8-5-2011

Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model

Benedikt Martens
University of Osnabrueck, benedikt.martens@uni-osnabrueck.de

Frank Teuteberg
University of Osnabrueck, frank.teuteberg@uni-osnabrueck.de

Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model

Benedikt Martens
University of Osnabrueck
benedikt.martens@uni-osnabrueck.de

Frank Teuteberg
University of Osnabrueck
frank.teuteberg@uni-osnabrueck.de

ABSTRACT

More and more companies are making use of Cloud Computing Services in order to reduce costs and to increase the flexibility of their IT infrastructures. Currently, the focus is shifting towards problems of risk and compliance which include as well the realm of Cloud Computing security. For instance, since the storage locations of data may shift or remain unknown to the user, the problem of the applicable jurisdiction arises and impede the adoption and management of Cloud Computing Services. Therefore, companies need new methods to avoid being fined for compliance violations, to manage risk factors as well as to manage processes and decision rights. This paper presents a reference model that serves to support companies in managing and reducing risk and compliance efforts. We developed the model on the solid basis of a systematic literature review and practical requirements by analyzing Cloud Computing Service offers.

Keywords

Cloud Computing, Reference Modeling, Compliance Management, Risk Management

INTRODUCTION

Industry analysts have made several enthusiastic projections on the potential of Cloud Computing to transform the entire computing industry (Pring, Brown, Frank, Hayward and Leong, 2009). The three main types of Cloud Computing Services are: Software as a Service (SaaS), which refers to application services like Salesforce; Platform as a Service (PaaS), i. e. developer platforms like the Google AppEngine; and finally Infrastructure as a Service (IaaS), which mainly encompasses storage services and computing power services like Amazon Web Services (Mei, Chan and Tse, 2008; Weinhardt, Anandasivam, Blau, Borissov, Meinl, Michalk and Stößer, 2009). However, the question arises whether there are any obstacles on the way to mature Cloud Computing environments. Along with the increasing spread of Cloud Computing concepts and technologies, new fields of activity entailing new risk factors emerge and require new approaches to Risk and Compliance Management (RCM) (Martens, Pöppelbuß and Teuteberg, 2011; Martens and Teuteberg, 2009). We approach this topic from the perspective of a governance, risk and compliance perspective which is understood as an established framework for decision rights and accountabilities to successfully accomplish IT imperatives in response to an enterprise' environmental and strategic imperatives (Weill and Ross, 2004). In that we focus strongly on Risk and Compliance Management (RCM). For instance, companies could face regulatory compliance risks, if they transfer and process sensitive data which are exposed to legal regulations (Talukder, Zimmerman and Prahalad, 2010). Often they are held responsible for the actions of their contractor (Kamara and Lauter, 2010) and the location of the data center determines the jurisdiction (Chaput and Ringwood, 2010). On the other hand, several Cloud Computing providers hide the location of their data centers to prevent physical attacks against them or change the physical location of the stored data to obtain economies of scale (Onwubiko, 2010). As well, several compliance regulations claim for technical and physical IT security mechanism or an implemented control systems (for instance data protection acts (Kamara and Lauter, 2010; Pearson, 2009) or requirements of the Sarbanes Oxley Act (Chaput and Ringwood, 2010)). Thus, the compliance to regulations includes often security mechanisms, which need to be monitored to prevent the exposure of risk factors. Generally, companies should establish a working framework to fulfill requirements from compliance and risk management as well as governance practices to realize Cloud Computing advantages.

In this paper we present an application reference model for RCM of Cloud Computing Services which supports developers during the conceptual phase of a software development project and serves as a solid base to rely on common-practice within this field (Ahlemann and Riempp, 2008; vom Brocke, 2007). The main goals are to support the development of RCM processes, the requirements analysis for RCM software and the specification and design of such software (Ahlemann and Riempp, 2008). Furthermore, our application reference model describes a structured semi-formalized application problem (Rosemann and Van Der Aalst, 2007). Thus, our work focuses on the following research questions (RQ):

- RQ 1: Which specific characteristics and common-practices should been considered during the design and development of reference models for RCM in Cloud Computing environments?
- RQ 2: What are the "inputs" that support and enhance the design and development of RCM processes, the requirements analysis and the specification of RCM software in Cloud Computing environments?

