Research Center
Finance & Information Management

Fraunhofer FIT
Project Group
Business & Information
Systems Engineering

Discussion Paper

A Reference Model to Support Risk Identification in Cloud Networks

by

Robert Keller, Christian König

in: Proceedings of the 35th International Conference on Information Systems, ICIS, Auckland, New Zealand, December 2014

University of Augsburg, D-86135 Augsburg
Visitors: Universitätsstr. 12, 86159 Augsburg
Phone: +49 821 598-4801 (Fax: -4899)

University of Bayreuth, D-95440 Bayreuth
Visitors: F.-v.-Schiller-Str. 2a, 95444 Bayreuth
Phone: +49 921 55-4710 (Fax: -844710)

www.fim-rc.de

WI-457

A Reference Model to Support Risk Identification in Cloud Networks

Completed Research Paper

Robert Keller
FIM Research Center
University of Augsburg
Universitätsstraße 12, 86159 Augsburg
Germany
robert.keller@fim-rc.de

Christian König
FIM Research Center
University of Augsburg
Universitätsstraße 12, 86159 Augsburg
Germany
christian.koenig@fim-rc.de

Abstract

The rising adoption of cloud computing and increasing interconnections among its actors lead to the emergence of network-like structures and new associated risks. A major obstacle for addressing these risks is the lack of transparency concerning the underlying network structure and the dissemination of risks therein. Existing research does not consider the risk perspective in a cloud network's context. We address this research gap with the construction of a reference model that can display such networks and therefore supports risk identification. We evaluate the reference model through real-world examples and interviews with industry experts and demonstrate its applicability. The model provides a better understanding of cloud networks and causalities between related risks. These insights can be used to develop appropriate risk management strategies in cloud networks. The reference model sets a basis for future risk quantification approaches as well as for the design of (IT) tools for risk analysis.

Keywords: Cloud computing, Cloud Networks, Risk Identification, Reference Model, Taxonomy

Introduction

Cloud computing has emerged as a new outsourcing paradigm during the last few years (Bresnahan et al. 2011). In 2013, the yearly spending on cloud computing nearly hit the 50 billion dollar mark and is expected to climb up to over 100 billion dollars in 2017 (IDC 2013). Accompanied by rising adoption, the inherent risks of cloud computing must be addressed. Recent IS research examines these risks, for example, see Armbrust et al. (2009), Troshani et al. (2011), or Clarke (2012a). Additionally, risk avoiding strategies like multi-sourcing (AlZain et al. 2012) or attack avoiding strategies (Zissis and Lekkas 2012) are described and may be progressively adopted in practice. Therefore in the future, even more companies will dare to move into the cloud when cloud computing has overcome its current Trough of Disillusionment (Linden and Fenn 2003) with the guidance of IS research.

The increasing adoption of cloud services and rising interconnections among actors in cloud computing lead to the emergence of network-like structures in the cloud business. These structures are similar to complex supply networks known from the manufacturing industries (compare Hallikas et al. 2002). In the following, we will refer to these structures as cloud networks.

Besides "traditional" cloud computing risks that mostly focus on a vendor or a customer, new network-induced kinds of risk are emerging and should be addressed by adequate risk management practices, anchored in IT governance. An incident at one place can lead to cascading effects that affect many other participants in the network. Cloud networks may adopt some characteristics and risks of supply chain networks or even the financial industry (compare Buyya et al. (2008)). In 2011, for example, an outage of Amazon EC2 occurred which affected many of its customers (Clarke 2012b). Among them were Heroku, Engine Yard, and DotCloud, which build their platform services on Amazon's EC2 infrastructure services and provide them to other companies like ASICS or Audi that were consequently not able to provide their built-on application services to their respective customers (Harris 2011).

One major obstacle for addressing these risks in cloud networks is the lack of knowledge on the underlying network structure and thus, the possible risks. Without this knowledge, no appropriate risk management strategy can be applied. Until now, the existing literature on risks in cloud computing focuses mostly on compliance and general risk management approaches as well as on identification and quantification of risks for a specific company. For example, Martens and Teuteberg (2011) designed a reference model for risk and compliance management for cloud services. Wherein the authors aim to "support companies in managing and reducing risk and compliance efforts" (Martens and Teuteberg 2011). They provide a UML (OMG 2011) class diagram that describes the required components of cloud risk management in companies. Armbrust et al. (2009) or Dillon et al. (2010) focus on the risk identification from a technological point of view at the customer side. Several authors provide approaches to measure cloud risks. For example, Harnisch and Buxmann (2013) evaluate cloud services with methods of supplier selection and Saripalli and Walters (2010) propose a quantitative impact and risk assessment framework for cloud security. However, we have not found any approaches that examine risks of cloud computing from a network perspective. Authors that do focus on cloud networks, such as Böhm et al. (2010), Marinos and Briscoe (2009), or Bleizeffer et al. (2011), do not consider risks in their approaches.

In this paper, we will answer the following research questions as a first step to address this lack of knowledge:

RQ1: What actors exist in cloud networks?

RQ2: What risks affect the actors of cloud networks?

On this basis, we construct a reference model that contributes to the understanding of the nexus of globally distributed cloud networks and its respective risks. The goal of a reference model is to cover "general patterns in order to raise the efficiency and effectiveness of specific modeling processes" (Vom Brocke and Thomas 2006). In line with Hevner et al. (2004), we build our reference model as a specific "artifact" and evaluate it in the course of our search process, which is similar to the approach of Knackstedt et al. (2009). In order to "enhance the quality" of our reference model, we follow the "guidelines of modeling" by Schuette and Rotthowe (1998). We use a slightly simplified version of UML (OMG 2011) as a semi-formal modeling language for information modeling in order to describe our artifacts in a clear and comprehensible manner. We examine actors and risks of cloud networks and

display them in tree based structures through generalizations in UML class diagrams. These two taxonomies (*RQ1* and *RQ2*) build a solid basis for our reference model. The taxonomies are grounded on existing literature in cloud computing and related literature from other disciplines, such as supply chain networks or the financial industry, and then elaborated with our own critical reflection. We develop the reference model by identifying connections between actors and the causalities between different risks, respectively. The taxonomies are evaluated trough real world examinations following a conceptual-to-empirical approach proposed by Nickerson et al. (2013). In addition, we discussed the taxonomies with industry experts to guarantee the reflection of existing market structures. The reference model is also evaluated in discussions with industry experts. Furthermore, we elaborate the reference model through instantiation on the basis of a real world example to demonstrate its applicability. We used the insights from the interviews to improve the taxonomies and the reference model. Due to the limited space, we only illustrate the final versions of our reference model and the partial models. We describe the iteration steps of improvement in the evaluation section.

On the basis of our reference model, the dissemination of risks throughout the cloud network can be examined. In this context, dissemination describes the passing on of a risk from one actor to another whereby the first actor still is affected. Practitioners can display relevant actors and structures in cloud networks. By using the reference model as a template and instantiating it for their specific scenarios, they can identify impending risks. In addition, the reference models supports a better understanding of the effects of risks on the holistic system. Referring to the risk cycle of Zhang et al. (2010), our reference model enables practitioners to select relevant critical areas and identify the respective occurring risks. The reference model displayed in a semi-formal diagram sets a basis for future risk quantification approaches as well as for the design of (IT) tools for risk analysis. On this basis, appropriate risk management strategies can be developed.

The paper is structured as follows: To address the problem relevance, we outline the development towards cloud networks in Section 2. In Section 3 and 4, we develop a taxonomy of actors in cloud networks and a taxonomy of risks in cloud networks. In Section 5, we create two partial models based on the two taxonomies. Finally, we merge these two partial models to the reference model. In Section 6, we provide an evaluation of the taxonomies and the reference model. In Section 7, we discuss implications, address the applicability of the model and provide an outlook on future research.

Developments towards Cloud Networks

In addition to the increasing adoption of cloud services, we observe new developments in cloud computing. These developments lead to the aforementioned emergence of cloud networks:

- First, a trend towards an increasing *standardization* in cloud computing exists (Vaquero et al. 2009), strengthening the interchangeability of cloud services between different actors in cloud computing. In an outlook on future market structures, Buyya et al. (2008) describe cloud exchanges with brokers that trade standardized cloud products.
- Second, the *specialization* of cloud services increases to provide software for specific "intended user groups" such as private users or specific business groups (Höfer and Karagiannis 2010). Due to low barriers to market entry (Clemons and Chen 2011), a huge variation of application services surfaces.
- Third, the *dependencies* among actors in cloud networks are rising. These dependencies are caused by the aforementioned developments as well as the concept of multi sourcing in the cloud to prevent outages, as suggested by Armbrust et al. (2009) and analyzed by König et al. (2013).

In addition, new market structures and actors emerge in cloud computing. Some companies developed to large players in cloud computing during the last years, such as Amazon, Salesforce, or Microsoft. On the one hand, the variety of offerings on the infrastructure as a service (IaaS) market shrinks as the large players offer lower prices and higher availability than mid-size infrastructure providers could ever achieve (Harris 2014). On the other hand, the variety of software as a service (SaaS) offerings enlarges. This leads to a market with a lack of transparency where many different actors *depend* on only a few. In this market, we observe the genesis of new business models like the Deutsche Boerse Cloud Exchange or the Massachusetts Open Cloud project as an exchange platform for *standardized* infrastructure services, or VMware Service Market Place and the HP Aggregation Platform which offer software and platform services. Actors in cloud computing are now able to outsource *specialized* functions (Troshani et al. 2011).

