Recommending Cloud Service Suppliers
Use of organizational criteria for Cloud Service Provider Selection

Renee M.L. Vaessen
Student number 2539546

Supervisor:
Patricia Lago
Second Reader:
Damian A. Tamburri

Master Thesis, submitted in fulfillment of the requirements for the degree of MSc Information Sciences, Faculty of Sciences, Vrije Universiteit Amsterdam
September 2014
Declaration of authorship

I, Renee Vaessen, declare that this thesis and the work presented in it, is my own. I confirm that:

- This work was done wholly or mainly while in candidature for a Master of Science degree at this University.

- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.

- Where I have consulted the published work of others, this is always clearly attributed.

- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.

- I have acknowledged all main sources of help.

- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date: September 15, 2014
Recommending Cloud Service Suppliers
Use of organizational criteria for Cloud Service Provider Selection

Renee M.L. Vaessen
September 2014

Abstract
Cloud services are provided by a large number of Cloud Service Providers (CSP). Both these CSPs and the provided services differ in characteristics. In order to select a CSP and its services, the client organization has to take several selection criteria into account, relevant for their organization and the use cases. In general these criteria concern the functional requirements or configuration, the quality (Quality of Service, QoS) and the cost of the provided service. However, organizational characteristics of the CSP and its services have to be included, in order to improve the outcome of the selection process. These organizational characteristics concern the CSP as cloud service supplying organization as well as the client's internal cloud service deployment. The study focuses on CSP selection for public Infrastructure as a Service (IaaS).

The organizational characteristics are identified from literature and then structured in a decision support model or framework, using the Grounded Theory approach. The framework contains organizational characteristics that are structured along two axes and depicted as boxes: the first axis is a clustering of properties, related to the cloud service itself, the relationship between the client and the CSP, compliance and sustainability. The second axis relates to the decision making level (strategic, tactical and operational). The characteristics then relate to selection criteria for these boxes.

The framework was evaluated by content experts in a series of interviews. A case study into an IaaS selection process for a software development company showed that most organizational characteristics were integrated in their decision process. Applying the framework to a selection process should result in a better match between a CSP and the client, because of the broader view of the selection criteria and the awareness of the decision levels. However, this requires governance of the clients decision process.

As Small and Medium Enterprises (SMEs) in Europe are relatively unfamiliar with cloud computing, the results of this study will be helpful for these companies when they start to deploy cloud services and subsequently have to select a CSP. However, metrics for the selection criteria and the scores of the CSPs for these criteria have to become available.
Acknowledgements/Foreword

Hector Fernandez
Hector initially defined the master project Recommending Cloud Vendors. I took advantage of his expertise in the technical field of cloud computing; his continuous support and feedback during the whole study, eventually from Spain, was of great importance.

Damian Tamburri
Damian took over the daily supervision in May 2014, when Hector left for the USA/Spain. He offered guidance on the research method and monitored the progress of the study. The almost weekly meetings helped me to continue the (at some times lonely) expedition into the cloud computing jungle.

Patricia Lago
Patricia became the main supervisor after Damian returned to Italy in July 2014. She provided valuable feedback on the preliminary results and their consistency. I also thank her for the guidance on the thesis structure and the feedback, necessary to improve the final report.

Albert Mahler
Albert provided me with experience-based views on systematic management of cloud deployments and he acted as an intermediary for the expert interviewees. I thank him for the constructive meetings at the Simagine office, in which we discussed the method and results of my study, with regard to the interfaces between my study and the CIPL-method he is developing.
# Table of contents

1. **INTRODUCTION** ........................................................................................................... 1  
   1.1. **Problem Description** .......................................................................................... 1  
   1.2. **Description of Research Question** ..................................................................... 3  
   1.3. **Research Relevance** ......................................................................................... 4  
   1.4. **Research Method Introduction** ......................................................................... 5  
   1.5. **Structure of Thesis** .......................................................................................... 5  

2. **RELATED WORK** ......................................................................................................... 6  
   2.1. **Introduction to Related Work** ........................................................................... 6  
   2.2. **Technical Standards, Security and Governance** ............................................... 6  
   2.3. **Alignment of IT-, Organizational and Business Requirements** ....................... 6  
   2.4. **Decision Support and MCDM** .......................................................................... 8  
   2.5. **General Supplier Selection** .............................................................................. 8  
   2.6. **Decision Making Level** ................................................................................... 9  
   2.7. **Cloud Implementation and Procurement Library 1.0** ....................................... 10  

3. **RESEARCH DESIGN** .................................................................................................. 11  
   3.1. **Method: Grounded Theory** .............................................................................. 11  
   3.2. **Structured Literature Review for Organizational Factors** ............................... 12  
   3.3. **Interviews** ...................................................................................................... 13  
   3.4. **Case Study of IaaS Selection** .......................................................................... 14  
   3.5. **Focus and Limitation of Study** ....................................................................... 14  

4. **ANALYSIS AND RESULTS** ....................................................................................... 15  
   4.1. **Codes, Categories and Theory from Grounded Theory** .................................. 15  
   4.2. **Axis: Clustering of Criteria** .............................................................................. 15  
   4.3. **Final Decision Framework** .............................................................................. 16  
   4.4. **Evaluation of Framework in Interviews** ......................................................... 19  
   4.5. **Evaluation of Case Study** ................................................................................ 20  

5. **DISCUSSION** ............................................................................................................. 21  
   5.1. **Expected Results and Outcome of the Study** ................................................... 21  
   5.2. **How to Use Framework** ................................................................................... 21  
   5.3. **Limitations of the Research Method** ............................................................... 22  
   5.4. **Limitations to Optimal Decision Making** ....................................................... 22  

6. **CONCLUSIONS AND RECOMMENDATIONS** ........................................................ 24  
   6.1. **Introduction to the Conclusion** ....................................................................... 24  
   6.2. **Answering the Research Question** ................................................................. 24  
   6.3. **Applicability of Model and Use of Decision Framework** ................................. 25  
   6.4. **Recommendations for CSP Selection Process** ............................................... 25  
   6.5. **Suggestions for Future Research** .................................................................... 26  

7. **REFERENCES** ........................................................................................................... 27  

Appendix A: Interview minutes (including case study)  
Appendix B: CIPL introduction  
Appendix C: Organizational factors; coding, sorted by cluster  
Appendix D: Organizational factors; sources and descriptions
1. Introduction

1.1. Problem description

1.1.1. Business drive for cloud computing and provider selection
The essence of Cloud computing is that variable computational power (servers), data storage facilities and a collaboration infrastructure is made available, on demand, over a network (commonly via the Internet). In addition, multiple software applications or services are available to the end user (Hill, Hirsch, Lake, & Moshiri, 2013, p. 3). In general, developing and deploying applications requires variable computing needs. In order to fulfill this dynamic computational need within a private datacenter, the in-house compute volume has to be large enough to fulfill the maximum requirements. This provisioning for maximum capacity is very costly, compared to externally acquiring the flexibly needed computational resources (that are more or less predictable in capacity and schedule). The added value of cloud computing depends on the nature of the end users’ business process; e.g. use cases with a volatile pattern of compute requirements will benefit more.

From the point of view of the end user, two business characteristics distinguish cloud computing from regular IT deployment in proprietary datacenters and from managed services in specialized datacenters (Hill, Hirsch, Lake, & Moshiri, 2013, p. 13): business agility and transition from capital expenditure costs (CAPEX) to operational expenditure costs (OPEX). These features are the main drivers for the current growth in using cloud services. In addition to these business related drivers, cost saving on operational IT-support advances interest in cloud computing.

On the service provider side, many companies and data centers see a business opportunity in offering cloud services. The differences in characteristics of the services themselves, contractual variety and the track record of the providers result in a multitude of offerings of cloud services. This makes it hard to compare and evaluate the CSP offerings. Moreover, as cloud computing is new to many clients, their requirements are not yet apparent and may evolve during the selection process.

In order to select a cloud service provider (CSP), the client has to formulate selection criteria for the services that will be deployed. Generally recognized criteria concern functional requirements or configuration, the quality (Quality of Service, QoS) and the cost of the service. However, organizational characteristics of the CSP and its services are also important in matching the requested service with the offerings. Security and privacy risks, vendor-lock in and availability of support are examples of these organizational factors. Taking organizational factors into account will improve the outcome of the selection process of the CSP and its services.

1.1.2. Definition of Cloud Computing
The definition that is often cited is the NIST definition (NIST, 2011). In a concise form:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). These resources can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of:

- five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service);
- three service models (Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)); and,
- four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud).
The SaaS service model means that the end user deploys the provider's application, which runs on a cloud infrastructure. Following this, the application is accessed from a variety of client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. For PaaS, the CSP provides programming languages, libraries, services, and tools. This is in contrast with IaaS, which implies that the end user only deploys processing, storage, networks, and other fundamental computing resources, and is able to deploy and run arbitrary software, e.g. operating systems and applications in the cloud. In addition, services like XaaS (anything/everything as a service) and Virtual Desktops or Data Storage are mentioned as future or distinct services.

The key element of a public cloud is that the owner of the resources (the CSP) offers services to anyone who wants to make use of that service. This implicates additional security issues because of the multi-tenancy of the resources. For a private cloud, however, the resource owner is the end user of the service, and the services are hidden behind a firewall. A hybrid cloud is a mix of public and private cloud, in a non-specified configuration (Hill, Hirsch, Lake, & Moshiri, 2013, pp. 22, 27, 29). A community cloud is shared by and supports a specific group of organizations or individuals (a community) that have a mutual concern (e.g. compliance consideration for governmental use, (NIST, 2011). Two of the underlying technologies for cloud computing are grid-computing, which emerged in the 1990’s, and hardware virtualization. For grid computing, a combination or grid of computers from multiple sources is configured to execute a specific compute task. Middleware is used to divide and allocate workloads to the constituent computers. Nowadays with cloud computing, the ‘grid’ is accessed over the Internet. In virtualization, a so-called hypervisor intermediates between the physical hardware (‘bare metal’) and the virtual machines (VMs, servers) that deliver the actual computational power/storage/memory capacity.

Cloud computing offers the opportunity to adjust the supply to the variable demand for computing resources (elasticity). Often, the comparison is made with the power grid, in that computing resources become a utility, for which the customers only pay for the amount of power they use (Databarracks, 2013)

1.1.3. Cloud Service Providers (CSPs)

Cloud computing capabilities are offered by Cloud Service Providers (CSPs), thus providing the requested services to the end users and exploiting this business opportunity.

For SaaS, examples of large CSPs or Application Service Providers are Salesforce (CRM-system), SAP (ERP-system) and Google with its Google Apps (e.g. Google Mail, Google Docs and Google Drive).

For IaaS, the best-known worldwide operating CSPs originate from the United States: Amazon Web Services (AWS), Google Compute Engine, Microsoft Azure, Softlayer (with IBM) and HP Cloud. They all have European datacenters, often in the UK. Other large US IaaS providers with European data centers are GoGrid and Joyent (both have their EMEA HQs in Amsterdam). Rackspace, that differentiates with its ‘fanatical support’, even has a Dutch support office and website.

In Europe as well as in the USA, many local providers are offering their IaaS services, often on a small and local scale.

1.1.4. Cloud Brokers

Consultancy and system support for CSP selection is the specialty of cloud brokers. ‘Cloud Broker’ has two meanings: first, a person or organization that acts as an intermediary, and second, a software application that facilitates the distribution of work between different clouds service providers. This second type of cloud broker is called a cloud agent.

The business model for cloud brokers (as human intermediaries) is still evolving. At its simplest, the end user hires a broker at the beginning of a project, to research the clients opportunities for cloud computing and to analyze the services from different CSPs. A further role is that the cloud broker negotiates contracts with cloud providers on behalf of the customer.
A broker system acts as a cloud aggregator when the end user is provided with application program interfaces (API) and user interfaces (UI), thus hiding complexity. This ‘cloud portfolio management’ presents the end user a variety of cloud services seemingly purchased from a single CSP, which leads to the reduction of complexity for the end user (TechTarget, 2013).

1.1.5. Other support companies
Clients with larger deployments or service deployments from multiple CSPs may need additional support in order to control and govern their spending. Two companies that supply tools to optimize deployment, control costs and gain business and data insight are Cloudability and Cloudability. Cloudyn (Cloudyn, 2014) supplies system support for optimizing cloud deployment for three cloud providers, Amazon AWS, Google Cloud and Open stack. For AWS and Google Cloud the deployments performance and cost can be compared. Cloudability (Cloudability, 2014) supplies a cloud cost management tool for multi cloud deployment, by automatically pulling billing data from several providers, including Amazon AWS, Rackspace, HP Cloud and Softlayer.

1.1.6. Focus on IaaS
Cloud Infrastructure as a Service (IaaS) is a standardized offering of compute resources, in combination with storage and networking capabilities, which is on demand offered to the end user. The resources, owned by a CSP, are scalable and elastic in near real time, and metered by use (Gartner b, 2013). IaaS enables investment and maintenance cost savings as well as agile provisioning of the compute need. For Public IaaS, the services are available to any end user. The focus of the study is on public IaaS, in order to reduce complexity. Because IaaS is viewed as a public commodity, the match between business functionality and service (PaaS and SaaS) is omitted, as well as specific security issues that necessitate private IaaS.

The main use cases for IaaS are: (Gartner c, 2013) and (Hill, Hirsch, Lake, & Moshiri, 2013) and (Amazon, 2014)

- Application development and testing, both for internal and external (commercial) use (e.g. IT-companies that offer their products as SaaS). The development projects can be locally organized or global collaborations.
- Production environments, both internal (backend) and customer-facing (front end) applications.
- Batch computing (e.g. big data, high-performance computing (HPC) or specific research functions.
- Disaster recovery.
- Start ups or short running projects: no up front investment required, easily scalable in case of success (and failure), e.g. campaigns and events.
- Web applications, with worldwide coverage.

Depending on the characteristics and use cases of the end users the specific requirements for IaaS differ. IaaS is suitable for a wide range of application design patterns, including "cloud-native" application architectures and enterprise application architectures. IaaS use cases include single-application workloads as well as combinations and varieties of workloads, even those supporting mission-critical workloads. All use cases can have a local/regional character or can be on a global scale.

1.2. Description of research question

1.2.1. Selection criteria for IaaS
Cloud services can be described with three sets of characteristics: the functional requirements or configuration, the quality (Quality of Service, QoS) and the cost of the service. Although the relation and difference between functional requirements and quality attributes is sometimes argued (Bass, Clements, & Kazman, 2013), the three-way distinction proved very useful for this study. Research on decision support and commercial comparison programs focus on part of these characteristics (e.g. on QoS and cost (Muntes-Mulero, Matthews, Omerovic, & Gunka, 2013),
configuration and cost (RightScale PlanForCloud, 2014). This is further illustrated in chapter 2. In addition to the service characteristics, organizational and social characteristics or properties influence the selection of a CSP and its services. Examples of these properties or factors (aggregate properties) are certification requirements, vendor lock-in, sustainability issues, security and governance and the track record of the providers. The way in which a client organizes the use of cloud services is also important for the match and fit with a service provider. Requirements for billing (e.g. in multiple currencies), the level of support and customization of the service may be critical for the client. The selection criteria are in turn related to the service characteristics and organizational factors, and are grouped into in four clusters, as illustrated in Figure 1 selection criteria.

Not all of the organizational factors are commonly part of the CSP selection process. To improve the decision-making process, these organizational factors must be identified and validated. Depending on which factor, measuring its (aggregate) value will be possible. Alternatively, only a qualitative description can be given. Moreover, the end user characteristics and the use case impacts the relative importance of the organizational factors. Subsequently, these weighted organizational requirements for a specific end user and use case are then matched with offerings from CSPs.

1.2.2. Research Question
In order to evaluate all applicable criteria for CSP selection, the organizational factors have to be identified. Subsequently, taking these factors into account in a selection process should result in a better match between a CSP and the client. This results in a main research question, which is divided into two sub questions.

The main research question (RQ) is:

\[ RQ: \text{How to evaluate organizational factors in the selection of a CSP} \]

This RQ is divided into two sub questions:

- \[ RQ-A: \text{What organizational factors are important when selecting a CSP?} \]
- \[ RQ-B: \text{How does integration of these factors influence the outcome of a specific IaaS use case selection process?} \]

The outcome should be a recognizable and validated set of organizational factors, with an evaluation of the integration of these factors into the CSP selection process, for a specific case.

1.3. Research Relevance
In general, CSP recommendation methods or systems focus on the cost, the functional requirements and the QoS of the required configuration/service. For cloud computing in general, most academic, governmental and business studies, as well as standardization efforts focus on technical or operational topics, on governance and security issues or are business related with a focus on large enterprises. This study is additional in that field, as it has a broader view, including organizational factors, and concerns small and medium enterprises (SME).

Taking organizational factors into account in a CSP selection process should result in a better match between a CSP and the client. Furthermore, the results can be used in other (academic) studies into (operational) service selection, to illustrate the relation to the business environment in which they function.
1.4. Research method introduction
In order to improve the decision-making process, organizational characteristics (that denote CSP selection criteria) have to be identified and structured. These organizational characteristics and criteria that are of interest for the selection of an IaaS Cloud Service Provider and their services are derived from literature study. A second step is to aggregate and structure these characteristics and criteria into a limited number of clusters. This should result in a model or theory for applying organizational factors in a CSP selection process. Interviewing stakeholders from both academic and business background then validates this model. The final step is to apply these criteria to a specific IaaS use case selection process and evaluate their added value. This approach is following the method of the grounded theory study (Robson, 2011, pp. 79, 146-151). In chapter 3, the method is described in detail.