To build the model on the theoretical basis of IT governance theory (Racz, Weippl and Seufert, 2010; Weill and Ross, 2004) we entail the four perspectives Compliance, Risk, Key Performance Indicators (KPI) and Cloud Computing Services. The main goal of the developed artifact is to provide a tool for the monitoring and strong understanding of information assets, risk factors and related legislative and regulatory compliance requirements over the company's data (Chaput and Ringwood, 2010) and to reduce risks by identifying ex ante open RCM issues (Durkee, 2010). To come to a flexible approach we do not focus during the model description on certain legal frameworks.

The paper is structured as follows: in section 2, we discuss related work on the topic of RCM in Cloud Computing. In section 3, we present the research approach. The reference model is introduced in section 4. A conceptual evaluation of the reference model is illustrated in section 5. In section 6, we describe our future research to evaluate the model in detail. Finally, in the concluding section we summarize the research results and discuss implications of our research.

RESEARCH APPROACH

The developed reference model underwent several cycles of development. It is based on a combination of deductive and inductive elements and draws on our own preliminary considerations, the systematic literature review (see section 3) as well as analysis of Cloud Computing Services in our database *CloudServiceMarket* (www.cloudservicemarket.info). With the help of our database, we could identify and classify compliance regulations that are necessary for the usage of Cloud Computing Services. Additionally, this analysis of more than 200 Cloud Computing Services allows us to extract common elements of Cloud Computing Services into our reference model. Throughout the construction process we applied well known principles, conventions and standards in reference modeling to enhance the quality of our models (e. g. the principles (guidelines) for reference modeling such as construction adequacy, language adequacy, and clarity (Frank, 2007; Schuette and Rotthowe, 1998)). Figure 1 illustrates this process of development. At present, our project is at the evaluation-stage. The iteration loop has already been run with the help of the first conceptual evaluation results.

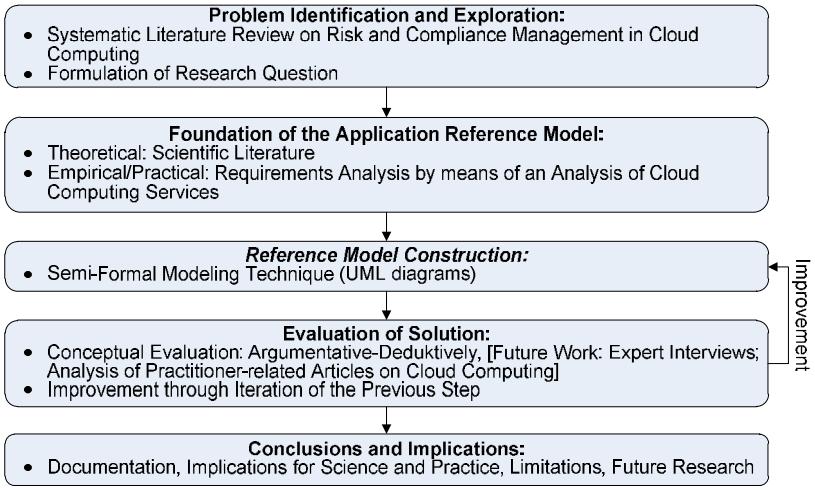

Figure 1. Underlying Research Approach for the Construction of the Reference Model

RELATED WORK

To build this paper on a solid base, we applied the method of a concept-centric systematic literature review (vom Brocke, Simons, Niehaves, Riemer, Plattfaut and Cleven, 2009; Webster and Watson, 2002). As a first step we defined the review scope and concentrate on RCM in Cloud Computing. Key words for the search belong to the realm of RCM Cloud Computing and include terms like regulat*, audit*, law, complian*, govern*, risk combined with "cloud computing" and "as a Service". The applied wildcards assure the identification of related, conjugated terms. Next we applied these key words to scientific databases like EBSCO (Business Source Complete, EconLit (full text)), Science Direct, SpringerLink and AISeL to

receive scientific, peer-reviewed papers. To enlarge the number of papers we used forward (review of reference lists) and backward search (author-centric review).

