. For this thesis, it was decided to follow the approach of [21] and categorized the factors as technical, economical, and organizational. Instead of adding factors that reflect the relation between an organization and its environment to organizational factors, the category relational from [37] was used. Other approaches include the categorization in non-technical [39] and technical, managerial and relational [37] factors. Factors identified from other papers have been reassigned to the categorization used in this thesis. The factors are listed alphabetically, and are not sorted according to importance. Unless explicitly stated, the factors are discussed from an CSC's perspective.

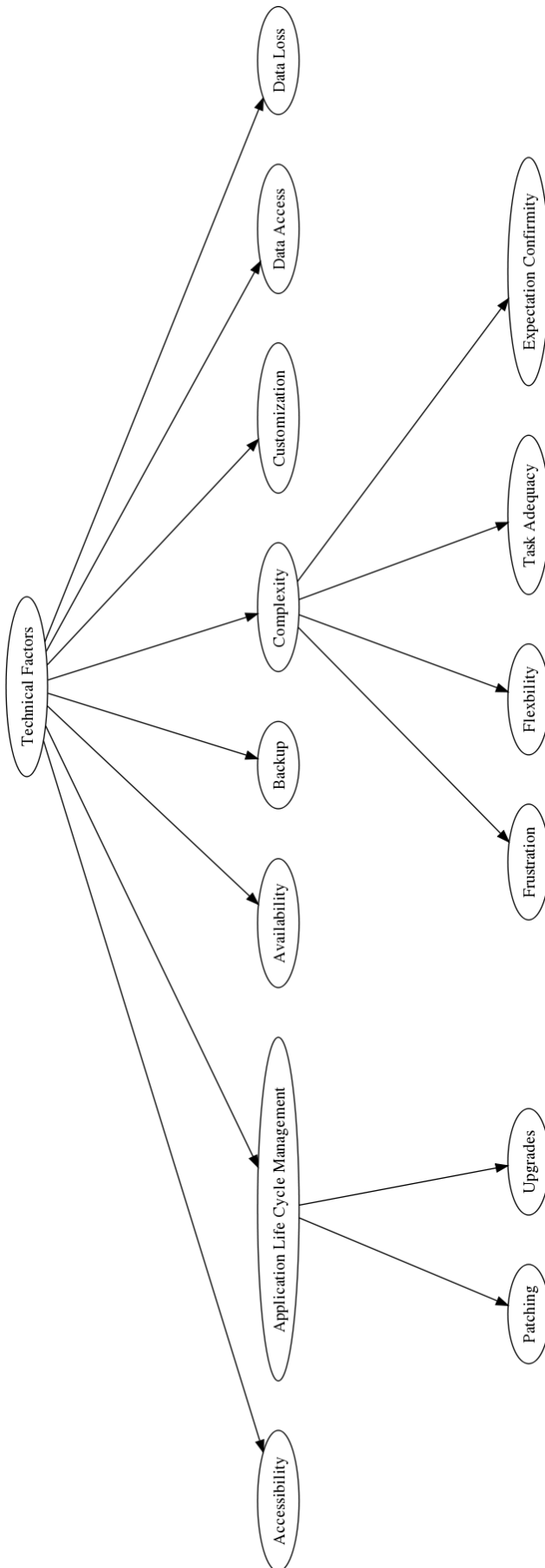


Figure 4.1: Overview of Technical Factors 1/5

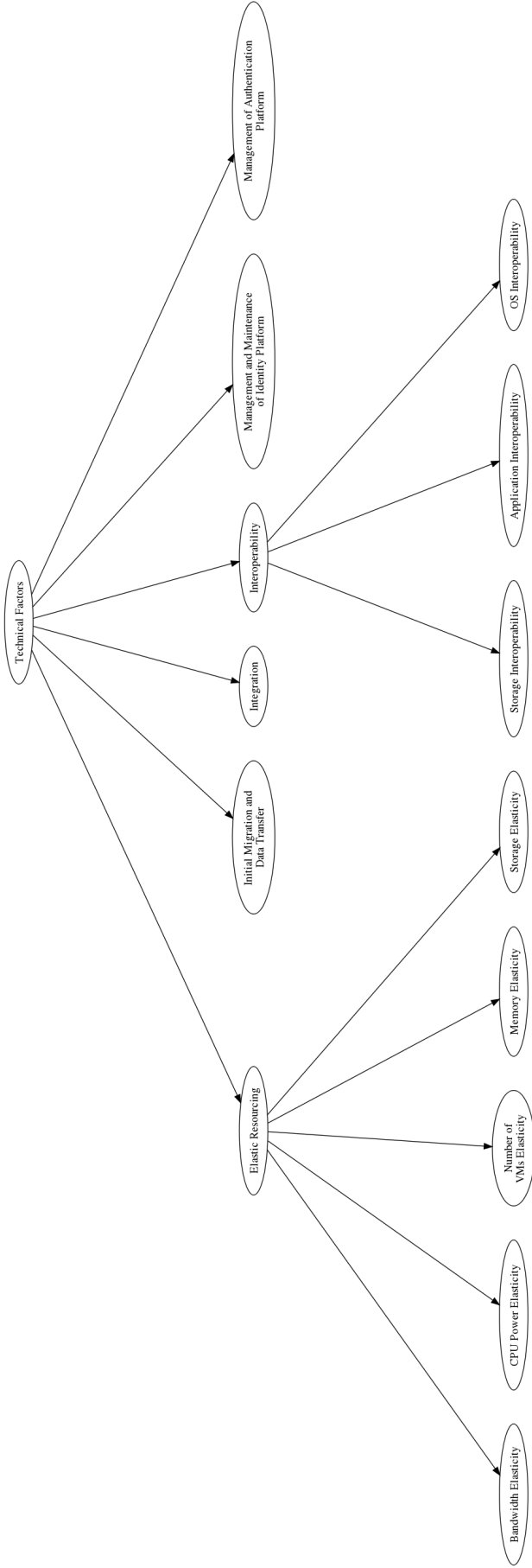


Figure 4.2: Overview of Technical Factors 2/5

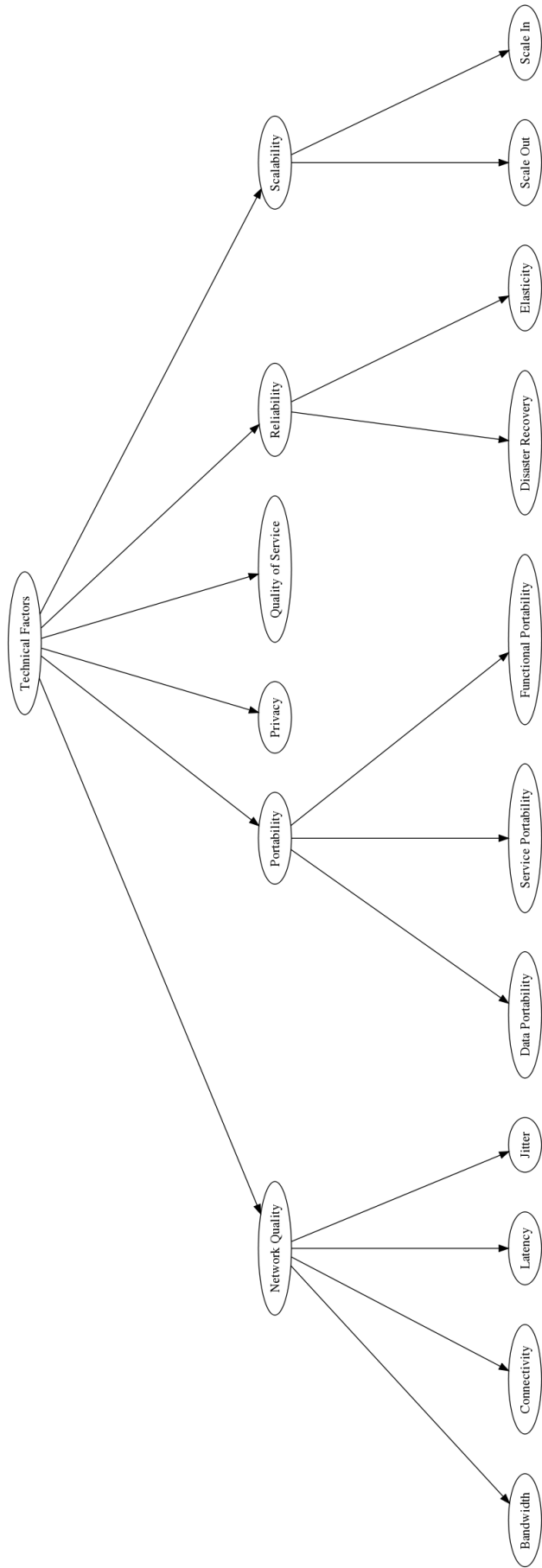


Figure 4.3: Overview of Technical Factors 3/5

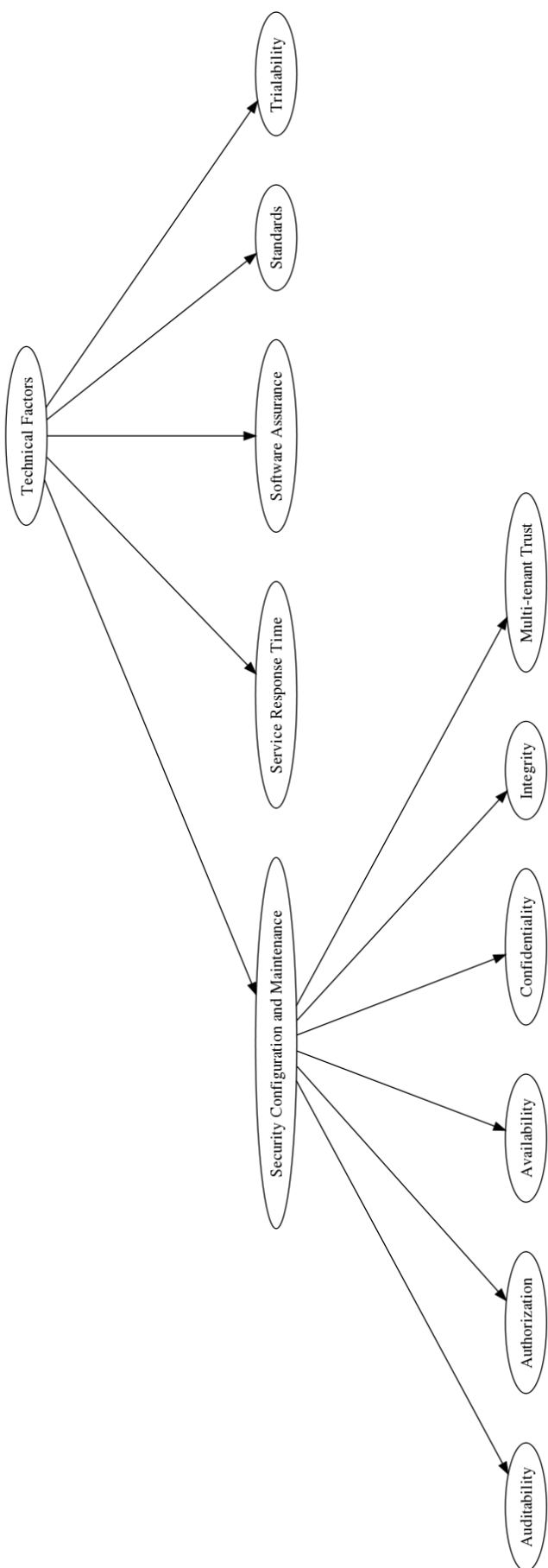


Figure 4.4: Overview of Technical Factors 4/5

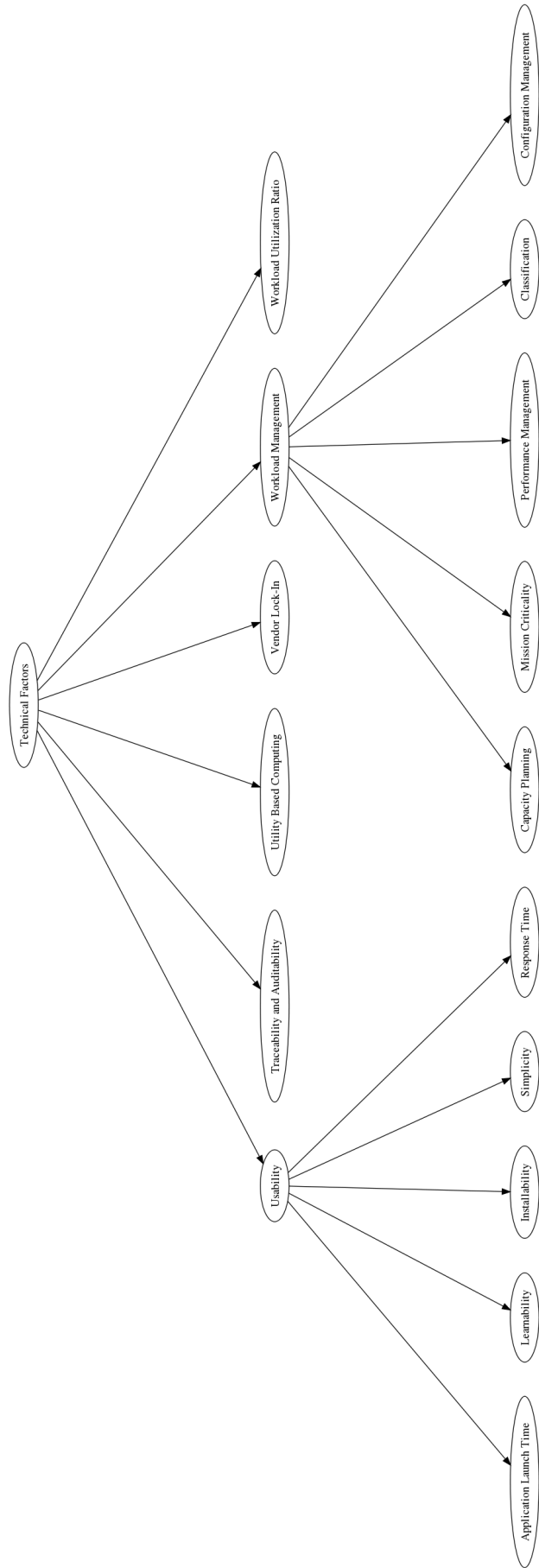


Figure 4.5: Overview of Technical Factors 5/5

4.1 Technical Factors

Technical factors include all the factors, which are required for the functionality of an organization. They include physical resources (such as computers and network equipment) and collective resources that give organizations functionality [23].

4.1.1 Accessibility

Accessibility refers to the difficulty to access a service. Cloud-based services are delivered via broadband network connections and therefore accessible from anywhere anytime. For SaaS, accessibility often includes independence of the device used, *e.g.* the service can be accessed from mobile devices. Accessibility is less important for other service models, as CSCs run their own applications and therefore they can control the accessibility. Accessibility is beneficial for CC and important for all deployment models. CSPs are not liable to offer solutions with high accessibility, but it increases the attractiveness of their service. CSCs who need certain accessibility (*e.g.* mobile access) should compare different providers and include it in the contract.

4.1.2 Application Lifecycle Management

Application Lifecycle Management (ALM) generally refers to the different phases of software development, from initial planning to retirement. In a cloud environment, ALM depends on the perspective taken. From a consumer's point of view on a SaaS level, ALM is handled by the CSP. However, from a consumer's point of view on PaaS level who uses cloud to host an application, changes in the environment on the cloud have to be taken into consideration. Furthermore, when migrating a legacy application to the cloud or migrating to a new cloud solution, the life cycle of the existing/to be replaced application has to be considered. CC allows for simpler ALM and is therefore an advantage for cloud-based computing adoption. ALM can further be broken down into patching and upgrades, while advantages and disadvantages stay the same.

Patching

Using cloud services to host your own application, in any cloud deployment model, allows for centralized patching. Instead of releasing and distributing a patch to the end users, the patch can be applied on the cloud, and does not require any further interactions from the end users.

Upgrades

Similar to patching, upgrades for applications hosted in the cloud can be installed directly. They do not require any interactions from end users. All users work with the same version of the application.

4.1.3 Availability

Availability is the time that a system is accessible and usable by an authorized entity. It can be measured by dividing the time it was available through the total time. Public CSPs typically offer higher availability than traditional architectures [60]. Multiple data centers, redundancy and failover mechanism help to increase availability. Availability therefore is a benefit of CC. In private cloud deployment models, availability is similar to traditional systems. The liabilities are defined in the SLAs. The risks of low availability for the CSCs is highly dependent on applications they run in the cloud. An application which does not directly influence the core business of an organization will not affect the company as a more crucial one. For CSPs, the risks include financial losses and reputational damage, if they do not deliver an availability as promised by the SLAs.

4.1.4 Backup

Backups protect against data loss and the lack thereof results in a immense business risk. Depending on the service model, the responsibilities differ. In a SaaS and PaaS scenario, the CSP should ensure backups. The terms and liabilities are usually defined in the SLAs. In case of data loss, the CSP does not only risk demands based on the contracts and SLAs, but it can also lead to reputational damages, which are difficult to quantify.

Considering IaaS scenarios, it is the CSC's responsibility to ensure backups. The lack of backups can result in data loss. Not all data is equally important. The loss for CSCs, financial and reputational, highly depends on the importance of the data. CSCs might also want to consider to use a different CSP to backup data from SaaS and PaaS. This allows them to have better control over their data, as they still own a copy of the data, even if the CSP fails to create its own backups or goes out of business.

4.1.5 Complexity

Complexity refers to the difficulty to understand a new technology and how easy it is to use. It can be measured by quantitative and qualitative feedback from users. There are no liabilities for the CSC or CSP. However, it is in the interest of CSPs to offer services with low complexity, as they are more attractive to CSCs. Complexity is important for all deployment models. From a service level perspective, it is especially interesting in a SaaS scenario. In SaaS, the cloud-based solution will directly be used by the end users. In other service models, the cloud-based service is used to host own applications, services or storage. While complexity is of course still relevant in the other service models, the number of people affected by complexity is smaller, *e.g.* when a developer publishes an web-application on PaaS, the complexity of the PaaS will only affect him, the complexity of his application all the users. Complexity can be further broken down into the following sub-factors [59]:

Frustration

Frustration refers to the perceived difficulty to fulfill a certain task.

Flexibility

Flexibility refers to how rigid the system is, *i.e.* if there are multiple ways to achieve the same goal or if a very specific order of steps has to be taken.

Task Adequacy

Task adequacy is about the adequacy of the system to complete a given goal. A system which has a perceived low complexity has a high task adequacy.

Expectation Conformity

Expectation conformity is about the expected behavior of a system. If a system behaves differently than a user expects, the perceived complexity is higher.

4.1.6 Customization

Customization refers to the degree a service can be adjusted to ones needs. For CC, this can refer to the software solution in a SaaS scenario or the specifications of a VM in an IaaS scenario. Customization is hard to measure and there is no liability for the different stakeholders. However, highly customizable solutions can be more attractive for CSCs. Therefore, it is in the interest of CSPs (and CSBs) to offer solutions which have high customization. The consequences for CSCs, when choosing a solution with is not very customizable, depends on the service. In a SaaS scenario, a highly customizable solution can be adjusted to the needs and current processes of the organization. If the solution does not allow any customization, the business processes need to be redesigned. In an IaaS scenario, a highly customizable solution can be adjusted exactly to the needs of the customer.

4.1.7 Data Access

Adopting cloud-based services often means that data is being moved outside the organization. Many companies fear that third parties can access their data in CC, especially in public cloud models. In private cloud scenarios, data access is usually not an issue, as the CSCs still have full control over their data.

Before CSCs decide upon a CSP it is therefore important to review the CSP's security practices [60]. The CSPs liability is to protect the data of their customers and make sure that no unauthorized parties can access it. Data access is more of a concern in SaaS and PaaS scenarios, than in IaaS scenarios. In IaaS, CSCs have at least partial control over data access, as they can use encryption to protect data from third parties. The risk of unauthorized data access, for both the CSC and CSP, is in financial losses (contracts with other parties) and reputational damages.

4.1.8 Data Loss

The risk of data loss must be considered. Data loss can have catastrophic consequences for companies, therefore the risk must be evaluated, compared to legacy approaches, and it must be clear who is accountable for data losses. The risk of data loss is applicable in all deployment scenarios. Liability questions should be addressed in the SLAs. The risk and the consequences of data loss are difficult to quantify. Financial and reputational losses depend on the importance of the data.

4.1.9 Elastic Resourcing

Elastic resourcing refers to the adjustability of resources to match demand. The goal of elasticity is, that the automatically provisioned resources match demand as closely as possible at any given time [27]. Elastic resourcing is a major advantage of CC. Especially public clouds and multiple-cloud deployment models can benefit. Elasticity can be measured by the mean time to expand or contract the service capacity and the maximum capacity [22]. The importance of elasticity is especially high for applications which tend to fluctuate and spike at certain times (*e.g.* online TV streaming and a highly anticipated soccer game). Elastic Resourcing can be further broken down into the different resources in computing.

Bandwidth Elasticity

The elasticity of the assigned and available network bandwidth.

CPU Power Elasticity

Refers to elasticity in processing power of cloud services.

Number of VM Elasticity

Instead of increasing processing power and available memory in existing VMs, the number of VMs can also be elastic.

Memory Elasticity

The amount of primary memory that is available to services.

Storage Elasticity

The amount of storage that is available to services.

4.1.10 Fault Tolerance

Fault tolerance refers to the effects faults have on the system. Fault tolerance in CC requires “careful consideration and analysis”, due to the complexity and inter-dependability of cloud-based computing [8]. Depending on the deployment model, an instance of a server might run on multiple virtual machines, in a multiple cloud scenario on the hardware of different CSPs. If there is a fault caused at one CSP, it should not affect the others. Also, in public clouds, if there is an issue caused by a customer, the others should not be affected by it. Ensuring fault tolerance is the CSPs responsibility.

Reactive

Reactive fault tolerance reduces the effects of an error after it occurred. This happens using recovery mechanisms, such as check points and restart, replication, or user defined exception handling [8].

Proactive

Proactive fault tolerance is about avoiding faults before they happen. Proactive fault tolerance is about preventing recovery mechanisms [8].

4.1.11 Functionality

When considering adopting cloud, especially when considering adopting a SaaS solution, the functionality of the software will be compared to legacy applications. [3] notices, that cloud applications might be lacking features compared to legacy applications. While this is dependent on both the legacy solution and the cloud solution, the functionality affects the decision if a legacy software should be replaced with SaaS. As mentioned by [60], cloud applications “were not as feature rich as premised based solutions”. Even though that has changed in the last years, CSCs have to make sure that “critical features and controls are available in the offering”. The lack of features can hinder cloud adoption, this applies to all deployment models.

4.1.12 Initial Migration and Data Transfer

Adopting cloud-based services can lead to situations where existing data, which was kept on premise, has to be transferred to the CSP. If a private cloud solution is acquired, and hosted within the same premise as before, the data can be easily transferred to the new solution. As [7] states, migrating data to external locations via network connections can take a long time (over 45 days for 10TB at 20Mbits/sec) and that shipping data via hard disks is often faster. Several CSPs do offer such services. Depending on the data, it might even change within the time it is migrated. Therefore, it is important that data is migrated as fast as possible and synchronized before the system is changed. Issues in data migration can occur at every service model, it can be measured in time and hinders cloud adoption. While CSPs are not forced to reduce these barriers, they can reduce migration issues by supporting standards and resumable uploads.

4.1.13 Integration

Integration is the configuration of multiple applications which involve some degree of functional dependence [50]. Integration requires interoperability (see next section), but goes a step further. Integration is about forming a system, to fulfill the required tasks of the users. Therefore, an integrated system requires interoperability, but interoperability does not automatically lead to an integrated system.

In the context of CC, integration has several implications. First of all, a cloud based solution might be integrated with existing traditional systems. Only part of larger system might be migrated to the cloud. Secondly, integration can also occur between different solutions of different CSPs.

To ensure integration, the interoperability of both the existing system and cloud system (or two different cloud systems) must be checked. In a multiple cloud, including hybrid cloud scenario, it is of course the CSP's or CSB's responsibility to ensure integration between the different solutions. CSCs should ensure interoperability between existing systems and different cloud solutions.

4.1.14 Interoperability

Interoperability in a cloud context refers to the extent cloud systems can communicate with each other, allowing for information to be shared between two or more systems [52]. In comparison to integration, for which interoperability is needed, the dependence between the systems is lower. In a highly integrated system, an error in one of the involved systems affects the whole workflow [50]. Interoperability between systems is a technical problem and only refers to the degree systems can communicate with each other. The system does not have to be fully integrated, *i.e.* it does not form one homogeneous system.

Interoperability is highly problematic in the context of CC, as it prevents combining providers as wished. Low interoperability has several implications. These implications occur at all deployment models, and are especially problematic for SaaS. Interoperability should be considered from two different perspectives: Interoperability between existing traditional systems within an organization and interoperability between different CSPs and solutions. Interoperability between existing systems and cloud solutions allows for a less disruptive change of technology and workflows. Existing systems can be mixed with cloud solutions, gradually migrating different applications to the cloud. Interoperability between cloud solutions is important to allow for different solutions by different providers. Interoperability can be increased by standards and open application programming interfaces (APIs). There are no liabilities for the CSP or CSB, unless in a multiple cloud scenario, but services CSCs are well-advised to examine supported standards and APIs of potential cloud solutions. In a multiple cloud scenario, interoperability between systems must be ensured, as multiple clouds cannot communicate otherwise.

Storage Interoperability

The degree on which information data can be shared between and interpreted by different systems.

Application Interoperability

The degree to which applications can exchange information.

OS Interoperability

The degree on which different operating systems can communicate and understand each other.

4.1.15 Management and Maintenance of Identity Platform

An identity platform is used to manage information about users. New users should easily be added and old users removed, so that they access (or not access any longer) the cloud services. The identity platform is especially important in public, multiple cloud and community cloud solutions. In these deployment models, often many people have access to the cloud. The CSC wants to control which user has access to what resources in the cloud. Without a good identity platform, CSCs risk that private data is accessible by unauthorized entities.

4.1.16 Management of Authentication Platform

Authentication is the process of confirming the truth of an entity. Unlike the identity platform, the authentication platform ensures that entities are who they claim to be. Without trustable authentication and ensuring authorization, the value of the identity is reduced. CSPs are liable for ensuring that only authenticated and authorized entities can access the service.

4.1.17 Network Quality

As cloud services are delivered over network connections, the network quality between the CSP and the CSC is essential. Both have to ensure that there are no bottlenecks on their end. Bad network quality hinders cloud adoption. The importance of network quality depends less on the deployment or service model, but more on the kind of application, which will be discussed for the different sub-factors. When a private cloud is used and hosted within the same premises as an existing system, there is no change in the network quality. Network quality is influenced by various sub-factors.

Bandwidth

Bandwidth is the capacity of the network between the consumer and the cloud. It can be measured in bits per second. Bandwidth is especially important if lots of data is transmitted. For an office application, where only few documents and text data is transmitted, bandwidth is less important. However, slow bandwidth can lead to slower cloud applications and downloading larger files will take more time [3]. Bandwidth must also be considered when migrating a legacy system to a cloud solution. Low bandwidth will delay the migration if lots of existing data has to be transmitted initially. Not enough bandwidth will result in long waiting times for the consumer, therefore affecting the usability of CC.

Connectivity

Connectivity refers to the existing connection to the CSP. It is the time the link between service and the user is available and can be measured as percentage (*i.e.* if there are never connection issues, the connectivity is 100%). Connectivity and availability cannot be used as synonyms. Connectivity only refers to the link, *i.e.* the network connection between

the consumer and the provider. Lower availability can be caused by connectivity issues, but can also be caused by other reasons, such as a broken server.

Connectivity issues can be caused by either the CSP, the CSC or third parties. The consequences of reduced connectivity highly depends on the application and the dependence of the CSC on it.

Latency

Latency is the time it takes a request to reach the destination. It can be measured in milliseconds. An increase in latency will therefore increase the time a CSC must wait for a response from the cloud. While for many applications, *e.g.* applications which are just used for analytics of long term financial decisions, an increase in latency is not problematic. There are several applications, like high-frequency stock trading, where high latency has a negative impact [6].

Jitter

Jitter, similar to latency, is influenced by the time in milliseconds that packages require to reach their destination. Unlike latency, jitter refers to the variation in latency, *i.e.* the differences in time that it takes a packet to reach the destination. Jitter is especially problematic for real-time applications, such as VoIP and video conferencing.

4.1.18 Portability

Portability refers to the possibility to use and move components or systems in different environments [52]. For CC, this therefore means that the service can be moved to a different environment, which depends on the service level. In SaaS, the portability allows for changing the software used. In PaaS, it allows the hosted application to be moved to a different CSP. In IaaS, portability refers to the possibility to move VMs between different providers (or from a traditional architecture to the cloud). Low portability hinders CC adoption, as CSCs risk to be locked-in at one provider. Portability must be considered in all deployment models. The risk in a lack of portability for the CSC is vendor lock-in. Non-portable services lock the CSC at a certain CSP, as migrating to another CSP would require large investments. CSCs which want to ensure portability, should check the supported standards of the CSPs.

Data Portability

Data portability in the context of CC refers to the possibility to move data from one CSP to another.