1.5. Structure of thesis
In chapter 2, the related research concerning CSP selection is described. This includes research on alignment of IT-requirements with organizational and business related necessities, studies on decision support methods, in specific MCDM and general supplier selection studies. The final section related to decision-making levels in organizations and decision processes.
The third chapter explains the Grounded Theory method, the structured literature review (SLR) and the approach of the interviews and the case study.
In chapter 4, the analysis and results are described, following the steps of the Grounded theory. The evaluation of the results from the interviews and case study completes this chapter.
Chapter 5, Discussion, evaluates the outcome of the study, concerning both the substantive results as well as the applied method. The final chapter, conclusions and recommendations, recapitulates the main findings of the study and advises on its use for future research and professional practice.
2. Related work

2.1. Introduction to related work
Cloud computing is a recent development and quickly developing. The related work describes significant findings in several fields that are important CSP selection. The increasing importance of cloud computing reveals a number of technical challenges, which are studied. Furthermore, the use of public cloud services poses security and governance challenges. This is a second important field of research. Clients that start to deploy cloud computing are also faced with the selection of a CSP, from a vast offer of services. The alignment of the business and organizational requirements with the provided cloud services is topic of a few studies. Decision making support is a fourth subject of related studies. In general, the focus of academic research on Decision Support Methods is not on organizational factors. However, a few governmental and commercial organizations have built a support system for cloud provider selection. A final topic is general supplier selection. Research in this field is partially applicable for cloud provider selection. Apart from academic research, studies from research organizations (both profit and public private partnership research organizations) and studies that are commissioned by the EU are taken into account. In addition, publications and research from standardization organizations are analyzed. Commercial, confidential publications and methods (e.g. roadmaps, assessment tools) private consultancy firms are not taken into account in this study.

In general, the focus of these studies is on technical or operational topic, on external governance and security issues or business related with a focus on large enterprises. My research has, on one hand, has a broader view, as it integrates organizational issues with the aforementioned topics. On the other hand, it focuses on small and medium enterprises (SME).

2.2. Technical standards, security and governance
Several sources provide information in this field. First, the Institute of Electrical and Electronics Engineers (IEEE) has a Community for Cloud Computing and Big Data and organizes international conferences on Cloud computing. (IEEE, 2014). The research presented at these conferences is generally on technical topics (e.g. performance and migration); it does not include studies on cloud provider selection, apart from the operational resource allocation.
Second, the US National Institute of Standards and Technology (NIST) develops security recommendations and guidelines for cloud computing, for use by USA’s Federal agencies. These recommendations and guidelines are also relevant for nongovernmental organizations and can be used on a voluntary basis (NIST, 2014). NIST does not provide support for cloud provider selection.
The third sources are the EU/European Commission (EC) initiated research programs, often in collaboration with academic and business partners. The European Cloud Computing Strategy (part of the Digital Agenda, (EC Digital Agenda for Europe, 2014)) is of great importance, but focuses on technical standardization and governance/privacy.

2.3. Alignment of IT-, organizational and business requirements

2.3.1. Academic research
The view of clients on alignment of the services with their business and organizational characteristics is topic of two studies by Repschlaeger (Repschlaeger, Wind, Zarnekow, & Turowski, 2011), (Repschlaeger, Erek, & Zarnekow, 2013). The study from 2011 presents a provider independent classification model for Infrastructure as a Service (IaaS), in order to compare and classify cloud providers. Target dimensions and classification criteria for cloud computing were defined from a client view. Sources were expert interviews, literature review and an analysis of the CSP market for IaaS and hosting. The second study, from 2013, focused on preferences for CSP selection for start-up companies. A specific set of cloud provider characteristics were identified for this type of clients and five types of start-up-clusters were
distinguished, each with certain requirements for cloud provider capabilities/properties. A study from Muntes-Molero (Muntes-Mulero, Matthews, Omerovic, & Gunka, 2013) discusses risk, in addition to quality of service and cost (and functional requirements) in multi-cloud environments. The topic is avoiding vendor lock-in by facilitating the substitution of services by other services from alternative providers. Costs and Quality of Services are primarily taken into account for this comparison. Furthermore, risks are analyzed for this approach of substitution. The research of (Omerovic, Muntes-Mulero, Matthews, & Gunka, 2013) into risk assessment, quality and cost prediction is closer to the topic at hand. Their research aims at developing a decision support method (DSM) for multi-cloud environments. The complexity and lack of transparency in services, cost and QoS makes the run-time adaptation and replacement of services almost impossible. In addition, the providers as well as the cloud services themselves differ in the business models, functionality, quality of service, cost, value etc. Their findings distinguish different types of actors in the decision process, including the decision maker, who is aware of the business model and the strategy of the company (p 164). Moreover, the decision process is decomposed into phases. In the first phase, a high level description of the system architecture is defined, based on initial input, including business models and architecture requirements.

2.3.2. Standardization and non-governmental research organizations

The European Telecommunications Standards Institute (ETSI) is officially recognized by the European Union as a European Standards Organization. One of its projects is the ETSI Cloud Standards Coordination initiative, which describes the Acquisition of Cloud Service phase in its report (ETSI, 2013, pp. 14, 15). A person in the customer manager sub-role performs this activity (GEN_1.1). The short description of this acquisition activity is focused on operational QoS, security and governance. Criteria for measuring the services are not provided. The standard for quality aspects and metrics of software is ISO 25010 (ISO/IEC, 2011) (the successor of ISO/IEC 9126 Software engineering — Product quality). It defines eight (software) product quality characteristics, which are for the most part applicable to describe the quality of cloud services (at operational level).

The Cloud Services Measurement Initiative Consortium (CSMIC) is an international private public partnership that develops a Service Measurement Index (SMI). The publicly available SMI provides a standardized method for measuring and comparing a business services, by means of business-relevant categories and attributes of CSPs and its services (CSMIC, 2014). The CSMIC is developing a set of business-relevant Key Performance Indicators (KPIs) to measure the cloud services.

A well-known business research organization with a European focus is Gartner. It provides market research and product analysis reports of the IT industry. Part of their research is business oriented and addresses organizational challenges for cloud computing. Its Magic Quadrant publications for IaaS and European managed hosting (Gartner, 2013 b) (Gartner, 2013 c) presents the evaluation of important cloud providers, with an assessment of their technology capabilities and market position. These studies use a common set of organizational evaluation criteria, with a strategic business focus, mainly for medium to larger enterprises. A third study, focused on security for SaaS cloud contracts (Gartner, 2013 a), provides recommendations on contractual risk mitigation. A fourth applicable Gartner study (Gartner/Leong, L., 2013) states that public cloud IaaS offerings are not commodities. Clients have to match their use case and specific needs with the specific offerings. The study assesses several public cloud IaaS services against nine critical capabilities, in four use cases.

The broker company RightScale (RightScale , 2014, pp. 11, 13) supports Cloud Portfolio Management for their customers, to accelerate their delivery of applications while optimizing the customers cloud usage to reduce risk and costs. In their annual survey, several organizational factors are mentioned, e.g. cloud maturity of the end user organization.
2.4. Decision support and MCDM

2.4.1. Academic research and (governmental) research organizations
Research on Decision Support for cloud service selection generally addresses the service composition at the operational level. A recent systematic literature review (Jula, Sundararajan, & Othman, 2014) presents the service composition problem as follows: selecting the atomic simple services, in order to satisfy both the functional and QoS requirements based on the end-user requirements with the obtained complex composite services. A broker function between the user and the services is presented. The study further concentrates on the QoS and does not take organizational factors into account.

Multi Criteria Decision Making is a general approach for the selection process of cloud services (Rehman, Hussain, & Hussain, 2011, p. 2), (Rehman & Hussain, 2012, pp. 246, 250), including the the agent or broker based Cloudle research (Sim, 2012). Although these studies address the operational service selection and focus on QoS criteria, the method of MCDM is applicable for CSP selection with additional (organizational) criteria. Research on general supplier selection (see section 2.5) supports this finding (Boer, Labro, & Morlacchi, 2001), (Ho, Xu, & Dey, 2010). To apply MCDM, three essential requirements are that (1) clients have to indicate the relative importance of a criterion for the use case(s) at hand, and (2) a measurement method for scoring on the criteria is needed, and (3) the scoring of a CSP on these criteria is available (current or historical data). Difficulties arise if clients do not define or include all criteria and CSP scores are not present for all criteria. Benchmarks are rare, even at the operational level, and complex constraints complicate the matching process (Ngan, Tsai, Keong, & Kanagasabai, 2012, p. 751).

2.4.2. Public Private Partnership research organizations
The MODAClouds (Model Driven Approach) project aims to develop a decision support system for cloud services selection, at design- and run-time (MODAClouds, 2014). Quality attributes and costs are the main building blocks of the model. In the initial phase of the modeling, functional and non-functional requirements, related to the architecture and the behavior of the application, are added to the model (MODAClouds, 2014, p. 13). The implicit limitation of this research is on the functional requirements at the operational level.

2.4.3. System support for CSP selection
In the UK, the Government provides a website, Cloudstore (G-Cloud, no year) which gives an overview of cloud providers that are ‘approved by HM government’. This online marketplace allows end users in public sector organizations to buy off the shelf cloud-based services on a pay as you go basis, via the G-Cloud framework. It covers infrastructure, platform, software and support services, e.g. a ‘Buyers Guide’ (G-Cloud, 2014).

The PlanForCloud application (RightScale PlanForCloud, 2014) from the commercial broker company RightScale enables modeling of cloud configurations, including usage scenarios that incorporate growth, seasonality and other variability in the consumption of cloud resources. Deployments can be simulated; this results in a detailed 3-year forecast cost report (as the prices are continuously changing, this can only be indicative cost forecast).

2.5. General supplier selection
Research into general supplier selection methods (Boer, Labro, & Morlacchi, 2001, p. 84) distinguishes two different types of selection, depending on the phase of the selection process. The first type is the prequalification of suppliers; this is a sorting problem, in which acceptable suppliers are selected. The second type is the supplier selection: this is approached as a ranking problem, in which acceptable or preferred suppliers are graded. The selection methods are a variety of Multi Criteria Decision Making approaches.

(Boer, Labro, & Morlacchi, 2001, p. 82) mention several optional enhancements for supplier rating methods: the introduction of minimum levels for a criterion and compensating between criteria. To enhance consistency, the analytical hierarchy process (AHP) could be followed, in which pair-wise comparison of scoring (2 providers) or weight (2 criteria) is carried out. The
Fuzzy sets theory allows for modeling vague preferences (e.g. criterion Y should have a weight of around 0.8).

However, (Boer, Labro, & Morlacchi, 2001, p. 77) note on choice of decision method (italics in original):

> We argue that situational factors such as the number of suppliers available, the importance of the purchase and/or the supplier relationship and the amount and nature of uncertainty present, are far more determinative for the suitability of a certain decision method in a particular purchasing situation.

Another warning on the use of MCDM is from (Ho, Xu, & Dey, 2010, p. 22):

> In reality, the weightings of supplier evaluating criteria depend a lot on business priorities and strategies. In cases where the weightings are assigned arbitrarily and subjectively without considering the “voice” of company stakeholders, the suppliers selected may not provide what the company exactly wants.

### 2.6. Decision making level

Decision-making is generally divided in three levels, strategic, tactic and operational level (see Figure 2 Decision level, from Wikipedia 2014). These levels are related to the management level, scope, added value for business goals and impact of the decision at hand.

On the strategic level, the future overall direction of the end users organization, internally and especially with regard to its competitive environment is decided on (Wikipedia, 2014). For the tactical level decisions are made to meet the strategic objectives with the available resources (Gorry & Scott Morton, 1971, pp. 50-51).

![Figure 2 Decision level, from Wikipedia 2014](image)

Operational decisions concern the execution of tasks and deployments; they are based on set rules, within fixed, measurable boundaries.

With regard to CSP selection, these levels are described as follows:

1. Strategic selection concerns the long-term goal setting of the cloud deployment, in order to evaluate the long term viability, portfolio development and compliance capabilities of the supplier.
2. On the tactical level, the main concern is the preferred supplier selection, depending on the projects and use cases, within the boundaries set at the strategic level.
3. On the operational level, the scope is on the service selection. Design/build and run time choices are distinguished (MODAClouds, 2014):
   * For design/build time selection, a preliminary match is made between offered cloud services and the functional requirements, requested QoS and cost restrictions.
   * Run time decisions concern the actual selection of a service for deployment (resource provisioning).

In the strategic and tactical selection of a CSP, the objectives and policies of the end user-organizations are taken into account, including the plans and allocated resources to achieve their goals and objectives. On these levels, the emphasis lies on selecting the Service Provider (as an organization). For the operational level (both design/build and run time choices for deployment), the focus is on selecting specific services from a CSP.
From the strategic level down, constraints are specified, starting with aggregate, abstract and sometimes implicit considerations, developing into to specific criteria. Provisions for feedback loops are implemented in the decision process, in order to adjust or review decisions at a higher level. This is a governance process that records the alignment of decisions at different organizational levels. A definition of corporate governance, including its goal, is (Economic Times, 2009):

Corporate governance refers to the set of systems, principles and processes by which a company is governed. They provide the guidelines as to how the company can be directed or controlled such that it can fulfill its goals and objectives in a manner that adds to the value of the company and is also beneficial for all stakeholders in the long term.

2.7. Cloud Implementation and Procurement Library 1.0

Independent business research has been carried out by Albert Mahler, in cooperation with former colleagues from the HEM-group. The aim is to develop a method that facilitates and controls multi cloud deployments, on the level where business and ICT interact (Cloud Implementation and Procurement Library, CIPL, see appendix B. The core of the approach consists of four subsequent steps, in which the strategy for cloud deployment is defined, from strategic business level to operational cloud deployment. Governing the subsequent decisions is a central theme. The current CIPL version (1.0) is a starting point for further development, in which improvement and additional best practices are gathered and made available.

The first step is to assess the cloud readiness of an organization or part of an organization; the primary processes are evaluated to determine the appropriate cloud scenario, followed by a cloud maturity assessment. Results are the Cloud Scenario, the general service model for the business (SaaS, PaaS or IaaS, public or private), and the Cloud Implementation Strategy.

In the second step, the overall cloud strategy from the first step is translated into higher-level policies or guidelines for the distinct business functions (Generic Cloud Policy, as recorded in the Policy Set).

The focus of the third step is on specific business processes or use cases. Implementation aspects and governance of the process are analyzed, including support processes for cloud deployment. The generic cloud policy is refined for the specific business process into a Specific Cloud Policy, recorded in the Control Set).

The implementation of the cloud deployment for the specific business process or use case, including the required adaptations of the business process as well as ICT support. The implementation rules and constraints are recorded in the Config Set.

The alignment of the steps is governed with the help of the Policy Set, Control Set and Config Set, resulting from step two, three and four, in which the decision outcomes and constraints are recorded.
3. Research Design

3.1. Method: grounded theory

3.1.1. Grounded Theory in general

In order to evaluate the organizational factors that influence the CSP selection, organizational characteristics and selection criteria are analyzed and clustered. This clustering (in concepts) generates a structured framework for these criteria, supporting the selection process. These data are qualitative in nature, which implicates the use of a method for analyzing qualitative data. Grounded Theory is an important and widely used framework for this. Its goal is to generate a theory out of (qualitative) data (Bryman, 2008, pp. 541-545).

The approach of the Grounded Theory is both inductive and iterative. It is an inductive method because a theory or concepts is/are generated from the data. This is in contrast to validating a predefined theory or hypothesis, based on pre-classified data. The approach is iterative, as there is a continuous interplay between data collection and data analysis.

For Grounded Theory, coding is an essential process, in which labels/codes are given to important parts of the field under study. Codes are used to label, separate, aggregate and organize data (Bryman, 2008, p. 542). These codes are constantly revised and changed during the first phase.

Depending on the approach, coding is distinguished in two or three types (as cited in (Bryman, 2008, p. 543). Following the original approach of Strauss and Corbin, open coding, axial coding and selective coding are defined. Kathy Charmaz, who distinguishes initial coding and selective or focused coding, further developed the method. Both coding methods start with detailed coding, close to the original data, followed by structuring and reviewing the codes in order to generate concepts on the phenomenon that is studied (Bryman, 2008, p. 543). The first coding steps result in detailed and fractured data, in both approaches. Selective coding, the final process of both coding approaches, brings coherence or structure into the coded data. In this phase, codes can be dropped or combined into new codes. The coding phase ends when further data collection does not illuminate the concepts any further and reviewing the data coding does not lead to altering concepts or categories (theoretical saturation).

The main outcomes of Grounded Theory are concepts, categories, properties, hypothesis and theory (Bryman, 2008, p. 544). Concepts are the building blocks that result from the coding process. Categories are elaborated concepts, of a higher level of abstraction and include connections or relations between the categories. They represent a real world phenomenon. Properties are attributes of a category.