The Cloud Computing governance model by Guo, Song and Song (2010) addresses requirements and objectives of service, policy, security, risk and compliance management in Cloud Computing and supplements detailed descriptions and important information on the required system design. Their main contribution lies in the development of an architecture for RCM which focuses on the controlling of services and policies (compliance regulations) by means of monitoring Cloud Computing Services. Due to the few solutions for small-scale application on the market, (Guo et al., 2010) emphasizes in their work the importance of software products or Cloud Computing Services that meet the requirements for a holistic RCM approach in Cloud Computing. An overview of RCM in Cloud Computing provide Chaput and Ringwood (2010). They discuss different types of RCM regulations like laws and industry regulations affecting the adoption of Cloud Computing. Four main aspects discussed are security methods like data classification, access control, authentication and authorization, risk management methods like business impact analysis and business continuity, certifications and auditing standards. They conclude that control over the company's information assets is of major importance when adopting Cloud Computing Services. In the realm of compliance management Matthews, Garfinkel, Hoff and Wheeler (2009) propose virtual machine contracts, which extend the open virtual machine format. Since regulations often touch the IT infrastructure and IT security requirements for compliance, the suggested virtual machine contracts could specify and implement them and provide support for the audit of IT infrastructures. These electronic contracts describe and formalize technical requirements as e. g. firewall rules, transport protocols, source and destination addresses as well as source and destination ports, e. g. to configure the virtual machines for a particular network segment. In the work of Kamara and Lauter (2010) methods and architectures for the encryption of cloud storage are presented. One objective is to secure storage services for regulatory compliance by encrypting the data on-premise to avoid access to the data by a third party. Kamara and Lauter (2010) argue that this approach reduces legal exposure for both customer and provider and thus reduces the exposure of these risk factors. For the implementation they apply searchable encryption methods like Symmetric Searchable Encryption (SSE), Asymmetric Searchable Encryption (ASE), Efficient Asymmetric Searchable Encryption (ESE) and the multi-user Symmetric Searchable Encryption (mSSE). The developed architecture models include instances of a data processor, a data verifier, a token generator and a credential generator to secure access to the encrypted data while they are shared with cooperating companies. To provide empirical evidence Heinle and Strebel (2010) conducted 27 expert interviews to investigate organizational factors, which influence the adoption of IaaS. They developed an acceptance model on the base of agency, IT governance and diffusion of innovation theory. Major findings deal with the inhibition of IaaS adoption due to the lack of processes for assessing provider risk and reputation as well as a lack of monitoring and reporting software solutions. Moreover, (Heinle and Strebel, 2010) argue that data protection acts require complex regulations (e. g. for the processing of personal data) which conflict with the basic IaaS principles of an unknown data location and the accompanied economies of scale. An extension of Service Level Agreements (SLA) with regard to compliance issues is presented in the work of (Brandic, Dustdar, Anstett, Schumm, Leymann and Konrad, 2010). They introduce Compliance Level Agreements (CLA) and develop a high-level architecture for compliance management in Cloud Computing. The basis of the CLA is a Domain Specific Language (DSL) to include expert knowledge and map it to CLA templates and finally to the actual CLAs. The paper focuses exclusively on the technical implementation of the developed artifacts and masks particular details and descriptions. Anstett, Karastoyanova, Leymann, Mietzner, Monakova, Schleicher and Strauch (2009) chose a purely technical approach by presenting a general compliance architecture for compliance monitoring of outsourced business processes to the Cloud. The objective is to gather evidence by means of compliant business processes from providers. Technically the developed prototype is set up with a BPEL engine to review the generated events and the audit trail. Thus, the architecture relies on the principles of service, resource, action and event to track activities. Finally, standardization efforts are promoted by the National Institute of Standards and Technology (NIST), a standard-giving organization and the Security Alliance, a network of several industry partners and stakeholders that are providing best practices for security management in Cloud Computing. During the literature analysis process we identified several often discussed open issues on RCM in Cloud Computing. During the model construction process we tried to account for most of these issues to increase the user awareness:

- Location of the data center causes the applicable jurisdiction (Govindarajan and Lakshmanan, 2010)
- Foreign law may allow government access to the outsourced data (Weinhardt et al., 2009) or restricts or prohibited the export of data to another country (legislation) (Gagliardi and Muscella, 2010)
- Occasionally unknown location of the data center and thus uncertain jurisdiction (Govindarajan and Lakshmanan, 2010)
- Data are spread across multiple data centers or are replicated in a different data center with several jurisdictions (Govindarajan and Lakshmanan, 2010)

- Lack of control over the physical infrastructures (Khajeh-Hosseini, Sommerville and Sriram, 2010), which constrains infrastructure audits
- Lack of monitoring and auditing approaches and software products (Govindarajan and Lakshmanan, 2010; Heinle and Strebel, 2010)
- Governance issues like people and decision rights are less important in contrast to major concerns about risk and compliance issues (Brandic et al., 2010; Guo et al., 2010)

As a result, we can conclude that RCM issues in Cloud Computing have been identified as a major concern but only little research has been conducted yet. We find that governance issues are related to compliance, risk and security issues. In particular, it does not become clear how a software solution should be built to tackle these problems. The developed artifacts by (Matthews et al., 2009) and (Kamara and Lauter, 2010) indicate the need for such methods and approaches, since companies could face penalty payments which could balance the cost advantages of Cloud Computing. Moreover, Govindarajan and Lakshmanan (2010) and Yunis (2009) found that software products or services do not exist on the market yet. First insights towards the development of a reference model are provided in the literature (Anstett et al., 2009; Brandic et al., 2010). Since they often focus on non-functional requirements, we extend the body of knowledge by introducing a more functional-driven approach to the topic. The scientific quality in the field of compliance management in Cloud Computing lacks high-quality research, as e. g. publications in journals.

REFERENCE MODEL

Meta-Reference Model and Sources for Model Construction

Figure 2 introduces a meta-reference model which serves as a regulation framework to structure the application problem and its different aspects. It illustrates the grouping and interrelations between the model perspectives KPI, Risk, Compliance and Cloud Computing Services. Due to the limited presentation space, we split the reference model up in two figures (cf. Figure 3 and 4). We chose the Unified Modeling Language (UML) as modeling language and use class diagrams for the presentation of the reference model. The UML fulfills the basic principle of the systemic construction of reference information models and is directly compatible to object-oriented programming languages.

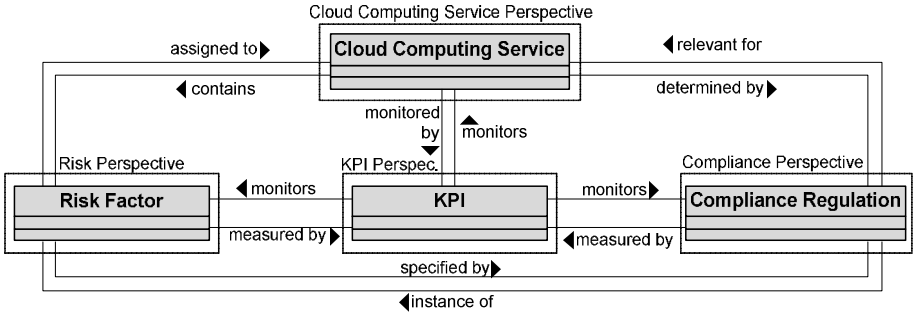

Figure 2. Meta-Reference Model for Risk and Compliance Management in the Cloud

The theoretical foundation of the model relies on governance, risk and compliance research, which is as well as Cloud Computing, a practitioner-driven topic (Racz et al., 2010). Racz et al. (2010) define governance, risk and compliance as a holistic approach to align ethical, risk, policy and regulatory compliance with the company's strategy, processes, technology and people to improve efficiency and effectiveness. Thus, we need several application components to fulfill the requirements of this approach. For instance, governance is included in several components: Processes are presented in the Cloud Computing Service perspective and an accountability framework is included in each component, by adding accountable roles to each major model class. The KPI component plays a critical role within the application problem, since it offers decision-makers monitor and control mechanisms. The risk and the compliance perspective represent a detailed description of both risk and compliance factors as well as auditing efforts and results.