Service Portability

Service portability refers to the possibility to migrate a service from one CSP to another.

Functional Portability

Functional portability is similar to service portability, but about migrating functional behavior.

4.1.19 Privacy

Privacy is a huge concern of CSCs. While privacy concerns are less of an obstacle in a private cloud or IaaS model, they are problematic in all other deployment and service models. In a private cloud model, the organization using the cloud owns it and, even if it is not self hosted, they can ensure that only authorized users have access to the data. In IaaS, CSCs can control measures to protect data (*e.g.* cryptography) themselves. In SaaS and PaaS however, data is stored and managed by the CSP. Data cannot only include information about individual users, but also other secret information [70]. The responsibilities and liabilities of the different stakeholders is influenced by legal and regulative constraints and further discussed in Section 5.1.

4.1.20 Quality of Service

Quality of service (QoS) “denotes the level of performance, reliability, and availability” and poses challenges to CSPs, who have to find the right trade-off between QoS delivered and OPEX [5]. QoS is collective term which can include several other factors, *e.g.* availability, network quality and scalability. It is therefore important for all deployment and service models. The QoS parameters and liabilities are defined in the SLAs. The risk for CSCs in having to low QoS levels is in the usability of the service. CSPs promising too high QoS might face claims based on the contracts if they cannot deliver as promised.

4.1.21 Reliability

Reliability is the probability that a system will function as expected over a period of time. Reliability can for example be measured using the mean time between failures (MTBF). High reliability means, that the system will function under various conditions and produce the expected output. While it is important in all deployment and service models, it is of special interest in public cloud services, since resources are shared with multiple consumers. The conditions in public clouds, (*e.g.* number of users, processes etc.) can vary greatly. Low reliability hinders CC adoption. The risks for CSCs are less dependent on the service and deployment model, but rather on the actual application running in the cloud. The risk for the CSPs include both reputational as also financial claims depending on the contracts and SLAs.

Elasticity

Elasticity is the responsiveness towards sudden changes in demand. It is one of the main benefits of CC. In the context of CC and reliability, it refers to how well spikes are handled, *i.e.* if the system is still able to function as expected.

Disaster Recovery

Even short downtimes can lead to high financial losses [68]. Unlike elasticity, which is proactive, disaster recover is reactive. In case of failure, disaster recovery is about the time and resources required to have the service up and running again. Disaster recovery

requires backups. More frequent or real-time backups allow for less data loss in case of a disaster. The importance of disaster recovery is again less defined by the service and deployment model, but the actual application or service running.

4.1.22 Scalability

Scalability is the ability of a system to adjust to the load required. CC has a major advantage over traditional systems as cloud applications scale “infinitely” [11]. It is required for elasticity [27]. Unlike elasticity, it does not include temporal (how fast, how often) aspects and scalability also does not have to be automatic. To achieve scalability, CSPs and CSBs need resources, in-house or external. Offering services to multiple consumers (or sharing working together with other CSPs), allows them to assign resources to where they are needed. In a private cloud scenario, scalability is less of an advantage, as resources are only for one consumer. For CSCs it is important to find a CSP which can offer the scalability required. CSPs must ensure that they can deliver the expected and agreed upon scalability. The risks for CSCs are that they lose one of the main advantages of CC when they cannot scale according to their needs. Risks for the CSP can either originate from the SLAs or be reputational. Cloud federations and multi clouds allow for even better scalability, as resources can be acquired from multiple CSPs. Scalability is important in all service models. Scalability can be realized either horizontal (scaling out) or vertical (scaling up). Scalability can be calculated by the range of resources available [22], *i.e.* the proportion of increase of resources.

Scale Out

Scaling out refers to increasing resources of the same type, *e.g.* increase the numbers VMs to handle more requests.

Scale Up

Scaling up refers to increase the existing resources and can include physical memory upgrades, CPU speed or network bandwidth upgrades.

4.1.23 Security Configuration and Maintenance

In public and in multiple cloud scenarios, data and software are hosted outside the control of the CSC. As security is an important concern for companies [22], the perceived security level from the provider is influencing the decision of cloud adoption. Security is also an issue in traditional architectures, but increases in public and multiple cloud scenarios, as they introduce more risks. In private cloud scenarios, the security concerns are the same as in traditional architectures. However, as soon as a multi-tenant model is used, more users can access the service on purpose. The importance of security, its configuration and maintenance depends on the data in the cloud. A CSC only using the cloud for anonymized, non-critical data will not have the same requirements as a CSC which stores and processes confidential information in the cloud. Security configuration is more of a concern in SaaS, PaaS and public cloud models. In IaaS, when the CSC runs a VM,

the CSC has some control over security (*e.g.* can encrypt data). The risks for the CSC include that confidential data might be leaked. Risks for the CSP include financial and reputational losses. Liabilities of the stakeholders are based on regulation and defined in the SLAs. They are discussed in Chapter 5.

Confidentiality

Confidentiality ensures that only authorized entities have access to the protected data. CSCs in public clouds storing confidential information depend on security of the CSP [3]. Data breaches are an increased risk in CC (except for private cloud models), due to the increased number of entities [71]. CSCs must consider confidentiality breaches and include the liabilities in the SLAs.

Integrity

Integrity refers to the fact that data should only be changed by authorized entities [71]. It prevents that data is changed or deleted by unauthorized parties. It is the CSPs responsibility to ensure data integrity and inform the CSC in case of any breach.

Availability

Availability refers to the “system being accessible and usable upon demand of an authorized entity” [71]. The system needs to be available, even if some entities misbehave or in case of a security breach [71]. Availability is the responsibility of the CSP. Consequences for not delivering the agreed upon availability should be, as the expected availability, defined in the SLAs.

Auditability

Auditability refers to the disclosure of information. Information relevant for auditability in CC includes which entity logged in from where (*e.g.* with what IP address), information and security settings that were changed. It is the CSPs responsibility to allow auditability.

Multi-tenant Trust

Multi-tenancy refers to the sharing of resources and is one of the main characteristics of CC. Memory, programs, network and data are shared between different consumers at different network, hardware and application levels [71] in public CC. While multi-tenancy is required for many benefits of CC, it also introduces security risks. One of this risks is object reusability. Multi-tenancy may lead to “unwilling disclosure of personal data” and also introduces the risk that users maliciously scan for sensitive data [71], as multiple users share the same physical resources. Ensuring multi-tenant trust is the CSPs responsibility.

Authorization

Authorization is part of security. Users need identities and authenticate themselves to prove that they are who they claim to be. Authorization refers to validating that a user is not only who he claims he is, but also that the identity is authorized to access the requested data. Authorization is the liability of the CSP. However, CSCs also protect their identities and use strong authentication measures to ensure that third parties cannot use valid authentication to gain unauthorized access to the cloud, which would lead to a privacy breach [71].

4.1.24 Service Response Time

The time required from a service to respond to an input. The perceived effect of a slow response time to the user is similar to high latency, but it occurs at different stages. Service response time is from the service itself, *i.e.* the processing on the server, latency is occurring at a network stage. Unlike latency, the service response time is not influenced by external factors (*i.e.* the network in between the CSP and CSC). Service response time should be part of the SLAs. Higher service response time decrease the usability of a service. The liability of the CSP is to provide the agreed upon service response time, consequences for not delivering this should be defined in the SLAs.

4.1.25 Software Assurance

The committee of national security systems defines software assurance as “Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle and that the software functions in the intended manner” [14]. For a cloud environment, software assurance translates to the likelihood that the cloud service performs as expected and/or promised in the SLA [22]. It can be calculated by measuring the expected values against the actual values. Typical factors defined in the SLAs that have to be considered for software assurance include availability, elasticity, and service response time. Software assurance is important for all cloud deployment and service models. As software assurance is set by the contract, it should be at 100%. The risks for the CSC depend on the parameter (*e.g.* availability) which is not working as expected/agreed upon, and are discussed the in factors related to software assurance. Consequences for the CSP should to be defined in the SLAs. Risks for the CSP do not only include financial liabilities, but the potential loss of customers to competitors.

4.1.26 Standards

Standardization refers to the degree to which “different manufactures provide more interchangeability than is logically necessary” [18]. Standards in CC increase interoperability, portability and therefore reduce the risk of vendor lock-in. Important examples for standardization in CC include ISO (ISO/IEC JTC 1/SC 38), the Open Grid Forum (OGF) and the Open Cloud Consortium (OCC). CSPs are not liable for implementing standards. However, CSCs who want to reduce the risk of vendor lock-in will actively seek CSPs that implement standards, and CSPs can therefore increase competitiveness by support standards. As vendor lock-in can occur at all deployment and service models, it is important in all.

4.1.27 Trialability

Trialability refers to the degree to which an innovation may be “experimented with on a limited basis” [54]. The possibility to try a cloud service before signing a contract increases

cloud adoption, as it decreases uncertainty. To many cloud adopters, the ability to try and experiment with cloud systems is crucial [44]. Trialability is important for all deployment and service models, but especially for SaaS and PaaS. In SaaS, the actual application can be tested, ensuring that functionality and usability meets the expectations. There are no liabilities for the different stakeholders concerning trialability, but it is beneficial for CSPs to offer it, as it increases their transparency. It helps to set the right expectations of a service. This reduces the risk, that after committing to a provider/solution, it is realized, that the service does not match the requirements. This is also beneficial to CSPs, as satisfied customers are more likely to stay with the provider and fluctuation is reduced.

4.1.28 Usability

Usability refers to the experience a user has with the cloud service. The easier a service is to learn and use, the faster an organization can adopt it [22]. Usability can be measured using qualitative and quantitative feedback from the users and metrics, such as application launch time. Usability is important for all deployment and service models. It is in the interest of CSPs to offer services with high usability to attract CSCs. CSCs that require certain metrics for usability (*e.g.* minimum average response time) should not only try the service, but include these in the SLAs.

Application Launch Time

The time it takes the application be up and running. Longer application launch times reduce the usability

Installability

Refers to how difficult it is to install. The simpler a service or application is to install, some SaaS might not be installed at all, the simpler it is to use.

Simplicity

Simplicity refers to how difficult it is to reach the desired goal. Simplicity increases the usability of a service.

Learnability

Learnability refers to the time and effort required to learn a new system, service or application. For CC this means, that learnability should be good, as this allows for faster adoption.

Response Time

The time a service requires to show an update to a request of a user. It includes the service response time and the latency. According to [46], a response time of up to 0.1 second is considered as instantaneously. A response time below and up to 1.0 second is required, so that the user's is not interrupted in flow of his thought. Response times of 10.0 and above will lead to a situation where the user performs different tasks while waiting for a response. Increased response time reduces usability.

4.1.29 Traceability and Auditability

Traceability and auditability refers to the extent the usage and changes of a service and data can be tracked. Traceability and auditability is not only relevant to ensure that the billing is correct, but is also relevant for legal compliance. The possibility of increased traceability and auditability of changes in information benefits CC adoption [44]. Traceability and auditability is important in all service and deployment models.

4.1.30 Utility Based Computing

Utility based computing is a great advantage of CC. Instead of buying the computing resources organizations require, they are available as utility as needed and with a pay-as-you-go model. This allows organizations only to pay for the resources required, maximizing efficiency and minimizing costs. Utility based computing requires elasticity and scalability to work. It is especially an advantage in public and multiple cloud scenarios. The advantage of utility based computing is less dependent on the different service levels, but on the demand for the service. It is especially beneficial for services where the demand fluctuates.

4.1.31 Vendor Lock-In

Vendor lock-in occurs, when a customer cannot change the vendor. Once a CSC moved data and/or applications to the cloud, it can be technically difficult to move to another provider [60]. Vendor lock-in can be caused by a lack of standards and portability. It can be evaluated by analyzing the portability and supported standards. Vendor lock-in is an obstacle for cloud adoption [21]. The risk for the CSC is the lock-in effect, as he is dependent on the CSP and cannot switch it without great cost.

4.1.32 Workload Management

Workload management is used to distribute work over resources to achieve optimal performance. Using a public cloud model, the workload management is outsourced to the CSP. From an CSC's perspective, it is of great interest when considering a private cloud model as the resources should be used efficiently. It is important for all service and deployment models. In deployment models except private clouds, it is the liability of the CSP. The risk of bad workload management is that, even though resources might exist, they are not used efficiently. This can lead to worse availability and decreasing usability due to higher service response time.

Capacity Planning

Capacity planning is essential for workload management. There must be enough resources to handle demand.

Performance Management

Includes tools to monitor and analyze performance metrics. Potential issues and shortcomings must be recognized as early as possible to plan accordingly.

Classification

The different classifications of work. *E.g.* the expected runtime or memory usage of a task.

Mission Criticality

Workload should be classified into different importances. Critical workloads tasks and processes should have higher priority.

Configuration Management

To enable workload management, configuration is needed. Configuration management enables the identification and control over assets. If changes in assets are necessary, configuration management need them to be evaluated and coordinated.

4.1.33 Workload Utilization Ratio

The workload utilization ratio is the degree resources are used. A low workload utilization ratio means that the existing systems are not used efficiently. This is often the case in traditional architectures if the demand varies depending on time. With traditional systems, organizations need more hardware to cover peak times, even though this results in a poor workload utilization ratio. Public and multiple cloud models that allow for high scalability can increase the workload utilization ratio. The systems can be adjusted to the demand. Workload utilization ratio is important in all service levels. It is also in the interest of CSPs to have a high workload utilization ratio. However, it must always be considered that peaks must be covered. Therefore, either there must be enough backup resources in-house (resulting in a lower workload utilization ratio) or available from other sources (*e.g.* other CSPs in multiple cloud models).

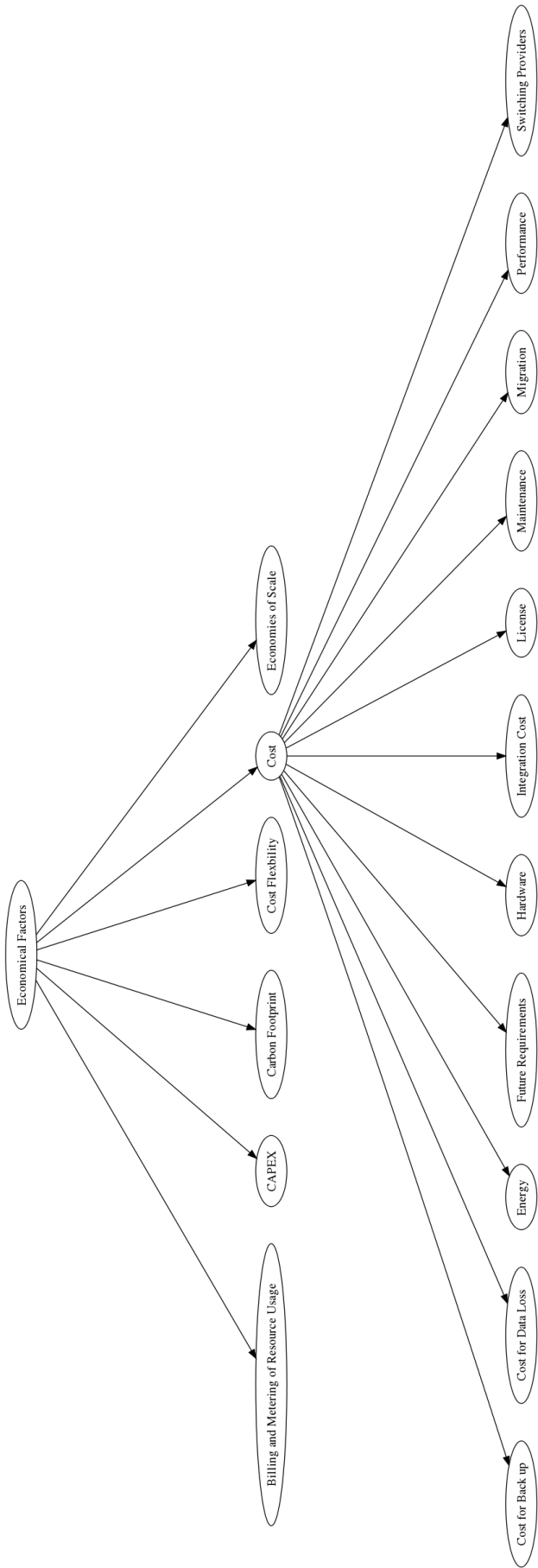


Figure 4.6: Overview of Economical Factors 1/2

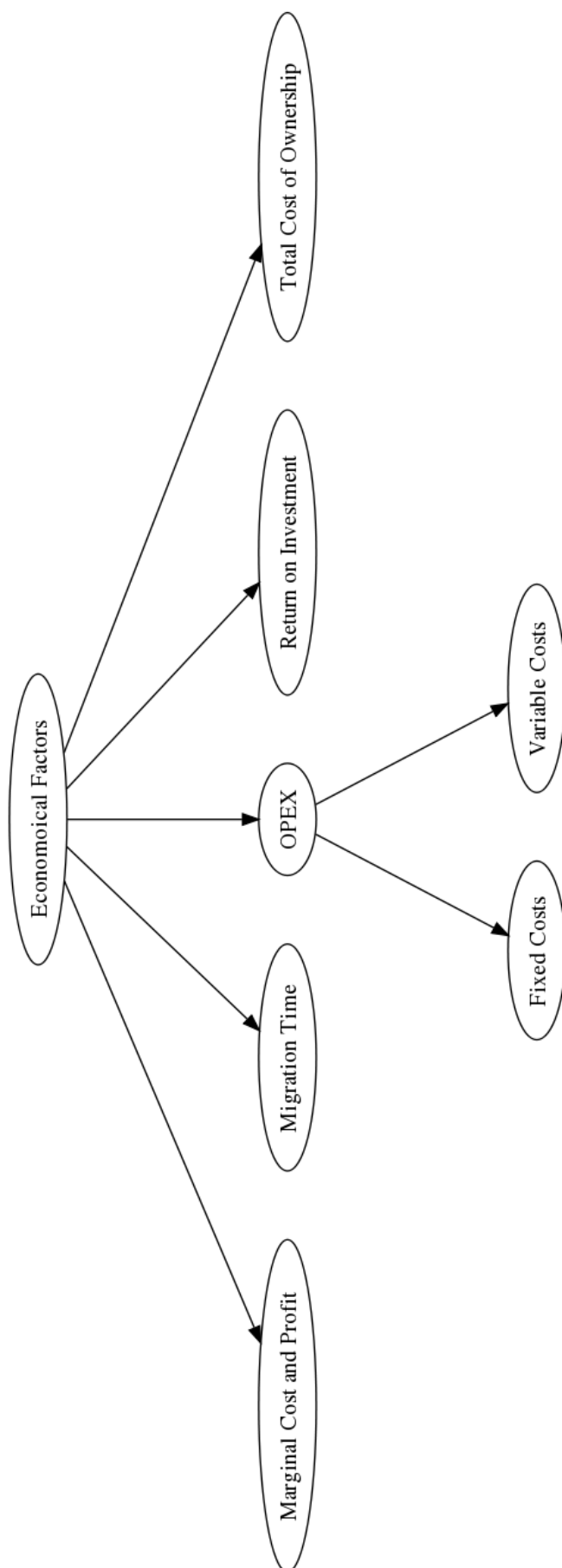


Figure 4.7: Overview of Economical Factors 2/2

4.2 Economical Factors

Economical factors include all the factors that are primarily related to costs and prices.

4.2.1 Billing and Metering of Resource Usage

CC allows CSCs to receive the resources they require on-demand, in terms of “duration and quantum of utilization” [45]. Especially for services which highly vary in demand, elastic resourcing is beneficial. To benefit from CC, the way the resource usage is billed and metered has to be considered. It is an advantage for a CSC if the CSP allows for exact metering of the service, and bills according to it. This allows CSCs to pay for their actual demand.

Exact billing and metering of resource usage is less important in private cloud scenarios, as the infrastructure is dedicated to the customer. For CSPs in multiple cloud scenarios, *e.g.* federated clouds, it is important that the accounting and billing is “carried out in a fair and standardized way” [15] between the CSPs involved and the CSCs.

4.2.2 Capital Expenditures

Capital Expenditures (CAPEX) are costs associated with long term investments. It includes investments in new or existing fixed assets. This includes investments into servers and other IT infrastructure equipment. Cloud-based computing allows organizations to reduce their CAPEX, as IT infrastructure is outsourced and acquired as needed. CAPEX are less affected in a private cloud model than in others, especially when hosting the cloud in-house. This requires up-front investments, which have to be classified as CAPEX. In other cloud deployment models, CAPEX can be drastically reduced over traditional architectures.

The reduction of CAPEX especially benefits smaller and medium organizations, as funds for large up-front investments might be missing. Growing organizations can benefit, as they do not have to invest into new assets, but use cloud-based services with a “pay as you go” model [7].

4.2.3 Carbon Footprint

Carbon Footprint is extent to which organizations affect the environment. It is measured in units of carbon dioxide. The reduction of the organizational carbon footprint is “one of the major goals” for many organizations considering moving to the cloud [21].

4.2.4 Cost Flexibility

Cost flexibility refers to how elastic costs are. While traditional architectures often require capital expenditures, CC allows for better flexibility with utility based services. This is especially beneficial for organizations with changing demand in IT infrastructure, as they only incur the costs for the resources needed at any given time. Cost flexibility depends on the cloud deployment model. Private cloud do not offer greater cost flexibility than traditional architectures. Public clouds with a pay-as-you-go model allow for more flexible costs that match the required usage better than legacy systems [44].

4.2.5 Cost

Cost includes all monetary spendings that are influenced by CC. It is one of the main drivers for cloud adoption. Different deployment models change the cost structures. While private clouds still have high initial costs, other deployment models reduce the up-front spendings. In hybrid-cloud scenarios, the cost is split between different organizations. The larger an organization, the easier it can benefit from economies of scale. Outsourcing the IT to a CSP can decrease costs, as the CSP can benefit from economies of scale and offer prices that are lower than hosting the IT infrastructure in-house. Costs occur for many different factors. For many of these factors, public clouds the costs for the CSC as the CSP is responsible for them [44].

License

All the cost associated with licenses. Organizations that adopt cloud software do not have to buy software packages for every computer, as it is directly accessed in the cloud [3]. However, if a private cloud is considered, license costs are still relevant [60].

Maintenance

Maintenance costs are costs associated with keeping the infrastructure running. If the cloud solution is not hosted in-house, maintenance is handled by the CSP and included in the service cost.

Backup

Information is a valuable resource. Having backups is therefore essential. Organizations must consider the costs for backups at one or multiple CSPs and in-house as well as the tradeoff to costs for data loss.

Energy

Includes the energy costs for running the IT infrastructure. In a cloud scenario, these costs are outsourced to the CSP and included in the service fees.

Hardware

As computation is done in the cloud, users require less expensive (*e.g.* less powerful) computers [3]. Some of the required IT infrastructure (*e.g.* servers) can be completely outsourced. As with many other economical factors, the costs vary greatly for different deployment models. Private cloud scenarios will not affect costs for hardware, unlike other cloud deployment models will do.

Migration

Organizations considering migrating to the cloud should not only consider the costs for their traditional infrastructure and the new one. Migration towards CC will require initial monetary investments, *e.g.* to acquire new knowledge or data transmission.

Future Requirements

Organizations considering cloud-based computing should not only consider their current requirements. They also have to consider costs which can occur in the future, if their requirements change. Especially when considering SaaS, organizations must consider the possibility of changes in their requirements. If a cloud-based solution cannot fulfill future requirements, CSCs might have to switch providers, which can be associated with great costs.

Performance

[22] defines performance as the level of functionality, service response time, and accuracy. The costs considered for performance therefore includes costs associated with these factors, *e.g.* computational power and network infrastructure. In traditional architectures performance requires better hardware, in cloud-based computing the performance level is defined via contracts and SLAs.

Data Loss

Data loss can be very costly, sometimes even fatal for organizations. The costs that occur for data loss in a cloud environment should be taken into consideration and the trade-off between costs for data loss and backups should be considered.

Switching Providers

Once an organization has migrated to the cloud, there is the possibility that it considers switching to another CSP. This migration can be costly, depending on the portability of the service. Costs for switching providers cannot only include migration of data and setup-fees, but can be higher if data needs to be transformed first. This is especially problematic in SaaS scenarios, where the data format from one CSP might not be compatible with another. The costs for switching providers highly affects vendor lock-in.

Integration

Integration costs includes all monetary spendings associated with integrating the cloud with existing systems and processes. Considering technical factors, integration costs are highly dependent on the interoperability between existing systems. Like the migration costs, integration costs occur when switching to a cloud-based service.

System Administration Costs

Traditional systems require technical expertise in-house. The system has to administrated to ensure that it is working without any issues. All costs associated with this process are considered under system administration costs.

4.2.6 Economies of Scale

Economy of scale refers to cost benefits due to the size of an organization. CSPs can benefit greatly from economies of scale, therefore offer their services cheaper to CSCs. This is of true for public clouds (and might be true for community clouds), but not for private clouds [11]. If a private cloud or another cloud deployment model is considered, where the cloud is managed by the using organizations, the economies of scale depends on the number of users [60]. According to [23], cloud implementation leads to better economies of scale for the CSC, but only for short term, as competitors can easily imitate.

4.2.7 Marginal Cost and Profit

Marginal costs are the costs for an additional unit and marginal profit the profit for an additional unit. In CC, marginal cost and profit can be considered from the perspective of a CSP. For a CSP, the marginal cost refers of an additional consumer. The marginal profit is calculated by subtracting the costs from the revenue of the additional CSC.

4.2.8 Migration Time

The time required for migrating from the existing solution to a cloud solution. An increase in migration time will increase the cost for migration, as both solutions must run at the same time. Expertise is required for both solutions and data consistency must be warranted. A shorter migration time is beneficial for cloud adoption. Migration time is relevant for all deployment and service models.

4.2.9 Operating Expenditures

Operating expenditures (OPEX) requires all the costs required for operating a business. It includes expenditures which do not affect the business for longer than a year, therefore OPEX do not include investments in IT infrastructure that will be used for longer than a year. For organizations considering adopting a non-private cloud, CAPEX decrease and costs are shifted towards OPEX [44]. However, a shift from OPEX to CAPEX is not necessarily an advantage. CPCs with varying demands in resources rather benefit from a pay-as-you-go model than the shift from CAPEX to OPEX. This shift mainly is beneficial to smaller organizations, as no high up-front investments are necessary. It is also beneficial in the sense that the available resources can grow with the organizations, without having to invest into expensive infrastructure.

Fixed Costs

Fixed costs do not depend on the output produced or usage of a service. From a CSCs perspective, these costs are incurred independently of the number of users or the resources required. Considering costs in a traditional architecture, this can include a system administrators salary. In CC, it can be a service fee independent of the usage.

Variable Costs

Variable costs depend on the output produced or the usage of a service. From a CSCs perspective, it includes cost which vary with the usage. This is highly dependent on scalability and metering of the service. CSPs might charge CSCs according to the time the service was used, the computational resources or the storage space that was used. Unlike traditional architectures, utility based computing with a pay-as-you-go model, allows for greater variable costs. CSCs can benefit from only having to pay the resources they require. Considering the variable costs is especially important for CSCs with varying demand, as it allows them to ensure, that they do not have high costs, when they have low demand.

4.2.10 Return on Investment

Return on Investment (ROI) is the ratio of the benefit of the investment against the cost of the investment [42]. Therefore, it is

$$ROI = \frac{(Initial\ cost - Final\ cost) - Investments}{Investment}$$

As CC can increase the profitability of the CSC. The ROI formula for CC should therefore include this additional profit. [42] defined the following formula for ROI in CC

$$ROI\ for\ cloud = \frac{Increase\ in\ profit + Reduction\ in\ cost - Cloud\ costs}{Cloud\ costs}$$

A positive ROI makes cloud-based computing attractive to CSCs. Organizations should however not only calculate any expected ROI for cloud-adoption, but also consider investments in their traditional architecture and the expected ROI of these investments.

4.2.11 Total Cost of Ownership

The total cost of ownership is a financial estimate that includes the total cost of purchasing/subscribing to and running a service or product [1]. In CC, this number must be compared to on-premise solutions. The total cost of ownership for cloud-based computing does not only include the costs for service, but also other investments required. These investments include, but is not limited to, migration costs, costs for expertise that has to be acquired and costs for potential compliance issues. The total cost of ownership for traditional infrastructure can be calculated by calculating the cost of each server [42] :

$$TCO\ for\ each\ server_{Traditional\ Infrastructure} = costs\ of\ (electricity + cooling + maintenance + manpower + software + backup\ power)$$

$$Total\ TCO_{Traditional\ Infrastructure} = \sum(TCO\ for\ each\ server)$$

For CC, the factors influencing TCO are discussed in Section . The TCO is required to calculate the benefit in the return on investment. Organizations should consider both the TCO of different cloud solutions and traditional architectures.