Thereby, they can focus on their core competencies by consuming other *specialized* cloud services in order to simplify their operational business or enhance their own service offerings. Vendors may, for example, use payment handling services and development platform services from other cloud actors to provide their own application services. Market places strengthen the bonding between actors of a cloud network, while facilitating a rapid exchange of cloud services. This development is especially displayed in *standardized* interfaces in cloud market places and in a strong movement towards *standardization*, pushed forward by organizations such as the "Cloud Standards Customer Council" with important industry players like IBM or Symantec (Cloud Standards Customer Council 2014). The emergence of cloud exchange markets will in turn additionally strengthen the drive for *standardization* of cloud services (see Buyya et al. (2008)).

These developments are likely to transform the current cloud landscape towards complex, globally distributed cloud networks, consisting of many different actors and connections. In these cloud networks, risks can disseminate between different actors. For example, Microsoft Yammer, an enterprise social network that supports collaboration between employees, uses the cloud service Crocodoc to convert PDF and Microsoft Word Documents into HTML5. Crocodoc itself is hosted by Amazon Web Services (AWS). Hence, the services from Microsoft depends to some extent on the availability of AWS. A recently emerged risk occurred after Facebook bought Instagram and released new license agreements. The emerging bad publicity on Instagram pushed many users to services of competitors. These competitors were then struggling to provide the required infrastructure resources in short-term to keep their services running (Laurent 2013).

Taxonomy of Actors in Cloud Networks

Several cloud computing taxonomies exist in IS literature, such as Hoefer and Karagiannis (2010), Hoefer and Karagiannis (2011), or Rimal et al. (2009). These taxonomies classify cloud services in terms of technical properties. In contrast to these approaches, we focus on the business perspective of cloud computing. Within this perspective, we only consider actors that participate in the production of cloud services and therefore provide, process, or transmit services in cloud networks. As a basis for the construction of our taxonomy, we refer to Böhm et al. (2010) who address "the business perspective of IT provisioning", and extend it with results of other authors. Leimeister et al. (2010) describe the value transfer between actors in cloud computing. In addition, we use the differentiation of provisioning models that is described by Marinos and Briscoe (2009). They identify "vendors", "developers", and "end users" as actors related to IaaS, platform as a service (PaaS), and SaaS, which are described in detail in the ontology of Youseff et al. (2008). Marinos and Briscoe (2009) state that a "vendor" provides IaaS, PaaS, and SaaS whereas the "developer" consumes IaaS and PaaS and provides SaaS. The "end user" consumes SaaS. We adopt this "input/output" view for our classification logic.

As mentioned earlier, cloud networks may share some characteristics with supply chain networks and the financial industry. Regarding supply chain literature, such as Lambert et al. (1998) or Harland (1996), we identified equivalents to the actors that are already described in the literature on cloud computing. In a supply chain network, many customer/vendor relationships exist, including value-adding steps between the stages of the production process. Each producer is able to produce goods parallel or sequential to other producers. We adopt the way of distinguishing actors between the respective positions in the network and between the respective products. Regarding the financial industry, the interconnections of banks and other financial institutions with their respective dependencies can be compared to the interconnections among cloud services to some extent. Information is exchanged in real time and is often organized as an on demand self-service. Certain actors, such as the exchange market or aggregator/broker, already exist or are evolving in cloud computing. From the financial industry we additionally adopt the actor "market place" and the idea of a liquid market where standardized cloud services are exchanged.

Our taxonomy is based on existing literature with a focus on the business perspective and extended with our own observations. Within the taxonomy, we categorize the actors with the help of three layers:

- In a *Position Layer*, we distinguish between the positions of the actors in a cloud network. A *Provider* is the first node in the network whereas the *Client* represents the final node. Between these nodes we identified *Intermediaries* that use services produced by other participants of the cloud network, enhance or aggregate these services, and provide them afterwards to their own customers.
- In a *Business Model Layer*, we distinguish within the three categories of the position layer and consider the different business models of the respective actors. We regard *Initial Producers*, *Value-Added Resellers*, and *Catalysts* which strengthen the interconnections among cloud actors and increase the frequency and easiness of interactions (like market liquidity) in the cloud network.
- A *Product Layer* specifies the actors by the respective provided product. Therefore we use the technical layers of cloud computing (IaaS, PaaS, SaaS). In addition, we introduce the *Aggregator* as a new form of a *Value-Added Reseller*.

In order to address research question *RQ1*, we illustrate the hierarchical taxonomy of actors in a UML class diagram in Figure 1 through generalizations. A generalization represents an "is a" relationship whereby a specific element "inherits the features of the more general" element (OMG 2011). The taxonomy contains all identified *Actors*, layers, and inheritance between the layers. The classes of the *Position Layer* inherit from the super-class *Actor*. The classes of the *Business Model Layer* inherit from the super-classes in the *Position Layer*. The classes of the *Product Layer* inherit from the super-classes in the *Business Model Layer*. It can be read as follows: An *Aggregator* is a *Value-Added Reseller* is an *Intermediary* is an *Actor*. We explain the identified *Actors* in detail on a *Product Layer* level in Table 1 in the appendix.

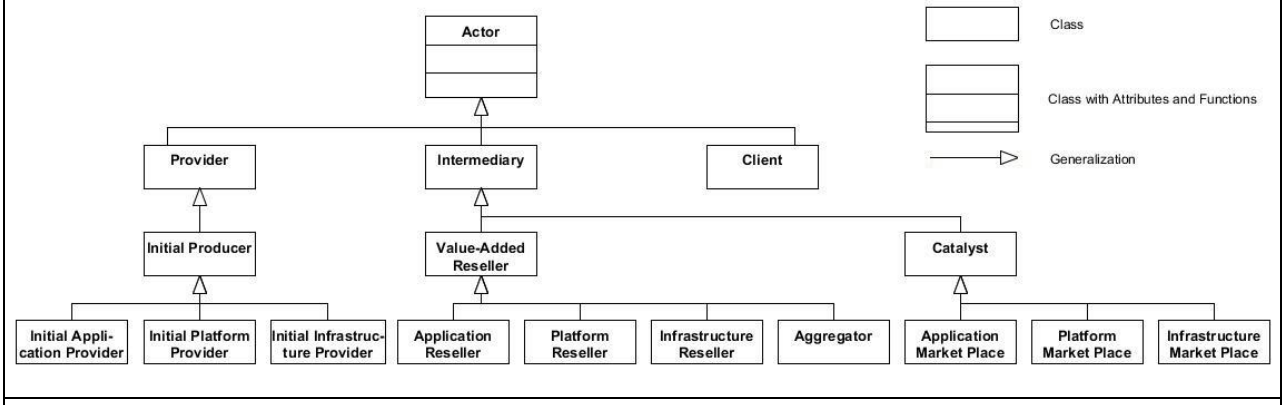

Figure 1. Taxonomy of Actors

Taxonomy of Risks in Cloud Networks

Clarke (2010) states that the risks of cloud computing are similar to those of in-house operations yet more opaque. Grobauer et al. (2011) propose a taxonomy of the general term risk, which implies "loss event frequency and probable loss magnitude". Many authors examine the risks of cloud computing but only a few address risks in cloud networks. Nevertheless, these examinations described below serve as a solid basis for our taxonomy of risks in cloud networks. Clarke (2012a) provides a checklist that lists risks and benefits of cloud computing in sub-categories. The author distinguishes between operational, contingent, security, commercial, and compliance risks. Troshani et al. (2011) divide cloud failure risks in technical risks, like data transit risk or malicious activities, and organizational risks, like lock-in or security and privacy risks. Jansen (2011) identifies six key security issues, namely trust, architecture, identity management, software isolation, data protection and availability, while explicitly describing cascading outages in cloud networks in the latter case. AlZain et al. (2012) identify three main cloud security risks, namely data integrity, data intrusion, and service availability. Armbrust et al. (2009) discuss obstacles for cloud computing, including for example the availability of the service, data lock-in, data confidentiality and auditability, data transfer bottlenecks, performance unpredictability, or reputation fate sharing. Moreover, Clarke (2012b) examines real world cloud reliability issues from 2005-2011.

Again, we take a look at the areas of supply chain networks and the financial industry. Regarding supply chain networks, Hallikas et al. (2004) identify the four types of risks "too low or inappropriate demand", "problems in fulfilling customer deliveries", "cost management and pricing", and "weakness in resources, development, and flexibility". For cloud networks, we can adopt the risk of shifts in demand and of a lack of flexibility. Prater (2005) distinguishes between eight uncertainty factors. From that, we borrow "variable uncertainty" which covers factors such as weather, market behavior, or political influence factors. We also adopt the described parallel supply chain effects that refer to the dependency on several input goods with the possibility of missing input. In addition, chaotic demand peaks can be caused by wrongly conditioned enterprise resource planning (ERP) systems. This may also be relevant for cloud networks. In the financial industry, the term risk refers especially to "uncertain environmental variables that reduce performance predictability, as well as the lack of predictability in firm outcomes itself" (Miller 1992). These variables encompass general environmental, industry, and firm-specific risks (Miller 1992). Many of the thereby included risks are also found in literature on cloud risks, especially legal uncertainties (Armbrust et al. 2010; Jansen 2011) and input market specific uncertainties such as outages (Armbrust et al. 2010; Chow et al. 2009; Clarke 2010; Jansen 2011). In addition, we adopt the risk of unexpected demand shifts or price changes from the financial industry.