A hypothesis is an initial idea about the relationship between concepts; a theory is composed of systematically related categories, forming a framework that explains a relevant phenomenon. Studies can follow the process steps strictly and generates all outcomes. However, studies ‘... using a grounded theory approach generate concepts, rather than theory as such.’ (Bryman, 2008, p. 541).
3.1.2. Process steps and outcomes
The process steps and outcomes as defined in the scheme from Bryman (Bryman, 2008, p. 545) are the basis for the following description. The first step is to define the research question (see 1.2.2). For the readability of this section it is recapped. The main research question is
\[ RQ: \text{How to evaluate organizational factors in the selection of a CSP}, \]
and its consists of two sub questions:
\[ RQ-A: \text{What organizational factors are important when selecting a CSP?} \]
\[ RQ-B: \text{How does integration of these factors influence the outcome of a specific IaaS use case selection process?} \]
To identify applicable selection criteria, sources for organizational selection criteria were identified. The data were collected from structured literature research (SLR) and interviews with experts (from both business and academic background). The data collection and coding process were executed iteratively, near to theoretical saturation. Time constraints of the study limited additional data collection (especially interviews) and the code- and concept-reviewing phase. However, further data that were incidentally encountered confirmed the saturation level. The hypothesis phase led to the initial framework for the organizational characteristics and criteria for CSP selection. After interviews with experts (used for additional data collection as well as hypothesis testing), the final framework was defined. This framework is a theory in the Grounded Theory approach, as it describes categories of characteristics/aspects of Cloud Service Providers and their services, as well as the relationships between the categories.

3.2. Structured Literature Review for organizational factors

3.2.1. Variety of recent sources
Cloud computing is a recent phenomenon and developing fast. Therefore the time range for the search inquiries is generally restricted from 2010 to this date.
Both business opportunities and technology changes are driving the cloud computing (r)evolution. In addition to academic sources, data is collected from research organizations (both profit and public private partnership research organizations), from studies commissioned by the EU research and from standardization organizations. Commercial sources were also included in the data collection.
For the structured literature review (SLR), the search function of VU University Library and Google Scholar were used; in addition, Google search was used for non-academic sources. In addition, the supervisors provided initial sources. Backward and forward snowballing led to other studies and key authors.
The SLR was executed between January and June 2014.
The description of the organizational factors that were identified and analyzed is in appendix D.

3.2.2. Academic research
Queries for literature searches as executed in the VU library system, the first words ‘in title’; sorted by ‘Date-newest’
\[
\begin{align*}
1. & \text{IaaS AND (cloud computing OR provider OR broker OR selection)} \\
2. & \text{selection AND (cloud service OR CSP)} \\
3. & \text{supplier selection}
\end{align*}
\]
The results were selected or dismissed based on title, subsequently on abstract and full content. In addition, IEEE conferences on cloud computing were analyzed on applicable studies, however, they were very technical in nature. Research on operational cloud service composition was excluded because of the focus on decision models and exclusion of organizational factors.
Similar queries were executed in Google Scholar; the selected studies were accessed via the VU library.
Three studies were selected as sources for organizational factors. Two studies by the German researcher Repschlaeger, from 2011 and 2013, were analyzed (Repschlaeger, Wind, Zarnekow, & Turowski, 2011), (Repschlaeger, Erek, & Zarnekow, 2013). The study from 2011 presents target dimensions and classification criteria for cloud computing. The second study presents a specific set of cloud provider characteristics for start-up companies. Research from Muntes-Molero (Muntes-Mulero, Matthews, Omerovic, & Gunka, 2013) discusses risks; they classify as organizational factors.

3.2.3. Governmental and Business research
The Gartner Magic Quadrant publications for IaaS and European managed hosting are significant for the organizational factors and evaluation of the CSPs (Gartner, 2013 c; Gartner, 2013 b). These studies define a set of evaluation criteria, directed at the strategic business level of medium to large enterprises. These evaluation criteria are part of the analysis. The security levels, as presented in the Gartner study on security for cloud contracts (Gartner, 2013 a), classify as organizational factors. Critical capabilities for public IaaS are defined in the final Gartner study (Gartner/Leong, L., 2013). These capabilities are grouped into categories and classify as organizational factors. The Gartner studies were accessed via the VU library system (‘gartner’ as search term).
The Cloud Services Measurement Initiative Consortium (CSMIC) defined a Service Measurement Index (SMI). Business-relevant categories and attributes of CSPs and services (CSMIC, 2014) are defined. The attributes classify as organizational factors.

3.2.4. Commercial sources
The PlanForCloud website and application (RightScale PlanForCloud, 2014) gives an overview of support services and security certifications of the CSPs it brokers for. The support services and security certifications classify as organizational factors;

3.3. Interviews
In order to complement the findings of (academic) literature, interviews with expert practitioners were scheduled. The interviews were intended for data collection as well as for evaluation of the model. The use of surveys to acquire feedback on the model was not feasible, as the topic was too complex. The limitation on information gathering and evaluation is discussed in 5.1.3.
A former colleague introduced me to Albert Mahler, who is business consultant with experience in cloud computing projects. He contacted two interviewees that are members of the working group ‘Dutch Practice Guideline Cloud computing and innovation (NPR 5317) of the Netherlands Standardization Institute (NEN). The first interviewee is an expert on adopting open standards for governmental organizations; the second is internal controller of information and privacy protection at an academic hospital. A colleague of Mr. Mahler recommended the third interviewee, an independent ICT consultant who manages cloud transition project for business clients.
The interviews were semi-structured, one to one, in Dutch, and were conducted in July. In the first part of the interviews, the background of the research was explained: improvement of decision support for Cloud Service Provider (CSP) selection. The apparent limitations of the current selection process were explained (focus on operational selection criteria and security issues; disregard of levels and phases in the decision process). The collection of selection criteria in the preliminary framework were discussed, as well as the decision process in discussing experiences with cloud deployment projects. For some topics, the interview concentrated on specific issues the interviewee was working on. The minutes and interview structure are documented in appendix A.
3.4. Case study of IaaS selection

The purpose of the case study is to validate the decision framework, with respect to the decision-making levels and the use of all identified criteria. In addition, the actual selection process for the specific IaaS use case should be re-performed, taking all criteria into account. Then this simulated outcome would be compared to the outcome of the actual CSP selection. The limitation of the outcome of this case study is discussed in 5.1.4

A private software development company was chosen for the case study. In general, their use cases are relatively simple and isolated, and as IT companies they have an understanding of the matter. This reduces the complexity of the case study and eases the communication, from both sides. The subject of the case study, ADA, a Dutch software development company, is especially interesting as they initially selected and deployed AWS and migrated afterwards to a smaller provider in the Rotterdam area.
The interview, also in July, was held with the operational manager who is responsible for the cloud deployment and was involved in both provider selection processes. The interview followed the chronology of the subsequent cloud deployments, explaining the triggers and involved parties (relating to the decision process levels). As for the selection criteria, similarities and differences between the involved CSPs were discussed. The minutes are documented in appendix B.

3.5. Focus and limitation of study

The focus of the study is on (European) public cloud services for small and medium-sized enterprises (SMEs, with a limited number of employees and turnover/balance sheet total (EU/European Commission, 2014)). The SME clients in Europe are relatively unfamiliar with cloud computing. The results of this study will improve their knowledge of the topics that come up when they are going to deploy cloud services and subsequently have to select a CSP.
The second focal point the framework is the limitation to public IaaS, in order to reduce complexity: IaaS is viewed as a public commodity; therefore the match between business functionality and service (PaaS and SaaS) is omitted, as well as specific security issues that implicates the need for private IaaS.

Further improvement of a Decision Support Method (DSM) or Decision Support System (DSS) requires additional research. For Multi Criteria Decision methods, (MCDM), three conditions have to be met. First, the relative importance of a criterion for a specific use case must be indicated; second, a measurement method for scoring on the criteria is needed, and third, the CSPs scoring on these criteria is available. Developing a scoring/measuring method for the organizational factors is out of the scope of this research, as well as evaluating the CSPs and their offerings along these factors.
4. Analysis and results

4.1. Codes, categories and theory from Grounded Theory

4.1.1. Initial distinction of service characteristics
As pointed out in 1.2.1, the basis for the description of cloud services are the functional requirements or configuration, the quality (Quality of Service, QoS) and the cost of the service. In order to select a service that matches the client's requirements, organizational characteristics have to be included in the selection process.

4.1.2. Coding phase
All selected sources were studied and analyzed for codes on CSP selection, and the first concepts were formed (see appendix D for an overview of the basis for the coding). These concepts implicitly involved the decision making level, as they distinguished the cloud service, the service portfolio and the service provider as preliminary concepts. Because of the focus on the strategic and tactic evaluation of CSPs, the Gartner documents were again analyzed (Gartner, 2013 b) (Gartner, 2013 c), as well as the SMI for its business related attributes (CSMIC, 2014). This led to a series of eight concepts (see 4.2.1).
Combining these concepts with the distinction in decision-making level (see 2.6) resulted in a complex model, without a clear structure and distinction in categories. Further analysis and coding, with the decision level in mind, led to four aggregate concepts, or categories, as described in 4.2.2.

4.1.3. Defining a selection process framework (theory)
Combining the four categories of organizational CSP characteristics with the decision-making levels resulted in a framework for CSP selection properties, along two axes:
- Axis decision level (described in 2.6)
- Categories or clusters of properties and related criteria
The framework includes the organizational criteria as well as, on the operational level, the functional requirements or configuration, the quality (Quality of Service, QoS) and the cost of the service. This framework is elaborated in 4.3

4.2. Axis: clustering of criteria

4.2.1. Initial concepts
The first analysis of the sources resulted in a series of concepts, derived from common, strongly related codes. The concepts are:
- CSP viability concerned competition and partnerships, global coverage and collaboration and innovative capabilities of the CSP.
- Customer relations management included the sales process, account management, the contracting and negotiation process and client specific activities.
- Entry and exit support and facilities consists of trial periods, benchmarking support and portability options
- Security, certification and privacy relates to security policy, certification compliance, global legal strategy, cross border facilities and track record and 'trust'
- Compliance and internal governance of CSP
- Pricing strategy and tactics, costs are about the price level compared to competition and included services, contract periods and necessity of up front payment, pricing options depending on predicted usage pattern, the actual costs and billing facilities.
- For the cloud service itself, criteria on availability, performance, agility were repeatedly found, as well as on usability, support, interoperability and portability.
- The sustainability effort of the CSP was also mentioned a few times.
4.2.2. Limited number, further clustering:
These concepts were subsequently combined and clustered into four categories or clusters, after plotting them against the decision level. The resulting four clusters are
- Cloud service, as provided by the CSP (with an internal subdivision that is related to functional requirement, QoS and cost of the service). This is the central cluster, which denotes the deployment characteristics of the cloud service, or the execution of the IT-operations, fulfilling the compute requirements of the client. Depending on the decision level, the concern is on the actual execution of future possibilities for deployment.
- CSP-Client relation, concerning support, partnership and dependency. In general this are CSP characteristics that relate to the way of doing business, personnel requirements and duration and intensity of the cooperation.
- CSP Compliance relates to the capability of the CSP to provide the service consistent with the client's requirements and agreed on costs, service and security levels.
- CSP Sustainability concerns the efforts of the CSP to reduce the carbon footprint of their services, as well as their effort towards Corporate Sustainability Responsibility.

4.3. Final Decision Framework

4.3.1. Combination of two axes
Mapping out the four categories against the decision-making level resulted in a framework for criteria for CSP selection as illustrated in Figure 3 structure of CSP selection framework.

<table>
<thead>
<tr>
<th>Strategic decisions</th>
<th>Tactical decisions</th>
<th>Operational decisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSP- Client relation</td>
<td>Cloud Service from CSP</td>
<td>CSP Compliance</td>
</tr>
<tr>
<td>CSP Compliance</td>
<td>CSP Sustainability</td>
<td></td>
</tr>
</tbody>
</table>

- Functional requirements
- QoS
- Cost

The decision-making levels and their relations, including constraints and feedback loop are described in 2.6.

4.3.2. Decision-making framework with Cloud Service Provider properties
The complete model is shown in Figure 4 Decision model for CSP selection with CSP properties. The top row denotes the categories and the left columns denote the decision level. For each decision level and category, a box is defined in the model. The name of the box indicates the properties or characteristics of the cluster at the specific decision level.
The light blue boxes in the bottom row denote the cloud service, subdivided into functional requirement, QoS and cost. The surrounding darker blue boxes are the organizational characteristics or properties, for each level and cluster-combination. These properties are related to criteria, which impact the selection of a CSP at that specific decision level.

In the next sections, the boxes are described; the first entry is ‘cluster’, starting with the Cloud Service as the central cluster. The second order is the decision-making level, bottom up. This approach first conveys the essential distinction of the broad cloud-computing topic into the four categories. Subsequently, the elaboration for all decision levels is similar for each cluster. Within each cluster description, the bottom up approach demonstrates that the decisions taken at a certain level often are within boundaries that are set at the next higher level. Although, in general, a client representative operates at a specific decision level, his or her primary concern will be a specific cluster; therefore the structure of the description follows this line of reasoning. The CSP characteristics or properties in a specific box are related to selection criteria for that CSP or service property. Many of these selection criteria are defined and publicly available, for other boxes the criteria are incomplete (and in some cases the properties are not fully available in the sources). An overview of the available properties or criteria for each box is given in appendix C; the description of the criteria is available in appendix D.

4.3.3. Cloud Service cluster
The central and main cluster is the Cloud Service. Depending on the decision level, the Cloud Service has different occurrences.
At the operational level the Cloud Service is the individual service; the service at this level is subdivided into boxes for functional requirement, QoS and cost. For IaaS the functional requirements (or configuration) consist of compute or processing capacity, data storage facilities and a network infrastructure. The Quality of Service characteristics (e.g. availability and performance) of the provided service constitute the QoS box; the costs-properties of the service are in the Cost box, including the billing characteristics. Cloud service selection at the operational level implies a match of the provided configuration with the functional requirements, the QoS necessities and the cost constraints for the deployment. As this study focuses on the organizational criteria, not all available sources are analyzed; additional
The Cloud Service occurrence on tactical level is the service portfolio. The subdivision into functionality, QoS and costs is to a certain degree applicable. Functional requirements concern the portfolio and combination of services, including self-service provisioning facilities; monitoring and capabilities to ensure availability and performance are quality related. Pricing tactics of the CSP, system support to match the billing process with the client’s internal financial process, cross border and multi-currency billing are cost related properties. In addition, development potential, customization possibilities and the agility of the CSP to respond to universal changes in functional requirements from their clients and installed base are CSP characteristics on this level.

On the strategic decision level, the Cloud Service is labeled as service development strategy. Concerns are product development and strategy of the CSP, in relation to its competitors and partners, their knowledge of the clients’ industry and innovation strength (functional concerns). The CSPs strategy to execute operations (with regard to QoS) and the pricing strategy influence the decision on this level (if explicitly acknowledged in the CSPs policy).

4.3.4. CSP-Client relation

The adjacent cluster on the left is the CSP-Client relation, concerns the cooperation and dependency between the parties. This cluster is placed on the left to indicate a time sequence; establishing a relation with the CSP is preceding the actual deployment. The CSP-Client relation cluster also has different occurrences, related to the decision level.

The operational level of CSP-Client relation concerns the operational support and interoperability. Training opportunities for end users, availability of documentation, customer experience and usability impact daily operations. Furthermore, the need for client staffing is considered here. Problem support properties are, among others, response time, support channels, subscription to extra support and the knowledge of support-employees. Opportunities for (multi-) language support and providing a community forum are other characteristics at this level. Interoperability is, in general, a technical issue and not extensively describe here as the focus of the study is on uncomplicated IaaS deployment; the research of (Jula, Sundararajan, & Othman, 2014) and (MODAClouds, 2014) illustrates the interoperability challenges (see and 2.4.1 and 2.4.2).

The CSP-Client relation on tactical level is labeled as Exit/entry support and portability. Customer Relations Management (CRM), the location of offices and datacenters to accommodate visits and contracting experience locations belong to this level. Furthermore, opportunities for trial periods, benchmarking support and contract periods are properties in this box. Very important is the ownership of data and the portability options, the latter depending both on the CSPs data center/compute technology (standards) and the willingness to support data/system extraction.

Location, viability and partnership are the properties of the strategic level of the CSP-Client relation. In the first place this concerns the location of the CSP (datacenter as well as offices). The location is directly related to the requirements resulting from the client’s geographic business policy (e.g. worldwide or local deployment, latency) and legal constraints for some use cases. In addition, the viability of the CSP and the partnership options are evaluated in this box. The size of the CSP and its willingness to deal with their client’s requests for (strategic) cooperation or third party involvement is also input for selection at this level.

---

1 Reminder: The name of the box indicates the properties or characteristics of the category/cluster at the specific decision level.
4.3.5. CSP Compliance
The cluster on the right of the central Cloud Service is the CSP Compliance cluster. CSP Compliance relates to the capability of the CSP to comply with both legal and specific client’s security and privacy requirements, and provide the service according to service level agreements. This cluster incorporates the CSPs internal governance process, including certification and auditing.

CSP Compliance at the operational decision level concerns operational governance. The main issue is SLA verification (logging, performance and availability measurements, cost control and reporting). Additional capabilities are access control and privilege management. Disaster recovery measures should be available in accordance with the contracts.