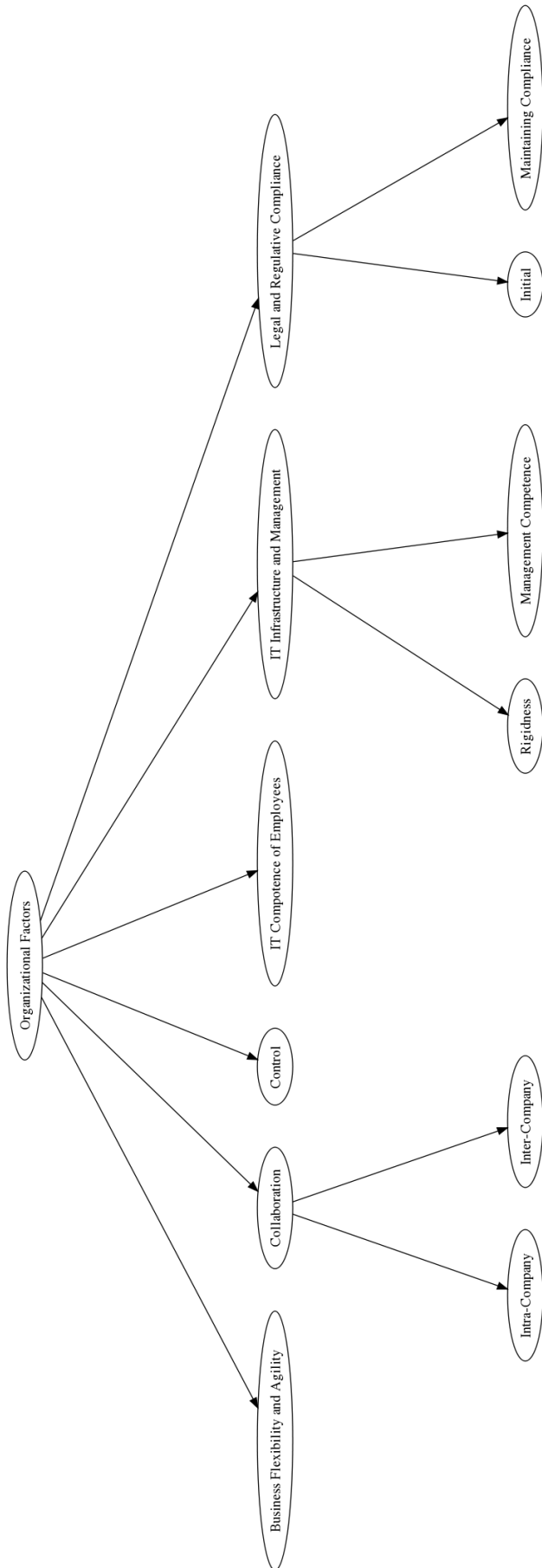


Figure 4.8: Overview of Organizational Factors 1/2

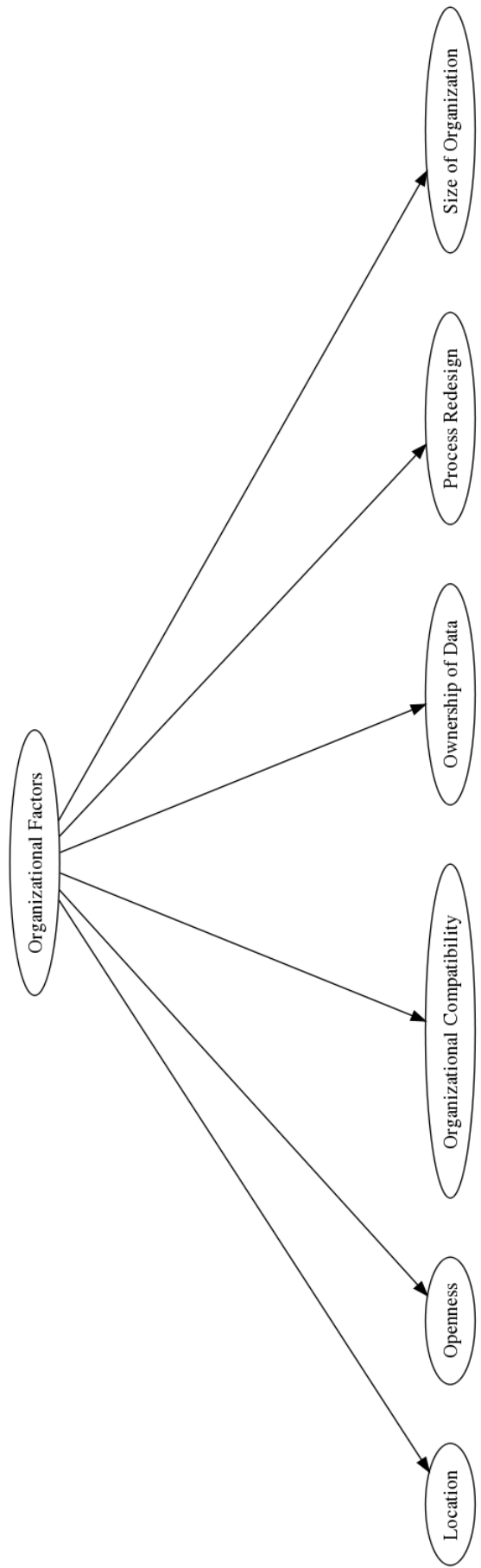


Figure 4.9: Overview of Organizational Factors 2/2

4.3 Organizational Factors

Organizational factors are attributes of the organization that considers cloud adoption.

4.3.1 Business Flexibility and Agility

Business flexibility and agility can be interpreted in different ways: It can be that an organization needs to be flexible and agile to successfully move to the cloud, for example when considering using existing SaaS. But CC can also allow for “agile addressing of new markets and offerings” [11], for organizations that use the cloud to bring their own services to end customers. Furthermore, cloud enables organizations to “expand and change” at limited costs [22]. It also allows for better integration with existing business partners and customers, it helps with information sharing and business processes across value chains and geographies [11]. For a cloud solution across the value chain, a community cloud is especially interesting.

4.3.2 Collaboration

Collaboration is the process of working together to achieve a common goal. Collaboration can either be within an organization or between different organizations. Collaboration can increase with CC, as projects and documents are available in the cloud and not only locally [3]. If an organization considers the benefits of collaboration it is less dependent on the cloud deployment and service model, but rather how important collaboration is and if, and how, it can be increased with CC.

Intra-Company

Intra-company collaboration refers to all collaboration which is within the same organization, *e.g.* between different sections of an organization. CC can improve intra-company collaboration, as the resources are on the cloud, accessible by the different actors of an organization.

Inter-Company

Inter-company collaboration refers to collaboration between different organizations. CC enables organizations to integrate business partners and end customers, and thereby improve collaboration [11]. Multiple organizations working along the same value-chain, but with high security concerns, can consider community clouds. Community clouds allow the organization to have a cloud environment which is suitable for their security and resource demands, split costs and increase collaboration.

4.3.3 Control

Control refers to the authority over an organization and its processes. Many organizations that consider cloud adoption fear the risk of loss of control [44]. The loss of control can occur over data and resources [21]. While a private cloud deployment model will still be under control of an organization, it has less influence in other deployment models. Organizations that consider adopting a SaaS from a public CSP have little control over the service. The loss of control is especially problematic combined with a high vendor lock-in effect. Organizations lack control over the services from the CSP and cannot switch to another provider easily.

4.3.4 IT Competence of Employees

Cloud adoption will influence the work progress of the employees using the services. The level of IT competence and adjustability of the employees need to be considered. Increased efficiency and collaboration with CC can only be realized if the employees understand the technology and accept it. If employees cannot adapt with the changes, benefits cannot be fully harvested. Furthermore, if non-IT employees, or their management, are involved in IT decisions, it is essential that they understand the technology and have a positive perception towards it [11]. The IT competence is relevant for all deployment and service models.

4.3.5 IT Infrastructure and Management

The likeliness of cloud adoption and its success is highly dependent on the IT management within the organization. Especially important is the rigidness and competence of the IT management. Furthermore, the existing IT infrastructure has to be considered. An organization which recently invested into servers and other infrastructure has to realize that cloud adoption might make this infrastructure futile. IT management which is against change, is less likely to adopt CC.

Rigidness

Rigidness refers to likeliness of change within organizations. Rigid IT infrastructure and management are less likely to change, and it is therefore less likely to adopt and fully benefit from CC [23].

Management Competence

IT Management within an organization must recognize the value of CC for an organization. If the IT management fails to see advantages, the resistance against adopting CC will rise. For that, the IT management has to fully understand the technology and the business processes within the organizations to take full advantage of CC [23]. IT management competence does not automatically lead to higher cloud adoption. It is possible, that it is realized, that an organization cannot benefit from CC.

4.3.6 Legal and Regulative Compliance

Compliance refers to the effort required for an organization to comply with the legal and regulative environment. This factor is used as anchor for the different legal and regulative constraints discussed in Chapter 5. Legal and regulative compliance highly depends on the location of an organization and the location of its customers. CC introduces several implications from a regulative perspective, which are discussed in Chapter 5. Organizations in a strict legislative environment are less likely to adopt cloud-based computing [11]. Organizations should not only consider the initial efforts to reach compliance and maintaining compliance.

Initial

Refers to the effort required to initially reach compliance. This includes research, negotiations with CSPs and development of contracts and SLAs.

Maintaining

The effort required for maintaining compliance, after it was initially achieved. This includes monitoring of changes in the legal and regulative environment and adapting towards it.

4.3.7 Location

Location refers to the physical position of an organization. The location of the CSP has also to be considered, as it matters from a legal perspective. The location of an organization does not have to be considered because of different service and deployment models, but because it defines the legal and regulative constraints.

4.3.8 Openness

Openness in an organizational context refers to the companies acceptance of new ideas. Organization with low openness will less likely consider cloud-based computing, as it would bring changes. An open culture is therefore beneficial for adopting CC. The more changes CC brings, the higher the importance of openness.

4.3.9 Organizational Compatibility

Compatibility can be interpreted as the degree to which an innovation matches existing values, experiences, and needs [54]. For CC, this has two different aspects to consider. First of all, it depends on the believes of the employees and management. If organizations consider CC beneficial, organizational compatibility increases. The second aspect is about the processes within the organization. If cloud-based solution are compatible with the organization, *i.e.* employees do not have to change their workflow, compatibility also increases.

4.3.10 Ownership of Data

From an organizational perspective, ownership of data is important as information is a valuable commodity. When considering a private cloud, this is not an issue. However, when considering a public or community cloud, it is important to have clearly defined who owns the data, who is liable to what extent for leakage and in case of data loss. Potential loss of ownership of data is a concern for CC adoption.

4.3.11 Process Redesign

Process redesign is about changes in the workflow within an organizations. This influences the way employees work. The migration from in-house server to an IaaS might not have any influence on processes and the workflow of employees at all. However, adopting SaaS might mean that employees have to change the way they work. The more CC adoption requires process redesign, the higher resistance against it to be expected.

4.3.12 Size of Organization

The size of an organization influences cloud adoption. Larger organizations are likely to have more resources, and therefore can afford the migration more easily. However, the concept of CC can prove more interesting for smaller organizations by preventing large upfront costs and not requiring an on-premise enterprise system [11]. Larger companies might rather be more interested in private clouds or hybrid clouds, while smaller companies will try to avoid the required upfront spendings and rather look into public cloud solutions.

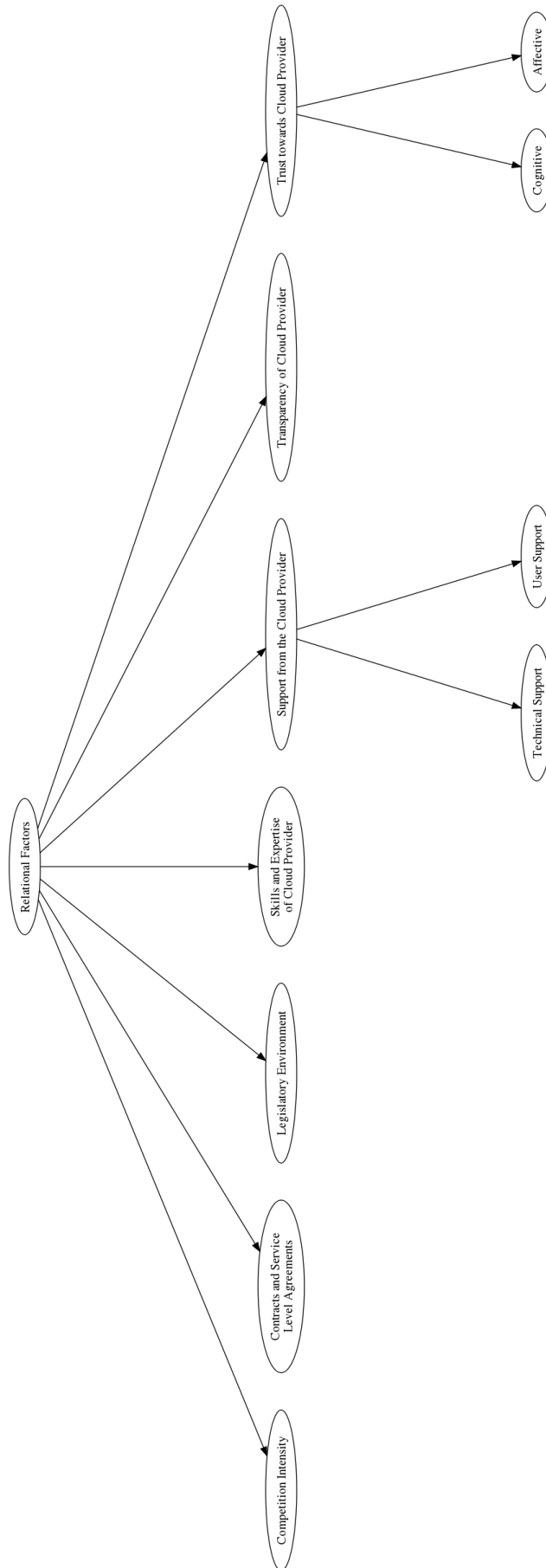


Figure 4.10: Overview of Relational Factors

4.4 Relational Factors

Relational factors include the factors that depend on the relation between an organization and its environment. It especially includes the relation between the CSP and the CSC.

4.4.1 Competition Intensity

Competition intensity refers to the amount of competition to an organization. It can be measured by the market concentration, *e.g.* using the Herfindahl-Hirschmann Index (HHI). Competition intensity requires companies to react to their competitors by adjusting their offerings and by allocating more resources to innovation. As CC enables companies to “quickly establish new services without major upfront investments”, higher competition intensity is associated with a positive impact on CC adoption [11].

4.4.2 Reputation Fate Sharing

Reputation fate sharing refers to the effect, that organizations might be influenced by the misuse of another user [7]. It is especially problematic in public cloud scenarios. The misuse of a service can lead to downtimes or other negative effects, such as non-reachability due to blocked IP addresses.

4.4.3 Contracts and Service Level Agreements

Contracts and service level agreements are the agreement between two parties. The SLA defines the expected and guaranteed service levels between the CSP and the CSC. It includes the definition of the service, thresholds for technical factors such as availability and liabilities for the different parties. A clear SLA with agreed penalties is an important criteria when adopting cloud [60]. As contracts and service level agreements are influenced by contractual law, they are further discussed in Section 5.3.

4.4.4 Skills and Expertise of the CSP

The competence of the CSP regarding skills and expertise. It is highly doubtful that a company will adopt CC when it fails to find a CSP, which it perceives as skillful and acting with great expertise. Skills and expertise from the CSP are difficult to measure for a CSC. They can either trust the perception they have from communication with the CSP, or consider the amount of experience (*e.g.* time in business, other customers) or consult third parties (*e.g.* independent CSB, certifications acquired by the CSP).

4.4.5 User and Technical Support from the CSP

The level and quality of support from the provider. As with every migration of technology, it is likely that issues will occur. User and technical support from the CSP is important in all service and deployment models. In private deployment models, it depends if the cloud is hosted in-house or externally. User and technical support can be part of the contracts. It can be measured using different dimensions. This can include the typical time until a response is given and the measurements of the quality of the response (*e.g.* helpful or not). Often, the time to response is part of the contract. Also, the amount of support included in the service fee should be included in the contract.

4.4.6 Transparency of CSP

Transparency refers to the disclosure of information, such as privacy statements, security policies and availability guarantees. Transparency reduces the perceived risk of working with a certain CSP [51]. The transparency of CSPs can be used to compare different CSPs and measured using scorecards developed by [51]. It is important for all cloud deployment models.

4.4.7 Trust towards CSP

Trust describes the expectations from the CSC to the CSP, that it “will perform as expected and treat the client organization fairly and reasonably” [23]. In traditional IT architectures, trust is ensured by preventing access from unauthorized parties using security and access policies [71]. In CC, the importance of trust towards the CSP is dependent on the deployment and service levels. In private cloud deployment models, especially if hosted in-house, access to the whole system can be restricted using technical means (*e.g.* firewalls). However, in other deployment scenarios this is not possible. Organizations that have low trust towards potential CSPs are less likely to adopt their service. The more important the service is for an organization, the more important this trust relation is. If trust towards the CSP decreases after a service was adopted, it is more likely that a CSC will look into alternatives.

Cognitive

Cognitive trust builds on the perceived delivery from the CSP, *i.e.* if the provider delivers as promised and has the “requisite skills, abilities, and expertise” [23]. Cognitive trust is therefore influenced by deviations from the promised service agreements (*e.g.* promised availability and actual availability). As cognitive trust is subjective (the perceived expertise), it can only be measured by retrieving feedback from the CSC.

Affective

Affective trust is based on the perception of honest concern and care [23]. As affective trust is emotional, and not based on rational factors, it is difficult to assess and can only be measured by feedback of the CSCs.

Chapter 5

Legal and Regulative Constraints

Many of the legal issues are not unique to CC. They have been previously discussed in IT outsourcing or application service providing. However, in CC the relations between the different stakeholders are often more complex with entities from all over the world are involved [9]. Furthermore, the different service and deployment models increase complexity even further. Legal aspects that have to be considered in CC include data protection, contracts, copyright, environment and competition [9]. While all the different factors are considered, the focus in this thesis lies on data protection. This, since data protection is applicable in most cases, where the other are very case specific.

This chapter introduces the relevant laws, discusses their implications on CC and issues that arise with different cloud federation scenarios.

5.1 Privacy and Data Protection

Art. 12 of the Universal Declaration of Human Rights 1948 acknowledges privacy as a human right [64]. However, it does not define how privacy should be protected. Many of the existing laws and regulations also apply to CC, most of them are derived from the principles of the Organization for Economic Co-operation and Development (OECD) Privacy Guidelines and Transborder Flows of Personal Data [13]. This section is structured as follows: The nine core principles of the OECD Privacy and Transborder Flows of Personal Data are introduced, then the relevant articles from the EU are discussed including the relevant differences between the European Data Protection Directive (95/46/EC) and the General Data Protection Regulation, which is in draft state since 2012, and then the situation in the US is considered.

For this section, the deployment models can be split into two groups: Clouds in which a cloud is specifically assigned to one customer or a community of such, and clouds which are shared between independent customers (*i.e.* public clouds). In the first case, which includes private and community clouds, the organizational customer can dictate the necessary controls and safeguards. However, in the second group, the clouds are tailored

according to the need of many customers. They try to be as generic as possible, to appeal to a wide diversity of customers.

Furthermore, the service levels that have to be considered can also be split into two groups: Service models that allow customers to install and run their own applications (*e.g.* IaaS, PaaS) and service models in which the customers directly interact with a service which is under control of the provider (*e.g.* SaaS). In the first case, the consumer, which we will be referred to as data user, has control over what information is collected and stored in the cloud. This is not the case in the second group, where it is difficult to assess what personal information is collected and for what purpose by the CSP, who also acts as data user. This is problematic, as the service providers receive more information than required to offer the service, such as time of usage and location (IP address) of the user [13].

5.1.1 Core Principles of OECD Privacy Guidelines

To understand the implications in different service models, it is essential to understand the OECD privacy guidelines.

Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject [49].

Personal data should be collected for business purposes only if required and, where appropriate, this should happen with the knowledge or consent of the user. In a SaaS scenario, the provider, which is also the data user, can collect more data than actually required, *e.g.* location, usage patterns. This has to be carefully analyzed [13].

Data Quality Principle

The only data collected should be relevant to the purpose for which it is to be used, and should be accurate, complete and kept up-to-date [49]. This implies that any CSP must only collect relevant information, and also attempt to ensure accuracy, completeness as well as keeping data updated.

Purpose Specification Principle

Defines that the purpose for which personal data is collected must be specified latest at the moment it is collected, and that it should not be used for any other purposes at a later stage. Data should not be kept longer than necessary, and if not required any longer, it should be anonymized or deleted [49].

Use Limitation Principle

The use limitation principle states that data should not be disclosed, made available or otherwise used for purposes that are not in accordance with the purpose specification principle. There are two exceptions to this principle: Data can be used for other purposes either with the consent of the data subject or by the authority of law [49].

Security Safeguards Principle

This principle is about the security of personal data, which should be protected “by reasonable security” safeguards against various risks (loss, unauthorized access, destruction, use, modification or disclosure of data). As further discussed in paragraph 8 in the detailed comments of [49], safeguards include physical (locked doors, identification cards), organizational (authority levels for accessing data), and information measures (usage of enciphering, monitoring and taking action in case of unusual activities). It further defines modification as unauthorized input of data. In public cloud scenarios, it is therefore the CSP’s responsibility to ensure security of any personal data.

Openness Principle

This principle is about the open communication of the data user. The data user should have a “policy of openness” about their practices with personal data and disclosure of their identity and current address [49].

Individual Participation Principle

This principle is about the right of individuals. Individuals should have the right to obtain data from the data user. This includes foremost the disclosure if they have any data relating to the individual, and a copy of the information within reasonable time. Data subjects also have the right to “have the data erased, rectified, completed or amended as appropriate” [13]. Data users should therefore ensure that CSPs can fulfill these obligations.

Accountability Principle

It is the data user’s responsibility to ensure that all the above principles are assessed through a privacy impact assessment. It is also their responsibility to ensure that the chosen CSPs have “appropriate incident response and breach handling” [13].

Basic Principles of International Application: Free Flow and Legitimate Restrictions

Member countries should “take all reasonable and appropriate steps” to make data flows between borders secure and uninterrupted. Data should not be transmitted to jurisdictions which do not observe the foregoing data protection principles. Data users are therefore allowed to move data across borders, as long as they “establish the legal basis for entrusting personal data to CSPs”.

5.1.2 EU Data Protection Directive and General Data Protection Regulation

The current EU Data Protection Directive 95/46/EC (EU DPD) is the framework for all members of the EU, which implemented their own privacy and protection laws based on them. As previously stated, it is based on the general principles of the OECD. It is targeted to protect the privacy of all personal data that is processed for or about citizens of the EU [33].

The General Data Protection Regulation (EU GDPR), which exists as draft since 2012, is expected to supersede the EU DPD. As a regulation, unlike a directive, it is valid, self-executing and applies to all members of the EU. Therefore, it does not require implementation on a national level by the members. This section will discuss both the implications of the EU DPD, which other countries legislations, such as Australia, Canada and Argentina also comply with (and Switzerland partially), and changes that were made in the working copy of the EU GDPR.

Roles

The EU DPD and EU GDPR define personal data as “any information relating to an identified or identifiable natural person (‘data subject’)”. The data subject must not be directly identifiable. It is sufficient that the data subject is indirectly identifiable by a reference number or by one or more factors specific to physical, physiological, mental, economic, cultural or social identity. Therefore, it is considered personal data and consequently covered by the EU DPD and EU GDPR. Personal data is all information related to a data subject.

The EU DPD and EU GDPR both define three roles:

- Data controller: The data controller (DC) is “the natural or legal person, public authority, agency or any other body” that determines the goal and means of processing personal data, *i.e.* the data owner.
- Data processor: The data processor (DP) is “a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller”
- Recipient: The third role that is available in both EU DPD and EU GDPR is the recipient, “a natural or legal person, public authority, agency or any other body to whom data is disclosed”. However, while in EU DPD “authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients”, this exclusion is missing from the working copy of the EU GDPR.

While the three above stakeholders are present in both the EU DPD and EU GDPR, the EU DPD explicitly lists third parties as “a natural or legal person, public authority, agency or any other body” that is not defined in the other roles. While not included in the definitions (Art. 4), the EU GDPR still references third parties in several articles. Both the data processor and data controller have several criteria they have to meet, which will be discussed in the next section.

Responsibilities of the different Roles

According to the EU DPD, the data controller has the following responsibilities [33]:

- Ensure compliance with data protection law and added in the EU GDPR, transparent to the data subject

- Comply with Art. 6 of EU DPD/Art 5. of the EU GDPR. These articles define how personal data must be processed. They are based on the OECD core principles and define that data must be [16], [17]:
 - “processed lawfully, fairly and in transparent manner”
 - “collected for specific, explicit and legitimate purposes and not further processed”
 - “adequate, relevant and limited to the minimum necessary in relation to the purposes for which they are processed”
 - “accurate and kept up to date”
 - “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed”
 - “processed under the responsibility and liability of the controller” (added in EU GDPR)
- Give consent to the processor
- Be liable for data protection violations

The data processor on the other hand [33]:

- Do the processing according to the mandate
- Act as agent of the mandate
- Must be a separate legal entity

However, depending on the cloud scenario, the separation of roles can be difficult to assess. For example in a SaaS scenario, unless parts are outsourced, there is no distinction between the data controller and data processor. While the above roles and responsibilities are valid for both the EU DPD and GDPR, the GDPR brings several changes that will be discussed next.

5.1.3 Selected Changes in the EU GDPR Draft

While the roles and responsibilities are similar in both the EU DPD and EU GDPR, and both are based on the core principles of OECD, the EU GDPR introduces several changes.

The most noticeable difference between the EU DPD and EU GDPR is the change of instrument. The regulation will “contribute to having one single law applicable throughout Europe”, enabling greater consistency in Europe [12].

The EU GDPR also clarifies that a CSP will fall under the EU legislation when they offer services to data subjects in the EU or monitor the behavior of data subjects within the EU. A non-EU CSP, which has an English website and a UK support phone number, offering services to UK customers, would thereby have to comply with the EU GDPR [12].

Other changes include:

- Introduce articles that clearly state and specify the responsibilities of the controller (Art. 22) and the processor (Art. 26).
- The responsibilities of the processor are increased: Changes include that data processors are explicitly required to “maintain documentation of processing operations”, carry out data protection assessment and ensure that data which is moved outside of the EU is processed with the same level of protection.
- Clarifies the criteria for determining the main establishment, *i.e.* the way to evaluate the applicable law in Art. 4 (13) within the EU and the need for a representative within the EU for controllers with their main establishment outside the EU (with exceptions) in Art. 25.
- Clarifies on international data transfer, explicitly mentioning Binding Corporate Rules (BCR) in Art. 42 and extending in Art. 43 for both the data controller and data processor. Further issues in international data transfer will follow in Section 5.5.2.
- The right of the data subjects are increased and clarified. This includes that they must be informed of data transfer to third countries and retention time (Art. 14), the right to be forgotten is strengthened (Art. 17) and introduces that data controllers must “establish procedures” to ensure the data subject’s rights. Art. 18 introduces the right to “data portability”. Data portability here referring to the personal data, which must be made obtainable by the controller “in an electronic and structured format which is commonly used”.
- Explicitly states the need for a Privacy Impact Assessment (Art. 33) when specific risks to data subjects are present. It further clarifies when prior authorization and prior consultation from a supervisory authority is required (Art. 34).
- Explicit rules on data security are introduced in Art. 30, in the EU DPD these were to be defined according to national law (EU DPD Art. 17). Art. 31 and 32 add the need for informing authorities and data subjects in case of data breach.

The EU GDPR draft therefore specifies and clarifies many points relevant to CC. However, as of the time of writing, it is still in draft stage and the full impact of the EU GDPR is to be seen.

5.1.4 US and the Safe Harbor Agreement

Unlike in the EU, the US does not have a comprehensive data protection law, as no authorities have the power for a national privacy law. As for federated laws, the Privacy Act of 1974 regulates the collection and usage of data of personal information, but only for federal agencies and is only valid for personal data of US citizens [33]. While states in the US can have their own laws, and there are scattered laws that can apply to CC, some only applying to specific sectors such as financial services or healthcare, it can be concluded that there are “enormous differences” [32] between the regulation in the European Union and the United States [32], [4], [28].

Even though the level of regulation in the EU and the US varies greatly, the Safe Harbor Agreement¹ allows personal data transmission between the EU and the US. The US counterpart has to self-assess if they adhere to EU DPD and register with the Department of Commerce. Once this is completed, the US company is seen as safe harbor and personal data can be transferred as within the EU. While the recent revelations of Edward Snowden has led to discussion if the transmission is still legal in light of the US surveillance framework, in practice it remains the easiest solution for CSPs located in the US for now [58].

It is therefore in the interest of US CSPs which want to increase their market potential to Europe to comply with the EU DPD.

5.2 Competition Laws

As one of the major factors discussed in CC is the lock-in effect, which can be caused by a lack of standards. The competition/anti-trust laws goal is to protect customers [34]. As competition rules are “considered to be generally applicable norms” [66] and the lock-in effect harms customers, this chapter will explore the competition law and discuss the possibilities it has to prevent or decrease the consequences of the lock-in effect.

Art. 102 TFEU states that “any abuse (...) undertaking of a dominant position (...) shall be prohibited”. This includes situations where CSPs are excluded from competing for customers of dominant CSPs. However, the competition law is only partial applicable for the implications that exist in CC. Not only has the behavior to be “abusive”, but a CSP must also be in a dominant position. While there is no clear cut where a CSP is dominant, generally market shares above 40% are considered problematic and are looked into further [57]. Another factor that is considered are the market entry barriers [66].