The literature on cloud computing does not use the term risk uniformly. In order to create a taxonomy of risks, we refer to Kaplan and Garrick (1981) who differentiate between *Hazard* and *Risk*. We adopt this "cause-and-effect" view for our taxonomy:

- A *Hazard* describes the "source of danger" (Kaplan and Garrick 1981). It strikes directly at a specific actor and affects its service. The thereby caused resulting *Risk* is measurable at the actor's customers, which are, for example, unable to use the respective cloud service as an input factor. The likelihood of the occurrence of a *Hazard* may be influenced by safeguards.
- A *Risk* "involves both uncertainty and some kind of loss or damage that might be received" (Kaplan and Garrick 1981).
- In addition to *Hazards* and *Risks*, we introduce *Reinforcers*, which are caused by the underlying network structure and can alter the measurable *Risks*.

Companies are mostly concerned about securing supply and steady prices of their pre-products. The derived basic risks are *Supply Risk* and *Price Risk*, whereas the *Supply Risk* in cloud computing can be divided in *Loss of Data* and *Availability Issues*. In addition to these two *Risks*, we consider *Data Issues* because the transferred good is information. We divide *Data Issues* in *Data Security* and *Data Privacy*. *Hazards* mostly describe the "traditional risks" of cloud computing like *Technical Defects*, yet also include *Shifts in Demand and Supply*, which may be provoked by strategic decisions of companies. *Reinforcers* include network specific circumstances that become relevant if risks occur. In addition, *Automation Errors* in service provisioning systems may also intensify other risks. We use the term *Challenges* as a super-category for *Hazards*, *Risks*, and *Reinforcers* as these three categories represent challenges for a risk management in cloud networks. In order to address research question *RQ2*, we display the hierarchical taxonomy of risks in a UML class diagram with all identified *Hazards*, *Risks*, and *Reinforcers* in Figure 2. All sub-classes inherit from their super-classes. It can be read as follows: *Data Security* is a *Data Issue* is a *Risk* is a *Challenge*. We provide further information on all classes in Table 2 in the appendix.

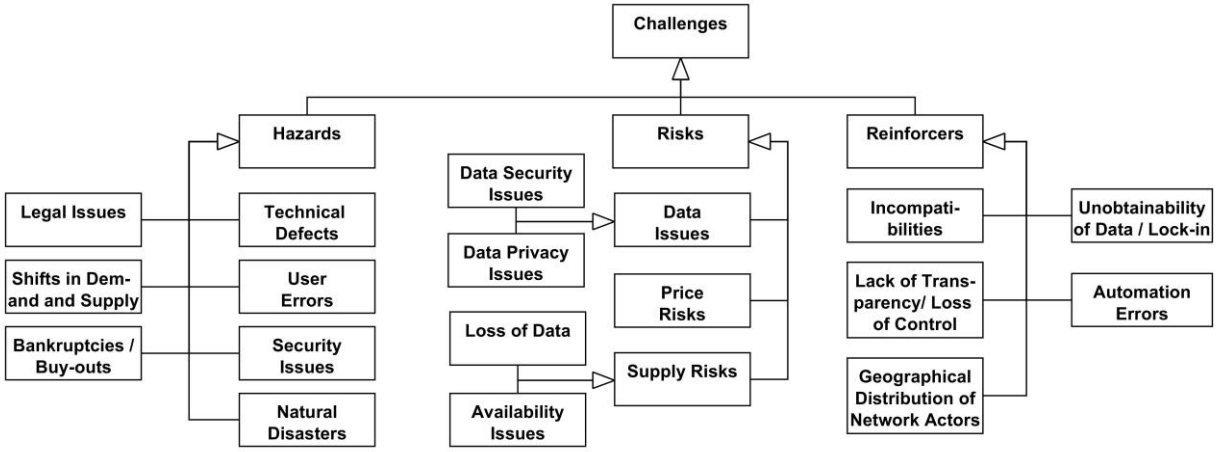

Figure 2. Taxonomy of Risks

Developing the Reference Model

We now construct the reference model, which is based on the taxonomies, in the following three steps: First, we identify the *Connections* between *Actors* in cloud networks that span a network, in a partial model. Second, we identify the causalities between *Hazards*, *Risks*, and *Reinforcers* in a partial model. Third, we assign the *Hazards*, *Risks*, and *Reinforcers* to specific *Actors* and display the possible dissemination of risks through a spanned network.

We constitute that the network consists solely of *Actors* and *Connections* between these *Actors*. In our reference model, *Actors* and *Connections* are vital parts of the network and do not exist without the network, which is displayed with the use of compositions. Further, in reality, one *Company* might appear as various *Actors* due to a manifold cloud service offering, which is again displayed with the use of a composition. Google, for example, acts as *Initial Application Provider* (GMail), *Initial Platform Provider* (Google App Engine), and as *Aggregator* (Google News). The *Connection* symbolizes the "uses a service from" (from the perspective of a customer) or "service is used by" (from the perspective of a vendor) relation between a vendor and a customer. Our identified structure in the reference model implicates the assumption that an *Actor* usually does not consume a service and provides it without processing. This assumption is based on the existence of administration costs that raise the price of the actor's product above the price of the original product. The *Connections* between the respective actor classes at the position layer are represented by association classes. In order to guarantee easy readability, we removed the cardinalities from the association classes. All *Connections* represent *n-m* relationships between the respective *Actors*. From this it follows that one *Actor* can provide a service for various other *Actors* (a very common case) and various *Actors* can provide services for one *Actor* (allowing for the depiction of diversification strategies using backup/failover providers). Below this abstraction layer, the *Actors* do not behave differently in terms of their interaction. In Figure 3, we illustrate the partial model of actors in cloud networks.

As clarified above, *Hazards* describe the cause of a *Risk*, whereas *Reinforcers* may increase the damage or the probability of a *Risk*. A *Risk* can be caused by various *Hazards* and a *Hazard* can cause several *Risks*, which equals an *n-m* relationship. Again, we removed these cardinalities from the association class to guarantee easy readability. The same is valid for the "cause-and-effect" relationship between *Reinforcers* and *Risks*. The sub-classes of *Hazards*, *Risks*, and *Reinforcers* inherit this feature from their super-classes. However, *Hazards* and *Reinforcers* have different effects on different *Risks*. For example, the *Incompability* cannot reinforce the *Data Security Issues*. In Table 3 and Table 4 in the appendix, we illustrate the possible combinations which have been elaborated by our own critical reflection. In Figure 4, we illustrate the partial model of challenges.

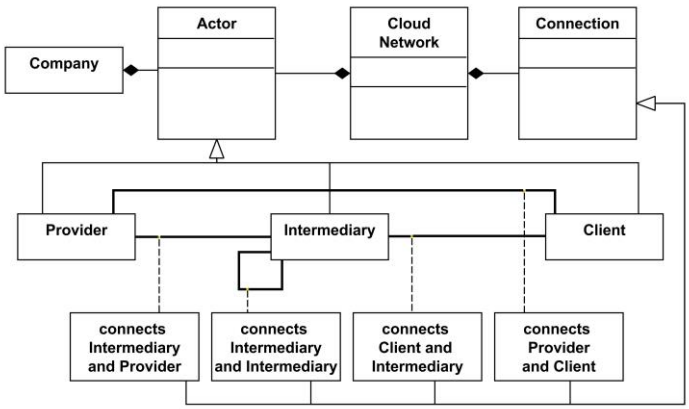

Figure 3. Partial Model of Actors in Cloud Networks

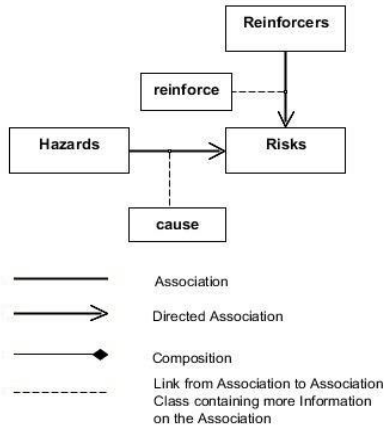

Figure 4. Partial Model of Challenges

We join the two partial models to a reference model. We illustrate the dependencies between *Risks* and *Hazards*/*Reinforcers* as association classes. A basic characteristic of our reference model is that *Risks* can be disseminated from one *Actor* to another through a specific *Connection*. Generally, *Risks* are disseminated from vendor to customer. This dissemination is represented in our reference model through methods in the *Connection* class. Specific *Hazards* strike at specific *Actors* in the cloud network. Also, specific *Risks* can be detected at specific *Actors* in the cloud network. Therefore we assign the *Risks* and *Hazards* classes to the *Actor* class. The *Reinforcers* are determined by the class *Cloud Network*.