The occurrence on tactical level is the certification/auditing. In order to comply with legal requirements (e.g. for privacy and on financial grounds), the CSP can acquire certifications. This is also applicable for certain ICT or standardization requirements. Associated with (but not limited to) certification are auditing opportunities, by a third party or by the client itself. Furthermore, capabilities for data loss protection and disaster recovery are evaluated at this level.

At the strategic decision level, CSP Compliance is labeled compliance and governance capability. Main topics are the CSP capability to meet the client’s compliance requirements and the CSPs internal governance policies (including testimony). Furthermore, the supply chain of the CSP, including vertical and horizontal collaborations, is important because of liability issues.

4.3.6. CSP Sustainability
The last cluster is CSP Sustainability. In general, the meaning of sustainability is limited to the efforts of the CSPs to reduce the carbon footprint of their services. However, Corporate Sustainability Responsibility (CSR) is a broader concept that may be pursued by the CSP. The sources for the coding only sparingly provided input for this category; therefore the description of this cluster is limited.

At the operational decision level, smart deployments that result in energy saving and use of sustainable energy are examples of operational efforts.

On tactical decision level, the evaluation takes capabilities to exploit green data centers (energy efficient and sustainable) into account. Furthermore, the CSPs sustainability policy can include the life cycle of the data center.

On the strategic decision level, CSPs sustainability concerns the aforementioned Corporate Sustainability Responsibility (CSR), and is labeled Social responsibility. Apart from the carbon footprint reduction, the CSP can have policies on additional social issues (e.g. ethicality, equal opportunity policies).

4.4. Evaluation of framework in Interviews
4.4.1. Conducted Interviews
The three conducted interviews resulted in an evaluation of the framework, with regard to the distinction in decision levels and the clusters for CSP selection. Furthermore, related to the subject matter of the interviewee’s job, experiences, standardization practices and challenges for cloud computing were discussed. The minutes of the interviews are documented in appendix A.

4.4.2. Decision making levels
The distinction in decision-making levels is recognized, various client parties are involved in the decision process. The decision-making process is iterative in nature and traverses different management levels. However, in practice the division of the decision-making levels is not explicitly made.

The IT department focuses on the decisions at operational and tactical level; the relation to business policy and added value for business processes is often not clearly discussed, except for cost savings.
4.4.3. Criteria clusters
The clusters are acknowledged as important topics and the distinction into the clusters is accepted, with a few variations in their interpretation. An important finding is that the weight of a certain box or criterion is very use-case specific, e.g. compliance/privacy requirements and location/geographic necessities.
Concerning the cloud service cluster, provisioning a cloud deployment with full scalability and self-service facilities is still difficult to accomplish, other than from the main global providers (specifically AWS).
For the CSP-client relation cluster, it is stressed that periodic evaluation of the provider is important, in order to adapt to changes in service requirements and the service portfolio, or to changes in the business environment (strategic challenges for the client). Although one of the characteristics of cloud computing is self-service, personal support is an important issue.
For the CSP compliance, requirements do differ according to the use cases, core business and size/competition of the client. Chain liability is a very important issue, as the end responsibility for the cloud-supported business processes remains with the client. Governing multiple inter- and intra- organizational data-transitions, across CSPs and their subcontractors, is a mayor challenge.
Sustainability is in general not explicitly taken into account in CSP selection. It is viewed as a CSP concern, to achieve cost savings and improve the company image.
An additional view on sustainability was mentioned in the governmental setting; ‘Duurzaamheid’ relates to the lifecycle of the (core) processes, for which IT-support is provided, including the use of cloud-services. However, this does not concern the CSP selection process itself.

4.5. Evaluation of case study
The aim of the case study was to evaluate the integration of the organizational factors in an IaaS decision process. The case study within the Dutch software development company ADA was conducted as an interview, in which the history of the cloud deployment and the prior decisions for CSP selection were discussed (see appendix A for the minutes). In the interview, questions regarding the distinct decision-making level and clusters were answered. As the company is rather small and privately owned, distinction in decision-making levels was implicit, however, strategic and tactical business considerations were part of the decision processes. The company initially selected a CSP in accordance with their client, who initiated and commissioned the cloud deployment. The second phase of cloud deployment concerned ADA’s own compute requirements. In selecting the CSP, the CSP-Client relation was very important for the company, in addition to the (operational) Cloud service characteristics. Both operational support and customer relations management (CRM) were essential in the selection process; CSP compliance is not vital for their use case. Sustainability issues were not taken into account.
In this case study, the distinction of decision-making levels is not explicit but implicitly the selection involves decisions on all levels. As for the cluster definition, CSP characteristics of the four defined clusters were evaluated, with an emphasis on Cloud Service and CSP-Client relation.
In conclusion, most organizational factors as defined in the framework are integrated in the CSP selection process.
5. Discussion

5.1. Expected results and outcome of the study

5.1.1. General findings and focus of study
The main advantages of cloud computing (cost savings, transition to operational expenditure (OPEX) and business agility) result in an exploding interest for cloud deployment. Many academic, governmental and business studies are commissioned, as well as standardization efforts. In general, the focus of these studies is on technical or operational topics, on governance and security issues or business related with a focus on large enterprises (see 2.1). This study adds to the research in that field, as it has a broader view, including organizational factors, and concerns small and medium enterprises (SME).
The purpose of this study was to identify the organizational factors that are important for CSP selection, for IaaS deployments. The expected outcome was a recognizable and validated set of organizational factors, evaluated for a specific case.

5.1.2. Decision making framework for CSP selection
The distinction of the decision-making level illustrates that different types of selection criteria are taken into account, and these are applicable for all clusters of CSP properties. Depending on the size of the client organization and the involved persons, this distinction is more or less explicit. However, making the distinction explicit improves the process of decision-making, as it elicits the feedback loops and governance process between the decisions at the distinct levels.
Clustering CSP properties or characteristics into four categories is a debatable decision, even as it is based on the coding method of Grounded Theory (described in 3.1). However, the clustering was evaluated in the interviews and all interviewees recognized the categories.
The Sustainability cluster stands out from the other three clusters, as it is viewed as less important for CSP selection. Still, many CSPs profile themselves in this regard, with ‘green computing’ programs. As energy saving (with its associated cost saving) is one of the drives for cloud computing, and in view of probable future importance, this cluster is incorporated in the framework.

5.1.3. Interviews
All interviewees had extensive knowledge and experience in their specific cloud computing related field and provided valuable input for the research. The time line of the study did not allow for additional interviews, interview rounds or focus group meetings. Planning this phase mid-summer complicated the availability of interviewees.

5.1.4. Case study
The case study proved to be interesting because of the two-time CSP selection and migration. Most organizational factors as defined in the framework were integrated in their selection process. Applying the complete framework, with hindsight, to this CSP selection process would require additional extensive meetings with all involved parties; this was not feasible due to the timeline of the study and the availability of the participants.

5.2. How to use Framework

5.2.1. CSP selection process for SME and relation to academic research
The study resulted in a framework for organizational properties and selection criteria, in addition to (operational) characteristics and criteria for functional requirements, QoS and cost; it was reviewed in interviews and evaluated in a case study. Limiting the categories resulted in a four-way division that was well suited for a straightforward framework, fitting for its use as a tool for SME clients that are not familiar with cloud computing.
This framework is a freely available model, based on scientific research and public sources. As European SME clients are relatively unfamiliar with cloud computing, the results of this study will be helpful when they are going to deploy cloud services and subsequently have to select a CSP. Applying the framework to a selection process should result in a better match between a CSP and the client, because of the broader view of the selection criteria and the awareness of the decision levels. Furthermore, the results are an additional input for other (academic) studies into (operational) service selection, in order to relate to the business environment in which they operate.

5.2.2. Description of framework for specific functions
The order of the description in the framework, as used in 4.3.2, is based on the four categories of the model, to make the user familiar with its setting. In general, a client's employee operates at a specific decision level and his or her primary concern is a specific cluster, related to a functional department (depending on the size of the client's organization). Depending on the need of the user in the client's organization, the order of the description of the framework can be adapted to the user's specific focus.

5.2.3. Relation of CSP selection to business policy and internal governance
The business strategy of an organization is leading for strategic decisions concerning cloud deployment. Aligning this business strategy with the IT strategy in this field is a prerequisite for value-added use of cloud services. Further elaboration of a cloud deployment strategy to tactical and operational level takes place within the boundaries set at the higher level, requiring dependable internal governance processes. This is the subject of CIPL (see 2.7).
CSP selection is a specific part of the challenges that organizations face when they decide to deploy cloud computing and it takes place in this setting of aligning business and IT-policies. Therefore, governing the business-IT alignment applies also to the CSP selection process and is constraining the options for CSP selection. These internal governance processes are distinct from the governance processes as specified in the CSP Compliance cluster, as they relate to the governance processes of the CSP. However, governing the client's decisions within the CSP selection framework is an essential requirement for exploiting the framework.

5.3. Limitations of the research method
The aim of Grounded Theory is to generate a theory from available, qualitative data. Selecting the data for coding is essential, and missing out on important sources is one of the risks of this study. A second constraint is the position of the researcher: generating a theory and subsequently evaluating it may not be without bias. This bias poses a risk for tunnel vision especially when conducting the study as the single researcher, without feedback from and complementary discussions with fellow researchers poses a risk for tunnel vision. In this study, feedback from the supervisors largely dealt with this limitation.
As noted previously, the number of interviews was limited, as well as the depth of the case study.

5.4. Limitations to optimal decision making
Academic research in this field presupposes rational decision processes, including explicit nomination of decision criteria. However, this presupposition has its limitations, and several difficulties may constrain the selection of the best CSP for a given end user-organization and use case.
First, the (environment of the) end user organization is a Complex Adaptive System (CAS), with three characteristics of its behavior: evolution, aggregate behavior and anticipation (Holland, 1992, p. 18). Because of the dynamic nature of the environment and the anticipative behavior of the end user, the resulting selection may not be optimal (Holland, 1992, p. 20). The client's assumptions for future developments, internally and externally, may be falsified, thus limiting the usefulness of the decision.
Second, according to a study from (Heiner, 1983), concerning behavior, a gap may exist between the competency (C) of the decision maker/agent and the difficulty (D) of the selection process. This C-D gap creates uncertainty. Heiner states:

[...] that when genuine uncertainty exists, allowing greater flexibility to react to more information or administer a more complex repertoire of actions will not necessarily enhance an agent's performance. (Heiner, 1983, p. 563).

Heiner’s research implicates that an optimal, rational solution for a CSP selection problem may not be feasible, as both exhaustingly analyzing the alternatives as well as making the selection process more complex might have counterproductive effects.

However, it is important to consider organizational and social factors when selecting a CSP. In the 1980's, IBM was often mentioned in a quote, in the selection process of buying hardware: "Nobody ever got fired for buying IBM". This is sometimes paraphrased as "Nobody ever got fired for buying AWS" (Plummer, 2012, p. 24), implicating an additional social factor in the CSP selection process, that is the position of the decision maker. Decision makers, at every organizational level, may have implicit motives, conscious or unconscious, that influence the decision process.
6. Conclusions and recommendations

6.1. Introduction to the conclusion
In order to select a cloud service provider (CSP), the client organization has to take several selection criteria into account, relevant for the use case and the services that will be deployed. Commonly accepted criteria concern the functional requirements or configuration, the quality (Quality of Service, QoS) and the cost of the service. Furthermore, organizational characteristics of the CSP and its services have to be included in matching the requested service with the offerings, to improve the outcome of the selection process of the CSP and its services. These organizational characteristics concern both the organization of the CSP as an external supplier institution, and the way in which a client organizes its deployment of cloud services.

This study focused on the additional organizational criteria, because of the lack of this view in many of the academic, governmental and business studies, as well as standardization efforts. In general, the focus of these studies is on technical issues, operational decision support methods, on governance and security challenges or business related with a focus on large enterprises. This study is supplementary in that field, as it includes organizational factors (aggregate properties or characteristics) and concerns small and medium enterprises (SME).

6.2. Answering the Research Question

6.2.1. Purpose of study
The intention of the study was to identify the organizational factors that are important for CSP selection, for IaaS deployments. The expected outcome was a recognizable and validated set of organizational factors, evaluated for a specific case.

The main research question (RQ) was:

RQ: How to evaluate organizational factors in the selection of a CSP

This RQ was divided into two sub questions:

- RQ-A: What organizational factors are important when selecting a CSP?
- RQ-B: How does integration of these factors influence the outcome of a specific IaaS use case selection process?

The expected outcome was a recognizable and validated set of organizational factors, with an evaluation of the integration of these factors into the CSP selection process, for a specific case.

6.2.2. Answer to Research Question A

- RQ-A: What organizational factors are important when selecting a CSP?

In identifying and structuring the applicable organizational factors, the Grounded Theory approach was used, which resulted in the decision framework that is presented in 4.3. This framework consists of organizational characteristics or properties of CSPs and their cloud services. The characteristics are structured along two axes and depicted as boxes: the first axis is a clustering of properties, related to the cloud service itself, the relationship between the client and the CSP, compliance and sustainability. The second axis relates to the decision making level (strategic, tactical and operational). The properties then relate to selection criteria for these boxes.

This framework was subsequently validated in a series of interviews. The results from the interviews stressed the fact that applying the criteria is very use case dependent; therefore it is essential to assign weights to the individual criteria.
6.2.3. Answer to Research Question B

- RQ-B: How does integration of these factors influence the outcome of a specific IaaS use case selection process?

The case study showed that most organizational factors as defined in the framework were integrated in their selection process (see 4.5). The CSP selection process was not, with hindsight, repeated and evaluated using the complete framework. The exact influence of integrating all identified organizational factors (or selection criteria) and the decision-making level into the decision process is therefore not analyzed. However, most organizational criteria were explicitly part of the selection process, as well as the (implicit) distinction of the decision-making levels. As the company in the case study is satisfied with their current CSP, it can be concluded that taking these organizational factors into account is at least partially accountable for the good-quality outcome of the selection process.

6.2.4. Answer to the main Research Question

RQ: How to evaluate organizational factors in the selection of a CSP

In conclusion, the study resulted in an evaluated decision framework for organizational characteristics for CSP selection, in addition to Functional Requirement-, QoS- and the cost-related criteria. Depending on specific use case requirements, related to the client's business, the importance of the cluster and the weight of the related criteria can be very different.

6.3. Applicability of model and use of decision framework

The focus of the study was on IaaS deployment for private small and medium enterprises (SME clients) because of limited security and privacy requirements and less complex use cases. The resulting framework will help European SME clients when they are going to deploy cloud services and subsequently have to select a CSP. Applying the framework to a selection process should result in a better match between a CSP and the client, because of the broader view of the selection criteria and the awareness of the decision levels. Furthermore, the framework is an additional input for studies into (operational) service selection, in order to relate to the business environment in which they operate.

6.4. Recommendations for CSP selection process

6.4.1. Improvement of CSP selection process

Integrating organizational criteria in the CSP selection process, by means of applying the framework will improve its outcome because of the wide-ranging selection criteria and the understanding of the decision-making levels. This implicates that CSP selection processes are organized with the distinction of decision levels and clusters in mind. Furthermore, cloud deployment policies should explicitly relate to business policies in order to realize the added value opportunities. Defining an internal governance process, across organizational levels, is a prerequisite for the above-mentioned recommendations.

6.4.2. Applicability of MCDM methods for CSP selection

As stated in 2.4 and 2.5, Multi Criteria Decision Making (MCDM) is commonly applied as a method for operational cloud service selection and for general supplier selection. Rating a supplier or service consists of summing up the score of the service or CSP on criterion A x the weight of criterion A for the use case, for each criterion. A recommendation system for CSP or service selection must therefore include and support

1. A scoring method for each (individual or aggregate) criterion, implying the availability of criteria and related metrics
2. The use of relative weights of criterions for different use cases
3. Data on service offerings and CSP characteristics, that are equivalent and validated.
This poses several challenges. Although criteria and metrics for evaluating cloud services at operational level are available, they are focused on internal quality requirements and not adapted for the specific use of the external provider selection. Second, CSP selection criteria for strategic and tactical level decisions are implicitly known but neither well defined nor well structured; the presented framework is a first step in defining and structuring criteria. Finally, the service offerings of CSPs have to be comparable; this means that the services have to be mapped onto a model of common CSP- and service attributes and that the scoring of the CSP and its services on these attributes is known and validated.

6.5. Suggestions for future research

The presented CSP selection framework is a first step in supporting the selection process for CSPs and their services. Applying the framework, evaluating the outcomes and completing the CSP and service characteristic (the content of the boxes) are further topics of study. Furthermore, focusing on small and medium enterprises as well as on the relatively simple IaaS offerings leaves room for additional research.

Methodological and system support for the internal governance of the CSP selection process is a third topic of additional study.

Finally, in order to establish system support for Multi Criteria Decision Making, metrics for the identified criteria have to be defined. This also requires the development of a generic cloud-service-model, in order to map and compare the characteristics of the distinct service offerings of the CSPs.
7. References


ETSI. (2013). *Cloud Standards Coordination Final Report*. Cloud Standards Coordination initiative. ETSI.