The current situation in CC, however, has no clear market leader, competition between provider (including Google, Microsoft, Amazon, Salesforce) is fierce [57] and it is unlikely that one of these providers will find itself in a dominant situation within the foreseeable future. Furthermore, while entry barriers exist, *e.g.* high initial costs, they cannot be considered “insurmountable” [57]. Therefore, even though the lack of standards, and issues with data portability, interoperability and other technical factors, can lead to disadvantages for customers, there is no evidence that there exists a situation which would call for an intervention from competitive law. However, if the leading CSPs act in a way to specifically shield their services, it might become a case for competition law. Competition laws should encourage open cloud systems, promoting open standards and monitor the market carefully[66].

¹<http://export.gov/safeharbor/>

5.3 Contracts and Service Level Agreements

The stakeholders in CC are typically in a relationship which is based on contracts. This does not only apply to the cloud customer and the CSP, but also applies for brokers. The SLAs have a central role in CC, they define the specification and quality of the service. They also define the consequences when a party does not deliver as agreed and can act as specifications, when services are defined in great detail[9].

CC SLAs typically include [30], [9]:

Definition of Services

This section includes the services agreed upon and how they are delivered. They must be accurate and include specific information for each agreed on service [30]. The terminology used within the SLA should also be clarified in this section [9].

Availability and Service Response Time/Latency

Of special interest for CC is the (technical) availability and agreed upon maximal response time of the service. These technical thresholds are an essential part of any SLA. For both of these factors, the SLA only applies to issues that arise at the CSP. If the cloud-based service is not available due to a third party (*e.g.* outage of Internet connection on the CSC's premises), the CSP cannot be made accountable [9].

Performance Management

To ensure that customers can recognize and take action on deviations from the agreed service levels, performance management is required. It is important that all agreed upon service levels can be measured. This section of the SLA specifies where the performance management monitored and measured results and benchmarks are available. Many of the public cloud solutions offer "best-effort-service", for which performance management is less relevant. If specific thresholds are defined, this sections becomes more important [9].

Problem Management

This section covers how incidents and issues are resolved. It often includes the timeframe in which issues have to be resolved by the CSP after an issue has been reported by the CSC. As with the availability and service response time, this only applies to issues where the CSP is responsible. This section should also include preventive measures [30], [9].

Customer Duties and Responsibilities

The SLA does not only define the responsibilities of the CSP, but also of the CSC. This can include how, when and how many users can access the service. If physical access to the CSP's premises is required, procedure and restrictions are also outlined here [30].

Warranties and Remedies

The penalties describe the consequences of when the service and quality levels agreed upon are not met. This can include fines but also termination (without cancellation period) of the service [9]. This section should also include third party claims, remedies for breaches and the exclusion of force majeure [30].

Security

The agreed upon security settings that have to be adhered to by the parties. This is especially important, as cloud services are available from everywhere. Therefore, the required authentication process and how authorization is granted has to be considered. Furthermore, it should be defined what information is logged, who has access to the logs and how anomalies are treated.

Disaster Recovery and Business Continuity

Cloud-based computing often leads to high dependencies for CSC, disaster recovery should be reflected within the SLA. At highest level, this section typically states “that there must be adequate provision for disaster recovery and business continuity planning to protect the continuity of the services being delivered” [30].

Termination

The termination agreement of the contract. It should cover how the termination at the end of initial term, termination for convenience, termination for cause and payments on termination [30].

As [9] points out, this section should also include how data is to be treated. This includes deletion of data and transferring data back to the CSC. For both of these, the level of security also has to be considered.

Subcontractors, Applicable Law and Place of Jurisdiction

This section covers further legislative questions. It is to be defined if the CSP can use subcontractors and define the accountability of using them, which laws are applicable and which is the place of jurisdiction[9].

Many details can therefore be covered in the SLA. However, it is important to note that SLAs have to comply with all legal aspects and are otherwise not valid.

5.4 Other Legislation and Industry Specific Regulations

While contracts and SLA are essential for CC in general, there exist legislations and industry specific regulations which can affect CC in specific cases, but consequences are case specific and therefore out of scope for this thesis. Several examples will be introduced within this section.

5.4.1 Copyright

CC introduces new challenges regarding copyright, both to the (public) CSP and the CSC. These challenges include whether CSPs are responsible for copyright infringements by their users and if the existing Internet Service Provider's (ISP) safe harbor legislation, which protects the ISPs from consequences of their subscribers regarding copyright infringements, is sufficient to satisfy all stakeholders.

While CC might increase the complexity, [62] concludes that “there is no immediate need to strengthen the protection of online intermediaries and CC providers”. Furthermore, as [33] explains, it is difficult to derive common requirements for CC from copyright laws, as they are typically case specific.

5.4.2 Ecological Legislation

Data centers typically require large amounts of energy [33] and with the target of reducing greenhouse gas emissions [40], ecological regulation can become a factor to be considered in CC. According to [38], (public) CC is attractive to “large IT infrastructures that want to reduce their carbon footprint”. Further goals in greenhouse gas reduction and corresponding laws and regulations can increase pressure on companies to reduce their carbon footprint, making CC a valuable option. Of course, CSPs are also affected by such laws. However, the eco-friendliness depends on many factors [33] and no regulations that specifically apply to CC exist.

5.4.3 Industry Specific Regulations

Unlike the previous discussed laws, there are also many regulations which only apply to specific industries. This is especially the case in industries where confidential personal data is required. There are more industries and many local regulations for different sectors, exemplarily we will consider the US financial and healthcare sector.

Financial Services

The financial industry in the US has to comply with the Gramm-Leach-Bliley Act (GLBA). It covers many topics, including information privacy and sets standards to ensure security against unauthorized access and other threats [28].

Healthcare

The healthcare sector is another example that is highly regulated. For the US, both the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) have to be considered by organizations which possess personal health data. HIPAA requires organizations to take specific actions to ensure confidentiality, integrity and availability of personal data [28].

5.5 Cloud Specific Issues

The different laws and regulations all influence CC, as the concept of CC leads to consequential issues. Such issues include the general concept of outsourcing, the location of the different stakeholders, subcontracting in relating to the contracts and SLAs.

5.5.1 Outsourcing

Public cloud-based computing is a form of outsourcing. This leads to several challenges:

Technical Safeguards for Identity Management and Authentication

Cloud-based computing services, especially in the case of public clouds, are often accessible from everywhere, all the time. While this increases the user's mobility, it introduces the need for identity management and authentication to comply with the data security principles and laws [13].

Proper Exit Plan, Data Erasure and Data Portability

Data processors are responsible that they comply with the collection limitation, use limitation and that data subjects can have their data deleted. It is essential, that a proper exit plan is agreed upon and it is ensured that data is deleted on termination of any contracts. Since under the EU GDPR it is also required, that data subjects can receive a copy of data stored in a common format, data portability must also be considered.

Limitations on the Data Use in the Cloud

Public CSPs might receive data from several of their customers on data subjects, in some cases the data subjects might use them directly. This leaves CSPs in a position, where they can combine data of different sources on data subjects. However, this is prohibited by the use limitation principle and laws derived from it. Data processors should include limitations on how data is to be used by CSPs in the contract [13].

Formal Data Breach Management and Notification Arrangements

Data subjects must be informed on data breaches. Plans for all eventualities should be in place from the very beginning, ensuring that in case of data breach data subjects are informed [13].

5.5.2 Location and Cross-Border Data Flow

CSPs often have data centers all over the world, or offer services in other regions than where they offer their services. CSPs can optimize use of their resources, increase availability for the consumers and act more flexible. While this makes sense for CSPs, it is problematic from a legal perspective as many legislations prohibit data flow between borders. Even if data is only stored in applicable states, it is still possible that the data is transmitted via third countries.

Personal Data in other Jurisdictions

As explained before, having data in different locations is beneficial. However, the data controller is responsible to comply with the law. When transmitting data to different locations, it is important to consider any exceptions to the prohibition of transmitting data between borders. In the EU, the already discussed safe harbor agreements and binding corporate rules can be applied. It must also be remembered, that depending on the legislation, data subjects must be informed that data is transmitted across borders.

If clouds are located in several territories, the question which laws and courts are responsible arises. In civil law the CSPs and CSCs can choose the law and responsible court. However, it must be either one of the locations of the CSP or the CSC. In private law, the applicable law is geo-location determined by the location of the CSP [43]. It is important for CSCs and providers to consider the competent court and the consequences of it. The EU GDPR will have consequences on place of jurisdiction, to what extent is still to be seen.

5.5.3 Subcontract Offerings

Scalability and elasticity are great advantages of CC. However, to achieve this, many CSPs work with several infrastructure providers. If the CSP cannot provide the capacity itself, subcontractors will allocate resources. Subcontractors might use subcontractors themselves for the same reasoning. From the perspective of a CSP, this is a reasonable action. However, it increases the risk of losing control over data for the CSC. While data subjects have to be informed about data movements to third countries under the EU GDPR, very few CSPs are transparent about subcontracting arrangements as of now. The use of subcontracts leads to several implications [13].

Lack of Formal Contractual Relationship

The CSC has no formal contract with the subcontractors of the CSP. In many cases, the CSC might not even be aware of the different subcontractors. In the case of a data breach or misuse, the CSC cannot hold the subcontractors contractually liable for any consequences. The missing direct link can reduce the perceived responsibility and loyalty of the subcontractors, leading to less sensitive handling of direct data. In the case of data breaches, the legal and reputational damages to the CSP can often not be “realistically compensated for by suing either the CSP or its subcontractors” [13].

Lack of Privacy Awareness and Legal Sanctions

Subcontractors in different locations might have a different attitude towards data privacy and lack the respect for it. This can be caused by the lack of legal sanctions available in their operating environment [13].

5.5.4 Standard Offerings, Terms of Usage and Service Level Agreements

CSPs often only provide a predefined set of services. These offerings include terms of usage and service level agreement. This is especially true for personal CSPs. The contracts in such offerings often include clauses that are “detrimental” to the CSC. Smaller costumers often lack the market power to receive better contracts, due to scale, size and resources [32].

CSCs should not consider CSPs’ standard offers that do not comply with their security requirements. Failing to do so puts personal data and personal data and business reputation at risk. While it can be difficult for smaller organizations to retrieve personalized contracts, the terms should always be discussed to ensure compliance with the different OECD core principles [13].

5.6 Legislative Implications in Cloud Federation Scenarios

While all of the previous issues of course also apply to cloud federations, they increase the legal complexity even further. [33] show the legal implications cloud federations have on their participators with different scenarios regarding responsibilities of the participators and locations. They differentiate three different participators:

- Service Provider
- Infrastructure Provider
- Users

The SP is, in the terminology of this thesis, the CSP, *i.e.* the entity responsible for the cloud. It can be a broker, a single SP with self managed infrastructure, or an SP with relations to one or several IPs. An IP manages resources that are typically owned or leased by an organization (in case of a private cloud) or by an SP, but do not offer direct services to users (if an IP offers direct services, he would be considered as SP). Users represent the CSCs. From a legal perspective, the participators can have different responsibilities in different scenarios.

5.6.1 Roles according EU DPD in Cloud Federation Scenarios

Cloud federations introduce an increased complexity in the legislative environment. The difficulty to assign responsibilities to different roles is one of the challenges. To depict these implications of cloud federations, seven general scenarios and seven location based scenarios are considered. The general scenarios regard the roles and responsibilities for the different participators from the perspective of the EU DPD [33].

General Scenario G1

A user has a contract with a SP to store (and probably process) data. The SP leases infrastructure from an IP, where the data is stored on a database (DB) managed by a virtual machine (VM).

General Scenario G2

The user has a contract with an SP to store (and probably process) data. The SP has its own infrastructure, *i.e.* the SP is also the IP.

General Scenario G3

G3 is similar to scenario 1, but a reseller is introduced. The user has a contract with SP1, who resells the service of SP2, who has a contract with an IP.

General Scenario G4

As in scenario 1, the user has a contract with an SP. The SP has a contract with an IP (IP1). However, the IP1 has another contract with another IP (IP2) and some of the user's data is stored and processed at IP2. The SP might not know about this.

General Scenario G5

In this scenario, the user has a contract with the SP, who leases the infrastructure from an IP. The IP has a public interface that the user can directly access, *i.e.* without involving the SP.

General Scenario G6

The user has a contract with two different SPs, which both use IPs. The user migrates data between SP1 and SP2.

General Scenario G7

The user has a contract with two IPs and asks an SP to migrate data between IP1 and IP2.

The EU DPD Roles in the different Scenarios

Considering these scenarios and the EU DPD, the roles match as follows:

General Scenario	User	SP	IP
G1	-	DC	DP
G2	-	DC	-
G3	-	DC	DP
G4	-	DC	DC & DP
G5	DC	DC	DP
G6	DC	DC	DP
G7	-	DC	DP

Table 5.1: Responsibilities of Actors in Federations According to EU DPD [33]

Scenarios **G1-G3** are rather straight forward. The SP is the DC, and the IP the DP. If there is more than one on SP, the last SP contacting the IP is the DC. The exception to this is case is **G2**, where no DP exists as the SP is its own IP. In **G4** with different IPs, the IP transferring resources to another becomes a DC and the receiving IP is the DP. **G5** represents a situation where the user can directly access the data at the IP. The user therefore also is a DC. While in **G6** the user migrates between two IPs, the data is migrated by the SP in **G7**. Therefore, the user is a DC in **G6** but not in **G7** [33].

As shown, different cloud scenarios lead to different roles and responsibilities under the EU DPD. The complexity is increased further when considering the locations of the different actors.

5.6.2 Location and Applicable Jurisdiction in Cloud Federation Scenarios

The different roles and responsibilities are not the only legal issue in cloud federations. All these entities can be located and have establishments (E) in different locations and therefore different jurisdictions (J). They can be located in EU member states (ms). Jurisdictions define the practical authority of a court to preside over a case. To illustrate the issues in cloud federations, seven location scenarios are considered [33].

Location Scenario L1

The most simple scenario is **L1**. It includes a SP that also acts as IP and has one data center in a single jurisdiction.

Location Scenario L2

In the second scenario, the IP has different facilities in different jurisdictions. Data is stored and managed at the same establishment.

Location Scenario L3

Similar to the location scenario 2, an IP has different facilities. However, the machines managing data and the storage location are in two different jurisdictions.

Location Scenario L4

As before, the IP has establishments in several jurisdictions. One of them being J1.

Location Scenario L5

This scenario represents a similar situation as general scenario 4. IP1 in J1 uses resources from a different provider in J2, while the SP might be unaware of this.

Location Scenario L6

A broker, *i.e.* the SP is located in J1 and utilizes several IPs. One of the IPs is located in J2.

Location Scenario L7

As the previous location scenario, a broker in J1 uses several IPs. One of the IPs is also located at J1.

The applicable Jurisdiction in the different Location Scenarios

The EU DPD states that location of the DC determines the place of jurisdiction. Therefore, the following situation arises from the different scenarios:

Location Scenario	SP	IP	National Law of Establishment Applicable
L1	DC	-	E of SP
L2	-	DC	E_x of IP
L3	-	DC	E_i of IP
L4	-	DC	E_{ms} of IP
L5	-	DC & SP	E_{ms} of IP
L6	DC	DP	E of SP
L7	DC	DP	E_{ms} of IP

Table 5.2: Applicable Law in Cloud Federation Location Scenarios [33]

The situation in **L1** is straight forward. The SP only has one establishment within the EU, therefore the location of the single establishment sets the applicable national law. In **L2** the IP is the DC, therefore his location is decisively. E_x as the IP has more than one establishment in EU member states. Data is stored and processed in the same location, therefore the corresponding national law of them has to be applied. The third scenario, **L3**, includes data stored in different locations than managed. The national law applicable is decided upon the place where it is managed, not stored. This is denoted by E_i . **L4** introduces non EU member states. However, if one of the establishments is located in an EU member state, the member states law (E_i) is applicable. In **L4**, the SP might be unaware that the IP (IP1) transmits data to another IP (IP2). If IP1 is located in a member state, this location determines the applicable law. In this situation, IP1 is the DC and IP2 the DP. If IP1 is not located in a member state, but IP2 is, the location of IP2 determines the applicable law. Furthermore, the IP not located within a member state, must provide the same level of data protection as defined in the EU DPD. **L6** determines a situation where the SPs location determines the national law (recital (1) in the preamble of [16]), all used IPs must at least have the same level of data protection as determined in the EU DPD. In scenario **L7**, the SP is not necessary in a member state. If one of the IPs used is located in a member state, it determines the national laws applicable. Any non-member state actor must provide the adequate level of protection [33].

As the different scenarios show, not only the roles and responsibilities but also the national law applicable depend on particular situations and locations of all the actors. As soon as one actor is established within the EU, the construct is regulated by the EU DPD. The EU GDPR will reduce this complexity, as it is applicable, as soon as services are targeted at EU citizens. However, at the time of writing, every location has to be carefully considered in a cloud federation approach.

Chapter 6

Interrelations within Factors that Affect Cloud Computing

In the following chapter the most important interrelations between factors and the legal and regulative constraints are discussed. The relations have been grouped to increase readability. However, these groups are not self-contained. Several factors are included in several groups, therefore interconnecting the different groups.



Figure 6.1: Legend for Interrelations between Factors

6.1 Interrelations Affecting Availability

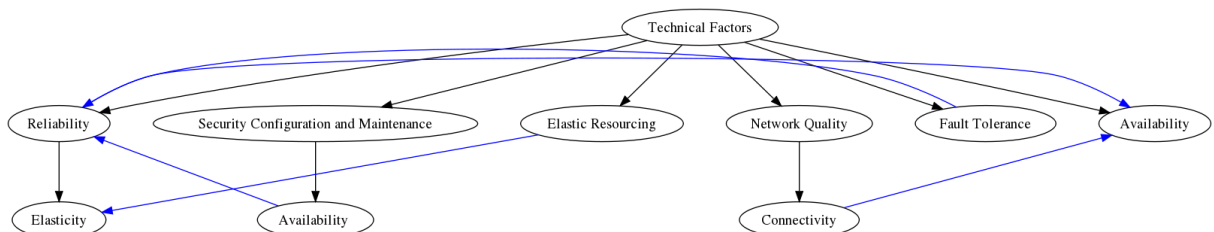


Figure 6.2: Interrelations Affecting Availability

The availability of a service is mainly influenced by technical factors. Firstly, it is influenced by the reliability of a service. Low reliability of a service has a negative effect on the

availability. The reliability of the service is influenced by three factors: Elastic resourcing, fault tolerance and the security system of a service. Elastic resourcing is important for elasticity in reliability. If the system does not have the capacities to assign more resources when required, it will fail or become unusable, and therefore availability is decreased. Increased fault tolerance also increases reliability. The system will not fail, even if there is some error in the system, which can be caused by another user. If fault tolerance is low, the availability is negatively affected, as the system cannot handle requests any longer.

The security system should be configured in such a way, that services are still available to authorized users, even if there is some misbehavior. If the security system locks the system down in case of misbehavior, the availability is reduced. Depending on the confidentiality of the data on the system, an aggressive behavior of the security system might be preferred over increased uptime. However, as especially in public cloud scenarios, many customers can be affected. In other cloud deployment models, *e.g.* private and community clouds, the stakeholders need to find the right balance between security and uptime.

Not all factors related to availability can be controlled by the CSP. The network quality, respectively the connectivity, also has an influence on the availability of a service. Even if there is no issue from the CSPs' site, it is possible that a cloud-based service is not available to the CSCs if there is a connectivity issue.

6.2 Interrelations Affecting Backups

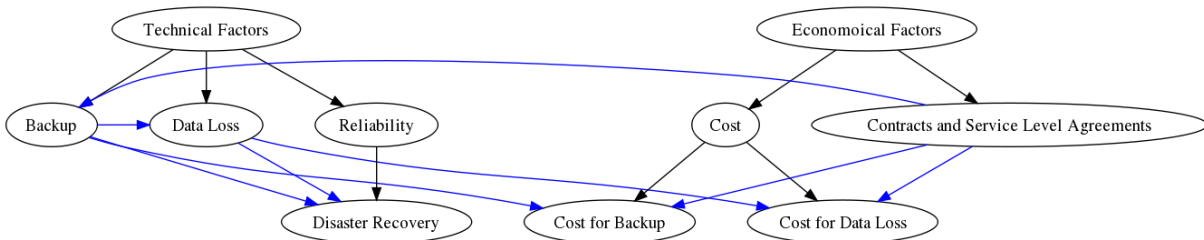


Figure 6.3: Interrelations Affecting Backups

Information is a valuable commodity of organizations. Backups can protect information and prevent data loss, as in case of hardware failure another copy of the information is available. Backups also influence disaster recovery. In case of a disaster, the backup can be used to continue the service at another place.

Backups have several economic implications. Considering the relation between a CSP and CSC, the terms of backing up data is defined in the SLAs. The costs for backups are therefore influenced by the SLAs, as should be the extent of backups. Furthermore, the SLAs should include the liabilities of the stakeholders. In case of data loss, this can include financial consequences for the CSP. Therefore, the SLAs do not only influence backups directly, but also the costs for backups and the costs for data loss. The costs for data loss are not only defined by potential remedies from the CSP, but also if data loss actually occurs, respectively if backups exist.

6.3 Interrelations Affecting Business Flexibility and Agility

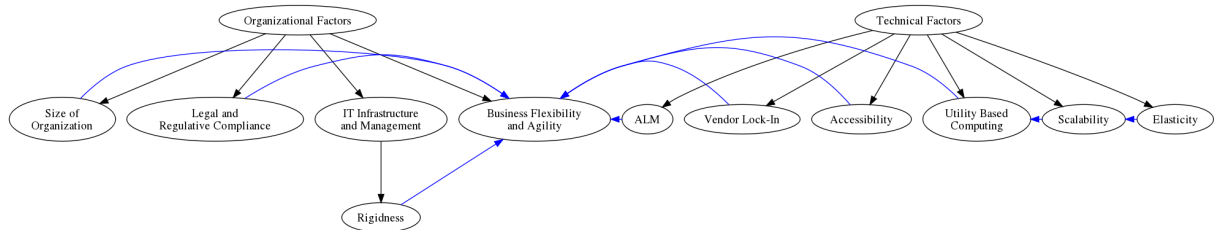


Figure 6.4: Interrelations Affecting Business Flexibility and Agility

One of the organizational benefits of CC is increased flexibility and agility. On one hand, business flexibility is interrelated to the technical factors of CC. Utility based computing allows organizations to obtain the resources they require on demand, not requiring large investments into hardware infrastructure. This allows organizations to quickly adapt to changes in demand, increasing their agility and flexibility.

As discussed in Section 4.1.22 and 4.1.30, utility based computing is related to scalability, which requires elastic resourcing. Increased scalability and elastic resourcing therefore both influence business flexibility and agility positively, as they enable utility based computing.

Accessibility, *i.e.* the difficulty to access and use the service, also influences flexibility and agility. Cloud-based services which allow high accessibility, *e.g.* SaaS which can be accessed from anywhere and with any device, increase the flexibility and agility.

The increased simplicity of ALM is also influences business flexibility and agility. Independent of the deployment model, deployment of changes is simplified and requires less time. This allows CSCs to quicker react to changes in the environment.

One factor influencing business flexibility and agility negatively is vendor lock-in. An increase in vendor lock-in increases the power of the CSP and reduces the flexibility and agility of the CSC, as the CSC loses control and cannot change the provider easily.

Business flexibility and agility is not only influenced by technical factors, but also depends on organizational factors. A large organization is likely to be less flexible and agile than a smaller one. Small organizations can react faster to changes in the environment. Another factor to be considered regarding business flexibility and agility is the legislative environment, represented as legal and regulative compliance. Higher regulation decrease the flexibility and agility, as it increases complexity to implement organizational changes. Organizations have to carefully consider the effects of changes on the legal and regulative compliance, increasing complexity. Finally, the rigidness of the IT infrastructure and management is also related to flexibility and agility. High rigidness decreases flexibility and agility, as more resistance to changes is to be expected.

6.4 Interrelations Affecting CAPEX

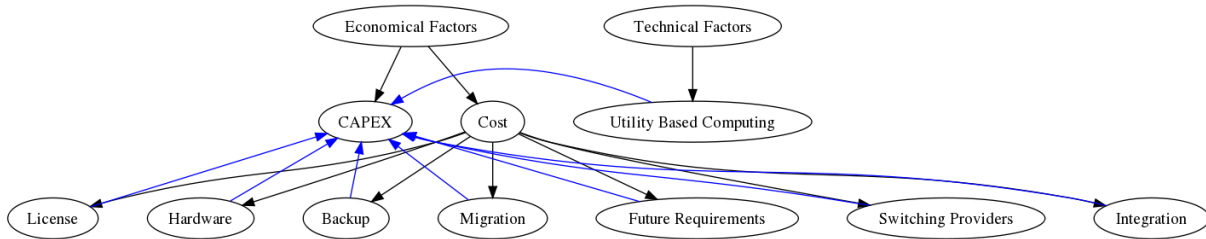


Figure 6.5: Interrelations Affecting CAPEX

CAPEX is affected by all expenditures into assets, which will affect an organization in the long term (over a year). It is affected by utility based computing, as cloud adoption typically shifts costs from CAPEX to OPEX. It is important to note that this is not the case for any in-house private cloud, as this also requires CAPEX expenditures, such as investments into hardware (*e.g.* servers) and infrastructure.

Considering the different cost factors identified in Chapter 4, this typically includes hardware and license costs. If licenses are CAPEX or OPEX depends on the license model, *i.e.* licenses which are bought once and used for longer than a year influence CAPEX, licenses based on a subscription model influence OPEX. Migration costs also influence CAPEX, as the migration towards the cloud can be considered as a long term investment which will result in reduced spendings and increased income in the long term. Therefore, it would be wrong to classify migration costs as OPEX, but they influence CAPEX. The same applies for costs concerning switching providers and integration costs. These costs are investments which influence the future of an organization.

The costs for future requirements also influence CAPEX. The decision to move towards cloud-based computing, the service and deployment model, and the chosen CSP all influence the future of the business and the costs to adjust for future requirements.

Finally, the costs for backups can be either OPEX or CAPEX. If investments are made to store backups in-house, these costs influence CAPEX, as they require investments. If however backups are stored in the cloud per subscription model, they influence OPEX, as they are part of the operational spendings.

6.5 Interrelations Affecting Collaboration

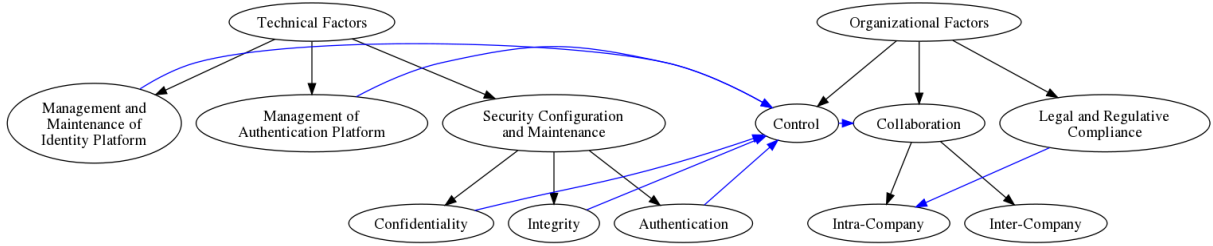


Figure 6.6: Interrelations Affecting Collaboration

Increased collaboration possibilities, both intra- and inter-company, are an advantage of CC. However, collaboration also introduces several risks, especially if it is between different organizations. Therefore, for both, intra- and inter-company collaboration, control has to be considered. Decreasing control influences collaboration negatively, as organizations will not risk losing control over their organizations for collaboration.

To ensure control, several factors of security configuration and maintenance have to be considered. Confidentiality and integrity are essential, to allow collaboration without losing control. It is likely that organizations have critical information in the cloud, independent of the service and deployment model, that should not be accessible by all entities (neither within one organization nor between organizations). To ensure this, authorization has to be considered. Both, the identity and authentication platform have to be considered, as these platforms are required to set access rights of the different entities and therefore to allow organizations to be in control.

Finally, organizations considering CC adoption to improve inter-company collaboration must consider the legal and regulative compliance. They especially have to consider the implications from privacy regulations, for the reasons discussed in Section 5.1.

6.6 Interrelations Affecting Control

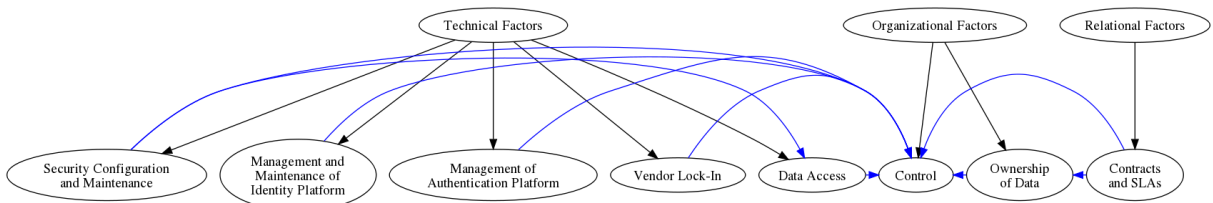


Figure 6.7: Interrelations Affecting Control

Control, respectively the fear of loss of control, is one of the factors hindering CC adoption. To reduce the risk of loss of control, the factors influencing control must be considered.