A *Hazard* strikes at a specific *Actor* and therefore affects the *Actor's* cloud service output. The *Actor's* customers using this service as input are able to measure the thereby caused *Risk*. If this *Risk* affects the cloud service output of the customer, the *Risk* is in turn disseminated to the customer's customer which again can detect the *Risk*. For example, in case of a *Technical Defect* at the *Initial Platform Provider* A, A fails to deliver the service correctly. Therefore *Application Reseller* B using this service can detect *Availability Issues* such as outages or bad performance. The *Availability Issue* may also affect the produced application services by B and in turn be disseminated to *Aggregator* C which uses B's service for the assembly of its own offerings. At B and C, the *Risk* might even be worsened through a *Lock-In*. In Figure 5, we illustrate the developed final reference model.

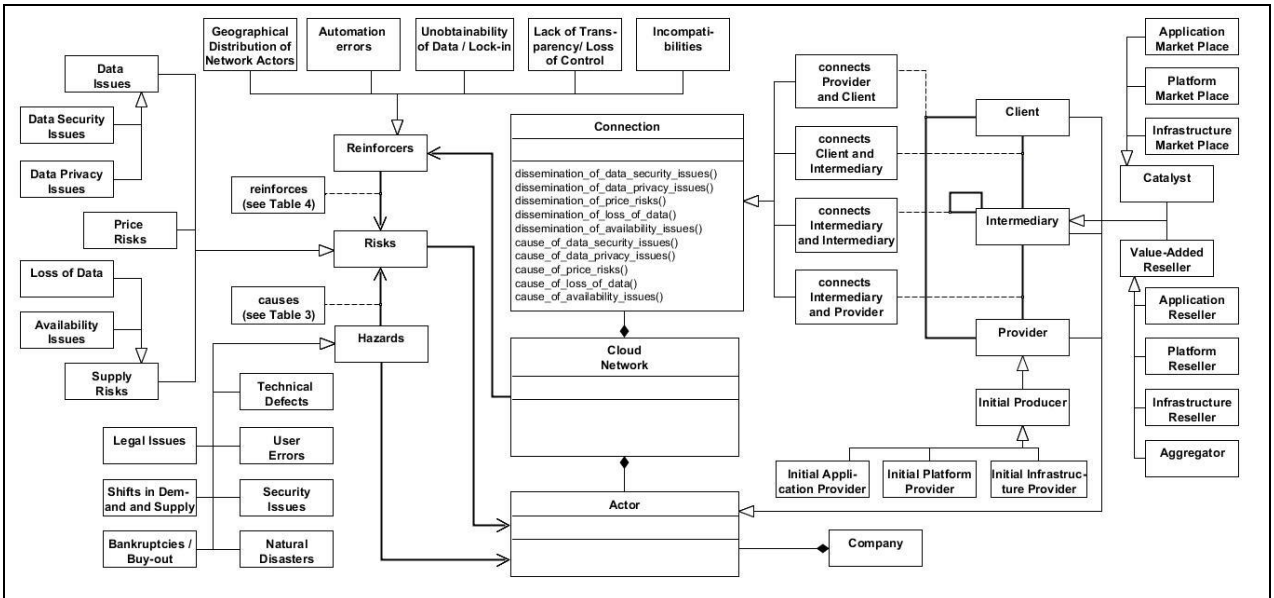

Figure 5. Reference Model to Support Risk Identification in Cloud Networks

Evaluation

As proposed by Schuette and Rotthowe (1998), our artifact is based on the body of existing literature in the field of cloud computing and other relevant disciplines. We constructed two taxonomies and used them as the foundation for our reference model. To evaluate our findings, we first evaluated the individual taxonomies. Second, we evaluated the reference model. For this purpose we applied a "multi-method" approach (Martens and Teuteberg 2011). For the taxonomies we used real world examples and, in accordance with Gregor and Hevner (2013), conducted semi-structured interviews with industry experts from focus group companies. For the reference model, we again conducted interviews with the industry experts and additionally instantiated the reference model with real world actors to demonstrate its applicability. We critically discussed any feedback received in the interviews with other researchers before incorporating it into our models, presented in the sections above.

For interviewee selection, we identified possible interview partners that (i) represented different kinds of actors in cloud networks and therefore covered a "wide spectrum of expert knowledge" (Martens and Teuteberg 2011) and (ii) could be considered "domain experts" with "expertise in the cloud computing area" (Boehm et al. 2010) due to holding important positions with several years of experience in the respective companies. We were able to conduct interviews with two available interviewees from two different companies. Their diverse business models and perspectives on cloud computing support a reasonable generalizability of our reference model. Our first interview partner is the CEO of company X. This company is a small sized customizing partner of Y, one of the world's largest SaaS ERP providers, and uses several cloud-based third-party add-ins which offer specific functionalities. Y hosts its services in the United States, whereas company X is located in Germany. The interview partner has extensive knowledge regarding dependencies among cloud services through several years of experience in customizing SaaS services for X's customers. Our second interview partner is the Head of IT Architecture of Company Z. This company is one of the world's largest, globally acting IT service providers. Offerings range from IaaS to SaaS in trusted public, private, and hybrid cloud environments for large commercial and governmental organizations. During the last year, the company invested approximately 2 billion dollar in their cloud-based developments. The interview partner has profound knowledge in the field of cloud services through years of experience in purchasing cloud services for the internal use in company Z, as well as through responsibility for the availability of the necessary IT resources for external cloud service consumers.

Concerning the problem relevance, both interview partners confirmed the developments towards cloud networks as well as the resulting lack of transparency and newly emerging risks. They particularly underlined the trend towards standardization of infrastructure services. Company X's customers consider availability and geographical location of the stored data to be main concerns. Many customers therefore implement local safeguards such as physically independent internet connections. However, the customers of company X do not usually address cloud network related risks. Company Z considers the loss of data and outages of cloud services to be major concerns. They propose multi-vendor sourcing and detailed service level agreements as safeguards to cope with these issues.

Evaluation of the Taxonomies

We discussed our taxonomies with the industry experts from company X and Z. We then incorporated the respective gained insights into the taxonomies. In the following, we illustrate some annotations of the experts with regard to our former artifacts:

- An interview partner noted that many companies in cloud networks might appear as various *Actors* at the same time. To overcome this issue, we came up with the class *Company* that consists of *1-n Actors*.
- Regarding the taxonomy of risks in cloud networks, an interview partner felt that a formerly depicted hazard *Bad Reputation* is a type of *Demand Risk*.
- Another issue was that our former distinction of *Data Issues* was not exact enough. Hence, we divided the respective risk *Data Security* (now *Data Issues*) into *Data Security* and *Data Privacy*.
- An interview partner remarked that performance issues could be a cause of a *Supply Risk*. We followed this advice by renaming the *Risk Outages* to *Availability Issues* which now also contains performance issues.

- Both interview partners confirmed the completeness of the taxonomy of actors and risks in cloud networks for their purposes and based on their expertise. Furthermore, all changes were discussed with other researchers.

In addition, we applied a conceptual to empirical approach described by Nickerson et al. (2013) during the construction of our taxonomies, which includes an evaluation through the identification of real world examples for the illustrated sub-classes. After several cycles of elaborating our taxonomies, we sufficiently matched the objective and subjective ending conditions described by Nickerson et al. (2013). Regarding the objective ending condition "every characteristic must be explained by an example", we could not find real world examples for the risks *Price Risk* and *Data Security Issues*. Information about such problems does usually not go public. However, the interview partners confirmed the existence of these risks. We could also not find real world examples for *Infrastructure Reseller* and *Platform Market Place*. As the developments towards cloud networks are still ongoing, not every described actor is already in business and therefore cannot be observed right now. However, our models are meant to include near future market structures in cloud computing. Therefore, we tried to explain circumstances under which such actors may likely exist in the near future. The interview partners confirmed the high likeliness of these actors. In addition to these objective ending conditions, we and our interview partners felt that the taxonomies had reached a state where they now were concise, robust, comprehensive, extendible, and explanatory (subjective ending condition). In Table 1 in the appendix, we illustrate the actors of cloud networks with a textual description and the identified real world examples. In Table 2 of the appendix, we illustrate the risks of cloud networks with a textual description and the identified real world examples.

Evaluation of the Reference Model

We discussed our reference model with the industry experts from company X and Z. Again, we then incorporated the respective gained insights into the reference model. In the following, we illustrate some annotations of the experts with regard to our former artifact:

- An interview partner annotated that the former illustration was very complex and required a long settling-in period. We were able to simplify the illustration by moving the direct connections between the actors and the associated risks into the association classes, which are now displayed in Table 3 and Table 4 in the appendix. The new illustration now allows an easier and more comprehensive adaption by practitioners without losing too much expressiveness in its depiction.
- A former version of our reference model allowed actors to disseminate hazards to other actors. An interview partner suggested that we should consider the dissemination of the respective risk itself. After discussions with other researchers we adopted this suggestion and adjusted our reference model accordingly.
- Both interview partners developed a good understanding of the reference model and described it as reasonable and applicable. Furthermore, all changes were discussed with other researchers.