8. Appendices

Appendix A: interview minutes (including case study)

Appendix B: CIPL introduction

Appendix C: organizational factors; coding, sorted by cluster

Appendix D: organizational factors; sources and descriptions
APPENDIX A

Summary of interview 1
Model of organizational factors for CSP selection

Interviewee: Marijke Salters (Logius, The Hague, marijke.salters@logius.nl)
Date/time: Monday July 14th 2014, 9.30-10.30
Interviewer: Renee Vaessen (VU, renee@komies.nl)

Ms. Salters is member of the NEN² working group NPR³ 5317 ‘Cloud computing and innovation’ and was recommended by Albert Mahler (my business supervisor), who attended a meeting of this working group. She works for Logius, at Bureau Forum Standaardisatie⁴, as a consultant in the field of adopting open standards for governmental organizations. The interview is conducted for the VU Master Information Studies 2013-2014, master thesis project ‘Recommending Cloud Vendors’⁵. The goal of the interview was to validate and improve the model of organizational criteria, influencing the choice for (IaaS) cloud providers. The interview was conducted in Dutch; the minutes of the interview will be drafted in English and sent to Ms. Salters for review.

First, the background of the research is explained: improvement of decision support for Cloud Service Provider (CSP) selection. In general, the focus of the selection process is limited to operational selection criteria and security issues; the different phases of the decision process are not taken into account. Sources for the criteria are (a.o.) Gartner⁶, SMI (Service Measurement Index)⁷ and European initiatives, partly in cooperation with commercial parties (e.g. ETSI, standardization; ENISA, security).

The model as shown and explained in general (decision level versus cluster, title added later):

CRITERIA FOR Cloud Service Provider SELECTION

---

² NEN = Netherlands Standardization Institute
³ NPR = Nederlandse Praktijk Richtlijn, Dutch Practice Guideline
⁴ https://www.forumstandaardisatie.nl/organisatie/bureau-forum-standaardisatie/medewerkers/
⁶ Gartner (2013). Magic Quadrant for European Managed Hosting, report ID: G00250051
Ms. Salters remarks on the model and criteria:

**General**
This model is also applicable for governmental organizations (as well as profit organizations)

**Cluster Compliance (all levels):**
For multi-cloud environments, compliance and security are the final responsibility of the client; this cannot be transferred to the cloud provider. Chain liability, both horizontal as well as vertical (subcontractors of CSP) belongs to the governance process of the client. Transparency and openness of the CSP are very important; this includes capabilities for monitoring and auditing.

Security levels are use case and client dependent: note differences in security levels for, e.g. the AIVD, privacy compliance for personal data in municipalities, versus the use and availability of open data (e.g. geographical data).

The ISO/IEC 27001 standard and certifications are applicable for security governance.

**Cluster Cloud Service**

**Costs (service at operational level):**
Cost saving are the main driver for government organizations.

**QoS (service at operational level):**
Quality of Service denotes the non-functional requirements of the service (important requirements).

**Service development (strategic level):**
A CSP should be open on its strategy for product development and the level of influence a client (group) has on this development. This also relates to the partnership with the CSP: offering of standard functionality, improvement of functionality in consultation or even customization for a user community.

**Cluster CSP-client relation, Partnership (strategic level):**
Public-Private Partnerships are established at this level. At the operational level the intentions of the partners may diverge, as the governmental organizations have multiple and sometimes fuzzy goals, whereas for the private parties the profitability is the main driver. Ms Salters advises to keep these different goals in mind, when entering into a partnership (especially a PPP).

Furthermore, local authorities (e.g. municipalities) are forming communities/horizontal partnerships with other (local) authorities to be able to manage the supplier(s), in accordance to the Governmental note on cloud computing.

**Cluster Sustainability ('Duurzaamheid' in Dutch):**
The meaning of ‘Duurzaamheid’ in the governmental setting is related to the lifecycle of the (core) processes that have to be executed and supported. It is an important concern for deciding on IT-support, including the use of cloud-services. This interpretation is closer to the meaning of sustainability as ‘social responsibility’, compared to ‘reducing carbon footprint’.

Ms. Salters mentions the **Bomos Project**, regarding the life cycle of open standards for Dutch (governmental) standardization communities, under a Creative Commons license. Developing,

---

8 General Intelligence and Security Service of the Netherlands
10 http://www.forumstandaardisatie.nl/nc/themas/adoptie-implementatie-en-gebruik/beheer-van-standaarden/?sword_list%5B0%5D=bomos
maintaining and governing cloud solutions in an open and transparent way are essential for the satisfaction of clients or suppliers needs. BoMOS is also applicable for generic services

**On cloud maturity of organizations and security challenges:** a study by RightScale (RightScale, 2014, p. 11) shows that ‘cloud beginners’ view security as the number one challenge. Conversely, for cloud focused organizations, security is a less important issue. This is related to the increase in security features of cloud providers as well as the availability of cloud security best practices. Ms. Salters argues the validity of this statement: with growing use of cloud services, the security issues are increasing because of multiple inter- and intra-organizational data-transitions that have to be governed. As was remarked with regard to ‘compliance’, the final responsibility resides is at the client. Any newspaper item on "loss of data" or "data going public" from governmental clouds will have a major impact.

**On use of standards for cloud computing:** some (technical) standards are universal and always applicable, others standards are applicable 9 out of 10 times (e.g. encrypted communication) but depend on the use case and client (see examples at ‘Compliance’). A new factsheet on use of open standards for cloud computing will be published on 27th of October 2014.
Standardization also takes place at the process level, to simplify the internal governance. At the operational level, the use of the standardized processes is especially helpful. An example is the use of a standardized DAP for different suppliers.

---

13 DAP, Dossier Afspraken en Procedures, operational procedures in addition to the SLA
Summary of interview 2

Structuring of organizational factors for CSP selection

Interviewee: Beer Franken (AMC, Amsterdam, b.franken@amc.uva.nl)
Date/time: Thursday July 17th 2014, 15.00-16.00
Interviewer: Renee Vaessen (VU, renee@komies.nl)

Mr. Franken is member of the NEN working group NPR 5317 ‘Cloud computing and innovation’ and was recommended by Albert Mahler (my business supervisor), who attended a meeting of this working group.

Mr. Franken works for the Amsterdam Medical Center (AMC) of the UvA in Amsterdam, as internal controller of information and privacy protection.

The interview is conducted for the VU Master Information Studies 2013-2014, master thesis project 'Recommending Cloud Vendors'. The goal of the interview is to validate and improve the model of organizational criteria, influencing the choice for (IaaS) cloud providers.

The interview was conducted in Dutch; the minutes of the interview will be drafted in English and sent to Mr. Franken for review.

First, the background of the research is explained: improvement of decision support for Cloud Service Provider (CSP) selection. Main sources for the criteria are Gartner, SMI (Service Measurement Index) and European initiatives, e.g. ENISA, security). In general, the focus of the selection process is limited to operational selection criteria and security issues; the different phases of the decision process are not taken into account.

The model as shown and explained in general (decision level versus cluster):

---

CRITERIA FOR Cloud Service Provider SELECTION

---

14 Open request for feedback
15 NEN = Netherlands Standardization Institute
16 NPR = Nederlandse Praktijk Richtlijn, Dutch Practice Guideline
18 Gartner (2013). Magic Quadrant for European Managed Hosting, report ID: G00250051
20 ENISA (2012) Procure Secure; a guide to monitoring of security service levels in cloud contracts
APPENDIX A
Renee Vaessen VU University Master Information Sciences, 2013-2014

Mr. Franken’s field of expertise is the compliance cluster, the interview focuses on this topic.

The NEN NPR 5317 guideline (draft stage) will be structured according to phases in the cloud deployment process: 1) what part of the application portfolio/use cases should be moved to the cloud,
2) which services and CSPs to deploy and 3) the evaluation of the operations.

Ad 1) In general, the application portfolio that moves to the cloud is divided and structured to minimize the interfaces; the applications that support the core business are treated in a different way.

For the AMC, privacy and intellectual property are very important because of the character of the data: personal (patient) data and research data, thus limiting overall and public cloud deployment.

- Some datasets are ‘open data’ and can be made available on a cloud platform;
- Short-term research is possible on European cloud platform (future ownership of CSP is uncertain factor)
- The amount of data and number of transactions is, in general, limited: the costs of the cloud service are in general, reasonably limited.

Ad 2) The contracts with the CSP are threefold: a high level contract, multiple SLAs and additional DAPs21 for operational procedures.

Ad 3) Monitoring and feedback takes place at multiple levels: both operational and higher organizational levels.

Remarks on the model and criteria:
Cluster CSP-client relation, Portability (tactical level):
A customized or unique service makes it hard to migrate to another CSP.
The possibility of re-migrating to an in-house solution should be left open, therefore maintaining (some of the) internal knowledge and experience is important.

Cluster Cloud Service
Service portfolio (tactical level), Standards and Open Source
- The NEN supports all ‘de facto’ industry standards and ‘conventions’ (best practices).
- Standards originating from the USA often lack the cross-border view that is necessary in Europe.
- Open source has the advantage of customization opportunities, in contrast to the limited influence of a smaller client on product/service development policy of a large CSP. However, the community that supports an open source system or standard decides on the functionality that is kept in future development; in order to avoid ‘non supported features’, it is advised not to rely on very specific functionality.

Cluster Sustainability
This aspect is not yet explicitly part of the NEN NPR 5317, but will probably be addressed in the finalization of the guideline.

For further inquiries on CSP selection, Mr. Franken refers to Pieter Jansen22, independent IT consultant, working for The Hague municipality and also partaking in NPR working group.

21 DAP, Dossier Afspraken en Procedures, operational procedures in addition to the SLA
22 pj@ictree.nl
Summary of interview 3
Practice of cloud transition and criteria for Cloud Service Provider selection

Interviewee: Menasseh Rotteveel (independent ICT consultant, Amstelveen, milga_rotteveel@casema.nl)
Date/time: Friday July 25th 2014, 9.00-10.30, Amstelveen
Interviewer: Renee Vaessen (VU, renee@komies.nl)

Mr. Rotteveel is an independent ICT consultant, who manages cloud transition project for business clients (e.g. LOI and Osira Amstelring) and from the CSP-side (e.g. Vancis). He was recommended by Roel Remkes, from Choice Company, who I met with the help of Albert Mahler (my business supervisor)

Menasseh is experienced in cloud transitions and was able to illustrate many of the practical and organizational challenges that accompany cloud computing.

The interview is conducted for the VU Master Information Studies 2013-2014, master thesis project ‘Recommending Cloud Vendors’. The goal of the interview was to gain insight in the practice of cloud deployment and to validate the organizational criteria for CSP selection.

The interview was conducted in Dutch, the minutes of the interview will be drafted in English and sent to Menasseh for review.

The first part of the interview focuses on the cloud transition cases Mr. Rotteveel was involved in, and the applicable CSP selection criteria. Two cases were used as example:

- LOI (education) opted for Amsterdam based Vancis (part of SURF), and
- Leidsche verzekeringen, acquired by an USA based insurance company (RGA); CSC is their cloud provider.

Generally involved parties:
- Client: the business department decides on the transition; the ICT department implements. Furthermore, business departments are involved in testing.
- The CSP's sales department and the operational department are often not fully aligned on their actual capabilities.
- In addition to the Client and the CSP, other parties are involved in setting up the cloud deployment, e.g. cable providers. Also, securing connectivity costs a lot of effort.
- Sometimes companies that act as CSP are in reality intermediates between the CSP and the client (brokers).

Comments on required cloud services:
- Data security is very important, and this leads directly to requirements for the data center location of the CSP. For 'local' cloud deployment, the first choice is a Dutch datacenter, but another European country, e.g. Germany, is also possible.
- Self-service provisioning is technically difficult, while other CSPs and portals/cloud management software (e.g. CloudController, and vCenter) do not meet the 'standard' that AWS has set for self-service.
- Scalability capacity of smaller CSPs is often disappointing, as they have to order servers: e.g. the lead-time for Cisco blade servers is approx. 1 month.

23 http://nl.linkedin.com/in/menassehrotteveel
24 roel.remkes@choicecompany.nl
25 http://www.choicecompany.nl/
27 https://www.vancis.nl/
28 http://www.csc.com/cloud
29 in contrast with worldwide deployment requirements
31 http://www.vmware.com/products/vcenter-server/
32 http://aws.amazon.com/console/faqs/
Selection criteria:

1. The ownership of the data as well as the location of the data-storage is essential, often limiting the choice of CSP to those located in the Netherlands.
2. The level and degree of self-service the CSP offers
3. Security features and procedures
4. (Automated) Billing requires accurate metering; this is problematic due to inadequate/absence of interfaces with Cloud components such as VM's and data storage (e.g. TSM).33
5. Availability (‘continuiteit’): is the fill-over capacity identified accurately? Is disaster recovery organized (if requested by the client, as it is expensive)
6. Scalability capacity (actual capacity and realistic fulfillment?)
7. Capacity management which includes timely supplement of resources such as blades/UCS's/storage
8. Strategy - Technology edge. Technology is constantly improving with technologies such as Flexpod34, het Cisco Unified Computing System UCSD35, and Nutanix36.

At the end of the interview, the main model (decision level versus cluster) was shown and commented on:

Menasseh’s remarks on the model:
Cluster **Cloud Service (top):**
Advice to make this more explicit and distinguish sub-boxes (location, self service, capacity management and automated billing)

Cluster **CSP-Client-relation:**
Portability and use of standards:
A combination of proven design and proven technology leads to best practices / de facto standards; e.g. FlexPod

---

33 IBM Tivoli Storage Manager (IBM TSM) is an enterprise class backup and archiving application. IBM TSM, like all enterprise backup software products, is designed to make copies of an organization’s data to protect against data loss
34 FlexPod is a converged compute, networking, and storage solution developed by Cisco and NetApp
Summary of the interview
Case Study of CSP selection for ADA, a software development company

Interviewee: Micha van Haaren (ADA, Oosterhout, Micha.van.Haaren@ada-ict.nl)
Date/time: Wednesday July 16th 2014, 13.00-14.30
Interviewer: Renee Vaessen (VU, renee@komies.nl)

Mr. van Haaren works as operational manager for ADA\textsuperscript{37}, a Dutch software development company. Herman Kalse, owner/CEO of ADA, is a former classmate who I contacted and asked for an opportunity to interview one of his staff members. ADA is interesting as a case study for IaaS vendor selection, because they initially selected and deployed AWS and later transferred to I3D\textsuperscript{38} in the Rotterdam area.

The interview was in Dutch; the minutes of the interview will be drafted in English and sent to Micha for review.

The interview is conducted for the VU Master Information Studies 2013-2014, master thesis project ‘Recommending Cloud Vendors’\textsuperscript{39}. The goal of the interview is to validate the organizational criteria that influence the choice for (IaaS) cloud providers, for the ADA case.

AWS

\textit{Trigger and involved parties}

The first IaaS cloud deployment was initiated by a project that ADA executed for Post NL. The Post NL IT-architect and the ADA development team opted for AWS, as AWS was the only ‘mature’ IaaS at that moment, (2008).

Initial drivers for cloud deployment were short provisioning lead-time and lower costs for the development and test infrastructure; in addition, the 24/7 availability is in conformance with the ‘new world of work’ (het nieuwe werken) for the development team.

\textit{Migration and operations}

- AWS provisioned the configuration including the licenses and provided installers.
- Uploading the data took some time (1-2 days), this could have been omitted by transferring data (on tapes/discs) directly to AWS, but wasn’t necessary with regard to the project schedule.
- The performance of the AWS cloud was lower compared to the in-house servers.
- The account management was difficult, compared to in house deployment, because of the access control to the ‘active directory’. Setting up a VPN connection between AWS and ADA solved this (AWS now supports this functionality via a Virtual Private Cloud).

\textit{Evaluation of support and availability}

Getting support from AWS was not easy, a ‘ticket’ was submitted and no direct contact was possible (with the support contract available (PostNL has the contract with Amazon. ADA has a contract with PostNL to maintain the Amazon environment).

About 4 years ago, a breakdown of several hours occurred and VM’s/images went missing (but were retrieved a few days later). AWS limits liability and only ‘refunds’ the downtime as free service in the next payment period. The way availability is measured is also disputable.

\textit{Migration to I3D}

\textit{Trigger and involved parties}

Other companies recommended I3D. This CSP with worldwide locations has multiple clients, including big players in the gaming industry. Its main office and one of its datacenters is located

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{37} \url{www.adai-ct.nl}
\item \textsuperscript{38} \url{http://www.i3d.net/dedicated/}
\item \textsuperscript{39} \url{http://wiki.cs.vu.nl/mp/index.php/Recommending_Cloud_Vendors_%28Working_Title%29}
\end{itemize}
\end{footnotesize}
in Rotterdam and was visited before migrating. The cost level of I3D, was distinctively lower at the time of migration (between 20-40% of the AWS level, depending on configuration / software licenses.)

ADA still deploys AWS, for Post NL, but migrated its other development and test systems to I3D. The ADA deployment at I3D is a little different in nature from a standard, public cloud service: ADA deploys physical servers, without a virtualization layer; dedicated servers are added and removed on demand (co-location).

**Evaluation**

- Compared to AWS, the costs of the I3Ds services are distinctively lower and the performance is much better.
- The SLA is ‘best effort’ based, which is sufficient for development and testing.
- I3Ds support is very good: both as a good partner to work with (at sales/tactical level), as at the operational level, because of their expertise. Self-service provisioning is possible, in general ADA consults the account manager and technical staff of I3D and they execute the provisioning.