One of the biggest threats in terms of control is vendor lock-in. With increased vendor lock-in, switching providers becomes very difficult for a CSC. CSCs should therefore be aware of vendor lock-in and its related factors, explored in Section 6.18.

Organizations should also ensure that they own all the data transmitted to the CSP. To reach this, they have to safeguard that the contracts and SLAs are in their favor, *i.e.* it should be stated that the data belongs to the CSC and liabilities for the CSP in case of data breach must be included. As mentioned, information is a valuable commodity of organizations. Giving up data ownership will decrease control, as organizations do not own this valuable asset any longer.

Data access must also be considered in regard of control. The first aspect of data access that has to be considered is that the data is protected from unauthorized access. Data breaches cannot only lead to reputational damages, but confidential information might be leaked. To ensure data access, the security configuration and maintenance must be considered. Data access also has to be considered from the perspective that the organizations need access to its information, at any time. Not being able to access data is a loss of control, as it is one of the required resources.

While contracts and SLAs are an important factor to ensure control, relying on them is not enough. The security management and maintenance is another important factor related to control. It contains the technical necessities to ensure that only authorized entities can access the service and data of the organizations and allows auditability of changes. Both, the authentication and identity platform are also required in this regard, and thereby influence control. Without considering technical factors, the CSP might be held responsible for potential data losses and other negative consequences, but CSCs themselves lose control over valuable assets and face reputational damages.

6.7 Interrelations Affecting Cost Flexibility

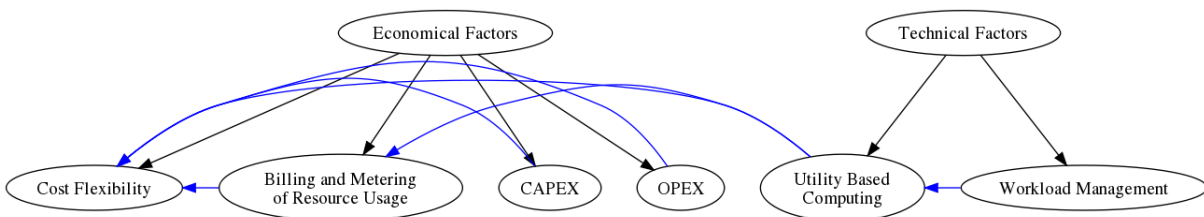


Figure 6.8: Interrelations Affecting Cost Flexibility

Increasing cost flexibility is especially interesting for SMEs, as it allows them to match their costs and demand. CC allow CSCs to benefit from cost flexibility, using utility based computing. Instead of having to invest into IT infrastructure (which influences CAPEX, as it requires investments), utility based computing allows organizations to pay for the utilities required at a given time. This increases cost flexibility, as the resources and costs associated with them, can be increased and decreased to match current demand.

Billing and metering of resource usage is also related to cost flexibility. If a CSP only offers “flat rate” services cost flexibility is smaller than if the CSP charges exactly for the resources required. While charging exactly for the resources required increases cost flexibility, it should be mentioned that it does not result in less costs for all CSCs. That can depend on the individual case. A “pay-as-you-go” utility based computing model does therefore not only directly influence cost flexibility, but also influences billing and metering of resource usage, which then also influences cost flexibility. Cost flexibility is further influenced by CAPEX and OPEX. The higher CAPEX and fixed OPEX are, the lower the flexibility. An increase in variable OPEX affects cost flexibility positively.

From the perspective of a CSP, offering utility based computing requires workload management, to ensure that it can optimize the workload utilization ratio and deliver CSCs the service promised according to the SLAs. Increased workload management allows it to offer more diversified services in terms of guaranteed performance. Furthermore, the workload management is required to ensure that the resources used by the different CSCs can be associated with the correct CSC.

6.8 Interrelations Affecting Marginal Cost and Profit

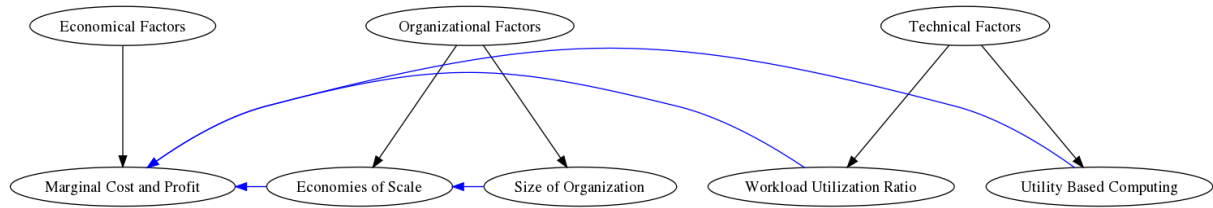


Figure 6.9: Interrelations Affecting Marginal Cost and Profit

The marginal cost and profit are influenced by several factors. Economies of scale can decrease marginal cost and thereby increase the marginal profit, as an additional unit costs them less. Economies of scale are mainly influenced by the size of an organization. Larger organizations are more likely to profit from economies of scale, as fixed costs can be split to more units produced.

From a CSPs perspective, or using a private in-house cloud, marginal cost and profit are also influenced by the workload utilization ratio. A low workload utilization ratio means the service is not used efficiently. An increase in the workload utilization ratio decreases marginal cost and increases marginal profit, as the additional output does not cause an increase in fixed costs. However, if the workload utilization ratio reaches 100% the service quality can decrease, and CSPs might need to invest in further hardware.

For a CSC, marginal cost and profit are also impacted by utility based computing. As long as the cost for additional resources is lower than the additional profit, CSCs profit. However, if the additional resources required from a CSC are more expensive than the benefit they generate, marginal profit decreases.

6.9 Interrelations Affecting OPEX

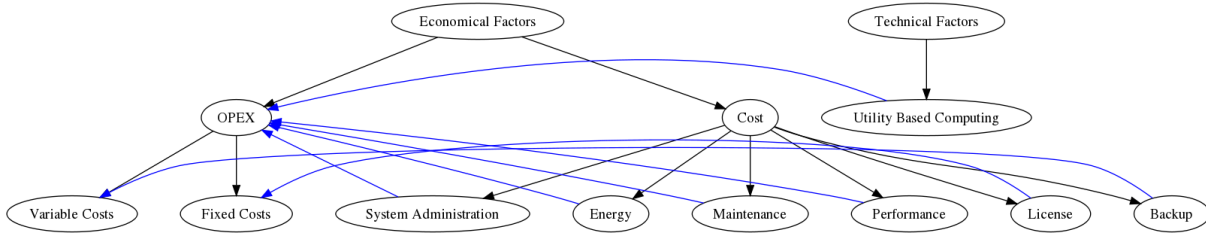


Figure 6.10: Interrelations Affecting OPEX

OPEX is influenced by all operating cost, *i.e.* costs which are not considered investments. The switch to utility based computing will influence OPEX, as it introduces a “pay-as-you-go-model”, therefore increasing OPEX and decreasing CAPEX. As cloud-based services can have a fixed basic fee and a variable fee depending on the resources required, they can influence both variable and fixed costs.

Other factors related to OPEX include energy costs, maintenance and system administration costs. As discussed in Section 6.4, backup cost and license cost can either influence OPEX or CAPEX. Whether these costs are considered as variable or fixed is case dependent. An organization with an internal system administration or a fixed service contract will consider system administration as fixed cost, while an organization with external system administration without fixed service fee will consider it a variable cost.

Energy costs can influence both fixed and variable costs. While IT infrastructure requires energy independent of the output, the level of energy required depends on the performance required.

License costs are typically fixed. The costs for backups that influence OPEX are typically based on the volume. Therefore, they influence variable costs. Performance costs in CC also influence OPEX. Performance levels defined in the SLAs can include fixed fees and fees which vary with demand and usage, therefore influencing both variable and fixed costs.

6.10 Interrelations Affecting Organizational Compatibility

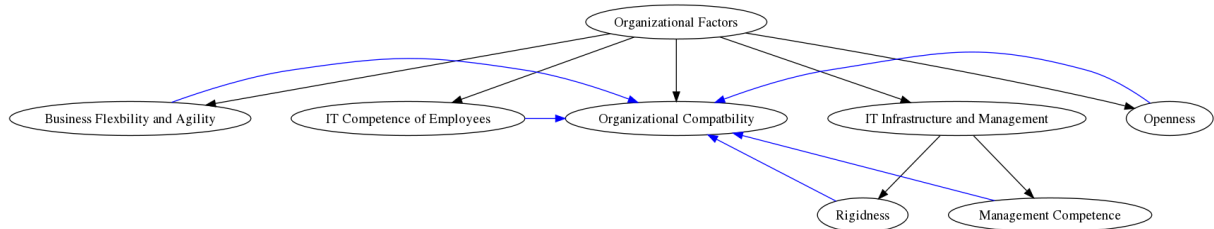


Figure 6.11: Interrelations Affecting Organizational Compatibility

Organizational compatibility is highly relevant in terms of required internal changes to successfully adopt CC, from both a process and value perspective. A high organizational compatibility influences CC adoption positively. The organizational compatibility itself is influenced by several factors from different areas.

The openness of an organization positively influences the organizational compatibility. A high openness means that the employees will not resist changes much, *i.e.* the introduction of cloud-based services. The IT competence of employees can also influence the organizational compatibility. An organization with less IT competence will have increased issues adopting CC, as it will take more training and time for the employees to adjust.

The same applies for the IT infrastructure and quality of the IT management. An organization with a rigid IT infrastructure will be less open to changes. Management does not only have to consider CC adoption as beneficial, but also persuade others of the benefits. Finally, the business flexibility and agility is also related to the organizational compatibility. If an organization can easily adjust, they will have less issues adopting cloud-based computing and therefore a higher organizational compatibility.

6.11 Interrelations Affecting Migration

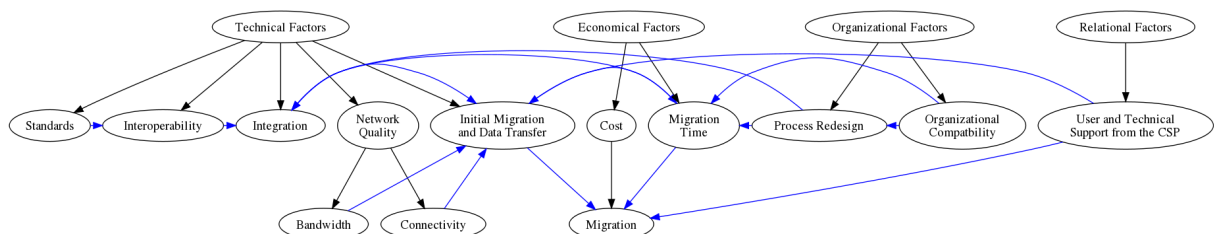


Figure 6.12: Interrelations Factors Affecting Migration

Migration, the phase in which a CSC first moves towards cloud-based computing and the associated costs, is influenced by factors of all the different fields.

From a technical perspective, the integration with existing systems has to be considered. If the cloud service is to be integrated with existing systems, the initial migration will take more time. This integration is influenced by interoperability between the existing solution and the cloud service, as interoperability is a requirement for integration. While a high level of standards does not guarantee interoperability, it increases the possibility for interoperability between systems.

The initial migration and data transfer is also influenced by the network quality, especially if much data has to be transmitted. Low bandwidth and connectivity issues will delay issues in the initial migration, as it takes more time to transmit the data. Furthermore, the consistency of the data has to be considered, when working with the data on the “old” system during migration. Technical and user support from the CSP can help with technical migration issues. The CSP might offer that data can be sent via HDDs, helping with the initial data transfer. The CSP will charge for services like that, thereby influencing the costs for migration.

From an organizational perspective, organizational compatibility influences migration. If the move to the cloud is associated with process redesign, more resistance is to be expected, employees need to be trained and get accustomed to the new routines. The longer the initial migration and data transfer takes, the more expensive it will become. This, as not only the CSP has to be paid, but it also has to be made sure that the existing system works until everything is migrated.

6.12 Interrelations Affecting Legal and Regulative Compliance

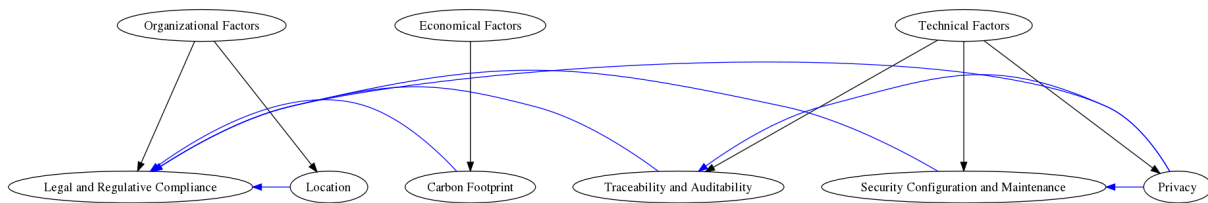


Figure 6.13: Interrelations Affecting Legal and Regulative Compliance

Legal and regulative compliance is affected by many different factors. As already stated, this factor is used as an anchor to introduce the legal and regulative concerns discussed in Chapter 5. The first factor influencing legal and regulative compliance is location. Both, the location of the CSC and the CSP have an impact on the applicable laws, regulations and the responsible jurisdiction. Furthermore, CSCs offering services to data subjects, must also consider the location of their target market according to the EU GDPR.

The legal and regulative compliance is affected by the security configuration and maintenance. CSCs using cloud-based services to offer their own services to data subjects, are

liable that security is sufficient to comply with the security safeguard principles discussed in Section 5.1.1.

Depending on the location and therefore the relevant legislation, organizations must comply with greenhouse laws and limit their carbon dioxide emissions. For these organizations, outsourcing their IT to a CSP can increase their compliance with the legislation.

Privacy concerns also influence the legal and regulative compliance. Unless the CSP is the data controller (*i.e.* not in SaaS scenario), it is the responsibility of the CSCs to ensure, that data subjects can obtain a copy of their personal data. They must also ensure that data subjects can have their personal data deleted and that it is not used for purposes not specified at the time of collection and that the data is protected accordingly. Therefore, the legal compliance is also influenced by the security configuration and maintenance.

To show compliance with privacy regulations, CSCs have to be able to show what data was collected, how it was collected and what happened with it. Traceability and auditability is therefore influenced by privacy concerns and influences legal and regulative compliance.

6.13 Interrelations Affecting Software Assurance

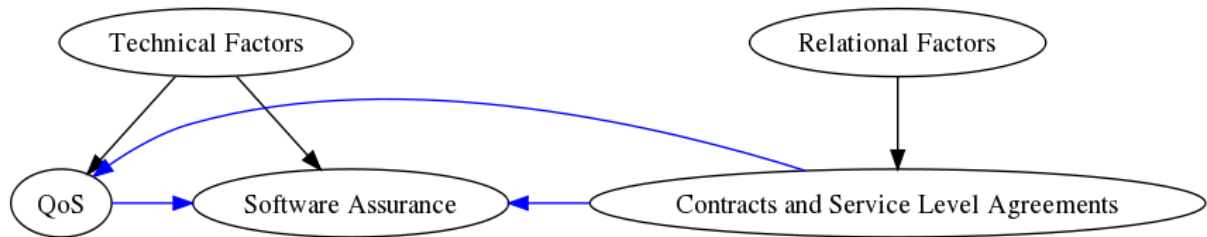


Figure 6.14: Relations Affecting Software Assurance

Software Assurance is the likelihood that a cloud service will perform as expected. It is mainly influenced by two perspectives: (1) Factors, that set the expectations, and (2), by the actual performance.

The main factors that set the expectations of the CSC are the contracts and SLAs. They define the service to be delivered, and the quality of service. They do not only set the expectations, but should also influence the level of the delivered service. Therefore, the contract and SLAs influence software assurance and the factors interrelated with QoS (see Section 6.14). CSPs might face financial remedies if they do not deliver as agreed upon, it is therefore in their interest to not over-promise.

However, just because it is defined in the contract and SLAs, it is not guaranteed that the CSP will deliver accordingly. As software assurance is the likelihood that a service works as expected, which is influenced by the SLAs, it is also affected by the actual delivered service. Therefore, it is influenced by the delivered QoS. A negative deviation in the factors defining the QoS, such as availability or service response time, will decrease

software assurance. If the CSP delivers as promised (or even better), software assurance increases.

6.14 Interrelations Affecting QoS

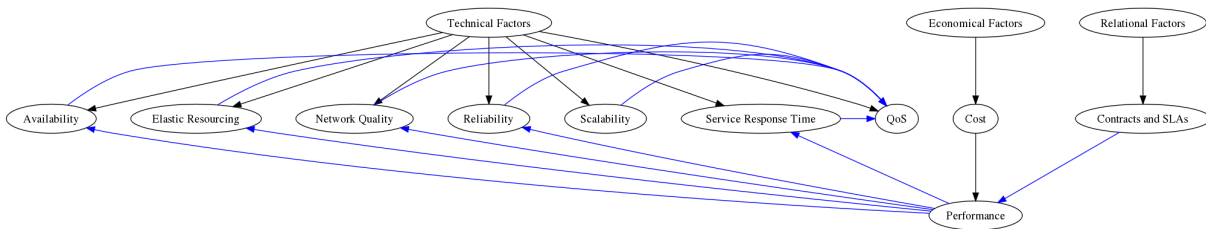


Figure 6.15: Interrelations Affecting QoS

QoS is defined as the level of performance, reliability and performance. It is therefore directly influenced by many technical factors.

The QoS is influenced by availability, elastic resourcing, network quality, reliability, scalability and service response time, as these factors define it. The expected quality for these factors should be explicitly mentioned in the contracts and SLAs. The level defined for these factors will influence the cost for the performance of the service. Higher promised quality will increase the price for the service. The performance cost of the service will therefore influence the level of performance for the technical factors mentioned above.

6.15 Interrelations Affecting Return on Investment

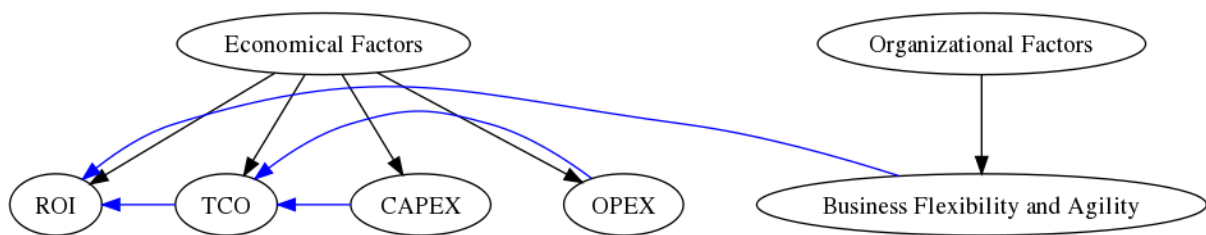


Figure 6.16: Interrelations Affecting Return on Investment

ROI is affected by the different costs and revenues. It is influenced by the TCO of CC, respectively the savings an organization has with CC against other options (*i.e.* TCO of CC vs. TCO of alternatives). The TCO is related to CAPEX and OPEX, as it includes all the costs for the service.

However, to calculate ROI, not only costs can be considered. Increase in profit, which can originate from benefits in CC, must also be taken into account. The increased business agility and flexibility can create new market opportunities and lead to additional profit, thereby improving the ROI of CC and influencing it.

6.16 Interrelations Affecting Trust towards the CSP

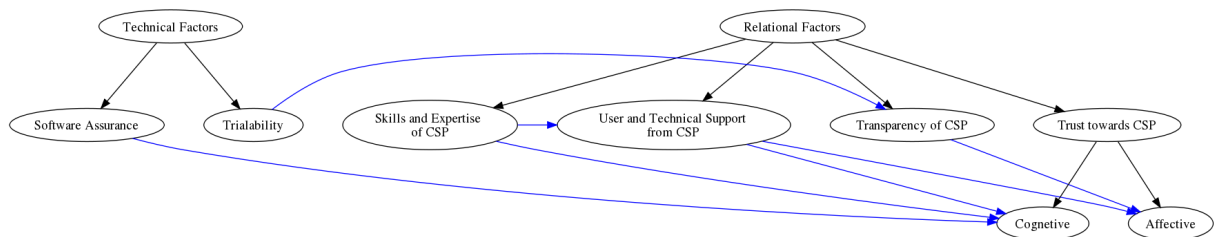


Figure 6.17: Interrelations Affecting Trust towards the CSP

Trust is a relational factor between a CSC and a CSP. Cognitive and affective trust are both influenced by different factors. As cognitive trust is built upon the delivery and the experienced expertise of the CSP, it is more rational than affective trust is. Affective trust is less rational, it builds on the perception of honest care by the CSP.

The main influence on cognitive trust is software assurance. With high software assurance, the CSC will trust that the CSP will also deliver as promised in the future. The expertise of the CSP can directly influence cognitive trust. Certifications and other indicators of expertise will influence cognitive trust positively. Skills and expertise can also increase the quality of user and technical support by the CSP, and can translate into better support.

Technical and user support, however, does not only influence cognitive, but also affective trust. As already discussed, cognitive trust is influenced by technical and user support, as these are indicators of the skill and expertise of the CSP. The communication required in support influences affective trust, as it influences the perception of honest concern and care.

Transparency of a CSP also influences the affective trust. Higher transparency cannot be equated with higher expertise or skills, but CSCs will perceive CSPs with high transparency as trustworthy, as they do not hide any information. A CSP can further increase its transparency, by letting the user try the service before committing to it. Therefore, trialability is positively associated with transparency of a CSP.

6.17 Interrelations Affecting Usability

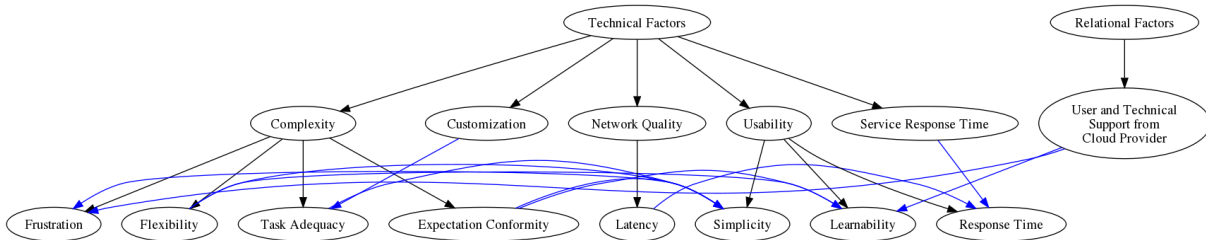


Figure 6.18: Interrelations Affecting Usability

Especially in SaaS scenarios, the usability, *i.e.* the user experience, of a service is of interest. Usability, and its sub-factors, are mainly influenced by technical factors.

First of all, the perceived simplicity of a service depends on the flexibility of the software. If there are several ways to achieve the same goal, the service is likely to be perceived as more simplistic. Flexibility also increases the learnability positively. As the same result can be achieved using different methods, learnability increases as not the exact steps have to be remembered.

Task adequacy also correlates to simplicity, as high task adequacy leads to low complexity. The better a service is suited for the task at hand, the simpler it is to reach the desired outcome. Task adequacy is influenced by customization. A service with high customization is more likely to be adjusted to the given task, than one with low customization. Low simplicity is related to frustration, as users will be frustrated by using the system, as they cannot fulfill the task easily.

Frustration can be lowered by the user and technical support of the CSP, as users have a point of contact that can help understand the system. Furthermore, the support from the CSP can increase learnability, if it provides required resources and is available to help with potential questions.

Waiting for response from the service decreases its usability, as users get distracted, if it takes the system too much time to respond. However, the response time can only be partly influenced by the CSP. It is influenced by the service response time, which can be influenced by the CSP, and the latency in network, which the CSP does not have full control over.

6.18 Interrelations Affecting Vendor Lock-In

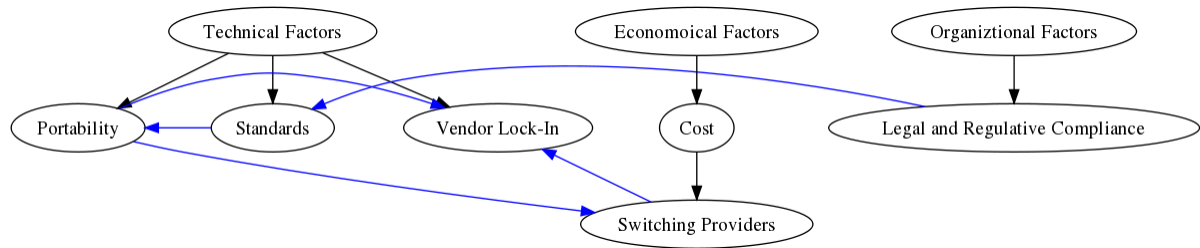


Figure 6.19: Interrelations Affecting Vendor Lock-In

Potential vendor lock-in is a great concern in CC adoption. It is interrelated with several technical and economical factors and is potentially affected by the legislation.

The first factor to consider are standards. Standards influence the portability of a service, it increases with an increase of standards and decreases with a decrease in standards. Portability defines the difficulty of moving a system, application or data between CSPs. A decrease of portability therefore increases the costs for switching providers, as the existing system cannot easily be migrated. It requires more resources to switch providers, as for example, data has to be manually adjusted to the new system. It also directly influences vendor lock-in, as it makes the technical switch to another provider difficult.

The costs for switching providers further influences the lock-in effect. The more expensive switching providers is, the higher the lock-in effect and the less likely CSCs can afford to switch. Standards are the key for decreasing vendor lock-in.

As discussed in Section 5.2, if CC drifts into a scenario where there is too little competition and abusive behavior of CSPs, regulators might interfere. One leverage they might use to decrease vendor lock-in, is the level of standardization that can be increased by forcing CSPs to support existing or new standards.

Chapter 7

Consequences of Changes in Cloud Computing

In the following chapter, effects of interrelations are further explored. Time-based graphs are used to model the consequences of changes in factors on other factors, including legislation. To do this, scenarios are created, and the trends of interrelated factors are plotted and discussed.

These graphs help to identify factors, which can be used as leverages to positively influence CC and reduce risks. Considering the different leverages to influence a factor is especially important, since some factors can be influenced more easily than others from within an organization. For example, business flexibility and agility is both influenced by the legislation and the usage of utility based computing. Changing external factors, such as the legislation, is hard to impossible to achieve, while adopting utility based computing is relatively easy in comparison.

The reason for the changing value of a factor can be versatile. After considering a broad approach and visualizing many relations, including relations of sub-factors, it was realized that this approach would not lead to the envisioned goal. Therefore, the focus is mainly on higher level visualization, exploring the reasons in depth. These reasons can be based on changes in sub-factors.

The graphs are created from the perspective of CSCs. Creating time-based graphs of interrelated factors pose a methodology to model and visualize the effects of interrelations of CC, to be used as a base of decision making and risk assessment, for different stakeholders. As the interrelations are versatile and sometimes similar, the chosen graphs are not claiming to be exhaustive. For this thesis, interrelated factors were chosen where CC can either be positively influenced by the CSC, thus identifying opportunities, or interrelations were attentiveness is required towards external influences (*e.g.* standards, legal influences).

Since the interest is on the effects of interrelations, the graphs focus on trends. Therefore, the steepness of a curve should not be considered by itself, only the difference between the steepness of changes in two factors is relevant. In the next section, examples are introduced to further clarify the setup of the graphs.

7.1 Time-Based Graphs Explained

The graph shows different scenarios over a period of time on the x-axis and the two factors plotted on the y-axis. The graph is split in different scenarios on the x-axis. These scenarios are independent of one another, each one of them represents a single scenario.

The interest is on the dynamics between the factors, not comparing the two factors with each other (*i.e.*, factor 2 is not “worse” than factor 1). As explored in Chapter 6, many factors are influencing each other. To visualize how one factor influences another, the first factor (represented in blue) is the factor that is changed, and the changes in factor 2 (orange) are a result of this or external changes related to the first factor.

As the goal is to explore the influence of one factor on another, it is mostly assumed that other factors interrelated with factor 2 are not changed. The reasons for why factor 1 might change are discussed in the description of the graph, and can be caused by changes in other factors as well. Consider the following example:

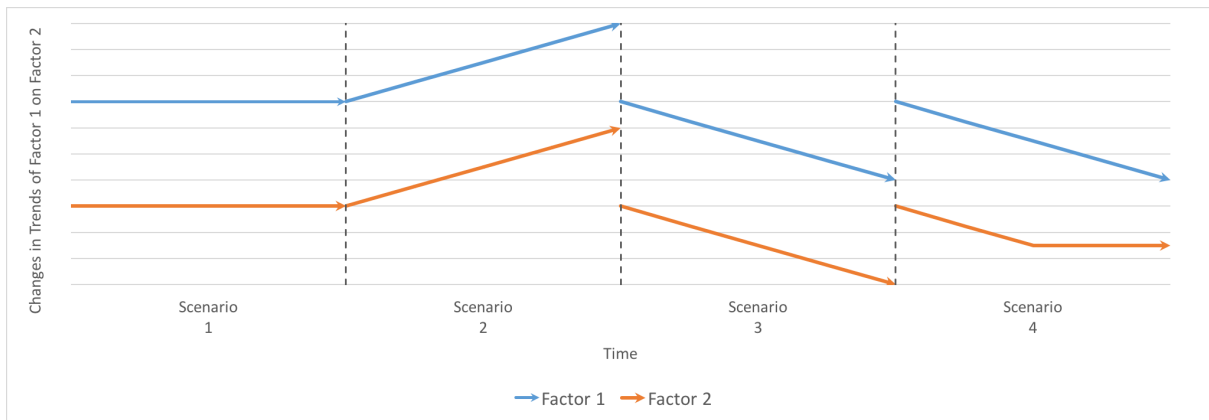


Figure 7.1: Legend for Time Based Graphs

This graph is split up into four different scenarios and shows the interrelations between factor 1 and factor 2. Each starting point of a scenario represents an independent point of time.