Next, we demonstrate the applicability of our reference model by instantiating it with real world actors. In order to remain consistent with the UML class diagram, we use an UML object diagram. We chose the already described dependencies between Amazon EC2 and Microsoft Yammer and expanded it with SAP Spotlight which is another customer of Crocodoc. In our example, we look at a *Client* "ACME" which consumes services of the two *Application Resellers* Yammer and SAP Spotlight to support its business operations. We assume that the datacenters of Amazon and Microsoft are located in the same area and therefore are both affected by a blackout due to a lightning storm (*Natural Disaster*). Subsequently, Amazon causes risks (*Price Risk*, *Loss of Data*, and *Availability Issues*) at their customer Crocodoc that in turn disseminates the risks to its customers Yammer and SAP Spotlight. Yammer and Spotlight are able to measure these *Risks* that affect their service input. At the same time, the affected Microsoft Servers cause *Risks* (*Price Risk*, *Loss of Data*, and *Availability Issues*) at Yammer. As Yammer consumes services from Amazon EC2 and the Microsoft Servers, the *Hazard* affects Yammer even more. We speak of the *Reinforcer* "*Geological Distribution of Network Actors*". This *Reinforcer* worsens the magnitude of Yammer's *Risks*. In the following, the *Risks* at Yammer and SAP Spotlight are disseminated through the cloud network until the last node (company ACME) is affected. In addition, we assume a user mistake (*User Error*) at SAP Spotlight. Therefore, this actor also causes *Risks* (*Loss of Data*, *Availability Issues*, *Data Security*, and *Data Privacy*) at company ACME. These *Risks* add up to the *Risks* disseminated from

the lightning storm (*Price Risk*, *Loss of Data*, and *Availability Issues*). We illustrate this instantiation of our reference model in Figure 6. The depicted model provides transparency on the existing dependencies. The dissemination of risks through the cloud network can be displayed and the respective actors are able to identify the impending risks.

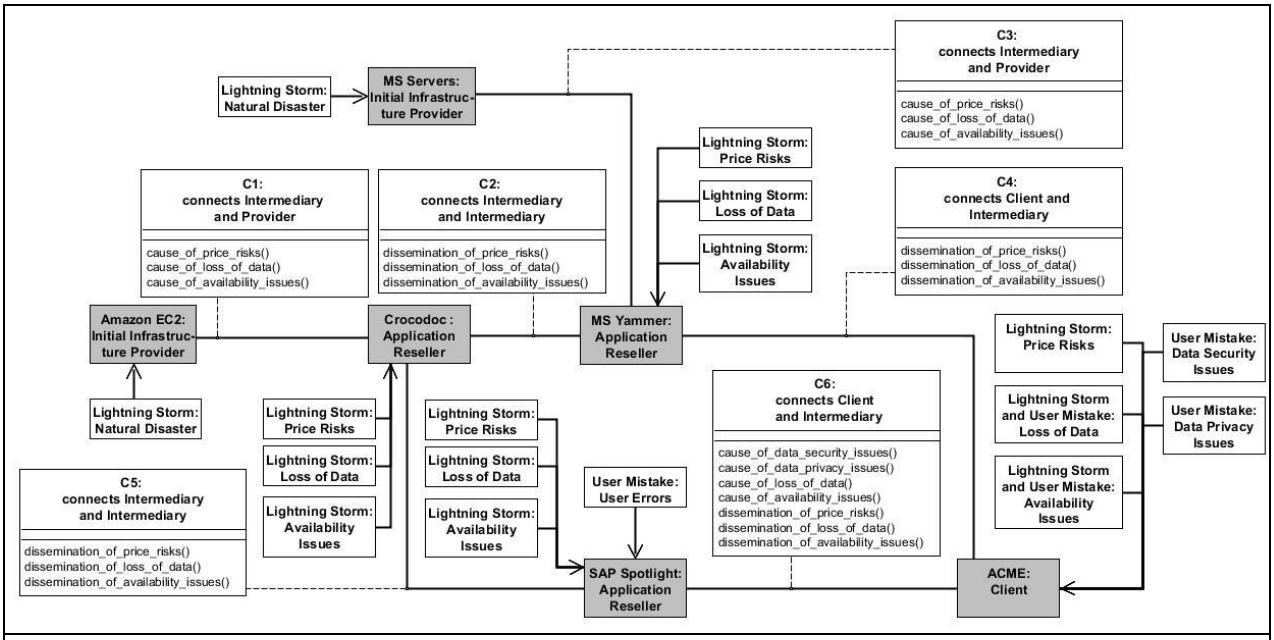

Figure 6. Instantiation of the Reference Model

Implications, Applicability, and Future Research

In our paper, we describe ongoing developments in cloud computing, such as standardization, specialization, rising dependencies, new actors, and new market structures. These developments are likely to transform the current cloud landscape into complex, globally distributed cloud networks with new emerging risks. In order to provide a better understanding of the underlying structure and the inherent risks, we develop taxonomies of actors and risks in cloud networks (*RQ1* and *RQ2*). On this basis, we build a reference model based on UML class diagrams that can be instantiated and supports risk identification in cloud networks. We evaluate the taxonomies and the reference model through real world examples and interviews with industry experts.

Cloud networks are participant governed networks in which, regarding governance, no clear responsibilities are yet determined. As cloud networks become more complex and the number of participants increases, there is a need for cloud network governance which, considering the research of Provan and Kenis (2007), might be best addressed by a network administrative organization. Zissis and Lekkas (2012) also propose a trusted third party to enforce cloud governance. However, as the implementation of an institution that will provide a holistic cloud network governance may need some years, practitioners need to address the prevailing risks on their own in the meantime. In both ways, clear defined cloud network governance principles and processes are needed. Therefore, existing approaches from a single company view may be adapted, e.g. Guo et al. (2010) or Zhang et al. (2010). Also, existing knowledge on network governance (e.g. Jones et al 1997 and Provian and Kenis 2007) or supply chain governance (e.g. Bitran et al. 2006, Gereffi et al. 2005, Richley et al. 2010, and Wathne and Heide 2004) could be incorporated.

Following the risk cycle of Zhang et al. (2010), which is based in the NIST Risk management guide (Stoneburner et al. 2002), risk analysis (or risk identification) is an essential step in terms of risk management and should also be part of risk management in a network (Hallikas et al. 2004). The reference model could be applied by practitioners in terms of a government process that coordinates "cloud-based services management and policy implement across the enterprise" (Guo et al. 2010). More

specific, the reference model enables practitioners to select relevant critical areas and identify the respective occurring risks (Zhang et al. 2010). In addition, it provides a depiction of actors in the cloud network and thereby the implementation of "threat identification" (Zhang et al. 2010). Concluding, the reference model provides practitioners and researchers with a better understanding of the nexus of cloud networks and related risks, thereby supporting risk identification:

- Relevant actors and structures in cloud networks can be displayed and thereby impending risks can be identified.
- The dissemination of risks throughout cloud networks can be examined.

Considering its application, responsibility for instantiating the reference model in the course of implementing cloud network governance structures lies with the individual participants of the cloud network for now. To instantiate the reference model for their own specific eco-system, practitioners need to gather information on actors and hazards. Similar to the existence of industry-specific associations in supply chains like e.g. the automotive industry, which provide information on possible suppliers (Choi and Hartley 1996), cloud industry-specific associations may arise in the future which might be used for information gathering on relevant actors. In addition, information on actors can originate from information pages of respective actors, from communication with respective actors, from cloud marketplace directories (e.g. Amazon Web Services Marketplace 2014), or from publicly available research results (e.g. CloudServiceMarket 2014). In the future, there may be some kind of automated information interchange on the underlying network as it is already practiced in supply chain networks today (compare Spekman et al. 1998). Information on hazards may be a bit harder to obtain as cloud actors have no interest in making these events publicly available. Hence, our taxonomy of risks could be used as a guideline for examining possible hazards. Also, cloud industry-specific media reports on past events might serve as an indicator for prevailing hazards. We argue, that even the instantiation with limited obtainable information in a rather small cloud eco-system should provide added value in terms of risk management in cloud networks as it will shed some light on at least a part of the existing risks, thereby making risk mitigation possible. Yet, the development of a detailed risk analysis process for cloud network governance, including the reference model as a necessary step, is subject to further research.

Cloud computing is a highly dynamic market. Many new market structures and challenges may change during the next several years. Therefore the validity of our current model cannot be guaranteed for the future and will be subject to continuous adjustment and development. Furthermore, as of now, we have only modeled one real-world example. In future research, we will collaborate with more practitioners and experts in order to further examine relevant actors and challenges and to display more partial cloud networks. These partial views could be connected to a large "cloud network map" that displays the dependencies among many existing cloud actors. With the identified causalities between hazards, risks, and reinforcers and the identified dissemination of risks modeled as a semi-formal diagram, we have set a basis for risk quantification approaches. In the next step, we will apply existing criticality measures to identify the key actors in cloud networks. Subsequently, we want to develop new cloud network specific risk measures and our reference model could serve as a basis for the development of an IT tool for risk quantification. The estimation of possible input values for this tool could be subject to future empirical research. After gaining knowledge on existing risks and their possible impact, we are planning on developing and evaluating safeguards addressing the identified risks. Thereby, the effect of different types of risks and actors on the respective appropriate risk management strategy could also be investigated further.