ADA intends to deploy their non-core administrative systems to SaaS, but that migration partly depends on the available resources (if they are not making billable hours)

**General remarks on lead-time and costs:**

- Shorter lead-time: as the suppliers don’t have stock anymore, the hardware often has to be ordered from the manufacturer, leading to several weeks of delay.
- Cloud services are relatively expensive: for a stable workload during a long period, hosting is less expensive.

**Feedback on initial model:**

The functional requirements and the QoS (=non functional requirements) for IaaS are available as a commodity. For provider selection, both the costs and the organizational factors are important

Next the main model (decision level versus cluster) was presented in general:

**CRITERIA FOR Cloud Service Provider SELECTION**

- **Compliance**
  - Compliance and governance capability
  - Certification / auditing
- **Operational governance**
- **Operational support & interoperability**
- **Service: functional requirements**
- **Service: QoS**
- **Service portfolio**
- **Service development**
- **Partnership**
- **Exit/entry support and portability**
- **Sustainability**
- **Cloud Service**
- **CSP-customer relation**
- **Strategic decisions**
- **Tactical decisions**
- **Operational decisions**
Micha's remarks on the model and criteria:
Cluster CSP-client relation

**Operational support (operational level):**
For ADA this is a very important criterion: I3D has a proven track record and attention for customer relations (a trustworthy contact person and good advice)

**Portability (tactical level):**
ADA foresees no specific challenges for their use cases.

Cluster Compliance:
The test data and applications ADA uses and develops are not very privacy sensitive; security compliance is not critical for their business.

On certification: sometimes the value of (commercial) certifications of a CSP can be deceptive, because of the commercial interests of the certifying organization.
ADA periodically evaluates the cloud services they deploy, on an ad hoc basis.
Interview topic: Clustering of organizational factors for CSP selection
Structure of interviews and related questions

Introduction
- Who am I, relation to VU master study, why I conduct this interview
- Why I invited this interviewee/how I use the results (thesis)/procedure for interviewee feedback (minutes, to be approved by interviewee)
- Structure of interview (introduction of model, validation of (steps and) content)

Background
- Background of research question: improvement of decision support
CSP selection, lots of operational criteria, security issues
Decision process, SME, IaaS
Sources:
Gartner, SMI (Service Measurement Index), European initiatives, partly in cooperation with commercial parties (e.g. ETSI, standardization; ENISA, security), etc...

- Initial model of vendor selection criteria:
Cloud service, consisting of
- Functional Requirements,
- QoS and
- Costs

Organizational factors are high level, general criteria, related to:
- the customers internal way of organizing cloud deployment
- the use cases at business level
- partnership / the level of collaboration between the customer organization and the CSP
- security, compliance and privacy requirements of the customer and the capability of the CSP to match these.

- Decision process level
Analysis of factors and criteria: distinct decision level, in order to support supplier selection:
- Strategic decisions (internal and external aligning, long term business goals)
- Tactical process: preferred supplier selection (allocation of resources)
- Operational (design and run time choices for deployment)

- Combination of these two models
Separate cluster of factors
- Cloud Service (including internal organization of deployment and business level of use case)
- Compliance
- CSP-customer relationship
- Sustainability?
FACTORS FOR CLOUD SERVICE PROVIDER SELECTION

• Cluster of factors
Clustering of factors:
Description bottom up and top down, as
• for operational criteria (often cited) higher level questions have to answered
• mayor issues like portability and vendor lock in, security are important and have to be clarified in order to stop talking about muddy concepts

Blocks
• Service
Center cluster: service (non-limiting list)
1. on operational level described as service, with a subdivision in
   • Functional characteristics of the individual services
   • Quality characteristics (QoS) of the individual IaaS configuration
   • The cost of deployment of the individual IaaS configurations, operational billing process,
2. on tactical level described as service portfolio, the subdivision is still partially important
   • Innovation capability, agility of CSP to respond to customers/installed base changes in functional requirements
   • Capabilities of CSP to ensure availability and performance
   • The pricing tactics of the CSP, match of billing process with internal financial process, currency,
3. on strategic level described as service development
   • Product development and strategy, related to competition and partners, knowledge of industry, innovation capability
   • Strategy to execute operations with regard to service portfolio, geography, market share
   • The pricing strategy of the CSP, related to competition and partners

• Compliance
Adjacent cluster on the right: compliance (including security and privacy, certification and governance) (non-limiting list)
• Security
• compliance (legal constraints)
• governance policies of CSP
1. on operational level described as **operational governance** compliance and governance capability
   - SLA verification (logging)
   - Access control, privilege management
   - Disaster recovery measures (and reporting)
2. on tactical level described as **certification/auditing**
   - data ownership,
   - data privacy and data loss protection capability
   - security management of CSP
   - disaster recovery capability
   - standardization activities and incorporation
3. on strategic level described as **compliance and governance capability**
   - CSP supply chain liability
   - governance policies of CSP

   **CSP-customer relation**

Adjacent cluster on the left: CSP-customer relationship (non-limiting list)
1. on operational level described as **operational support and interoperability**
   - customer experience / usability
   - Support for operational problems (availability, response time, support options, costs
   - Knowledge of support-employees
   - Training opportunities for end user employees
   - Availability of documentation, community forum
   - (multi-) language support?
2. on tactical level described as **Exit/entry support and portability**
   - Trial period opportunity
   - Benchmarking support
   - Portability options/support
   - Customer relations management (Sales process, Account management, Contract management)
   - Geographic locations of offices (contact/visits)
3. on strategic level described as **partnership**
   - long term partnership with strategic support or portability as important requirements,
   - Customer support with ancillary tools, DevOps, standards for portability, ....

   **Sustainability issues**

1. CSP-sustainability (CSR, Corporate Sustainability Responsibility)
   - Certification
   - Sustainability activities
   - Track record
Holistic approach of CIPL method can prevent setbacks in deployment

Cloud is here to stay. Increasingly so companies explore cloud solutions to see if they offer opportunities for optimization of their business processes. Today this is often limited to contracting extra computing facilities for development and testing on an on demand basis and pay per use base. But cloud solutions are also getting a foothold in the area of the primary business processes. For example with solutions to facilitate the process when demand is extreme (both low or high). Furthermore cloud solutions facilitate sharing of system and data between different companies. This feature is interesting when evaluating strategic partnerships.

Planning horizon in a wider perspective
Complexity involved when solving capacity problems by contracting a cloud solution is relatively low. However when deploying cloud applications (SaaS) complexity of business decisions involved demands an approach that takes into account a wider and multi-disciplinary perspective and a longer term time frame. An example is deployment of the popular CRM-service offered by Salesforce. Deploying this solution impacts several departments in the company, bringing optimization opportunities but also pitfalls. CIPL (Cloud Implementation and Procurement Library) offers a step-wise approach for implementation that takes into account all effects for the company in both short and long run. CIPL uses available best practices and organises adaption of proven new practice within its framework. Key design principles are Management, Governance, Single sign on and Any device (any time, any place).

CIPL approach: a four phases model:
Cloud Readiness assessment: Gives instruments to analyse business issues. The outcome of this phase is a typification of the primary processes of the company. This typification corresponds with an appropriate cloud scenario. Second a cloud maturity assessment is executed. The company cloud strategy follows from the cloud scenario and maturity.
Generic cloud policy: The strategy is worked out by the different business disciplines such as IT, finance, marketing, security, sales, ... CIPL refers to the set of resulting guidelines as the "Policy set" Specific cloud policy: In this phase the focus is on a selected business process that is a candidate for implementation of a cloud solution. Implementation aspects and the governance of the process are analyzed. The generic policy set is translated to a "Control set" for this specific business process. Part of the specific implementation is an implementation of support processes. CIPL uses a template in which all support processes are specified, called the ECBP. (Enterprise Cloud Beheer Platform). Relevant parts for the specific implementation can be selected from the ECBP.
Specific business process implementation: planned and systematic accomplishment of the required changes in the business process at hand. The part of the control set that rules the implementation of the selected cloud solution is called the "Config set".
APPENDIX C
Renee Vaessen VU University Master Information Sciences, 2013-2014

APPENDIX C
The underlying data are captured in an Excel file with several worksheets; one for each source (for references, see appendix D). The CSP or service properties are coded according to the axes in the framework. This resulted in 4 worksheets, one for each cluster, with a list of properties and criteria, ordered by decision level.

Sources:

- **Gartner MQ** (Gartner, 2013 b) and (Gartner, 2013 c)
- **Gartner 2013 Cloud** contracts need **security** service levels (Gartner, 2013 a)
- **Gartner/Leong Critical Capabilities** for public Cloud IaaS (Gartner/Leong, L., 2013)
- **SMI**, from **CSMIC** (CSMIC, 2014)
- **Repschläger 2011** (Repschläger, Wind, Zarnekow, & Turowski, 2011)
- **Repschläger 2013** (Repschläger, Erek, & Zarnekow, 2013)
- **Muntes-Mulero** (Muntes-Mulero, Matthews, Omerovic, & Gunka, 2013)
- **Flexiant** Flexiant. (no year).
- **GCLOUD Government UK** (G-Cloud, no year), (G-Cloud, 2014)
- **Plan for Cloud** from RightScale , (RightScale PlanForCloud, 2014)
- **ETSI** (ETSI, 2013)
## APPENDIX C

Renee Vaessen  
VU University Master Information Sciences, 2013-2014

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>CHARACTERISTIC</th>
<th>DECISION LEVEL</th>
<th>CLUSTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSMIC</td>
<td>1-Provider business stability</td>
<td>1</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>2-Contracting experience</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>3-Provider Ethicality</td>
<td>3</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>4-Provider Personnel Requirements</td>
<td>4</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>5-Transparency</td>
<td>5</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>1-11 negotiation of master agreement</td>
<td>1</td>
<td>A</td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>1-5 data return</td>
<td>1</td>
<td>A</td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>1-6 date deletion (end contract)</td>
<td>1</td>
<td>A</td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>2-1 widely used ICT technology</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>2-12 vendor lock-in</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>2-2 multi cloud interoperability</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>2-3 portability</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>2-11 data deletion and exit</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>2-11 responsibility ambiguity</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>2-10 liability for incidents</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>2-20 migration costs</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>03a-sales execution</td>
<td>0</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>10-Sales strategy</td>
<td>1</td>
<td>A</td>
</tr>
<tr>
<td>Government UK 2014</td>
<td>3b account management</td>
<td>3</td>
<td>A</td>
</tr>
<tr>
<td>Government UK 2014</td>
<td>Consultancy</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>Government UK 2014</td>
<td>Free trials</td>
<td>2</td>
<td>A</td>
</tr>
<tr>
<td>Muntes-Muñero 2013</td>
<td>3-migration costs and complexity</td>
<td>3</td>
<td>A</td>
</tr>
<tr>
<td>Muntes-Muñero 2013</td>
<td>7-customization of SLA</td>
<td>7</td>
<td>A</td>
</tr>
<tr>
<td>Repschaegler 2013</td>
<td>10-Set-up time</td>
<td>10</td>
<td>A</td>
</tr>
<tr>
<td>Repschaegler 2013</td>
<td>11-Lock-in</td>
<td>11</td>
<td>A</td>
</tr>
<tr>
<td>Repschaegler 2013</td>
<td>11-Negotiation</td>
<td>11</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>5-Interoperability</td>
<td>5</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>1-Ease of doing business</td>
<td>1</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>7-Client personnel requirements</td>
<td>7</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>7-Instability</td>
<td>7</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>7-Learnability</td>
<td>7</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>7-Operability</td>
<td>7</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>7-Understandability</td>
<td>7</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>6-Retention/Disposition</td>
<td>6</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>7-Client personnel requirements</td>
<td>7</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>7-Instability</td>
<td>7</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>7-Learnability</td>
<td>7</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>7-Operability</td>
<td>7</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>7-Understandability</td>
<td>7</td>
<td>A</td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>24-interoperability with standards for API’s data</td>
<td>24</td>
<td>A</td>
</tr>
<tr>
<td>FLEXVANT</td>
<td>4-Multi-language support</td>
<td>4</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>4-User management</td>
<td>4</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>9-API</td>
<td>9</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>06-Customer experience</td>
<td>06</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>07-Operations</td>
<td>07</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>5-Enterprise integration</td>
<td>5</td>
<td>A</td>
</tr>
<tr>
<td>CSMIC</td>
<td>9-API</td>
<td>9</td>
<td>A</td>
</tr>
<tr>
<td>Government UK 2014</td>
<td>3a after sales service help desk</td>
<td>3a</td>
<td>A</td>
</tr>
<tr>
<td>Muntes-Muñero 2013</td>
<td>1-vendor lock-in due to unavailability of alternative services</td>
<td>1</td>
<td>A</td>
</tr>
<tr>
<td>PlanForCloud 2014</td>
<td>2-1 ticket system</td>
<td>2-1</td>
<td>A</td>
</tr>
<tr>
<td>PlanForCloud 2014</td>
<td>2-2 phone</td>
<td>2-2</td>
<td>A</td>
</tr>
<tr>
<td>PlanForCloud 2014</td>
<td>2-3 email</td>
<td>2-3</td>
<td>A</td>
</tr>
<tr>
<td>PlanForCloud 2014</td>
<td>2-4 response time</td>
<td>2-4</td>
<td>A</td>
</tr>
<tr>
<td>PlanForCloud 2014</td>
<td>3 monthly costs of support</td>
<td>3</td>
<td>A</td>
</tr>
<tr>
<td>Repschaegler 2011</td>
<td>1-provisioning time</td>
<td>1</td>
<td>A</td>
</tr>
<tr>
<td>Repschaegler 2011</td>
<td>6-support</td>
<td>6</td>
<td>A</td>
</tr>
<tr>
<td>Repschaegler 2011</td>
<td>6-usability</td>
<td>6</td>
<td>A</td>
</tr>
<tr>
<td>Repschaegler 2013</td>
<td>01-Internationality (language support)</td>
<td>01</td>
<td>A</td>
</tr>
<tr>
<td>Repschaegler 2013</td>
<td>01-Support services</td>
<td>01</td>
<td>A</td>
</tr>
<tr>
<td>Repschaegler 2013</td>
<td>05-Customer support</td>
<td>05</td>
<td>A</td>
</tr>
<tr>
<td>Repschaegler 2013</td>
<td>06-External integration capabilities</td>
<td>06</td>
<td>A</td>
</tr>
<tr>
<td>Repschaegler 2013</td>
<td>07-Manageability</td>
<td>07</td>
<td>A</td>
</tr>
<tr>
<td>Repschaegler 2013</td>
<td>10-Provisioning time</td>
<td>10</td>
<td>A</td>
</tr>
<tr>
<td>Repschaegler 2013</td>
<td>12-Service-ability</td>
<td>12</td>
<td>A</td>
</tr>
</tbody>
</table>
## APPENDIX C