In scenario 1, there is no change for factor 1, therefore there will be no effect on factor 2. Since the interest is on the effect of changes, this scenario is not considered for the other time-based graphs. Scenario 2 and 3 both represent a positive relation between the two factors. If factor 1 increases, factor 2 will also increase. As long as factor 1 decreases over time, factor 2 also decreases. Scenario 4 is more interesting. While factor 1 decreases over a period of time, factor 2 only decreases in the beginning and is then stabilized.

In some graphs, thresholds are introduced (black line). These thresholds represent limits where a factor changes its state when reached. An example for such a change of state is legal and regulative compliance. Either the level of a factor is sufficient to be compliant, or not. A further increase will result in “better” compliance. The consequences depend on the influenced factor, and are explored in the text. Consider the following example:

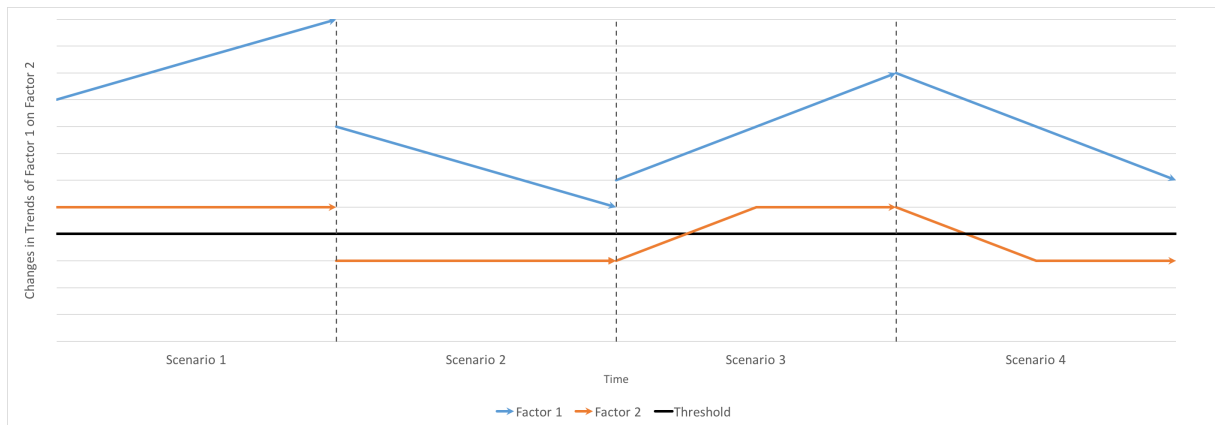


Figure 7.2: Legend for Time Based Graphs with Threshold

Factor 2 represents a factor with a binary condition, *i.e.* either it is achieved or not. It is positively influenced by factor 1, *i.e.* an increase in factor 1 will increase factor 2, until it is above the threshold. In scenario 1, factor 2 is already above the threshold. An increase in factor 1 does not influence factor 2 any more. The same applies in scenario 2. Factor 2 is already below the threshold, and therefore not influenced by a further decrease in factor 1. In scenario 3, the level of factor 2 is below the threshold. An increase in factor 1 will increase factor 2, until it reaches the threshold. Further increases do not have an effect on factor 2. Finally, in scenario 4, factor 2 is above the threshold. A decrease in factor 1 can push factor 2 below the threshold. Once below the threshold, it is not influenced by further decreases in factor 1.

In some instances, one should be aware that the threshold might change. For example, there might be a change in regulation, lowering or increasing the threshold to comply with the legal and regulative environment.

7.2 Changes in Trends of Backup on Cost

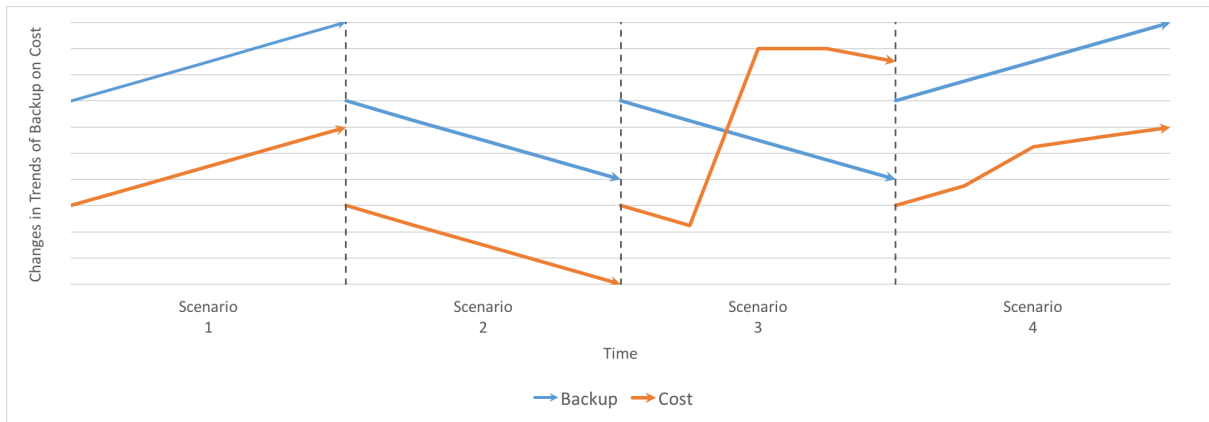


Figure 7.3: Changes in Trends of Backup on Cost

Backups can protect valuable data and enable disaster recovery (see Section 4.1.4 and 4.1.21). However, backups also increase cost for an organization. In this section, the consequences of a change in backup on cost are explored.

Scenario 1 and 2 represent simple cases, where there are no external influences. An increase in backup will influence the cost for backups, therefore costs increase. As long as there is no hardware issue or software loss, a decrease in backups will decrease costs, as costs for backups decrease and no other costs occur.

As mentioned, scenario 1 and 2 represent ideal cases, where there are no unexpected influences. Scenario 3 represents a case, where the costs are influenced due to a lack of backup (represented by a negative trend), due to external causes. As discussed in scenario 1, a lack of backups can actually decrease the costs of the organization. However, data is a valuable commodity of organizations. A lack of backup, visualized in this scenario as a decreasing trend, can have great implications in case of external influences. For example, hardware failure can lead to data loss. If there are no backups available, this can dramatically increase costs for an organization, visualized by the spike in cost of scenario 3. Costs will not increase due to higher costs for backup, but due to costs associated with data loss or disaster recovery. Recovering data can require high investments. Also, if an organization is not able to offer their service due the lack of backup, they lose potential revenues. Costs will increase rapidly, and stay at a high level until the issues can be resolved.

In scenario 4, the consequences of external influences, such as data loss, is considered, when an organization invests sufficiently in backups. This is represented by an increasing trend for backup. While more backup increases the cost of an organization due to higher backup costs, they are less influenced by external factors, such as data loss. In case of an emergency, such as hardware failure, the organization does not face the same consequences as in scenario 3. Costs can still increase for a short period of time, *e.g.* as getting the service back up running might still take some additional resources, but not comparable to the consequences discussed in scenario 3.

Organizations must therefore always consider the trade-off between potential financial losses in case of data failure and disaster recovery, and the costs for backups. Not investing enough into backups can lead to great costs, which are a lot higher than the costs that would have incurred for additional backup.

7.3 Changes in Trends of Complexity on Usability

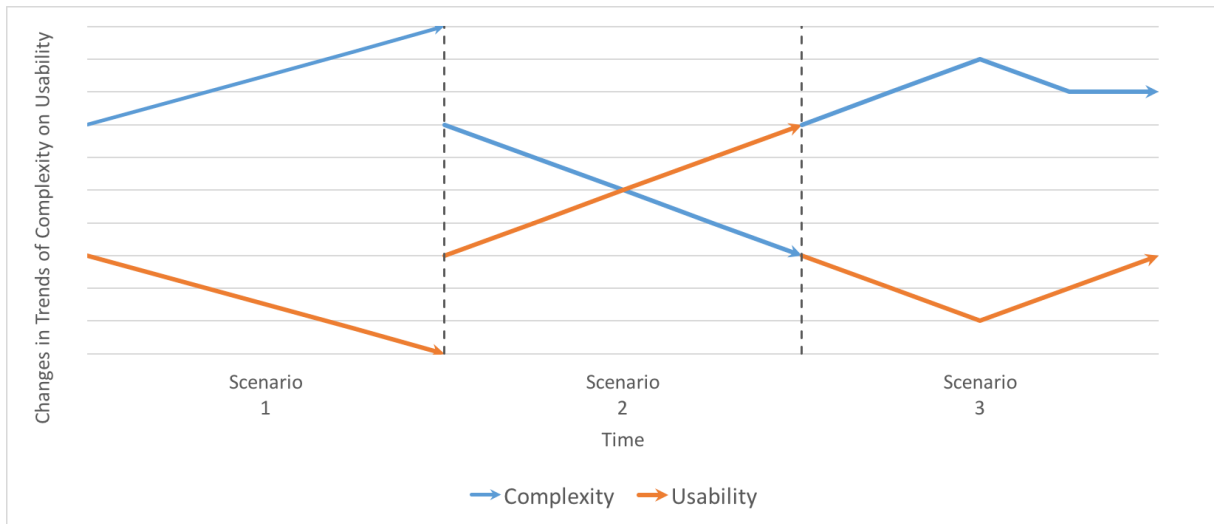


Figure 7.4: Changes in Trends of Complexity on Usability

The usability of cloud-based service is important for both the CSP and the CSC. The CSP improves the attractiveness of the service. For the CSC it directly influences the user experience. One of the factors affecting usability is complexity, which CSPs can influence to increase the usability.

If complexity increases (scenario 1), usability will decrease. Considering a SaaS scenario, the complexity of a service can increase due to an update. The CSP might introduce new functions or change the workflow of the application. Having to adjust to the new software can increase frustration for the user. The users have to learn a new version of the software, which has lower task adequacy than the old one. It might also lower the flexibility, decrease the simplicity of the software and thereby the usability. Decreasing task adequacy, and therefore increased complexity, can also occur due to a change of allowed customization of the software. So, if it was possible to adjust the old version of the SaaS solution to the organizational needs, but not the new one, usability will decrease. Finally, expectation conformity of the software might change with an update. As users know the “old way” of fulfilling a task, changing the workflow of an application is likely to decrease the expectation conformity. Expectation conformity influences and decreases usability via the sub factor simplicity and learnability.

Instead of increasing complexity, it of course is also possible (and more desirable by the CSP and CSC) that a new version decreases complexity. This will influence usability positively (scenario 2). Decreased complexity can originate from the same factors discussed

in scenario 1, *i.e.* a new version can also increase task adequacy, increase flexibility or increase customization, positively influencing usability. A new version can also increase expectation conformity, if the users did not adjust well to the old version.

In scenario 3, like in scenario 1, complexity increases in the beginning. Possible reasons for this are already discussed in scenario 1. However, in scenario 3, complexity decreases after a while. Now, while it would be possible that this happens due to the reasoning in scenario 2, there are also interventions by the CSP possible. It might, after an update, realize that the complexity is increased, *e.g.* due to feedback from the users. Instead of releasing another version of the software and influencing complexity as discussed in scenario 2, the CSP can also increase user and technical support. For example, the CSP could offer online courses, increasing learnability (directly influencing usability) and reducing user frustration. While the complexity of the service might still be higher than originally, the usability does not decrease thanks to increased support measures from the CSP.

A decrease in complexity and increase in usability does not introduce risks to the different stakeholders. It is beneficial for both of them. However, a decrease in usability can have negative consequences for the provider and the consumer. For a CSC it includes more frustrated employees, and that it takes more time to finish the same tasks as before. For the CSP, the main risk is the dissatisfaction of the CSCs and the consequential potential loss of consumers.

7.4 Changes in Trends of Cost on QoS

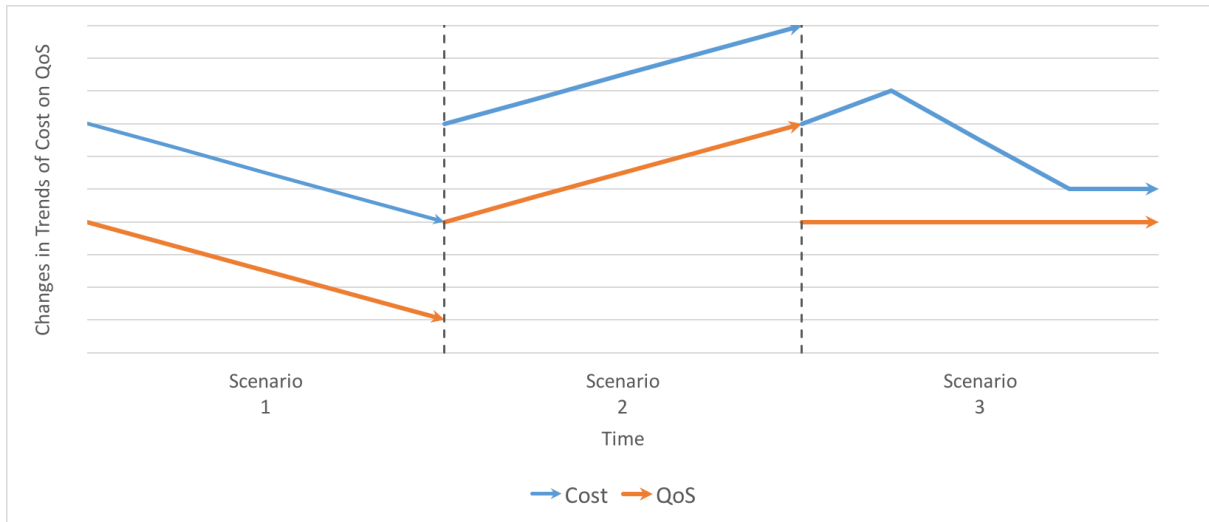


Figure 7.5: Changes in Trends of Cost on QoS

The QoS is of special interest to the CSC, as it can be influenced via the costs and is related to software assurance and usability. From an organizational perspective, the question arises as to how high the QoS has to be, to not affect the organization negatively.

In scenario 1, costs are reduced by decreasing costs for performance (see Section 6.14) via adjusted contracts and SLAs. This decreases the QoS a CSC can expect from a CSP, and the right point where cost and QoS balance must be found.

In scenario 2, the costs for performance are increased. Thereby, the expected QoS is also increased. Better QoS can result in higher availability, better service response time and other factors related to software assurance and usability.

Scenario 3 displays a scenario with a very competitive environment for the CSPs. In such an environment, it be possible, that cost can be lowered without affecting QoS, by switching to a different CSP or negotiating the existing SLA. This requires some initial investment, therefore the short increase in cost, but costs are then lowered, without affecting QoS.

CSCs have to find the right balance between cost and QoS. Whether they should increase or decrease costs is dependent on the organization, the service used and the importance of that service. Organizations spending more than required for performance, will decrease their marginal profit and they will be less profitable. However, not spending enough, and the subsequent negative impact on QoS can also influence the organization negatively.

7.5 Changes in Trends of Network Quality on Availability

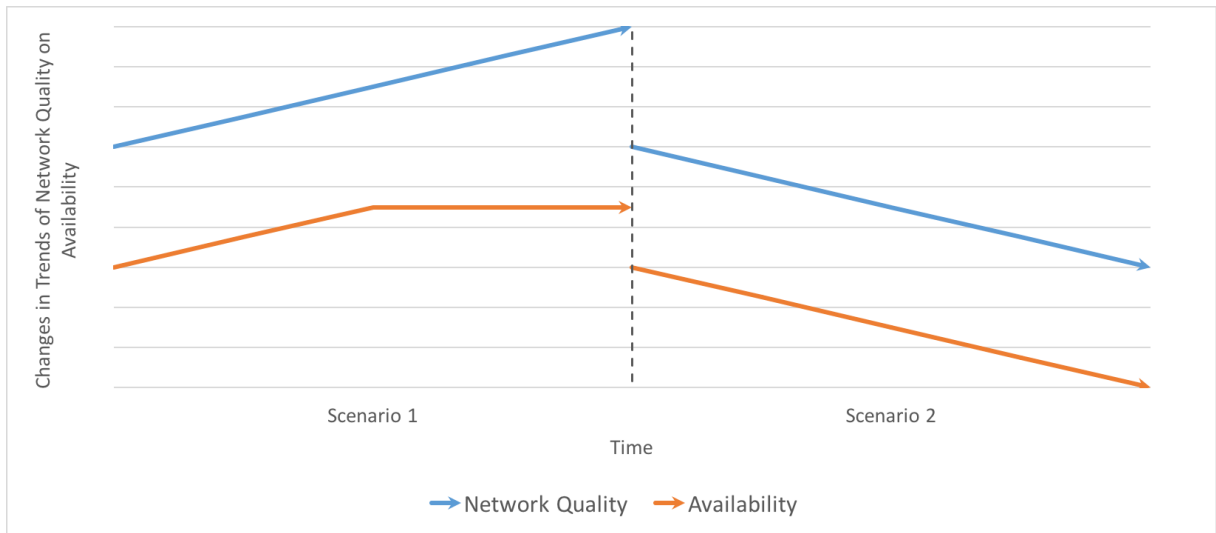


Figure 7.6: Changes in Trends of Network Quality on Availability

Availability, *i.e.* the time a service is reachable and usable for the CSC, is crucial for successful CC. To prevent the risks of low availability, discussed in Section 4.1.3, the CSC must consider the influence of changes in network quality on availability. Network quality might not always be easy to change from an CSC's perspective.

Scenario 1 represents a scenario where network quality increases. With increased network quality, any availability issues due to network quality will decrease. However, since availability is not only influenced by network quality (see Section 6.1), an increase in network quality will not result in a perfect availability. This means, that even if accessibility increases to 100%, availability will not.

In scenario 2, the network quality falls. This decrease in network quality can be due to decreased connectivity, which directly reduces the availability of the service. The worse the connectivity is, the lower the availability of the service. Unlike in the positive scenario, any further decrease in connectivity influences availability. Therefore, if accessibility drops to 0%, so will the availability.

Network quality has to be a major concern of any organization considering CC, as availability is essential. The risks of low availability have already been discussed in Section 4.1.3. As network quality can depend on the location of an organization, it must be considered in advance. Organizations which are aware of connectivity issues might want to consider not adopting CC for crucial parts of their business or using a private cloud solution, hosted in-house. If different ISPs are available to the CSC, they can consider using two alternative CSPs to reduce the risk of changes in network quality.

7.6 Changes in Trends of Organizational Compatibility on Migration Time

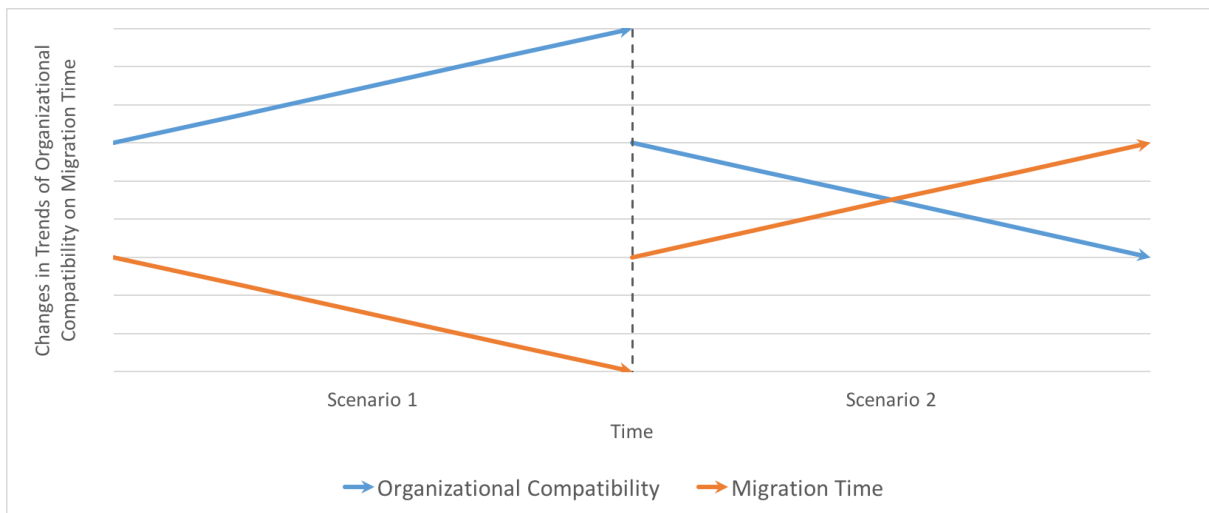


Figure 7.7: Changes in Trends of Organizational Compatibility on Migration Time

The initial migration to the cloud introduces several implications for an organization. A longer migration time does not only result in higher costs, but also introduces the risk of inconsistencies in data that have to be considered. One factor influencing the migration time is organizational compatibility.

7.6. CHANGES IN TRENDS OF ORGANIZATIONAL COMPATIBILITY ON MIGRATION TIME

In scenario 1, the organizational compatibility increases. This increase in organizational compatibility decreases the required migration time. The migration time is reduced, as less resistance can be expected from the employees. Furthermore, higher organizational compatibility leads to less required process redesign, further decreasing the required migration time. Organizational compatibility is influenced by several other factors (explored in Section 6.10). Increasing the organizational compatibility can be achieved by increasing the IT competence of employees, as it allows them to faster adapt to the changed technology. This is a factor that can be increased before migrating. Several measures can be used to increase the IT competence of employees. It can be achieved by offering courses and coaching. If an organization decides to adopt a SaaS, employees who will have to work with it, can be trained in advance. Another option would be to increase the general IT competence in the teams, by employing IT-affine people or train certain employees, which can then help others.

Other options that can lead to an increase in organizational compatibility include an increase in openness, decrease in rigidity of IT infrastructure and management, and management competence. Changing the openness of a organization can take a long time, as changing culture can take a long time. To increase openness, the source for the non-openness has to be found. It is possible, that certain employees or management have a negative impact on openness. Replacing these employees with employees that are more open, or train them, can increase openness. For the rigidity of IT infrastructure and management, and the competence of IT management, replacing certain management members or train them is also the key to increase organizational compatibility.

The final factor to be considered for increasing organizational compatibility is business flexibility and agility. From the perspective of adopting cloud-based service, this factor is difficult to influence. It is influenced by the size of an organization. Unless in a crisis or transformation phase, it is questionable that organizations want to shrink to increase organizational compatibility. Except for ethical reasons, size increases the probability to increase from economies of scale. Business flexibility and agility can also be due to the legislation. Organizations in sectors with high legislation will be less flexible, as they have to make sure changes do not conflict with legal and regulative compliance. The best chance to increase business flexibility and agility is , again, by decreasing the rigidity of the IT infrastructure and management.

Considering scenario 2, the organizational compatibility decreases. This will lead to a higher migration time, as more resistance is expected. Organizations want to prevent decreases in organizational compatibility if they consider adopting cloud-based services. However, not all possible reasons for this decrease are under their control. As discussed in scenario 1, a decrease in organizational compatibility can be caused by legislation via business flexibility and agility. An increase in legislative considerations will decrease agility and flexibility, but is outside of the control of an organization. It is also possible, that the openness of an organizations falls, without being realized.

A decreased migration time does not introduce risks to the stakeholders. It is beneficial, especially for the CSC, as it will cost less and as there are less concerns regarding data consistency. An increased migration time is problematic for the CSC, but not the other stakeholders. For the CSP it might even be beneficial, as the CSC will require more user

and technical support, for which the CSP can charge. This increase in required technical support can be a measure by the CSC to decrease migration time (see Section 6.11). The risks for the CSC have already been discussed. They primarily include higher costs, due to need to pay for the cloud service and the existing solution. Data consistency also has to be considered.

7.7 Changes in Trends of Scalability on Business Flexibility

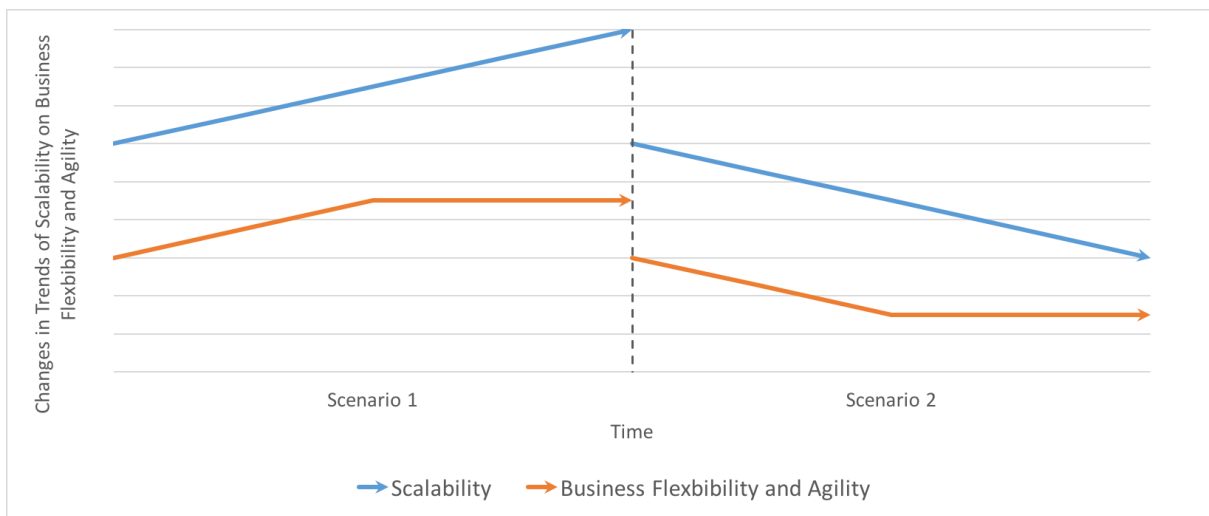


Figure 7.8: Changes in Trends of Scalability on Business Flexibility

As explored in Section 4.1.22, scalability is a great advantage of CC. As organizations can benefit from scalability by adopting (public) cloud-based computing, the effects on business flexibility and agility are of interest.

In scenario 1, scalability increases. This can be due to the actual adoption of cloud-based computing or switching to a deployment model which offers better scalability (*e.g.* from a private cloud to a federated cloud). While increased scalability will positively influence business flexibility and agility, endless scalability will not result in endless flexibility and agility. Business flexibility and agility will increase at first, as scalability allows organizations to quicker respond to changes in demand and the market. Increased scalability will only increase business flexibility and agility as long as they can use it to match the changes in the market. As the market will not be endlessly flexible, business flexibility and agility will not improve with scalability after a certain point. Furthermore, business flexibility and agility is also influenced by other factors than scalability, as discussed Section 6.3. If scalability is not the limiting factor, an increase in it will not further improve business flexibility and agility.

Scenario 2 shows a decrease in scalability. This decrease in scalability can be caused by moving from a public cloud to a private cloud, where resources are not “endless” any more.

7.8. CHANGES IN TRENDS OF SECURITY CONFIGURATION AND MAINTENANCE ON LEG

An organization might consider such a step for better control or for legislative reasons. As explored in scenario 1, business flexibility does not only depend on scalability. Therefore, a decrease in scalability will not completely end business flexibility and agility.

A increase in trends of scalability and its effects on business flexibility and agility introduces several chances for the CSC. It allows them to react faster to changes in the market and demand. A decrease in scalability and therefore flexibility and agility is especially problematic in a competitive environment. Not being able to quickly adjust to changes, while competitors can, will lead to customer loss, as the competitors will offer better service. Scalability also introduces risks for the CSP. Since scalability is one of the benefits of CC, it is requested by many customers. The CSPs need to make sure that they can handle the different scalability requests, while still considering the workload utilization ratio. A possibility for them to do this, is joining a cloud federation.