References

AlZain, M. A., Pardede, E., Soh, B., and Thom, J. A. 2012. "Cloud computing security: from single to multi-clouds," *in 45th Hawaii International Conference on System Sciences*, Maui, pp. 5490-5499.

Amazon Web Services Marketplace 2014. "AWS Marketplace," https://aws.amazon.com/marketplace. Visited: August 13th 2014.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., and Stoica, I. 2009. "Above the Clouds: A Berkeley View of Cloud Computing," *Technical Report UCB/EECS-2009-28, University of California, Berkeley,* pp. 1-23.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., and Stoica, I. 2010. "A view of cloud computing," *Communications of the ACM* (4:53), pp. 50-58.

Bitran, G., Gurumurthi, S., and Sam, S. 2006. "Emerging Trends in Supply Chain Governance," *MIT Sloan School of Management Working Report Paper 227*, pp. 1-33.

Bleizeffer, T., Calcaterra, J., Nair, D., Rendahl, R., Schmidt-Wesche, B., and Sohn, P. 2011. "Description and application of core cloud user roles," *in Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology*, Cambridge, pp. 1-9.

Blue, V. 2013. "Find out if your data was leaked in the Adobe hack," http://www.zdnet.com/find-out-if-your-data-was-leaked-in-the-adobe-hack-7000023065/. Visited: August 13th 2014.

Bresnahan, J., Keahey, K., LaBissoniere, D., and Freeman, T. 2011. "Cumulus: an open source storage cloud for science," *in Proceedings of the 2nd International Workshop on Scientific Cloud Computing*, San Jose, pp. 25-32.

Buyya, R., Yeo, C. S., and Venugopal, S. 2008. "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities," *in 10th IEEE International Conference on High Performance Computing and Communications*, Dalian, pp. 5-13.

Böhm, M., Koleva, G., Leimeister, S., Riedl, C., and Krcmar, H. 2010. "Towards a generic value network for cloud computing," *in Economics of Grids, Clouds, Systems, and Services,* Jörn Altmann and O. F. Rana (eds.) Springer, pp. 129-140.

Choi, T., and Hartley, H. 1996. "An exploration of supplier selection practices across the supply chain," *Journal of Operations Management* (4:14), pp. 333-343.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., and Molina, J. 2009. "Controlling data in the cloud: outsourcing computation without outsourcing control," *in Proceedings of the 2009 ACM workshop on Cloud Computing Security*, Chicago, pp. 85-90.

Clarke, R. 2010. "Computing clouds on the horizon? Benefits and risks from the user's perspective," *in 23rd Bled eConference*, Bled, pp. 569-590.

Clarke, R. 2012a. "A Framework for the evaluation of cloudsourcing proposals," *in 25th Bled Conference*, Bled, pp. 309-323.

Clarke, R. 2012b. "How reliable is cloudsourcing? A review of articles in the technical media 2005–11," *Computer Law & Security Review* (1:28), pp. 90-95.

Clemons, E. K., and Chen, Y. 2011. "Making the decision to contract for cloud services: managing the risk of an extreme form of IT outsourcing," *in 44th Hawaii International Conference on System Sciences*, Manoa, pp. 1-10.

CloudServiceMarket 2014. "CloudServiceMarket," http://www.cloudservicemarket.info/. Visited: August 13th 2014.

Cloud Standards Customer Council 2014. "Cloud Standards Customer Council," http://www.cloud-council.org/. Visited: August 13th 2014.

Dillon, T., Wu, C., and Chang, E. 2010. "Cloud computing: issues and challenges," *in 24th IEEE International Conference on Advanced Information Networking and Applications*, Perth, pp. 27-33.

Evolven 2012. "Downtime, Outages and Failures - Understanding their True Costs," http://www.evolven.com/blog/downtime-outages-and-failures-understanding-their-true-costs.html. Visited: August 13th 2014.

Gereffi, G., Humphrey, J., Sturgeon T. 2005. "The governance of global value chains," *Review of International Political Economy* (1:12), pp. 78-104.

Gregor, S., and Hevner, A. R. 2013. "Positioning and presenting design science research for maximum impact," *Management Information Systems Quarterly* (2:37), pp. 337-355.

Grobauer, B., Walloschek, T., and Stocker, E. 2011. "Understanding cloud computing vulnerabilities," *IEEE Security & Privacy* (2:9), pp. 50-57.
Guo, Z., Song, M., and Song, J. 2010. "A Governance Model for Cloud Computing," *in International Conference on Management and Service Science*, Wuhan, pp. 1-6.
Hallikas, J., Virolainen, V., and Tuominen, M. 2002. "Risk analysis and assess- ment in network environments: a dyadic case study," *International Journal of Production Economics* (1:78), pp. 45-55.
Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V., and Tuominen, M. 2004. "Risk management processes in supplier networks," *International Journal of Production Economics* (1:90), pp. 47-58.
Harland, C. M. 1996. "Supply chain management: relationships, chains and networks," *British Journal of Management* (1:7), pp. 63-80.
Harnisch, S., and Buxmann, P. 2013. "Evaluating Cloud Services Using Methods of Supplier Selection," *in Business Information Systems*, Poznan, pp. 1-13.
Harris, D. 2011. "Cloud Platforms Heroku, DotCloud & EngineYard Hit Hard By Amazon Outage," http://gigaom.com/2011/04/21/more-than-100-sites-went-down-with-ec2-including-your-paas-provider/. Visited: August 13th 2014.
Harris, D. 2014. "Did google just doom the lot of small-scale cloud providers?" http://gigaom.com/2014/03/29/did-google-just-doom-the-lot-of-small-scale-cloud-providers/. Visited: August 13th 2014.
Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design science in information systems research," *Management Information Systems Quarterly* (1:28), pp. 75-106.
Höfer, C., and Karagiannis, G. 2010. "Taxonomy of cloud computing services," *in IEEE GLOBECOM Workshops*, Miami, pp. 1345-1350.
Höfer, C., and Karagiannis, G. 2011. "Cloud computing services: taxonomy and comparison," *Journal of Internet Services and Applications* (2:2), pp. 81-94.
IDC 2013. "IDC Forecasts Worldwide Public IT Cloud Services Spending to Reach Nearly $108 Billion by 2017 as Focus Shifts from Savings to Innovation," http://www.idc.com/getdoc.jsp?containerId=prUS24298013. Visited: August 13th 2014.
Jaeger, P. T., Lin, J., and Grimes, J. M. 2008. "Cloud Computing and Information Policy: Computing in a Policy Cloud?," *Journal of Information Technology & Politics* (5:3), pp. 269-283.
Jansen, W. A. 2011. "Cloud hooks: Security and privacy issues in cloud computing," *in Proceedings of the 44th Hawaii International Conference on System Sciences*, Manoa, pp. 1-10.
Jones, C., Hesterly, W., and Borgatti S. 1997. "A General Theory of Network Governance: Exchange Conditions and Social Mechanisms," *The Academy of Management Review* (4:22), pp. 911-945.
Kaplan, S., and Garrick, B. J. 1981. "On the quantitative definition of risk," *Risk Analysis* (1:1), pp. 11-27.
Knackstedt, R., Lis, L., Stein, A., Barth, I., and Becker, J. 2009. "Towards a reference model for online research maps," *in Proceedings of the 17th European Conference on Information Systems*, Verona, pp. 2315-2326.
König, C., Mette, P., and Müller, H. 2013. "Multivendor portfolio strategies in cloud computing," *in Proceedings of the 21st European Conference on Information Systems*, Utrecht, pp. 1-12.
Lambert, D. M., Cooper, M. C., and Pagh, J. D. 1998. "Supply chain management: implementation issues and research opportunities," *The International Journal of Logistics Management* (2:9), pp. 1-20.
Laurent, O. 2013. "EyeEm photo-sharing app aims to enable photographers to sell their images," *British Journal of Photography*. http://www.bjp-online.com/2013/04/eyeem-photo-sharing-app-aims-to-enable-photographers-to-sell-their-images/. Visited: August 13th 2014.
Leavitt, N. 2009. "Is Cloud Computing Really Ready for Prime Time?" *Computer* (1:42), pp. 15-20.
Leimeister, S., Riedl, C., Böhm, M., and Krcmar, H. 2010. "The business perspective of cloud computing: actors, roles, and value networks," *in Proceedings of 18th European Conference on Information Systems*, Pretoria, pp. 1-12.
Linden, A., and Fenn, J. 2003. "Understanding Gartner's hype cycles," *Strategic Analysis Report Nº R-20-1971. Gartner Inc,* pp. 1-12.
Marinos, A., and Briscoe, G. 2009. "Community cloud computing," *in Proceedings of the 1st International Conference on Cloud Computing*, Beijing, pp. 472-484.
Martens, B., and Teuteberg, F. 2011. "Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model." *in 17th Americas Conference on Information Systems*, Detroit, pp. 1-10.