Renee Vaessen

VU University Master Information Sciences, 2013-2014

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>CHARACTERISTIC</th>
<th>DECISION LEVEL</th>
<th>CLUSTER</th>
<th>SUB-CLUSTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gartner MQ 2013 b.c</td>
<td>1. market responsiveness &amp; track</td>
<td>1 B</td>
<td>B</td>
<td></td>
</tr>
<tr>
<td>Gartner MQ 2013 b.c</td>
<td>11. Offering product strategy</td>
<td>1 B</td>
<td>B</td>
<td></td>
</tr>
<tr>
<td>Gartner MQ 2013 b.c</td>
<td>13. Vertical Industry strategy</td>
<td>1 B</td>
<td>B</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>4. Financial Structure</td>
<td>2 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>FLEXIANT</td>
<td>7. Support for multi-currency billing</td>
<td>2 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>2. Price classes</td>
<td>2 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>2. Price resilience</td>
<td>2 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>2. Price options</td>
<td>2 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>2. Charging type</td>
<td>2 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2013</td>
<td>2. Price range</td>
<td>2 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2013</td>
<td>2. Price stability</td>
<td>2 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>2. Adaptability</td>
<td>2 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>2. Extensibility</td>
<td>2 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>FLEXIANT</td>
<td>5. Self service provisioning</td>
<td>2 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>FLEXIANT</td>
<td>8. Differentiation</td>
<td>2 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Gartner 2013 a Cloud security service levels</td>
<td>8a. additional risk control internally, eg encryption</td>
<td>2 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Gartner/Leong 2013 critical capabilities</td>
<td>2. Architectural flexibility</td>
<td>2 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Gartner/Leong 2013 critical capabilities</td>
<td>4. Automation and DevOps enablement</td>
<td>2 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Gartner/Leong 2013 critical capabilities</td>
<td>6. Big data enablement</td>
<td>2 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Government UK 2014</td>
<td>3c. Portfolio of cloud services</td>
<td>2 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>3d. Add-on services</td>
<td>2 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>4. Connection opportunity</td>
<td>2 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2013</td>
<td>03. Portability</td>
<td>2 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>2. Scalability</td>
<td>2 B</td>
<td>F, Q</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>5. Data center redundancy</td>
<td>2 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>5. Network redundancy</td>
<td>2 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>2. Elasticity</td>
<td>2 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>2. Flexibility</td>
<td>2 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repschläger 2013</td>
<td>01. Market coverage</td>
<td>2 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repschläger 2013</td>
<td>01. Service offering</td>
<td>2 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>4. Cost</td>
<td>3 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>FLEXIANT</td>
<td>1. Accurate metering of resource usage</td>
<td>3 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Government UK 2014</td>
<td>1. Whole life cost</td>
<td>3 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Muntey-Mulero 2013</td>
<td>4. Unpredictability of costs</td>
<td>3 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>2. Payment options</td>
<td>3 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>2. Payment method</td>
<td>3 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>2. Charging granularity</td>
<td>3 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2013</td>
<td>02. Transparency</td>
<td>3 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2013</td>
<td>03. Flexible payments</td>
<td>3 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2013</td>
<td>04. Booking</td>
<td>3 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2013</td>
<td>04. Invoicing</td>
<td>3 B</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>5. Functionality</td>
<td>3 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>5. Suitability</td>
<td>3 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>7. Accessibility</td>
<td>3 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Government UK 2014</td>
<td>2b. Functional fit</td>
<td>3 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>3. Multi-tenancy</td>
<td>3 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>3. Instance type</td>
<td>3 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>6. Customising options of web portal</td>
<td>3 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2013</td>
<td>06. Internal integration capabilities:</td>
<td>3 B</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>3. Resilience/Fault Tolerance</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>3. Service stability</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>3. Availability</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>3. Maintainability</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>3. Recoverability</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>3. Reliability</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>3. Serviceability</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>5. Accuracy</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>CSMC 2014</td>
<td>5. Service Response Time</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>ETIS 2013</td>
<td>5-12 availability</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>ETIS 2013</td>
<td>5-13 integrity</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Gartner/Leong 2013 critical capabilities</td>
<td>7. Scalability</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Gartner/Leong 2013 critical capabilities</td>
<td>1. Compute resilience</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Government UK 2014</td>
<td>2a. Technical merit</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Government UK 2014</td>
<td>4. Non functional characteristics</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>3. Load balancing</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>3. Network access, connection bandwidth</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>3. Instance capacity</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2013</td>
<td>05. Reliability (reactive)</td>
<td>3 B</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>1. Network configuration</td>
<td>3 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>1. Changes/updates</td>
<td>3 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>1. System management</td>
<td>3 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>1. Resource scalability</td>
<td>3 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>1. Instance customizing</td>
<td>3 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>1. Virtualization</td>
<td>3 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>3. Storage service</td>
<td>3 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>3. Computing time</td>
<td>3 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repschläger 2011</td>
<td>6. System management</td>
<td>3 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Repschläger 2013</td>
<td>07. Scalability</td>
<td>3 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOURCE</td>
<td>CHARACTERISTIC</td>
<td>DECISION_LEVEL</td>
<td>CLUSTER</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>----------------</td>
<td>----------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>CSMIC 2014</td>
<td>1-Provider Supply Chain</td>
<td>1</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>3-04 assurance</td>
<td>1</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2011</td>
<td>5-liability and penalties</td>
<td>1</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2013</td>
<td>08-IT security</td>
<td>1</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2013</td>
<td>08-Quality management</td>
<td>1</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CSMIC 2014</td>
<td>1-Audiability</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CSMIC 2014</td>
<td>1-Provider Certifications</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CSMIC 2014</td>
<td>6-Proactive Threat &amp; Vulnerability Management</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CSMIC 2014</td>
<td>1-Governance</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>1-2 extra SLA objectives</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>1-4 SLA dispute</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>3-01 cross border legal issues</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>3-03 transapancy</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>3-05 certification</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>3-06 auditing</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>3-10 data location</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>3-16 forensic auditing</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>3-17 assurance against control loss</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Gartner 2013 a Cloud security service levels</td>
<td>1-annual audit and certification</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Gartner 2013 a Cloud security service levels</td>
<td>4b-additional risk control externally eg cloud security brokers</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Gartner 2013 a Cloud security service levels</td>
<td>2b-data integrity measures</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Gartner/Leong 2013 critical capabilities</td>
<td>3-Security and compliance</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>PlanForCloud 2014</td>
<td>1 certification</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2011</td>
<td>1-standardization</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2011</td>
<td>2-price transparency</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2011</td>
<td>5-disaster recovery</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2011</td>
<td>5-auditing</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2011</td>
<td>5-service transparency</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2011</td>
<td>5-availability</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2011</td>
<td>6-reporting and monitoring services</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2013</td>
<td>01-Certifications:</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2013</td>
<td>05-Reliability (pro-active):</td>
<td>2</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CSMIC 2014</td>
<td>6-Security Management</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CSMIC 2014</td>
<td>1-Compliance</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CSMIC 2014</td>
<td>6-Access Control &amp; Privilege Management</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CSMIC 2014</td>
<td>6-Data Integrity</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CSMIC 2014</td>
<td>6-Data Privacy &amp; Data Loss</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CSMIC 2014</td>
<td>6-Physical &amp; Environmental Security</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>1-3 monitoring of KPI</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>3-07 identity and access management</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>3-08 licences, services of other providers</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>3-09 multy tenancy and virtualization</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>3-14 confidentiality</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ETSI 2013</td>
<td>3-15 compliance</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Gartner 2013 a Cloud security service levels</td>
<td>2a-recovery time and recovery points</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Gartner 2013 a Cloud security service levels</td>
<td>2b- penalties if measures are missed</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Gartner MQ 2013 b.c</td>
<td>07-Operations</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Gartner/Leong 2013 critical capabilities</td>
<td>4-User management</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Munes-Mulerio 2013</td>
<td>2-security breach due to complexity</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Munes-Mulerio 2013</td>
<td>6-non-repudiation and accountability</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2011</td>
<td>4-hardware and software security</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2011</td>
<td>4-data protection</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2011</td>
<td>4-connection security</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2011</td>
<td>5-provider reporting</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2011</td>
<td>6-controlling</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Repsclaeger 2013</td>
<td>09-Reporting</td>
<td>3</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>FLEXIANT</td>
<td>2. High levels of white labelling and customization (resellers related)</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FLEXIANT</td>
<td>6. Highly automated workflow processes (resellers related)</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FLEXIANT</td>
<td>7. High levels of flexibility (resellers related)</td>
<td>C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### APPENDIX C

Renee Vaessen  
**VU University Master Information Sciences, 2013-2014**

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>CHARACTERISTIC,</th>
<th>DECISION LEVEL</th>
<th>CLUSTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSMIC 2014</td>
<td>1-Provider Ethicality</td>
<td>1</td>
<td>D</td>
</tr>
<tr>
<td>CSMIC 2014</td>
<td>1-Sustainability</td>
<td>2</td>
<td>D</td>
</tr>
</tbody>
</table>

**decision level** 1=strategic, 2=tactical, 3=operational

**Cluster** A=CSP-Client, B=Cloud Service, C=Compliance, D=sustainability

**Subcluster** F= functional requirement, Q=Quality of service, C=cost (if applicable)
APPENDIX D

Renee Vaessen
VU University Master Information Sciences, 2013- 2014

APPENDIX D
Content and naming of organizational characteristics

Different names for the properties and decision criteria on the organizational level

- Gartner MQ (Gartner, 2013 b) and (Gartner, 2013 c)
  - evaluation criterion
- Gartner Cloud contracts need security service levels (Gartner, 2013 a)
  - security service levels for cloud contracts
- Gartner Critical Capabilities for public Cloud IaaS (Gartner / Leong, 2013)
  - Capabilities, grouped in categories
- SMI (CSMIC, 2014)
  - category and
  - attributes,
  - KPIs to be defined
- Repschlager (Repschlaeger, Wind, Zarnekow, & Turowski, 2011)
  - Target dimensions,
  - abstract and operative classification criteria,
  - requirements/KPIs (at provider level or at service level)
- Repschlager (Repschlaeger, Erek, & Zarnekow, 2013)
  - Factor labels
  - customer preferences = provider capabilities/properties
- Muntes-Mulero (Muntes-Mulero, Matthews, Omerovic, & Gunka, 2013)
  - Risks, in addition to Quality of Service and costs (and Functional Requirements)
- Flexiant (Flexiant, no year)
  - From the viewpoint of the service provider: capabilities
- GCLOUD UK (G-Cloud, no year), (G-Cloud, 2014)
  - Criterium
- Plan for Cloud from RightScale , (RightScale PlanForCloud, 2014)
  - Support services and security certifications
- ETSI (ETSI, 2013)
  - Concern, issue, risk and challenge
GARTNER MQ 2013 EVALUATION CRITERIA and DEFINITION
From Gartner 2013 Magic Quadrant for IaaS (Gartner, 2013 c) and Magic Quadrant for European Hosting (Gartner, 2013 b)

Ability to Execute
1- **Product/Service:** Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

2- **Overall Viability (Business Unit, Financial, Strategy, Organization):** Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

3- **Sales Execution/Pricing:** The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

4 - **Market Responsiveness and Track Record:** Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

5- **Marketing Execution:** The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This mind share can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth, and sales activities.

6- **Customer Experience:** Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, SLAs, and so on.

7- **Operations:** The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems, and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision
8- **Market Understanding:** Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

9- **Marketing Strategy:** A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

10- **Sales Strategy:** The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

11- **Offering (Product) Strategy:** The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

12- **Business Model:** The soundness and logic of the vendor's underlying business proposition.

13- **Vertical/Industry Strategy:** The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

14- **Innovation:** Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

15- **Geographic Strategy:** The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

The Gartner evaluation criteria are focused on enterprise IaaS use; for SME's, the time frame and scale of IaaS deployment are smaller and the portability issues probably too.
GARTNER security service levels for cloud contracts
From Gartner Cloud contracts need security service levels (Gartner, 2013 a)
Primarily for SaaS, USA focus, enterprise

• SaaS contracts should allow for annual security audit and certification, by a third party; option to terminate contract if lack of compliance
• Include in SLA: recovery time and recovery points, data integrity measures (and penalties if measures are missed)
• Fee liability limits: negotiate for a longer period than the usual 12 months, and additional liability insurance of provider
• In addition to contracts, risk control should be improved by other control forms, e.g. encryption and cloud security brokers (gateways)
GARTNER Critical Capabilities 2013 EVALUATION CRITERIA and DEFINITION

From Gartner – Lydia Leong 2013 Critical Capabilities for Public Cloud Infrastructure as a Service (Gartner/Leong, L., 2013)
USA focus, enterprise

Recommendations

- Try several offerings before committing to any one service. Many public cloud IaaS offerings can be bought by the hour, without any contractual commitment.
- Assume that cloud IaaS offerings are not interchangeable, and that where you place a workload will be where it stays. Although there can be relatively little “lock-in” for public cloud IaaS, moving between providers is similar to doing a data center move; it can be time-consuming, expensive and risky. Consider the strategic future of a provider before migrating a significant, percentage of your applications into its cloud.
- Use cloud IaaS to drive IT transformation, not just to get VMs quickly. Many providers have features that can help you to drive more automated IT infrastructure, improve the quality of operations and transform toward a DevOps philosophy. While adoption of these features typically increases lock-in, it also significantly enhances the value you receive from the service.

Notes on division and scoring:
It is important to note that these are broad categories, not granular capabilities; they are inclusive of a range of features, and we do not provide a comprehensive list of these features. Because each of the categories includes a large number of features, the scoring in each category is directional. In general, a score of 3 indicates that a provider is able to fulfill the most critical features in that category. However, it is possible that a provider may be missing some important features in that category, yet has other strengths that increase its score in that category. You will need to conduct an in-depth evaluation of your shortlisted providers in order to determine whether they meet your specific needs.

Compute resilience

This category encompasses features that are important for VM availability, such as fast VM restart (rapid detection of physical host failure and automatic restart of the VMs on another host), reduction of maintenance downtime through live migration of VMs, and automated replication across data centers. While the availability of the control plane and other resource elements are considered here, the emphasis is strongly on VM availability, which is important for workloads that assume infrastructure resilience. Most non-cloud-native applications are architected with the assumption of compute resilience, and most enterprise virtualization environments take advantage of the compute resilience features of the hypervisor.

Architectural flexibility

This category encompasses features that provide a customer with a breadth of resource types and architectures. This includes elements such as flexible VM sizes, "bare metal" servers, complex network topologies and multiple tiers of storage.

Security and compliance

This category encompasses features that are important to security, compliance, risk management and governance. It covers specific security measures such as network access control lists (ACLs), intrusion detection and prevention systems (IDS/IPS), multifactor authentication and encryption. It also includes aspects such as the availability of audits, logging and reporting, and the ability to use the service if you have regulatory compliance needs, such as those of the Payment Card Industry Data Security Standard (PCI DSS), the Federal Information Security Management Act (FISMA) and the Health Insurance Portability and Accountability Act (HIPAA).
User management
This category encompasses features that are necessary to provision and govern multiple users of the service, particularly if you have large development, engineering or research teams. It covers aspects such as role-based access control, quotas, leases and integration with enterprise directory services.

Enterprise integration
This category encompasses features that are needed to operate in a "hybrid IT" environment. That includes secure extension of the organization’s WAN, data migration features and workload migration features.

Automation and DevOps enablement
This category encompasses IT operations management (ITOM) features, particularly those necessary to manage infrastructure in a DevOps fashion. It includes aspects such as the service catalog, templates, application life cycle management (ALM) and metadata tagging. It also includes additional complementary services, such as monitoring and database as a service.

Scaling
This category encompasses features related to scaling applications and workloads. It includes aspects such as load balancing, auto-scaling, resizing of existing VMs and speed of provisioning.

Big data enablement
This category encompasses features that are typically desired for large-scale data processing, such as access to large VM sizes, large quantities of capacity on demand and graphics processing units (GPUs). It also covers capabilities such as object storage and Hadoop as a service. ("Big data" is used as a convenient catch-all label for this criterion, rather than literally encompassing big-data-specific capabilities.)

API.
This category indicates the comprehensiveness of the API and its ability to provide full access to the provider’s range of capabilities. Aspects such as the availability of the control plane and API, and its responsiveness to a large number and high rate of requests, are also considered.
CSMI Service Measurement Index business relevant KPIs
FROM SMI (CSMIC, 2014)
The Service Measurement Index (SMI) is a set of business-relevant Key Performance Indicators (KPIs) that provide a standardized method for measuring and comparing a business service regardless of whether that service is internally provided or sourced from an outside company. It is designed to become a standard method to help organizations measure cloud-based business services based on their specific business and technology requirements. The Cloud Services Measurement Initiative Consortium develops the SMI.
The measurement spaces are divided into 7 top-level categories, each refined by several attributes. Currently, work is ongoing on the definition of the KPIs and measures related to the attributes. Some of these KPIs will be service specific while others will apply to all services (BPaaS, IaaS, PaaS, and SaaS) (CSMIC, 2014, p. 2)

1-Accountability
This category contains attributes used to measure the properties related to the cloud service provider organization. These properties may be independent of the service being provided.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>SMI Attribute Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditability</td>
<td>The ability of a client to verify that the cloud service provider is adhering to the standards, processes, and policies that they follow.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Standards, processes, and policies committed to by the cloud service provider are followed.</td>
</tr>
<tr>
<td>Contracting experience</td>
<td>Indicators of client effort and satisfaction with the process of entering into the agreements required to use a service.</td>
</tr>
<tr>
<td>Ease of doing business</td>
<td>Client satisfaction with the ability to do business with a cloud service provider.</td>
</tr>
<tr>
<td>Governance</td>
<td>The processes used by the cloud service provider to manage client expectations, issues and service performance.</td>
</tr>
<tr>
<td>Ownership</td>
<td>The level of rights a client has over client data, software licenses, and intellectual property associated with a service.</td>
</tr>
<tr>
<td>Provider business stability</td>
<td>The likelihood that the cloud service provider will continue to exist throughout the contracted term.</td>
</tr>
<tr>
<td>Provider Certifications</td>
<td>The cloud service provider maintains current certifications for standards relevant to their clients’ requirements.</td>
</tr>
<tr>
<td>Provider Contract/SLA Verification</td>
<td>The cloud service provider makes available to clients SLAs adequate to manage the service and mitigate risks of service failure.</td>
</tr>
<tr>
<td>Provider Ethicality</td>
<td>Ethicality refers to the manner in which the cloud service provider conducts business; it includes business practices and ethics outside the scope of regulatory compliance. Ethicality includes fair practices with suppliers, clients, and employees.</td>
</tr>
<tr>
<td>Provider Personnel Requirements</td>
<td>The extent to which cloud service provider personnel have the skills, experience, education, and certifications required to effectively deliver a service.</td>
</tr>
<tr>
<td>Provider Supply Chain</td>
<td>The cloud service provider ensures that any SLAs that must be supported by its suppliers are supported.</td>
</tr>
<tr>
<td>Sustainability</td>
<td>The impact on the economy, society and the environment of the cloud service provider.</td>
</tr>
</tbody>
</table>