7.8 Changes in Trends of Security Configuration and Maintenance on Legal and Regulative Compliance

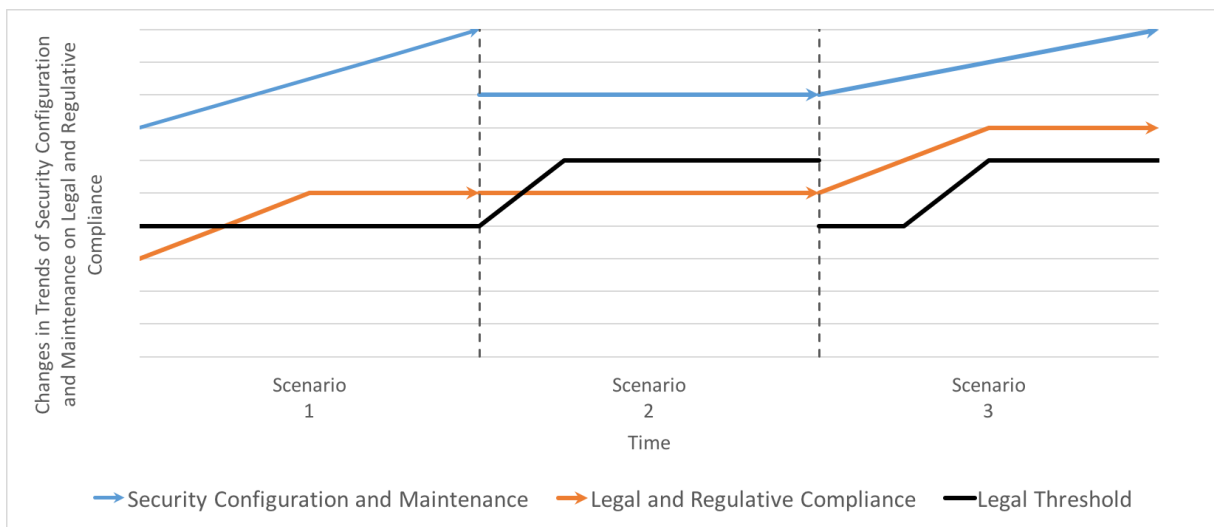


Figure 7.9: Changes in Trends of Security Configuration and Maintenance on Legal and Regulative Compliance

Data controllers need to make sure that personal data is protected by reasonable security, discussed in Section 5.1.1. Organizations considering CC service models different to SaaS and having personal data in the cloud, must therefore consider the effects of security configuration and maintenance on legal and regulative compliance. If a CSP offers a SaaS, the CSP is the data controller, and must therefore make sure to comply with the legislation and regulation.

Scenario 1 is a positive case. The available security configuration and maintenance was not sufficient to comply with the legislation and regulation regarding safety of data. However,

thanks to an increase in the security configuration, compliance is met. This can be caused by an update of the service by the CSP, or the CSC might switch to another CSP to ensure compliance.

Compliance with legislation and regulation must not only be considered when migrating towards the cloud. It must also be carefully monitored by the different stakeholders. As seen in Section 5.1.3, legislation can change. For example, the new EU GDPR will introduce changes, where any organization targeting EU citizen must comply with the new legislation. This can lead to a situation as shown in scenario 2, where even though there is no change in security of the service, legal and regulative compliance falls below the threshold, as this threshold is increased by the regulators. Any controller must therefore make sure, that if the legislation or regulation changes, the service does still comply with it (scenario 3).

Being below the legal threshold, the data controller risks to be sued by customers and to face legal consequences. For a CSP acting as data processor, not increasing the safeguards to comply with the legal and regulative environment, can lead to CSCs turning to other CSPs. CSCs will consider switching CSPs to ensure legal and regulative compliance.

7.9 Changes in Trends of Size of Organization on Marginal Cost

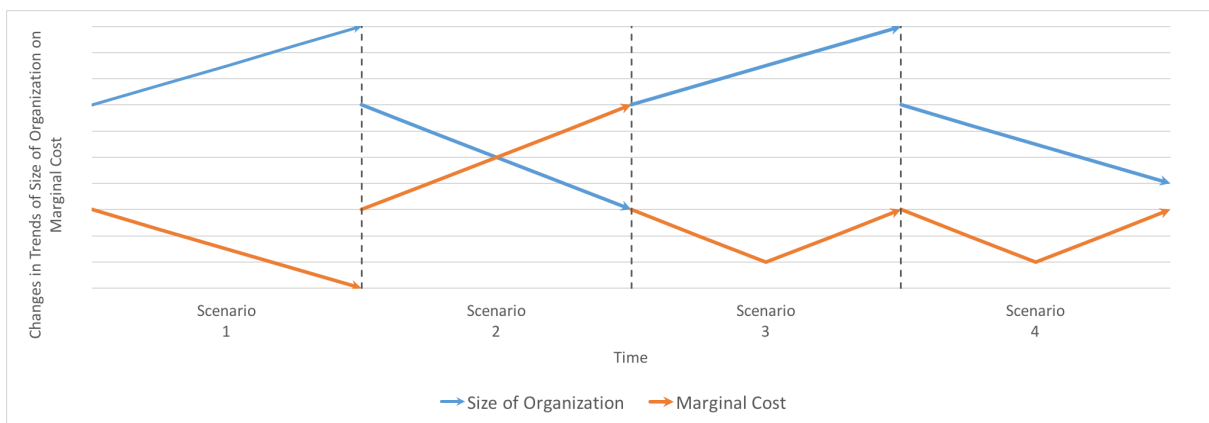


Figure 7.10: Changes in Trends of Size of Organization on Marginal Cost

Marginal cost and profit are of interest to organizations, as it allows them to offer better prices to their customers and be more competitive. Both factors were discussed simultaneously in Section 4.2.7. For the visualization, the marginal cost is considered. Assuming that a CSC uses the cloud to offer services to its customers and keeping the price constant, decreasing marginal cost will lead to increasing marginal profit.

The size of an organization influences economies of scale. Therefore, as shown in scenario 1, an increase of the size of an organization can lead to lower marginal costs. Similarly, in

scenario 2, decreasing the size of an organization can impact economies of scale negatively, increasing the cost per unit.

An increase in the size of an organization does not always lead to lower marginal cost. Considering scenario 3, an increase of size of an organization can first decrease marginal cost due to economies of scale. Further increasing the size of the organization can, however, lead to a situation where marginal cost start to increase with further growth of organization, due to the size of an organization. This is caused by diseconomies of scale, where complexity and processes in an organizations increase. Using a community or private cloud, increasing size beyond a certain point can require investments into the IT infrastructure and thereby increase marginal cost. Scenario 4 shows the opposite of scenario 3. Decreasing the size of the organization will decrease the marginal cost due to diseconomies of scale. However, after a certain point, marginal cost will increase again, as the size is not optimal any longer.

The size of an organization and marginal cost can be applied to both the CSP and CSC. Both benefit from the size of their organization, as long as they do not slip into diseconomies of scale. The risk of not being able to use economies of scale and reducing marginal cost is in the competitive power of an organizations. If competitors of an organization can benefit from lower marginal costs, they can offer the same service at a lower price. From a CSPs perspective, this leads to a situation where their service is less attractive to new customers and might also cause existing CSCs to switch providers, especially if the lock-in effect is low.

7.10 Changes in Trends of Software Assurance on Trust

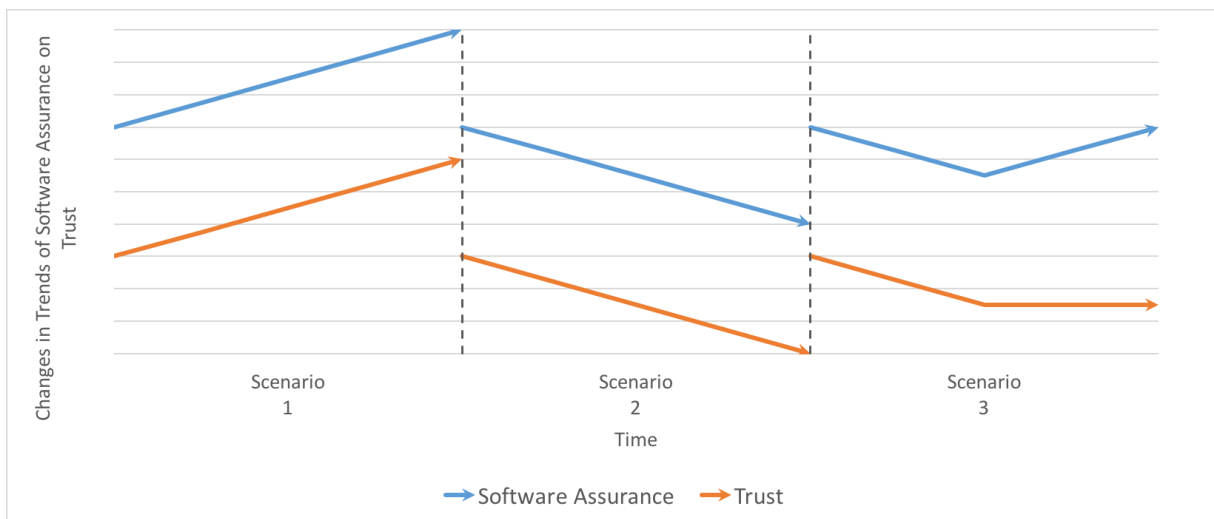


Figure 7.11: Changes in Trends of Software Assurance on Trust

Consider the consequences of changes in software insurance, defined in Section 4.1.25, on trust towards the CSP (Section 4.4.7). When there are no changes in other factors, there

will be no consequences on trust from the CSC towards the CSP.

In scenario 1, the CSP increases its software assurance, *i.e.* there are less deviations from the agreed upon SLAs. While it can take some time until the CSC notices the change, the trust towards the CSP will also increase, as the CSP delivers as promised.

Similarly, in scenario 2, the trust will fall with a decreasing software assurance, as the CSP does not deliver as promised.

Finally, in scenario 3, the software assurance first falls and then rises again. In this scenario, the trust first falls as in scenario 2. The question remains on how trust behaves when the level of software assurance rises again. When the deviation was only minor, relation between the CSP and consumer might not have been damaged badly and the trust rises again. However, if software assurance drops regularly or below an uncomfortable level of the CSC, the relationship can be damaged permanently. This effect is increased if there is no “honest concern” from the CSP, and the CSC feels not being taken seriously. The deviations from the agreed upon service will therefore influence cognitive trust, and the lack of honest communication the affective trust. Winning back the trust of the CSC can take a long time, and the CSC might switch providers, even after software assurance is increased again.

Causes for declining software assurance can be found in all factors defined in the SLAs. Therefore, it can for example be caused by deviations in availability or response time.

An increase in software assurance, and therefore in trust, does not introduce any severe risks for the involved stakeholders. It could be argued, that over-delivering does harm the CSP, as CSC are less likely to pay more for services with higher guaranteed quality.

A decrease of software assurance and trust has several implications. From a legal perspective, the deviation from SLAs can have the consequence, that the CSP might owe remedies to the CSC (see Section 5.3). If the trust is damaged badly, the CSC might look into alternatives, terminating the contract with the CSP.

From the perspective of a CSC, negative deviations in software assurance and the loss of trust towards the CSP, is also related to the QoS and therefore also the usability of a service. Depending on what the service is used for, this can be less problematic or have severe influences for the CSC. A slight negative deviation on the response time of a non-time critical application might not have any consequences at all, it might not even be noticed by the CSC. However, if a business critical application is not available for a longer period of time or not regularly, the CSC's business can be endangered. The loss of trust towards the CSP will motivate the CSC to find an alternative CSP.

7.11 Changes in Trends of Standards on Vendor Lock-In

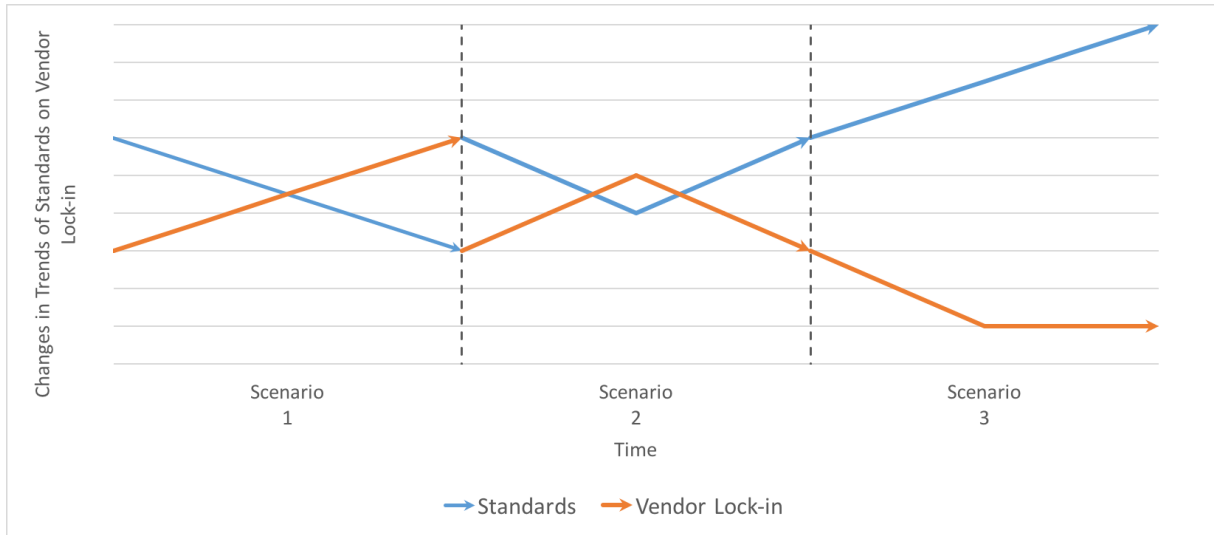


Figure 7.12: Consequences of Standards on Vendor Lock-In

Standards (Section 4.1.26), or the lack thereof, directly influences many technical factors and the costs for switching providers (see Section 4.2.5). Many of these factors increase the lock-in effect (Section 4.1.31). Furthermore, the lack of standards and the consequential vendor-lock in might lead to situation in which competition laws (Section 5.2) will target CC. This will be explored in scenario 2.

Consider the effect of standards on vendor-lock in. If the level of standardization decreases (scenario 1), the interoperability and portability will decrease. This leads to a situation, where costs for switching providers increase, and it is more difficult and expensive for CSCs to switch to a different provider. Due to this lock-in, CSPs have increased power and can change their prices, without risking to lose many customers. Scenario 1 considers the case, where there is no interference by the legislator. As explained in Section 5.2, competition laws only apply if there is a provider in a dominant market situation. As long as there are enough providers, it is unlikely that regulators will interfere with the market, even though vendor lock-in is very high. The market fails to regulate itself. CSPs do compete over customers, but focus on existing ones.

In scenario 2, like in scenario 1, standardization is also reduced. Interoperability and portability decreases, costs for switching providers and vendor lock-in increase. Unlike scenario 1, this decrease is only temporary. After a while, standardization starts to increase. There are several reasons why standardization will increase again. (1) Competition is too low. There is a dominant player in the market and regulators will interfere. (2) Self-regulation within CC. Instead of risking interference by regulators, CSPs decide that they are better off regulating themselves. Therefore, developing an interest in standardization. (3) Competition. Even though the CC-market is growing, the number of consumers is limited. In the long term, existing CSPs looking to expand will have to target customers

of different CSPs. (4) Partnerships to optimize workload utilization ratio. CSPs are interested in optimizing their workload. Instead of isolating themselves from the competition, CSPs can benefit from partnerships to increase their workload utilization ratio by bundling resources and forming cloud federations.

In scenario 3, standardization increases without decreasing first. This can be due to reason (2), (3) and (4) discussed in scenario 2.

An increased standardization and decrease in vendor lock-in result in a more competitive market for CSPs. CSPs do not only have to worry about acquiring new customers, but also have to ensure that existing consumers do not have incentives to switch to another provider. CSCs can switch easily between different CSPs. CSPs which cannot offer competitive prices or differentiate themselves from the competition in other areas, risk loosing all the customers and being forced out of business. For CSPs it is therefore important to benefit from economies of scale, or, if they are rather small or in a limited market, differentiate or form cloud federations with other providers. The risks for CSCs is limited in such a scenario. Too tense competition might lead to a situation where its current CSP is forced out of business, but due to high portability, migration to another provider is not associated with high costs.

Increasing vendor lock-in might seem interesting to CSPs. It makes it difficult for existing customers to migrate to another CSP and they can charge higher prices. For CSCs this introduces the risk of a high dependence on a specific CSP. Migrating to another CSP or going back to a traditional architecture is connected with high costs, *e.g.* there is no data portability. However, there are also risks for CSPs with a decrease in standardization. As discussed in scenario 2, regulators might interfere with the market. Autonomy is lost and the market (over-)regulated. Self-regulation and partnerships can be more beneficial to CSPs than a very high lock-in effect.

7.12 Changes in Trends of Traceability and Auditability on Legal and Regulative Compliance

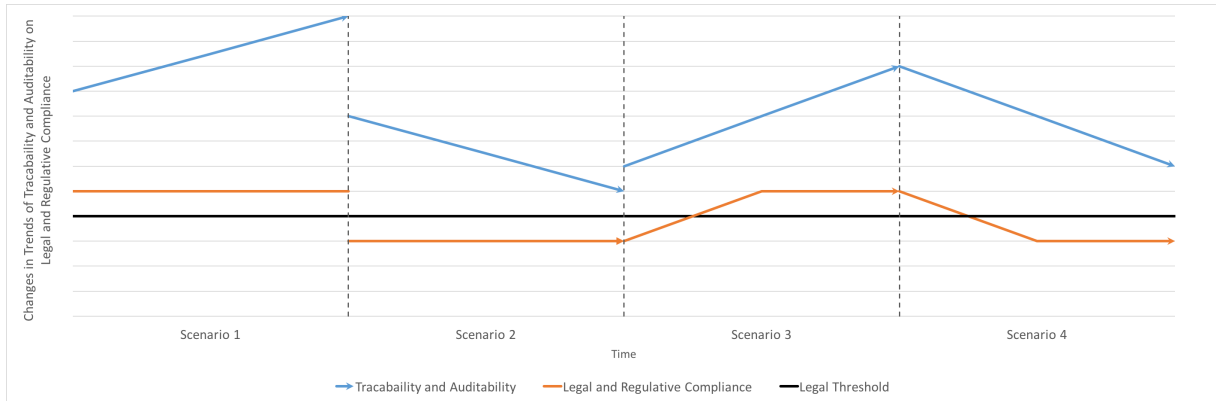


Figure 7.13: Changes in Trends of Traceability and Auditability on Legal and Regulative Compliance

Depending on the legislation, CSCs must be able to show what personal data is stored, for what purpose and what has happened with the data. To ensure this, the traceability (Section 4.1.29) and auditability and the effects on legal and regulative compliance (Section 4.3.6) have to be considered. Legal compliance will be considered as a binary factor in this graph, *i.e.* either it is sufficient or it is not.

Scenario 1 represents a situation where the traceability and auditability offered in the cloud-based service is sufficient to comply with the legislation. A further increase in traceability and auditability will not change compliance. Similarly, in scenario 2, if the offered traceability and auditability are not sufficient in the beginning, a decrease will not affect compliance.

In scenario 3, the available traceability and auditability does not comply with the legal and regulative constraints. An increase of auditability and traceability allows to meet the legal requirements. As compliance is a binary condition, further traceability and auditability increases will not have any effect on the legal compliance. As long as no data is collected or used in any unlawful way, this scenario only benefits the different stakeholders.

Scenario 4 is more problematic. The existing traceability and auditability functions were sufficient to comply with legal and regulative constraints. However, due to a decrease of traceability and auditability, compliance is not met any longer. This is especially complicated for the data processor, which can be either the CSP or the CSC, depending on the service level.

Being below the legal threshold, the data controller risks to be sued by customers and to face legal consequences.

7.13 Changes in Trends of Utility Based Computing on Cost Flexibility

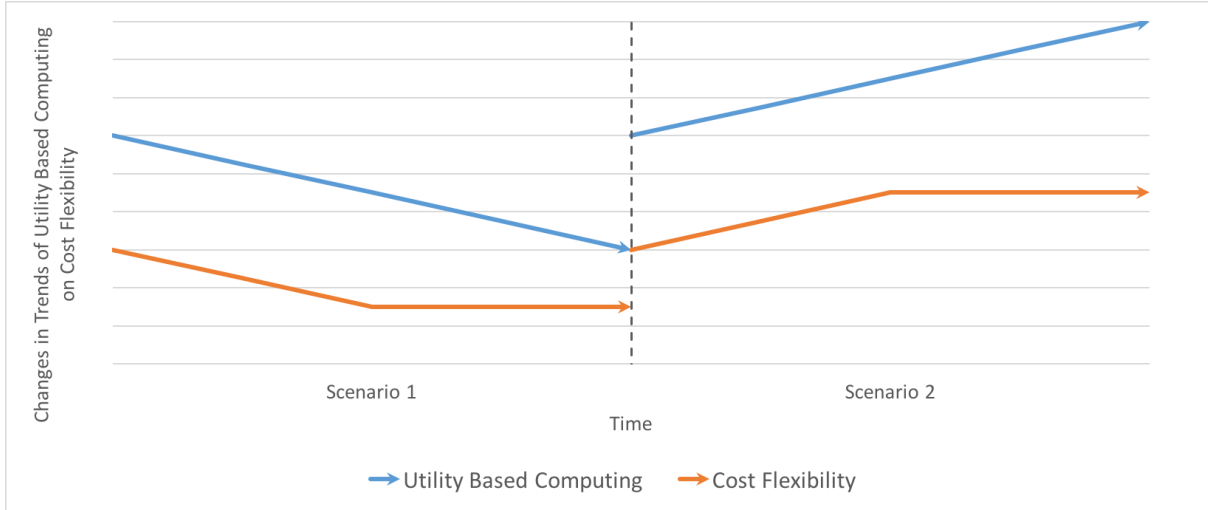


Figure 7.14: Changes in Trends of Utility Based Computing on Cost Flexibility

Utility based computing, as discussed in Section 4.1.30, is considered one of the greatest advantages of CC compared to traditional systems. It allows organizations to retrieve services with a pay-as-you-go-model. Within this section, the influences of changes in trends of utility based computing on cost flexibility are explored.

In scenario 1, cost flexibility decreases due to a decrease of utility based computing. This can be caused by switching between different CSPs or a different pricing model at the same CSP, *e.g.* from a model where billing and metering of resources is accurate and the CSC is exactly billed what it required, to a flat rate pricing model. It can also occur if the cloud deployment model is changed, *i.e.* if a CSC switches from a public or multiple cloud model to a private or community cloud, where the fixed costs are higher. This decreases the cost flexibility. The CSC will have more fixed costs and less variable costs. However, since not all costs of a CSC will be associated with the cloud service used (also see Section 6.7), the cost flexibility will not decrease endlessly. After a certain point, it will stay stable, even if utility based computing decreases further.

In scenario 2, utility based computing increases. This can be due to cloud adoption, switching CSPs, a change in the pricing model of the CSP, or by migrating to a different cloud deployment model (*e.g.* from private to hybrid). This increases the cost flexibility of a CSC. But, as explored in scenario 1, cost flexibility is not only influenced by utility based computing. Therefore, an increase in utility based computing does not endlessly increase cost flexibility.

Scenario 2 is beneficial for the CSC. The increased cost flexibility allows the CSC to incur lower costs when demand is low. For the CSP, utility based computing introduces the risk of unknown revenue. To operate successfully, CSPs must make sure to have enough costumers, so that the change of demand in one does not lead to a bad workload

utilization ratio. In scenario 1, the CSC has less cost flexibility. This introduces several risks the CSC. First of all, costs cannot be decreased as flexible as before in case of lower demand. For a CSC offering its services to consumers, this can lead to a situation, where the CSC has either to charge more or loses money in times of low demand. Having to increase costs for its customers to cover for this non-flexibility in cost will decrease the competitiveness of an organization.

Chapter 8

Summary, Conclusion and Future Work

As defined in the introduction of this thesis, the goal was to increase the global view and understand the effects of legal and regulative constraints on CC and its federated environment. This was achieved by developing an XML taxonomy for factors affecting CC and the in-depth discussion of these factors, including the risks and liabilities for the different stakeholders.

Then, the legal and regulative constraints were considered. Laws and regulations from the EU and US were explored, and laws from the domains of privacy, anti-trust, contractual and sector specific regulations identified and discussed. The key differences between the currently applicable EU DPD and upcoming EU GPDR were explored. Issues arising from the cloud-based computing business model within the legal domains were discussed. This included issues with outsourcing, cross border data flows, applicable legislation and problems with subcontracting. The increased complexity in cloud federation scenarios was considered regarding roles and responsibilities of the stakeholders and applicable jurisdiction.

Finally, interrelations arising within factors and regulative constraints were identified, visualized and discussed. These interrelations were then further analyzed using time-based graphs. These showed the effects of changes in trends of factors on other factors, and the risks of such influences for the different stakeholders were considered.

8.1 Conclusion

CC is a complex domain. Not only factors from different fields have to be considered, but also legislation. It shows that the legal and regulative constraints can be very case specific. Not only can the responsibilities for a specific stakeholder vary in different scenarios, but also the applicable jurisdiction can differ. Each scenario has to be carefully evaluated individually. The modeled and discussed factors in this thesis must be considered to

understand the effects of CC on an organization. The awareness of interrelations and consequences of changes in factors further improve the global perspective on CC.

This leads to the conclusion that CC adoption requires in-depth expertise. Especially organizations considering the adoption of public or multi clouds must ensure to acquire enough knowledge, either internally or externally, to fully understand the consequences of CC. They must not only consider the consequences and risks on their organization, but also understand the legal and regulative environment, the special implications in cloud federations and the importance of the SLAs. Developments in standardization and legislation must be observed attentively, so that changes can be implemented pro-actively.

8.2 Future Work

This thesis aimed at the broad picture of CC and the relevant legislation. To further improve the understanding of CC, especially the understanding of legal and regulative influences, work in the following areas can be considered:

The Final Influence of EU GDPR

As discussed in Section 5.1.3, the EU GDPR (which is in draft stage as of time of writing), will unify and introduce changes in the regulative environment of CC. The final influence is yet to be seen. Further research is required on the final version and the consequences.

Consideration of other Jurisdictions

The work on legal and regulative constraints in this thesis focuses on the EU and the US. The scope of research can be extended to other legislations.

In-depth Analysis of Sector Specific Regulations

As discussed in Section 5.4.3, several specific sectors (*e.g.* healthcare, financial services) have unique regulations. These can additionally vary from country to country. An in-depth analysis of these sectors opens another field for further research.

Case Studies and Case Law

Research of precedents can further improve the understanding of the legal interpretation of applicable legislation. Not only verdicts are of interest, but also the interpretations of cloud deployment and service scenarios, and how the applicable jurisdiction is chosen.

Bibliography

- [1] S. Aggarwal and L. McCabe. The Compelling TCO Case for Cloud Computing in SMB and Mid-Market Enterprises. Whitepaper, Hurwitz and Associates, 2009.
- [2] N. Ahmed. Measuring the Cybersecurity of Cloud Computing: A Stakeholder Centered Economic Approach. In *Proceeding of International Conference on Computing, Electrical and Electronics Engineering (ICCEEE), Khartoum, Sudan*, pages 294–299, August 2013.
- [3] A. Aljabre. Cloud Computing for Increased Business Value. *International Journal of Business and Social Science*, 3(1):234–239, 2012.
- [4] M. A. AlSudiari and T. Vasista. Cloud Computing and Privacy Regulations: An Exploratory Study on Issues and Implications. *Advanced Computing: An International Journal (ACIJ)*, 3(2):159–169, 2012.
- [5] D. Ardagna, G. Casale, M. Ciavotta, J. Pérez, and W. Wang. Quality-of-Service in Cloud Computing: Modeling Techniques and their Applications. *Journal of Internet Services and Applications*, 5(1), 2014.
- [6] M. Armbrust, F. Armando, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the Clouds: A Berkeley View of Cloud Computing. Technical report, Electrical Engineering and Computer Sciences University of California at Berkeley, February 2009.
- [7] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A View of Cloud Computing. *Communication of the ACM*, 53(4):50–58, 2010.
- [8] A. Bala and I. Chana. Fault Tolerance-Challenges, Techniques and Implementation in Cloud Computing. *IJCSI International Journal of Computer Science Issues*, 9(1):1694–0814, 2012.
- [9] M. Bedner. *Cloud Computing: Technik, Sicherheit und Rechtliche Gestaltung*. Forum Wirtschaftsrecht. Kassel University Press, 2013.
- [10] D. Bernstein. IEEE Intercloud Effort - Intercloud Testbed. Presentation at Cloud Expo Europe, February 2014.