Miller, K. D. 1992. "A framework for integrated risk management in international business," *Journal of International Business Studies* (2:23), pp. 311-331.

Miller, R. 2011. "Outage in Dublin Knocks Amazon, Microsoft Data Centers Offline," http://www.datacenterknowledge.com/archives/2011/08/07/lightning-in-dublin-knocks-amazon-microsoft-data-centers-offline/. Visited: August 13th 2014.

Nickerson, R. C., Varshney, U., and Muntermann, J. 2013. "A method for taxonomy development and its application in information systems," *European Journal of Information Systems* (3:22), pp. 336-359.

OMG 2011. "UML 2.4.1 Superstructure," http://www.omg.org/spec/UML/2.4.1/Superstructure/PDF/. Visited: August 13th 2014.

Paternò, F., and Santoro, C. 2002. "Preventing user errors by systematic analysis of deviations from the system task model," *International Journal of Human-Computer Studies* (2:56), pp. 225-245.

Prater, E. 2005. "A framework for understanding the interaction of uncertainty and information systems on supply chains," *International Journal of Physical Distribution & Logistics Management* (7:35), pp. 524-539.

Provian, K., and Kenis, P. 2007. "Modes of Network Governance: Structure, Management, and Effectiveness," *Journal of Public Administration Research and Theory* (2:18), pp. 229-252.

Richley, G., Roath, A., and Whipple, J. 2010. "Exploring a Governance Theory of Supply Chain Management: Barriers and Facilitators to Integration," *Journal of Business Logistics* (1:31), pp. 237-256.

Rimal, B. P., Choi, E., and Lumb, I. 2009. "A taxonomy and survey of cloud computing systems," *in 5th International Joint Conference on INC, IMS and IDC*, Seoul, pp. 44-51.

Saripalli, P., and Walters, B. 2010. "Quirc: A quantitative impact and risk assessment framework for cloud security," *in Proceedings of the 3rd International Conference on Cloud Computing*, Miami, pp. 280-288.

Schuette, R., and Rotthowe, T. 1998. "The guidelines of modeling–an approach to enhance the quality in information models," *in Conceptual Modeling–ER'98,* Tok-Wang Ling, S. Ram and M. L. Lee (eds.) Springer, pp. 240-254.

Spekman, R., Kamauff, J., and Myhr, N. 1998. „An Empirical Investigation into Supply Chain Management – A Perspective on Partnerships," *Supply Chain Management* (2:3), pp. 53-67.

Stoneburner, G., Goguen, A., and Feringa, A. 2002. "Risk management guide for information technology systems," *NIST special publication 800-30*, pp. 1-56.

Troshani, I., Rampersad, G., and Wickramasinghe, N. 2011. "On Cloud Nine? An Integrative Risk Management Framework for Cloud," *in 24th Bled Conference*, Bled, pp. 15-26.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., and Lindner, M. 2009. "A Break in the Clouds: Towards a Cloud Definition," *ACM SIGCOMM Computer Communication Review* (1:39), pp. 50-55.

Vom Brocke, J., and Thomas, O. 2006. "Reference Modeling for Organizational Change: Applying Collaborative Techniques for Business Engineering." *in Proceedings of the 12th Americas Conference on Information Systems*, Acapulco, pp. 680-688.

Wathne, K., and Heide, J. 2004. "Relationship Governance in a Supply Chain Network," *Journal of Marketing* (1:68), pp. 73-89.

Youseff, L., Butrico, M., and Da Silva, D. 2008. "Toward a unified ontology of cloud computing," *in Grid Computing Environments Workshop*, Austin, pp. 1-10.

Zhang, X., Wuwong, N., Li, H., and Zhang, X. 2010. "Information security risk management framework for the cloud computing environments," *in 10th International Conference on Computer and Information Technology*, Bradford, pp. 1328-1334.

Zissis, D., and Lekkas, D. 2012. "Addressing cloud computing security issues," *Future Generation Computer Systems* (3:28), pp. 583-592.

Appendix

Table 1: Description of Actors

Actor			Description
Provider	Initial Producer	Initial App. Prov.	Applications encompass software, web apps, or internet services, often summarized as SaaS, which are developed and made available on the provider's own infrastructure. The Initial Application Provider provides the "appropriate hardware and software infrastructure to run the service and the people to manage and maintain this infrastructure" (Bleizeffer et al. 2011). Services are provided to *0…n* Intermediaries and *0…n* Clients. *Examples: Microsoft Office 365, Google Mail.*
		Initial Plat-form Prov.	Initial Platform Providers offer an "environment within which cloud applications can be deployed" (Leimeister et al. 2010), including an operating environment, application programming interfaces (APIs), programming languages and so on (Boehm et al. 2010). The Initial Platform Provider uses its own infrastructure to provide its platform. Services are provided to *0…n* Intermediaries and *0…n* Clients. *Examples: Microsoft Windows Azure, Google App Engine.*
		Initial Infrastr. Prov.	Initial Infrastructure Providers provide IT resources such as "storing and processing capacity" (Vaquero et al. 2008). They are usually "companies with other web activities that require large computing resources" (Marinos and Briscoe 2009) and benefit from its economies of scale. Subcategories are the Initial Computing Provider and the Initial Storage Provider. Both provide services to *0…n* Intermediaries and *0…n* Clients. *Initial Computing Provider: Amazon EC2, Rackspace Cloud Servers.* *Initial Storage Provider: Amazon S3, Rackspace Cloud Databases.*
Intermediary	Value-Added Reseller	Application Reseller	The output of an Application Reseller is similar to the output of an Initial Application Provider, whereas the Application Reseller accesses services which encompass "hardware and infrastructure of the infrastructure providers" (Leimeister et al. 2010) or other application or platform services as pre-products and "adds value on top of a given service to ensure some specific capability" (Boehm et al. 2010). However, today's most common form is a self-hosted service that consumes other services as add-ins. An Application Reseller provides services to *0…n* Intermediaries and *0…n* Clients and receives services from *0…n* Providers and *0…n* Intermediaries. *Examples: Crocodoc, Netflix, Talentsoft.*
		Platform Reseller	The output of a Platform Reseller is similar to the output of an Initial Platform Provider, whereas the Platform Reseller accesses computing power or data storage of the Initial Infrastructure Providers or other platform services as pre-products. A Platform Reseller provides services to *0…n* Intermediaries and *0…n* Clients and receives services from *0…n* Providers and *0…n* Intermediaries. *Examples: Heroku, Bitbucket.*
		Infrastructure Reseller	The Infrastructure Reseller buys and sells infrastructure services. It is a virtual actor and nowadays may not exist. Infrastructure is a standardized commodity thus value can't be added. Markets of commodities are usually liquid and buying and selling an identical service leads to losses due to transaction costs. The optimization of load balancing between internal and external resources, as described by Armbrust et al. (2009), may be a special case when the reselling of infrastructure makes economic sense. An Infrastructure Reseller provides services to *0…n* Intermediaries and *0…n* Clients and receives services from *0…n* Providers and *0…n* Intermediaries. *We are not able to show this actor in a real world example due to missing insight in the internal optimization of Initial Infrastructure Providers. However, our interview partners confirmed the likeliness of its (future) existence.*
		Aggregator	An Aggregator generates value through the aggregation of services without adding new functionalities to existing services. The Aggregator ensures "that the different services work together neatly and that no losses occur via data movement between the systems" (Boehm et al. 2010). An Aggregator provides services to *0…n* Intermediaries and *0…n* Clients and receives services from *0…n* Providers and *0…n* Intermediaries. *Examples: HP Aggregation Platform for SaaS, Zapier.*

	Catalyst	Application Market Place	An Application Market Place matches customer demand with vendor offerings. Its main objective is to "bring customers and service providers together" (Boehm et al. 2010). It offers decision support for the customer through comparing various cloud services "based on certain selection criteria" (Boehm et al. 2010). The Application Market Place could offer additional benefits to both service providers and customers, such as SLA contracting or billing (Boehm et al. 2010). An Application Market Place links services of *0…n* Intermediaries or *0…n* Providers to *0…n* Intermediaries or *0…n* Clients. Independent from this, the Application Market Place may use services of 0…n Intermediaries or *0…n* Providers to run its own service. *Examples are VMware vCloud Hybrid Service Online Marketplace, Salesforce AppExchange.*
		Platform Market Place	A Platform Market Place is similar to the Application Market Place. However, the trading object encompasses platform services. Therefore a Platform Market Place links services of 0…n Intermediaries or *0…n* Providers to *0…n* Intermediaries or *0…n* Clients. Independent from this, the Platform Market Place may use services of *0…n* Intermediaries or *0…n* Providers to run its own service. *We are not able to show this actor in a real world example. However, our interview partners confirmed the likeliness of its future existence. For example, a platform market place could occur due to licensing of platforms such as Microsoft Azure by third party providers.*
		Infrastructure Market Place	An Infrastructure Market Place is similar to the Application Market Place. However, the trading object encompasses infrastructure services. Buyya et al. (2008) describe their vision of a cloud market with brokers that purchase cloud services for their customers. Due to high standardization, infrastructure exchanges may be compared to commodity exchanges which automatically map consumer demand with vendor offerings. An Infrastructure Market Place links services of *0…n* Intermediaries or *0…n* Providers to *0…n* Intermediaries or *0…n* Clients. Independent from this, the Infrastructure Market Place may use services of *0…n* Intermediaries or *0…n* Providers to run its own service. *Example: Deutsche Boerse Cloud Exchange.*
Client			A Client is "the starting point of a service request and the ending point of service delivery" (Boehm et al. 2010). The Client solely uses products produced by its vendors and consumes these products outside of the cloud network. A Client receives services from *0…n* Providers or *0…n* Intermediaries. *Clients mostly encompass "everyday users, Small and Medium sized Enterprises (SMEs), and ambitious start-ups" (Marinos and Briscoe 2009).*