2-Agility
Indicates the impact of a service upon a client’s ability to change direction, strategy, or tactics quickly with a minimal disruption.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>SMI Attribute Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptability</td>
<td>The ability of the cloud service provider to adjust to changes in client requirements.</td>
</tr>
<tr>
<td>Elasticity</td>
<td>The ability of a cloud service provider to adjust its resource consumption for a service at a rapid enough rate to meet client demand.</td>
</tr>
<tr>
<td>Extensibility</td>
<td>The ability to add new features or services to existing services.</td>
</tr>
<tr>
<td>Flexibility</td>
<td>The ability to add or remove predefined features from a service.</td>
</tr>
<tr>
<td>Portability</td>
<td>The ability of a client to easily move a service from one cloud service provider to another with minimal disruption.</td>
</tr>
</tbody>
</table>
### 3-Assurance
This category includes key attributes that indicate how likely it is that the service will be available as specified.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>SMI Attribute Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>The appropriateness of the service availability window, as well as the likelihood that the availability window will actually be provided to clients.</td>
</tr>
<tr>
<td>Maintainability</td>
<td>Maintainability refers to the ability for the cloud service provider to make modifications to the service to keep the service in a condition of good repair.</td>
</tr>
<tr>
<td>Recoverability</td>
<td>Recoverability is the degree to which a service is able to quickly resume a normal state of operation after an unplanned disruption.</td>
</tr>
<tr>
<td>Reliability</td>
<td>Reliability reflects measures of how a service operates without failure under given conditions during a given time period.</td>
</tr>
<tr>
<td>Resiliency/Fault Tolerance</td>
<td>The ability of a service to continue to operate properly in the event of a failure in one or more of its components.</td>
</tr>
<tr>
<td>Service stability</td>
<td>The degree to which the service is resistant to change, deterioration, or displacement.</td>
</tr>
<tr>
<td>Serviceability</td>
<td>The ease and efficiency of performing maintenance and correcting problems with the service.</td>
</tr>
</tbody>
</table>

### 4-Financial
The amount of money spent on the service by the client.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>SMI Attribute Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Billing Process</td>
<td>The level of integration that is available between the client and cloud service provider’s billing systems and the predictability of periodic bills.</td>
</tr>
<tr>
<td>Cost</td>
<td>The client’s cost to consume a service over time. This includes cost of transition of the service along with recurring costs (e.g., monthly access fees) and usage based costs.</td>
</tr>
<tr>
<td>Financial Agility</td>
<td>The flexibility and elasticity of the financial aspects of the CSPs services.</td>
</tr>
<tr>
<td>Financial Structure</td>
<td>How responsive to the client’s needs are the cloud service provider’s pricing and billing components.</td>
</tr>
</tbody>
</table>

### 5-Performance
This category covers the features and functions of the provided services.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>SMI Attribute Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>The extent to which a service adheres to its requirements.</td>
</tr>
<tr>
<td>Functionality</td>
<td>The specific features provided by a service.</td>
</tr>
<tr>
<td>Suitability</td>
<td>How closely the capabilities of the proposed service match the features needed by the client.</td>
</tr>
<tr>
<td>Interoperability</td>
<td>The ability of a service to easily interact with other services (from the same cloud service provider and from other cloud service providers).</td>
</tr>
<tr>
<td>Service Response Time</td>
<td>An indicator of the time between when a service is requested and when the response is available.</td>
</tr>
</tbody>
</table>

### 6-Security and Privacy
This category includes attributes that indicate the effectiveness of a cloud service provider’s controls on access to the services, service data, and the physical facilities from which services are provided.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>SMI Attribute Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control &amp; Privilege Management</td>
<td>Policies and processes in use by the cloud service provider to ensure that only the personnel granted appropriate privileges can make use of or modify data/work products.</td>
</tr>
<tr>
<td>Data Geographic/Political</td>
<td>The client’s constraints on service location based on geographic or political risk.</td>
</tr>
</tbody>
</table>
• **Data Integrity**  Keeping the data that is created, used, and stored in its correct form so that clients may be confident that it is accurate and valid.

• **Data Privacy & Data Loss**  Client restrictions on use and sharing of client data are enforced by the cloud service provider. Any failures of these protections are promptly detected and reported to the client.

• **Physical & Environmental Security**  Policies and processes in use by the cloud service provider to protect the provider facilities from unauthorized physical access, damage or interference.

• **Proactive Threat & Vulnerability Management**  Mechanisms in place to ensure that the service is protected against known recurring threats as well as new evolving vulnerabilities.

• **Retention/Disposition**  The cloud service provider’s data retention and disposition processes meet the clients' requirements.

• **Security Management**  The capabilities of cloud service providers to ensure application, data, and infrastructure security based on the security requirements of the client.

7-Usability

The ease with which a service can be used

<table>
<thead>
<tr>
<th>Attribute</th>
<th>SMI Attribute Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessibility</td>
<td>The degree to which a service is operable by users with disabilities.</td>
</tr>
<tr>
<td>Client Personnel Requirements</td>
<td>The minimum number of personnel satisfying roles, skills, experience, education, and certification required of the client to effectively utilize a service.</td>
</tr>
<tr>
<td>Installability</td>
<td>Installability characterizes the time and effort required to get a service ready for delivery (where applicable).</td>
</tr>
<tr>
<td>Learnability</td>
<td>The effort required of users to learn to use the service.</td>
</tr>
<tr>
<td>Operability</td>
<td>The ability of a service to be easily operated by users.</td>
</tr>
<tr>
<td>Transparency</td>
<td>The extent to which users are able to determine when changes in a feature or component of the service occur and whether these changes impact usability.</td>
</tr>
<tr>
<td>Understandability</td>
<td>The ease with which users can understand the capabilities and operation of the service.</td>
</tr>
</tbody>
</table>
Target dimensions and classification criteria (Repschlaeger 2011)

(Repschlaeger, Wind, Zarnekow, & Turowski, 2011) define 6 target dimensions (level 1), each with their abstract and operative classification criteria (level 2 and 3). At the 3rd level, criteria have to be operationalized, in order to be weighted and compared (p 170). At the 4th level, requirements/KPIs are defined, as provider requirements or service
Factors: Provider capabilities or properties and customer preferences (Repschlaeger 2013)

(Repschlaeger, Erek, & Zarnekow, 2013) distinguish 12 factors, aggregated from 51 provider properties.

1 Market penetration & service portfolio
   - Support services: individual consulting services, migration and implementation support, training services
   - Service offering: service bundles (user categories, groups of functionality etc.), add-on services of the provider (e.g. security or collaboration services)
   - Market coverage: number of customers, service adoption of other providers (e.g. Integration of Google Apps by Salesforce)
   - Internationality: support of multiple languages
   - Certifications: e.g., ISO 27001, SAS70

2 Pricing & transparency
   - Price range: selection of pricing options
   - Price stability: frequency of price changes q21
   - Transparency: detailed pricing information, service documentation (FAQ, manuals, videos, tutorials etc.)

3 Mobility
   - Portability: device support (especially mobile devices), data portability (e.g., standardized data formats, remote control), browser compatibility
   - Flexible payments: payment options (credit card, invoice, debit etc.), time of payment (Pre-Paid or Post-Paid)

4 Service accounting
   - Invoicing: service can be invoiced time-based (usage duration), account-based (per user, per account, per instance), volume-based (transaction, storage, traffic) q24, q25, q26
   - Booking: fixed price (subscription) or usage-dependent booking q23

5 Reliability
   - Reliability (re-active): disaster recovery management (backups, recovery plans) q40
   - Reliability (pro-active): redundant data centers (regional-redundant data storage locations), network reliability (multiple Internet Service Provider), regularly backups/snapshots q38, q39
   - Customer support: 24/7 hotline, support level, help desk q46

6 Interoperability
   - External integration capabilities: availability of interfaces (API), supported standards (e.g., REST, SOAP) q2, q5
   - Internal integration capabilities: Integration capability of internal provider services q3

7 Scalability
   - Scalability: maximum of available resources/services, automatically bookable resources q13, q18
   - Manageability: interaction via website (GUI) or automatic via API, Service controlling and monitoring functionalities q46, q49

8 Security & quality
   - IT security: location of the data center, information security (e.g., data protection) q1
   - Quality management: service quality (e.g., maintenance cycles), product roadmap q34

9 Provider profile & reporting
   - Reporting: regular reports generated by the provider (e.g., about SLAs, audit support (i.e. provider support external audits) q42, q43
   - Profile: revenue, employees, experience, reference projects q41

10 Time-to-market
   - Provisioning time: time needed for creating a user, starting an instance or booking a service q12
   - Set-up time: non-recurring time-consuming efforts, for instance: account registration, account verification q11

11 Terms of contract
   - Negotiation: customizing contracts q15
   - Lock-in: automatic contract renewal, contract length q14, q16

12 Usability
   - Service usability: self-service principle q30


**Risks (Muntes-Mulero 2013)**

(Muntes-Mulero, Matthews, Omerovic, & Gunka, 2013) distinguish 7 potential risks for multi-cloud environments, as opposed to a single provider environment.

1. Risk of unexpected lack of replacement and consequent vendor lock-in:
2. Risk of new security breaches due to the increased complexity of the system and new communications
3. Risk of non-viable migration due to migration costs and complexity
4. Risk of costs unpredictability
5. Risk of lack of provider interest in collaboration
6. Risk of unavailability of evidences in case of fraudulent actions
7. Risk of lack of negotiation on SLAs
Flexiant, supplier of management software for cloud providers
(Flexiant, no year)

Your cloud platform will need to be able to support the following:

1. **Accurate metering of resource usage.** This should be possible in a manner that is highly granular and that can be attributed to each reseller and their customer accounts to ensure accurate billing. This should be provided in detail to easily identify all of this even if there are multiple levels of resellers before the end consumer is reached.

2. **High levels of white labeling and customization.**
   Often the reseller will want to carry their own brand and to customize your products and services to meet specific demands from their customers. This should be made simple by your cloud management platform.

3. **Support for multi-currency billing.** Again, your cloud management platform and billing engine should support this since most cloud service companies either operate internationally or aspire to do so.

4. **Multi-language support.** To ensure that different geographical markets are targeted effectively, you need to support multiple languages within your platform.

5. **Self service provisioning.** This should be available for the reseller to configure and give to the end customer. This creates a highly effective consumption model for the reseller.

6. **Highly automated workflow processes.** Resellers do not want to spend time creating their own workflow processes. With very little exception, all common workflow processes should be available in one or two clicks with no configuration required by the reseller.

7. **High levels of flexibility.** This will allow the reseller to respond to and meet changing customer demands with significant involvement for you. This becomes increasingly important as more resellers are on-boarded.

8. **Differentiation.** This applies to products and services as well as functionality and ease of use.

A cloud management platform that offers these eight capabilities will help to facilitate a reseller program that will have a substantial impact on your business.
From GCloud UK
(G-Cloud, no year) (G-Cloud, 2014)

Criteria number Direct award criteria
1 Whole life cost: cost effectiveness; price and running costs
2 Technical merit and functional fit: coverage, network capacity and performance as specified in relevant service levels
3 After-sales service management: help desk, account management function and assurance of supply of a range of services
4 Non-functional characteristics

Choosing suppliers, awarding and ending contracts

Single supplier
If you have got to the shortlist and only one supplier meets your requirements, you may award the contract to them without needing to do anything else. This situation is called a direct award.

Multiple suppliers
Typically there will be a number of services on your shortlist. If all these services meet your core requirements and are like-for-like, you can select one on the basis of lowest cost alone.

Often the cheapest option will be obvious, but you might need to:
• look at combinations of different suppliers
• get specific information about volumes

The final selection should be based on best fit rather than ruling out suppliers that don’t meet either your current contract or an ideal set of terms.

If you need any extra information to help you make your final decisions you can request this directly from the suppliers. Some services also offer free trials that may help you decide on the right service for your needs.
Support and Security Certifications (from PlanForCloud)

Support services and security certifications,
(RightScale PlanForCloud, 2014)

Security certifications for 5 CSPs

- SSAE/16 (SOC1) Type II
- ISO 27001
- Fed RAMP (implies a FISMA rating)
- PCI-DSS
- HIPAA

<table>
<thead>
<tr>
<th>Support Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ticket System</strong></td>
</tr>
<tr>
<td>Amazon</td>
</tr>
<tr>
<td>Developer Support &amp; above</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
</tr>
<tr>
<td>Business Support &amp; above</td>
</tr>
<tr>
<td><strong>Email</strong></td>
</tr>
<tr>
<td>Developer Support &amp; above</td>
</tr>
<tr>
<td><strong>Response Time</strong></td>
</tr>
<tr>
<td>Developer - 12 Hours Business - 1 Hour Enterprise - 15 Minutes</td>
</tr>
</tbody>
</table>

Other Notes
- Basic support provides documentation and community forums. There are also other specific features which come with support, refer to Amazon Support.
- Rackspace also offer “Managed cloud”, an extra layer of support which provides monitoring, operating system and application infrastructure layer support.
- Bronze support provides documentation, community forums and billing support. There are also other specific features which come with support, refer to Google Support.
- Included support provides documentation, community forums and billing support. There are also other specific features which come with support, refer to Azure Support.
- Included support provides knowledge base, community forums and live chat.

Monthly Cost
- **Basic - Free**
- **Developer - $49**
- **Business - Greater of $100 or 10% of monthly usage up to $10K**
  - + 7% up to $60K
  - + 5% up to $250K
  - + 3% above $250K
- **Enterprise - Greater of $15,000 or 10% of monthly usage up to $15K**
  - + 7% up to $550K
  - + 5% up to $1M
  - + 3% above $1M
- **Included - Free**
- **Bronze - Free**
- **Silver - $450**
- **Gold - Greater of $1000 or 6% of monthly up to $10K**
  - + 7% up to $30K
  - + 5% up to $120K
  - + 3% above $120K
- **Platinum - Contact Sales**

References
- Amazon Support
- Rackspace Support
- Google Support
- Azure Support
- SoftLayer Support
- HP Support
Standards for cloud life cycle phases (ETSI Cloud Standards)

Introduction
ETSI (ETSI, 2013, p. 6) reports on major aspects of cloud computing standardization. The focus is on public cloud services, because of the EU funding. For the analysis, three distinct phases (important for the Cloud Service Life-cycle), common to all Use Cases, are distinguished:

1. Phase 1: Acquisition of Cloud Service
2. Phase 2: Operation of Cloud Service
3. Phase 3: Termination of Cloud Service

In addition, 3 perspectives were defined:
- The Service Level Agreement Perspective
- The Interoperability Perspective
- The Security Perspective

Five high-level use cases (App on a Cloud, Cloud Bursting, Processing Sensitive Data, Data Integrity and High Availability) were analyzed with regard to available standards, for each life cycle phase.

Organizational factors in analysis of standards from perspectives view
From this report, multiple criteria that are of importance for CSP selection were extracted. The structure of the report is followed (in order of perspectives)

The Service Level Agreement Perspective
- Customer's power to negotiate the overall formal Customer Agreement (Master agreement or Customer Agreement)
- Service level objectives in addition to availability/up time (e.g. performance, security and compliance/privacy)
- Monitoring of the state of KPIs defined in the SLA and the state of the SLA
- Possible discussion / dispute in the perception of the state of the SLA are disputed.
- Return of customer data to the customer
- Deletion of customer data from the provider’s systems

The key concern in the acquisition phase is that the customer must retrieve information about all the service level objectives and related metrics: transparency of the service

The Interoperability Perspective
- Cloud service customer should be able to use widely available ICT facilities in-house when interacting with the cloud services, avoiding the need to use proprietary or highly specialized software.
- Interoperability also includes the ability for one cloud service to work with other cloud services, either where the cloud service of one provider works directly with a cloud service of another provider, or where a cloud service customer uses multiple different cloud services in some form of composition to achieve their business goals.
- Portability to avoid lock-in; move cloud service customer data or their applications between multiple cloud service providers at low cost and with minimal disruption.
- Interoperability through the appropriate standardization of APIs, data models, data formats and vocabularies"
The Security Perspective
There are ‘.....significant security benefits in migrating applications and usage to the cloud, as noted by ENISA in their reports on cloud computing. The shared resources available in clouds also potentially include rare expertise, shared best practices and advanced security technologies, beyond the means or abilities of the vast majority of SMEs, most larger companies and even many government bodies.....’ (ETSI, 2013, p. 9).

‘On the longer-term, in particular once better certification schemes will have been put in place (based on the available set of security standards) and legal obligations will be better enforced, the variety and coverage of services available with the right level of security will be enlarged and offer significant business opportunities to the consumers.’

Major security objectives for cloud computing are the following:
- Protect data from unauthorized access, disclosure and modification
- Prevent unauthorized access to cloud computing resources
- Ensure isolation
- Ensure service availability
- Ensure effective governance, control and compliance processes are in place
- Ensure appropriate security provisions for cloud applications
- Ensure security of cloud connections and networks
- Enforce privacy policies
- Ensure incident prevention, detection and response

Key issues that need to be addressed when assessing security standards for cloud computing are
- Cross-border legal issues, including variations in data protection regulations
- Conflict of interest between cloud customers and national security of the hosting country
- Visibility and transparency
- Assurance and trust
- Certification, audit and testing
- Identity and Access Management
- Provider use of the services of other providers
- Virtualization and multi-tenancy risks
- Data location control
- Secure data deletion and the exit process

Typical risks and challenges concern: (ETSI, 2013, p. 8)
- Availability of services and/or data
- Lack of data classification mechanisms
- Integrity of services and/or data
- Confidentiality concerns
- Regulatory Compliance
- Repudiability and lack of forensic capability
- Loss of control of services and/or data
- Responsibility ambiguity
- Lack of liability of providers in case of security incidents
- Cost and difficulty of migration to the cloud (legacy software, etc.)
- Vendor lock-in
References for appendices C and D


ETSI. (2013). *Cloud Standards Coordination Final Report*. Cloud Standards Coordination initiative. ETSI.