- [11] H. P. Borgman, B. Bahli, H. Heier, and F. Schewski. Cloudrise: Exploring Cloud Computing Adoption and Governance with the TOE Framework. In *Proceeding of 46th Hawaii International Conference on System Sciences (HICSS)*, Maui, USA, pages 4425–4435, January 2013.
- [12] G. Buttarelli. Security and Privacy Regulatory Challenges in the Cloud. In *Proceeding of 2012 European Cloud Computing Conference, Brussels, Belgium*, March 2012.
- [13] H. Chang. Data Protection Regulation and Cloud Computing. In A. S. Cheung and R. H. Weber, editors, *Privacy and Legal Issues in Cloud Computing*, pages 26–42. Edward Elgar Publishing, 2015.
- [14] Committee on National Security Systems. National Information Assurance (IA) Glossary - CNSS-4009. CNSS Instruction No. 4009, April 2010.
- [15] E. Elmroth, F. Marquez, D. Henriksson, and D. Ferrera. Accounting and Billing for Federated Cloud Infrastructures. In *Proceeding of Eighth International Conference on Grid and Cooperative Computing (GCC '09)*, Lanzhou, China, pages 268–275, August 2009.
- [16] European Parliament, Council of the European Union. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995.
- [17] European Parliament, Council of the European Union. Proposal for Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), January 2012.
- [18] J. Farrell and G. Saloner. Standardization, Compatibility, and Innovation. *The RAND Journal of Economics*, 16(1):70–83, 1985.
- [19] A. J. Ferrer, F. Hernández, J. Tordsson, E. Elmroth, A. Ali-Eldin, C. Zsigri, R. Sirvent, J. Guitart, R. M. Badia, and K. Djemame. OPTIMIS: A Holistic Approach to Cloud Service Provisioning. *Future Generation Computer Systems*, 28(1):66–77, 2012.
- [20] R. Garg and B. Stiller. Trade-Off-Based Adoption Methodology for Cloud-based Infrastructures and Services. In *Proceeding of Monitoring and Securing Virtualized Networks and Services*, pages 1–13, Brno, Czech Republic, June 2014. Springer.
- [21] R. Garg and B. Stiller. Factors Affecting Cloud Adoption and Their Interrelations. In *Proceeding of 5th International Conference on Cloud Computing and Services Science (CLOSER 2015)*, Lisbon, Portugal, pages 87–94, 2015.
- [22] S. K. Garg, S. Versteeg, and R. Buyya. A Framework for Ranking of Cloud Computing Services. *Future Generation Computer Systems*, 29(4):1012–1023, 2013.
- [23] G. Garrison, S. Kim, and R. L. Wakefield. Success Factors for Deploying Cloud Computing. *Communication of the ACM*, 55(9):62–68, 2012.

- [24] P. Géczy, N. Izumi, and K. Hasida. Cloudsourcing: Managing Cloud Adoption. *Global Journal of Business Research*, 6(2):57–70, 2012.
- [25] K. Ghaffari, M. S. Delgosha, and N. Abdolvand. Towards Cloud Computing: A SWOT Analysis on its Adoption in SMEs. *ArXiv e-prints*, 2014.
- [26] S. Haag. *Management Information Systems for the Information Age: 9th Edition*. McGraw-Hill Higher Education, 2012.
- [27] N. R. Herbst, S. Kounev, and R. Reussner. Elasticity in Cloud Computing: What It Is, and What It Is Not. In *Proceedings of 10th International Conference on Autonomic Computing (ICAC 13)*, San Jose, CA, USA, pages 23–27. USENIX, 2013.
- [28] J. N. Hoover. Compliance in the Ether: Cloud Computing, Data Security and Business Regulation. *J. Bus. & Tech. L.*, 8(1):255–273, 2013.
- [29] Y. Jadeja and K. Modi. Cloud Computing - Concepts, Architecture and Challenges. In *Proceeding of International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, Tamil Nadu, India, pages 877–880, March 2012.
- [30] B. Kandukuri, V. Paturi, and A. Rakshit. Cloud Security Issues. In *Proceeding of IEEE International Conference on Services Computing (SCC '09)*, Bangalore, India, pages 517–520, September 2009.
- [31] K. Kaur and A. K. Rai. A Comparative Analysis: Grid, Cluster and Cloud Computing. *International Journal of Advanced Research in Computer and Communication Engineering*, 3(3):5730–5734, 2014.
- [32] J. Kerr and K. Teng. Cloud Computing: Legal and Privacy Issues. In *Proceedings of 12th Annual Academy of Business Disciplines Conference*, Ft. Myers Beach, Florida, USA, 2010.
- [33] A. Kertesz and S. Varadi. Legal Aspects of Data Protection in Cloud Federations. In *Security, Privacy and Trust in Cloud Systems*, pages 433–455. Springer, 2014.
- [34] J. B. Kirkwood and R. H. Lande. The Fundamental Goal of Antitrust: Protecting Consumers, Not Increasing Efficiency. *Notre Dame Law Review*, 84(1):191–244, November 2008.
- [35] T. Kurze, M. Klems, D. Bermbach, A. Lenk, S. Tai, and M. Kunze. Cloud Federation. In *Proceeding of Second International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2011)*, Rome, Italy, pages 32–38, 2011.
- [36] C. Low, Y. Chen, and M. Wu. Understanding the Determinants of Cloud Computing Adoption. *Industrial Management & Data Systems*, 111(7):1006–1023, 2011.
- [37] D. Marinescu. *Cloud Computing: Theory and Practice*. Elsevier Science, 2013.
- [38] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi. Cloud Computing - The Business Perspective. *Decision Support Systems*, 51(1):176–189, 2011.

- [39] B. T. McGeogh and B. Donnellan. Factors That Affect The Adoption Of Cloud Computing For An Enterprise: A Case Study Of Cloud Adoption Within Intel Corporation. In *Proceeding of 21st European Conference on Information Systems, ECIS 2013, Utrecht, The Netherlands*, pages 37–49, June 2013.
- [40] M. Meinshausen, N. Meinshausen, W. Hare, S. C. Raper, K. Frieler, R. Knutti, D. J. Frame, and M. R. Allen. Greenhouse-Gas Emission Targets for Limiting Global Warming to 2 C. *Nature*, 458(7242):1158–1162, 2009.
- [41] P. M. Mell and T. Grance. The NIST Definition of Cloud Computing, Special Publication 800/145. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, USA, 2011.
- [42] S. C. Misra and A. Mondal. Identification of a Company’s Suitability for the Adoption of Cloud Computing and Modelling its corresponding Return on Investment. *Mathematical and Computer Modelling*, 53(3):504–521, 2011.
- [43] J.-P. Moiny. Cloud and Jurisdiction: Mind the Borders. In A. S. Cheung and R. H. Weber, editors, *Privacy And Legal Issues In Cloud Computing*, pages 118–138. Edward Elgar, 2015.
- [44] L. Morgan and K. Conboy. Factors Affecting the Adoption of Cloud Computing: An Exploratory Study. In *Proceeding of 21st European Conference on Information Systems (ECIS 2013)*, Utrecht, The Netherlands, pages 124–136, June 2013.
- [45] A. Narayan, S. Rao, G. Ranjan, and K. Dheenadayalan. Smart Metering of Cloud Services. In *Proceeding of 2012 IEEE International Systems Conference (SysCon)*, Vancouver, BC, Canada, pages 1–7, March 2012.
- [46] J. Nielsen. *Usability Engineering*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1994.
- [47] M. Z. Nkhoma, D. P. Dang, and A. De Souza-Daw. Contributing Factors of Cloud Computing Adoption: A Technology-Organisation-Environment Framework Approach. *International Journal of Information Systems and Engineering (IJISE)*, 1(1):38–49, April 2013.
- [48] M. A. Obeidat and T. Turgay. Empirical Analysis for the Factors Affecting the Adoption of Cloud Computing Initiatives by Information Technology Executives. *Journal of Management Research*, 5(1):152–178, 2012.
- [49] Organisation for Economic Co-operation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. OECD Publishing, 2002.
- [50] H. Panetto and A. Molina. Enterprise Integration and Interoperability in Manufacturing Systems: Trends and Issues. *Computers in Industry*, 59(7):641 – 646, 2008.
- [51] W. Pauley. Cloud Provider Transparency: An Empirical Evaluation. *Security Privacy, IEEE*, 8(6):32–39, November 2010.

- [52] D. Petcu. Portability and Interoperability Between Clouds: Challenges and Case Study. In P. Maehoenen, K. Pohl, and T. Priol, editors, *Towards a Service-Based Internet*, pages 62–74. Springer, 2011.
- [53] D. Petcu. Multi-Cloud: Expectations and Current Approaches. In *Proceedings of 2013 International Workshop on Multi-cloud Applications and Federated Clouds (MultiCloud '13)*, New York, NY, USA, pages 1–6. ACM, 2013.
- [54] E. M. Rogers. *Diffusion of Innovations*. Simon and Schuster, New York, USA, 5th edition, 2003.
- [55] P. Saripalli and G. Pingali. MADMAC: Multiple Attribute Decision Methodology for Adoption of Clouds. In *Proceeding of 2011 IEEE International Conference on Cloud Computing (CLOUD)*, Washington, DC, USA, pages 316–323, July 2011.
- [56] J. Siegel and J. Perdue. Cloud Services Measures for Global Use: The Service Measurement Index (SMI). In *Proceeding of 2012 Annual SRII Global Conference (SRII)*, Washington, DC, USA, pages 411–415, July 2012.
- [57] J. P. Sluijs, P. Larouche, and W. Sauter. Cloud Computing in the EU Policy Sphere. *Journal of Intellectual Property, Information Technology and e-Commerce Law*, 3(1):12–32, 2011.
- [58] D. N. Staiger. Cross-Border Data Flow in the Cloud between the EU and the US. In A. S. Cheung and R. H. Weber, editors, *Privacy and Legal Issues in Cloud Computing*, pages 96–117. Edward Elgar, 2015.
- [59] M. Stieninger, D. Nedbal, W. Wetzlinger, G. Wagner, and M. A. Erskine. Impacts on the Organizational Adoption of Cloud Computing: A Reconceptualization of Influencing Factors. *Procedia Technology*, 16(1):85–93, 2014.
- [60] Symantec.cloud. Wheatering the Storm: Considerations for Organizations Wanting to Move Services to the Cloud. Technical report, SymantecCloud, 2011.
- [61] H. Takabi, J. B. Joshi, and G.-J. Ahn. Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security & Privacy*, (6):24–31, 2010.
- [62] G. Y. Tian. Cloud Computing and Copyright. In A. S. Cheung and R. H. Weber, editors, *Privacy and Legal Issues in Cloud Computing*, pages 160–179. Edward Elgar, 2015.
- [63] A. N. Toosi, R. N. Calheiros, and R. Buyya. Interconnected Cloud Computing Environments: Challenges, Taxonomy, and Survey. *ACM Computing Surveys (CSUR)*, 47(1):7, 2014.
- [64] UN General Assembly. Universal Declaration Of Human Rights. *UN General Assembly*, 1948.
- [65] D. Villegas, N. Bobroff, I. Roderio, J. Delgado, Y. Liu, A. Devarakonda, L. Fong, S. M. Sadjadi, and M. Parashar. Cloud Federation in a Layered Service Model. *Journal of Computer and System Sciences*, 78(5):1330–1344, 2012.

- [66] R. H. Weber. Legal Safeguards for Cloud Computing. In A. S. Cheung and R. H. Weber, editors, *Privacy and Legal Issues in Cloud Computing*, pages 43–68. Edward Elgar, 2015.
- [67] C. Weinhardt, A. Anandasivam, B. Blau, N. Borissov, T. Meinl, W. Michalk, and J. Stoesser. Cloud Computing - A Classification, Business Models, and Research Directions. *Business & Information Systems Engineering*, 1(5):391–399, 2009.
- [68] T. Wood, E. Cecchet, K. Ramakrishnan, P. Shenoy, J. Van Der Merwe, and A. Venkataramani. Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Challenges. In *Proceeding of 2nd USENIX Workshop on Hot Topics in Cloud Computing, Boston, MA, USA*, pages 1–7, 2010.
- [69] X. Xu. From Cloud Computing to Cloud Manufacturing. *Robotics and Computer-Integrated Manufacturing*, 28(1):75 – 86, 2012.
- [70] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou. Security and Privacy in Cloud Computing: A Survey. In *Proceeding of Sixth International Conference on Semantics Knowledge and Grid (SKG), Beijing, China*, pages 105–112, November 2010.
- [71] D. Zissis and D. Lekkas. Addressing Cloud Computing Security Issues. *Future Generation computer systems*, 28(3):583–592, 2012.

Abbreviations

ALM	Application Lifecycle Management
API	Application Programming Interface
BCR	Binding Corporate Rules
CaaS	Communication as a Service
CAPEX	Capital Expenditures
CC	Cloud Computing
CPU	Central Processing Unit
CSB	Cloud Service Broker
CSC	Cloud Service Consumer
CSMIC	Cloud Service Measurement Initiative Consortium
CSP	Cloud Service Provider
DaaS	Desktop as a Service
DBaaS	Databases as a Service
DB	Database
DC	Data Controller
DoI	Diffusion of Innovation
DP	Data Processor
DSS	Decision Support System
E	Establishment
e.g.	for example (<i>exempli gratia</i>)
EU	European Union
EU DPD	EU Data Protection Directive
EU GDPR	EU General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
HDD	Hard Disk Drive
HHI	Herfindahl-Hirschman Index
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
i.e.	that is (<i>id est</i>)
IaaS	Infrastructure as a Service
IM	Instant Messaging
IP	Internet Protocol
IP	Infrastructure Provider
ISO	International Standards Organizations
ISP	Internet Service Provider
IT	Information Technology

J	Jurisdiction
MaaS	Monitoring as a Service
MADMAC	Multiple Attribute Decision Methodology for Adoption of Cloud
MTBF	Mean Time Between Failures
NIST	National Institute of Standards and Technology
OCC	Open Cloud Consortium
OGF	Open Grid Forum
OECD	Organization for Economic Co-operation and Development
OPEX	Operating Expenditures
OS	Operating System
PaaS	Platform as a Service
QoS	Quality of Service
ROI	Return on Investment
SaaS	Software as a Service
SECaaS	Security as a Service
SLA	Service Level Agreement
SMI	Service Measurement Index
SME	Small and Medium Enterprises
SP	Service Provider
STaaS	Storage as a Service
SWOT	Strengths-Weaknesses-Opportunities-Threats(-Analysis)
TAM	Technology Acceptance Model
TCO	Total Cost of Ownership
TFEU	Treaty on the Functioning of the European Union
TOE	Technology-Organizational-Environment
UK	United Kingdom
US	United States (of America)
VM	Virtual Machine
VoIP	Voice over IP
XaaS	Everything as a Service
XML	eXtensible Markup Language

List of Figures

3.1	Overview of Stakeholders and their Interactions	14
4.1	Overview of Technical Factors 1/5	18
4.2	Overview of Technical Factors 2/5	19
4.3	Overview of Technical Factors 3/5	20
4.4	Overview of Technical Factors 4/5	21
4.5	Overview of Technical Factors 5/5	22
4.6	Overview of Economical Factors 1/2	38
4.7	Overview of Economical Factors 2/2	39
4.8	Overview of Organizational Factors 1/2	45
4.9	Overview of Organizational Factors 2/2	46
4.10	Overview of Relational Factors	51
6.1	Legend for Interrelations between Factors	71
6.2	Interrelations Affecting Availability	71
6.3	Interrelations Affecting Backups	72
6.4	Interrelations Affecting Business Flexibility and Agility	73
6.5	Interrelations Affecting CAPEX	74
6.6	Interrelations Affecting Collaboration	75
6.7	Interrelations Affecting Control	75
6.8	Interrelations Affecting Cost Flexibility	76
6.9	Interrelations Affecting Marginal Cost and Profit	77

6.10	Interrelations Affecting OPEX	78
6.11	Interrelations Affecting Organizational Compatibility	79
6.12	Interrelations Factors Affecting Migration	79
6.13	Interrelations Affecting Legal and Regulative Compliance	80
6.14	Relations Affecting Software Assurance	81
6.15	Interrelations Affecting QoS	82
6.16	Interrelations Affecting Return on Investment	82
6.17	Interrelations Affecting Trust towards the CSP	83
6.18	Interrelations Affecting Usability	84
6.19	Interrelations Affecting Vendor Lock-In	85
7.1	Legend for Time Based Graphs	88
7.2	Legend for Time Based Graphs with Threshold	89
7.3	Changes in Trends of Backup on Cost	90
7.4	Changes in Trends of Complexity on Usability	91
7.5	Changes in Trends of Cost on QoS	92
7.6	Changes in Trends of Network Quality on Availability	93
7.7	Changes in Trends of Organizational Compatibility on Migration Time . .	94
7.8	Changes in Trends of Scalability on Business Flexibility	96
7.9	Changes in Trends of Security Configuration and Maintenance on Legal and Regulative Compliance	97
7.10	Changes in Trends of Size of Organization on Marginal Cost	98
7.11	Changes in Trends of Software Assurance on Trust	99
7.12	Consequences of Standards on Vendor Lock-In	101
7.13	Changes in Trends of Traceability and Auditability on Legal and Regulative Compliance	103
7.14	Changes in Trends of Utility Based Computing on Cost Flexibility	104

List of Tables

2.1	Related Work	8
3.1	Overview Cloud Deployment Models from Cloud Consumers' Perspective .	12
5.1	Responsibilities of Actors in Federations According to EU DPD [33]	68
5.2	Applicable Law in Cloud Federation Location Scenarios [33]	70

Appendix A

Factor Index

Economical Factors, 40

- Billing and Metering of Resource

 - Usage, 40

- Capital Expenditures, 40

- Carbon Footprint, 40

- Cost, 41

 - Administration, 42

 - Backup, 41

 - Data Loss, 42

 - Energy, 41

 - Future Requirements, 42

 - Hardware, 41

 - Integration, 42

 - License, 41

 - Maintenance, 41

 - Migration, 42

 - Performance, 42

 - Switching Providers, 42

- Cost Flexibility, 41

- Economies of Scale, 43

- Marginal Cost and Profit, 43

- Migration Time, 43

- Operating Expenditures

 - Fixed Costs, 43

 - Variable Costs, 44

- Return on Investment, 44

- Total Cost of Ownership, 44

Organizational Factors, 47

- Business Flexibility and Agility, 47

- Collaboration, 47

 - Control, 48

- Inter-Company, 47

- Intra-Company, 47

- IT Competence of Employees, 48

- IT Infrastructure and Management, 48

 - Management Competence, 48

 - Rigidity, 48

- Legal and Regulatory Compliance, 49

 - Initial, 49

 - Maintaining, 49

- Location, 49

- Openness, 49

- Organizational Compatibility, 49

- Ownership of Data, 50

- Process Redesign, 50

- Size of Organization, 50

Relational Factors, 52

- Competition Intensity, 52

- Contracts and Service Level

 - Agreements, 52

- Reputation Fate Sharing, 52

- Skills and Expertise of the CSP, 52

- Transparency of CPS, 53

- Trust towards CSP, 53

 - Affective, 53

 - Cognitive, 53

- User and Technical Support from the CSP, 53

Technical Factors, 23

- Accessibility, 23

- Application Lifecycle Management, 23
 - Patching, 23
 - Upgrades, 23
- Availability, 24
- Backup, 24
- Complexity, 24
 - Expectation Conformity, 25
 - Flexibility, 25
 - Frustration, 24
 - Task Adequacy, 25
- Customization, 25
- Data Access, 25
- Data Loss, 26
- Elastic Resourcing, 26
 - Bandwidth Elasticity, 26
 - CPU Power Elasticity, 26
 - Memory Elasticity, 26
 - Number of VM, 26
 - Storage Elasticity, 26
- Fault Tolerance, 26
 - Proactive, 27
 - Reactive, 27
- Functional, 30
- Functionality, 27
- Initial Migration and Data Transfer, 27
- Integration, 27
- Interoperability, 28
 - Application, 28
 - OS, 28
 - Storage, 28
- Management and Maintenance of
 - Identity Platform, 29
- Management of Authentication Platform, 29
- Network Quality, 29
 - Bandwidth, 29
 - Connectivity, 29
 - Jitter, 30
 - Latency, 30
- Portability, 30
 - Data, 30
 - Service, 30
- Privacy, 31
- Quality of Service, 31
- Reliability, 31
 - Disaster Recovery, 31
 - Elasticity, 31
- Response Time, 35
- Scalability, 32
 - Scale Out, 32
 - Scale Up, 32
- Security Configuration and
 - Maintenance, 32
- Auditability, 33
- Authorization, 33
- Availability, 33
- Confidentiality, 33
- Integrity, 33
- Multi-tenant Trust, 33
- Service Response Time, 34
- Software Assurance, 34
- Standards, 34
- Traceability and Auditability, 36
- Trialability, 34
- Usability, 35
 - Application Launch Time, 35
 - Installability, 35
 - Learnability, 35
 - Simplicity, 35
- Utility Based Computing, 36
- Vendor Lock-In, 36
- Workload Management, 36
 - Capacity Planning, 36
 - Classification, 37
 - Configuration Management, 37
 - Mission Criticality, 37
 - Performance Management, 37
 - Workload Utilization Ratio, 37

Appendix B

XML Taxonomy

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE TAXONOMY [
  <ELEMENT TAXONOMY (FACTORS+)>
  <ELEMENT FACTORS (FACTOR+)>
  <ELEMENT FACTOR (SUBFACTOR*)>
  <ELEMENT SUBFACTOR EMPTY>

  <!ATTLIST FACTORS TYPE (Economical|Organizational|Technical|Relational)
  #REQUIRED>
  <!ATTLIST FACTOR NAME CDATA #REQUIRED>
  <!ATTLIST SUBFACTOR NAME CDATA #REQUIRED>
]>
```

```
<TAXONOMY>
  <FACTORS TYPE="Technical">
    <FACTOR NAME="Accessibility"/>
    <FACTOR NAME="Application_Lifecycle_Management">
      <SUBFACTOR NAME="Patching"/>
      <SUBFACTOR NAME="Upgrades"/>
    </FACTOR>
    <FACTOR NAME="Availability"/>
    <FACTOR NAME="Backup"/>
    <FACTOR NAME="Complexity">
      <SUBFACTOR NAME="Frustration"/>
      <SUBFACTOR NAME="Flexibility"/>
      <SUBFACTOR NAME="Task_Adequacy"/>
      <SUBFACTOR NAME="Expectation_Conformity"/>
    </FACTOR>
    <FACTOR NAME="Customization"/>
    <FACTOR NAME="Data_Access"/>
  </FACTORS>
```

```

<FACTOR NAME="Data_Loss"/>
<FACTOR NAME="Elastic_Resourcing">
  <SUBFACTOR NAME="Bandwidth_Elasticity"/>
  <SUBFACTOR NAME="CPU_Power_Elasticity"/>
  <SUBFACTOR NAME="Number_of_VMs_Elasticity"/>
  <SUBFACTOR NAME="Memory_Elasticity"/>
  <SUBFACTOR NAME="Storage_Elasticity"/>
</FACTOR>
<FACTOR NAME="Fault_Tolerance">
  <SUBFACTOR NAME="Reactive"/>
  <SUBFACTOR NAME="Proactive"/>
</FACTOR>
<FACTOR NAME="Functionality"/>
<FACTOR NAME="Initial_Migration_and_Data_Transfer"/>
<FACTOR NAME="Integration"/>
<FACTOR NAME="Interoperability">
  <SUBFACTOR NAME="Storage_Interoperability"/>
  <SUBFACTOR NAME="Application_Interoperability"/>
  <SUBFACTOR NAME="OS_Interoperability"/>
</FACTOR>
<FACTOR NAME="Management_and_Maintenance_of_Identity_Platform"/>
<FACTOR NAME="Management_of_Authentication_Platform"/>
<FACTOR NAME="Network_Quality">
  <SUBFACTOR NAME="Bandwidth"/>
  <SUBFACTOR NAME="Connectivity"/>
  <SUBFACTOR NAME="Latency"/>
  <SUBFACTOR NAME="Jitter"/>
</FACTOR>
<FACTOR NAME="Portability">
  <SUBFACTOR NAME="Data_Portability"/>
  <SUBFACTOR NAME="Service_Portability"/>
  <SUBFACTOR NAME="Functional_Portability"/>
</FACTOR>
<FACTOR NAME="Privacy"/>
<FACTOR NAME="Quality_of_Service"/>
<FACTOR NAME="Reliability">
  <SUBFACTOR NAME="Elasticity"/>
  <SUBFACTOR NAME="Disaster_Recovery"/>
</FACTOR>
<FACTOR NAME="Scalability">
  <SUBFACTOR NAME="Scale_Out"/>
  <SUBFACTOR NAME="Scale_Up"/>
</FACTOR>
<FACTOR NAME="Security_Configuration_and_Maintenance">
  <SUBFACTOR NAME="Authorization"/>
  <SUBFACTOR NAME="Availability"/>
  <SUBFACTOR NAME="Confidentiality"/>

```

```

        <SUBFACTOR NAME="Integrity" />
        <SUBFACTOR NAME="Multi-Tenat_Trust" />
    </FACTOR>
    <FACTOR NAME="Service_Response_Time" />
    <FACTOR NAME="Software_Assurance" />
    <FACTOR NAME="Standards" />
    <FACTOR NAME="Trialability" />
    <FACTOR NAME="Usability">
        <SUBFACTOR NAME="Application_Launch_Time" />
        <SUBFACTOR NAME="Installability" />
        <SUBFACTOR NAME="Simplicity" />
        <SUBFACTOR NAME="Learnability" />
        <SUBFACTOR NAME="Response_Time" />
    </FACTOR>
    <FACTOR NAME="Traceability_and_Auditability" />
    <FACTOR NAME="Utility_Based_Computing" />
    <FACTOR NAME="Vendor_Lock-in" />
    <FACTOR NAME="Workload">
        <SUBFACTOR NAME="Capacity_Planning" />
        <SUBFACTOR NAME="Performance_Management" />
        <SUBFACTOR NAME="Classification" />
        <SUBFACTOR NAME="Mission_Criticality" />
        <SUBFACTOR NAME="Configuration_Management" />
    </FACTOR>
    <FACTOR NAME="Workload_Utilization_Ratio" />
</FACTORS>

<FACTORS TYPE="Economical">
    <FACTOR NAME="Billing_and_Metering_of_Resource_Usage" />
    <FACTOR NAME="CAPEX" />
    <FACTOR NAME="Carbon_Footprint" />
    <FACTOR NAME="Cost_Flexibility" />
    <FACTOR NAME="Cost">
        <SUBFACTOR NAME="License" />
        <SUBFACTOR NAME="Maintenance" />
        <SUBFACTOR NAME="Cost_for_Back-up" />
        <SUBFACTOR NAME="Energy" />
        <SUBFACTOR NAME="Hardware" />
        <SUBFACTOR NAME="Migration" />
        <SUBFACTOR NAME="Performance" />
        <SUBFACTOR NAME="Future_Requirements" />
        <SUBFACTOR NAME="Cost_for_Data_Loss" />
        <SUBFACTOR NAME="Cost_for_Switching_Providers" />
        <SUBFACTOR NAME="Integration_Cost" />
        <SUBFACTOR NAME="System_Administration_Costs" />
    </FACTOR>
    <FACTOR NAME="Economies_of_Scale" />

```

```

<FACTOR NAME="Marginal_Cost_and_Profit"/>
<FACTOR NAME="Migration_Time"/>
<FACTOR NAME="OPEX">
  <SUBFACTOR NAME="Fixed_Costs"/>
  <SUBFACTOR NAME="Variable_Costs"/>
</FACTOR>
<FACTOR NAME="Return_on_Investment"/>
<FACTOR NAME="Total_Cost_of_Ownership"/>
</FACTORS>

<FACTORS TYPE="Organizational">
  <FACTOR NAME="Business_Flexibility_and_Agility"/>
  <FACTOR NAME="Collaboration">
    <SUBFACTOR NAME="Intra-Company"/>
    <SUBFACTOR NAME="Inter-Company"/>
  </FACTOR>
  <FACTOR NAME="Control"/>
  <FACTOR NAME="Legal_and_Regulative_Compliance">
    <SUBFACTOR NAME="Initial"/>
    <SUBFACTOR NAME="Maintaining"/>
  </FACTOR>
  <FACTOR NAME="Location"/>
  <FACTOR NAME="IT_Competence_of_Employees"/>
  <FACTOR NAME="IT_Infrastructure_and_Management">
    <SUBFACTOR NAME="Rigidity"/>
    <SUBFACTOR NAME="Management_Competence"/>
  </FACTOR>
  <FACTOR NAME="Openness"/>
  <FACTOR NAME="Organizational_Compatibility"/>
  <FACTOR NAME="Ownership_of_Data"/>
  <FACTOR NAME="Process_Redesign"/>
  <FACTOR NAME="Size_of_Organization"/>
</FACTORS>

<FACTORS TYPE="Relational">
  <FACTOR NAME="Competition_Intensity"/>
  <FACTOR NAME="Contracts_and_Service_Level_Agreements"/>
  <FACTOR NAME="Skills_and_Expertise_of_Cloud_Provider"/>
  <FACTOR NAME="User_and_Technical_Support_from_Cloud_Provider"/>
  <FACTOR NAME="Transparency_of_Cloud_Provider"/>
  <FACTOR NAME="Trust_Towards_Cloud_Provider">
    <SUBFACTOR NAME="Cognitive"/>
    <SUBFACTOR NAME="Affective"/>
  </FACTOR>
</FACTORS>

</TAXONOMY>

```

Appendix C

Contents of the CD

/Abstract.txt English abstract, as required by the department office

/Bachelorarbeit.pdf Digital copy of this thesis

/CD_Content.txt This index as plaintext

/Graphs_src Folder containing graphviz source files used to generate visualization of relations and taxonomy

/Presentations Folder containing the mid and final presentation

/Related Work Folder containing references used in thesis

/Taxonomy.xml The XML Taxonomy developed for this thesis

/Thesis Folder containing all LaTeX source files

/Thesis/graphics Folder and subfolder including all graphics and graphs used in thesis

/Time_Graphs.xlsx Excel file used to generate the time graphs for the thesis

/Zusfsg.txt German abstract, as required by the department office