Table 2: Description of Risks, Hazards, and Reinforcers

Challenge		**Description**
Risks	Availability Issues	Most customers worry about availability issues whereas cloud services have set new standards in high availability (Armbrust et al. 2010; Chow et al. 2009; Leavitt 2009). On the other hand, Jansen (2011) states that even a very high level of availability leads to a significant downtime over a year. That's why Clarke (2012a) describes that "outages are not uncommon, and they may last for some hours". In addition, Availability Issues also encompass connection interruptions and performance issues. We can distinguish between permanent and temporary availability issues (Clarke et al. 2010). *Amazon EC2 users were affected by an outage in 2011 Clarke (2012b).*
	Loss of Data	Loss of Data is permanent. In addition, a lack of data integrity describes "sustained correctness of the service, and of the data "Clarke (2012a). It can be compared to Loss of Data because the data is useless and is "harmful to the user and the users' customers" (Clarke 2010). Al Zain et al. (2012) state that data "can suffer from damage during the transition operations from or to the cloud storage". *Innocent companies were affected by an FBI raid in computing centers against a handful of companies that operated out of the centers (Jansen 2011).*
	Price Risks	Besides volatile prices, Price Risks include entry costs, switching costs, or operation costs (Clarke 2012a). Clarke (2010) states that customers are dependent on the prices of their vendors. In addition, the data transmission of large volumes is cost intensive (Clarke 2010). We also identified Price Risks in the literature on financial markets that may become more relevant with the ongoing drive for standardization and commoditization. *We are not able to show this risk in a real world example due to missing insights. However, our interview partners confirmed its existence.*

	Data Security Issues	Data Security Issues concern the security of the service itself and of company-related data. The size of a company has a huge impact on its Data Security, whereby large companies have higher investment volumes and therewith are generally more professional than small companies. However, they are more visible to attackers (Clarke 2010). Jansen (2011) states that data must not only be secured at rest but also when in transit and in use. *We are not able to show this risk in a real world example due to missing insights. However, our interview partners confirmed its existence.*
	Data Privacy Issues	Data Privacy Issues describe the risk of revelation of data that does not belong to the company itself, such as user data. Troshani et al. (2011) mention that besides security breaches, also privacy breaches "can result in serious economic loss". *Adobe was hacked in 2013 and over 100 million user data were revealed (Blue 2013).*
Hazards	Technical Defects	Technical Defects include, hardware, software, or network issues. In addition, Chow et al. (2009) state that some "third-party cloud would not scale well enough to handle certain applications". Cloud actors use redundancy in their infrastructure to improve availability (Armbrust et al. 2010). *Virgin Blue's airline's check-in and online booking systems went down due to a hardware failure, on September 26, 2010 (Evolven 2012).*
Hazards	User Errors	User Errors involve issues such as erroneous entries of data or passwords that can be easily cracked and enable the access to data for outsiders. User Errors are no cloud specific risk and are widely discussed in existing literature, such as (Paternò and Santoro 2002). *Clarke (2012b) mentions a user mistake that led to an outage of "Amazon IaaS" in 2011.*
Hazards	Security Issues	Security Issues include, for example, fraud, hacking, or denial of service attacks (Grobauer et al. 2011) and originate from external attackers or from attacks within the company. Chow et al. (2009) state that sourcing into the cloud enlarges the attack surface of an actor. *An example for a security issues is the leak of a huge amount of authentication names and passwords of Adobe users (Blue 2013).*
Hazards	Natural Disasters	Natural Disasters that affect cloud actors may be, for example, earthquakes, floods, or extreme storms. Jansen (2011) mentions natural disasters as possible source of unplanned outages. *A lightning strike caused a power outage that led to an outage of datacenters of Amazon and Microsoft near Dublin (Miller 2011).*
Hazards	Shift in Demand or Supply	Actors can be affected by demand shifts, which may be caused by strategic decisions of companies, bad publicity, or an outage of a competitor. The development of infrastructure exchanges will most likely raise the volatility of the demand side. On the other hand, supply may shift due to new players urging into the cloud market. Generally, in case of a Shift in Demand or Supply, several actors are affected. *After Facebook bought Instagram lots of Instagram users switched to similar offerings and caused an overstressing of the respective infrastructure which in turn caused outages (Laurent 2013).*
Hazards	Bankruptcy / Buy-out	Going out of business through bankruptcy can cause permanent outage of cloud services (Armbrust et al. 2010; Troshani et al. 2011). Buy-outs may lead to a permanent or temporary outages, modified products, or a new pricing of the service. Bankruptcy and Buy-outs mostly affect small or medium sized cloud actors. *Large IT companies like Oracle and IBM bought a huge amount of small/mid-size Cloud companies during the last years.*
Hazards	Legal Issues	Being target of regulatory actions is an important non-technical issue for cloud actors (Armbrust et al. 2010). In case of legal actions against a vendor or another customer of the vendor, customers may suffer. Furthermore, government surveillance and intellectual property disputes (Jaeger et al. 2008) (and hence attorney-client privilege issues) rise as additional hazards in the context of Legal Issues. *Jansen (2011) describes that the FBI "raided computing centers in Texas and seized hundreds of servers, when investigating fraud allegations against a handful of companies that operated out of the centers".*
Reinforcer	Incom-patibility	Today, cloud services often use proprietary protocols and interfaces (Dillon et al. 2010). Furthermore, initial service compatibility may fade over time, for example through updates, which makes diversification much more difficult. *Deviant update cycles can lead to incompatibility between former compatible actors. This incompatibility usually lasts only a few hours/days. Usually a vendor announces its forthcoming changes to the customers and the customer is able to react.*

	Lack of Transparency / Loss of Control	Migration to the cloud relinquishes control over the company's data and makes it dependent on the service vendor (Clarke 2010; Jansen 2011). Jansen (2011) state that actors that "subcontract some services to third-party service providers should raise concerns". Cloud services are often dependent on a single point of failure (Armbrust et al. 2010; Chow et al. 2009). *An outage can lead to a "cascade effect crippling all organisations dependent on that Cloud, and all those dependent upon them" (Marinos and Briscoe 2009). Due to the lack of transparency, an actor is not able to foresee such effects.*
	Unobtainability of Data / Lock-in	Large datasets at the vendor or proprietary interfaces often force customers to stay within its existing cloud environment (Armbrust et al. 2009). This lock-in of customers is profitable for the vendor (Armbrust et al. 2010) and increases the chance of opportunistic behavior on part of the vendor Clemons and Chen (2011). *Armbrust et al. (2009) compute that the transfer of 10 TB of data from U.C. Berkley to Amazon in Seattle would last over 45 days. A batch process with a huge amount of data is unable to perform with this speed. Additionally, the bandwidth is often quite volatile.*
	Automation Errors	Prater (2005) describes wrongly conditioned ERP systems in supply chain networks which cause "chaotic spikes" in the demand forecast of warehouse systems. Such problems, labelled Automation Errors, could also occur in cloud networks with automatized processes that may be wrongly conditioned and therefore lead to escalating risks. *Armbrust et al. (2009) describe that blacklisting of EC2 IP addresses by spam-prevention services may limit which applications can be effectively hosted.*
	Geographical Distribution of Network Actors	During the last years, data centers were built in areas with cheap energy, low temperature, and favorable legal position. Such preferred geological regions could pose a problem for cloud networks as for example natural disasters might hit different actors at the same time. *A lightning strike caused a power outage that led to an outage of datacenters of Amazon and Microsoft near Dublin (Miller 2011).*

Table 3: Relationships between hazards and risks

Hazard / Risk *If a hazard affects a risk, it is marked with "X".*	Data Security Issues	Data Privacy Issues	Price Risk	Loss of Data	Availability Issues
Technical Defects				X	X
User Errors	X	X		X	X
Security Issues	X	X		X	X
Natural Disasters			X	X	X
Legal Issues	X	X	X	X	X
Shifts in Demand and Supply			X		X
Bankruptcy / Buy-out			X	X	X

Table 4: Relationships between reinforcers and risks

Reinforcer / Risk *If a reinforcer affects a risk, it is marked with "X".*	Data Security Issues	Data Privacy Issues	Price Risk	Loss of Data	Availability Issues
Incompatibilities				X	X
Lack of Transparency / Loss of Control			X		X
Unobtainability of Data / Lock-in			X	X	X
Automation Errors	X	X	X	X	X
Geographical Distribution of Network Actors				X	X