In Table 1 we assigned the identified, most relevant literature references identified during the systematic literature review and other sources to each model perspective and element group. Within the references, the presented constructs are either modeled or discussed by means of (research) results.

Perspec-tives	Element	References
Cloud Computing Service	Broker	(Buyya et al., 2009)
	Location	(Armbrust et al., 2010; Chaput and Ringwood, 2010; CSA, 2011; Kamara and Lauter, 2010)
	Service Type and Resource	(Brandic et al., 2010; Buyya et al., 2009; Iqbal and Nieves, 2007)
	SLA	(Braun and Winter, 2005; Chen, 2008; COBIT, 2007; Iqbal and Nieves, 2007; Matthews et al., 2009)
	Security	(Chaput and Ringwood, 2010; CSA 2011, ENISA 2009, Helmbrecht, 2010)
KPI	Type	(Chen, 2008; Iqbal and Nieves, 2007; Talukder et al., 2010)
	Action	(Anstett et al., 2009; Brandic et al., 2010)
Risk	Risk Attitude	(Bahli and Rivard, 2003)
	(Macro) Effects	(Martens and Teuteberg, 2009)
	Risk Category	(Bahli and Rivard, 2003; COBIT, 2007, Martens and Teuteberg, 2009)
Compliance	Compliance Level	(Müller and Supatgiat, 2007)
	Compliance Audit	(Guo et al., 2010; Müller and Supatgiat, 2007)
	Type of Data Processing	(Khajeh-Hosseini et al., 2010; Pearson, 2009)
	Types of Compliance Regulations	(Chaput and Ringwood, 2010; COBIT, 2007, CSA 2011)

Table 1. Main sources drawn on for the construction of the reference model

Cloud Computing Service and Key Performance Indicator Perspective

The Cloud Computing Service perspective (SLA, business process, Cloud Computing Service characterization; illustrated in Figure 3) forms the center of the meta-reference model and is linked to all other perspectives via connectors. This perspective includes the particular characteristics of Cloud Computing Services like the importance of the location of service delivery and security measures (Armbrust, et al. 2010). Connectors link the Cloud Computing Service perspective to objects from other perspectives which are marked by a frame and the model name. For example, an Cloud Computing Service is monitored by means of one or several KPIs which are part of the KPI perspective and are further specified there (Braun and Winter 2005). Such standardized Cloud Computing Services can be individually combined with the help of brokers (Buyya, et al. 2009). A broker takes up the function of a mediator. It can either be operated internally (organizational role) or externally (third party service provider). The composition of Cloud Computing Services can result in economic advantages for the customer (Buyya et al., 2009). Correspondingly, an external broker can generate a profit by combining Cloud Computing Services. This profit can be defined as the difference between the company's added value and the original Cloud Computing Service costs. Furthermore, we added the objects for the definition of business processes that are supported by Cloud Computing Services and assigned to roles to fulfill business objectives (Braun and Winter, 2005). Each process consists of several process elements like functions, operators and events. SLAs in which the Cloud Computing Services are specified could be distinguished by means of their pricing scheme (Iqbal and Nieves, 2007). Both fixed prices and negotiable prices as well as specifications are characterized by means of costs, quality, duration, performance and the software usage (e. g. operation system of platform services).

The KPI perspective supports the operationalization of measures and strategic objectives (Iqbal and Nieves, 2007). KPIs monitor the performance of e. g. Cloud Computing Services, risk factors and compliance issues (KPI types) and are interrelated with each perspective within the reference model. The different values of a KPI, as the target, current and range (lower and higher limit) values trigger actions to improve the actual KPI value. These actions are conducted by organizational roles that compose reports (Braun and Winter, 2005). Within the formal characterization it is differentiated between qualitative and quantitative KPIs and different types of scales (Guo et al., 2010).

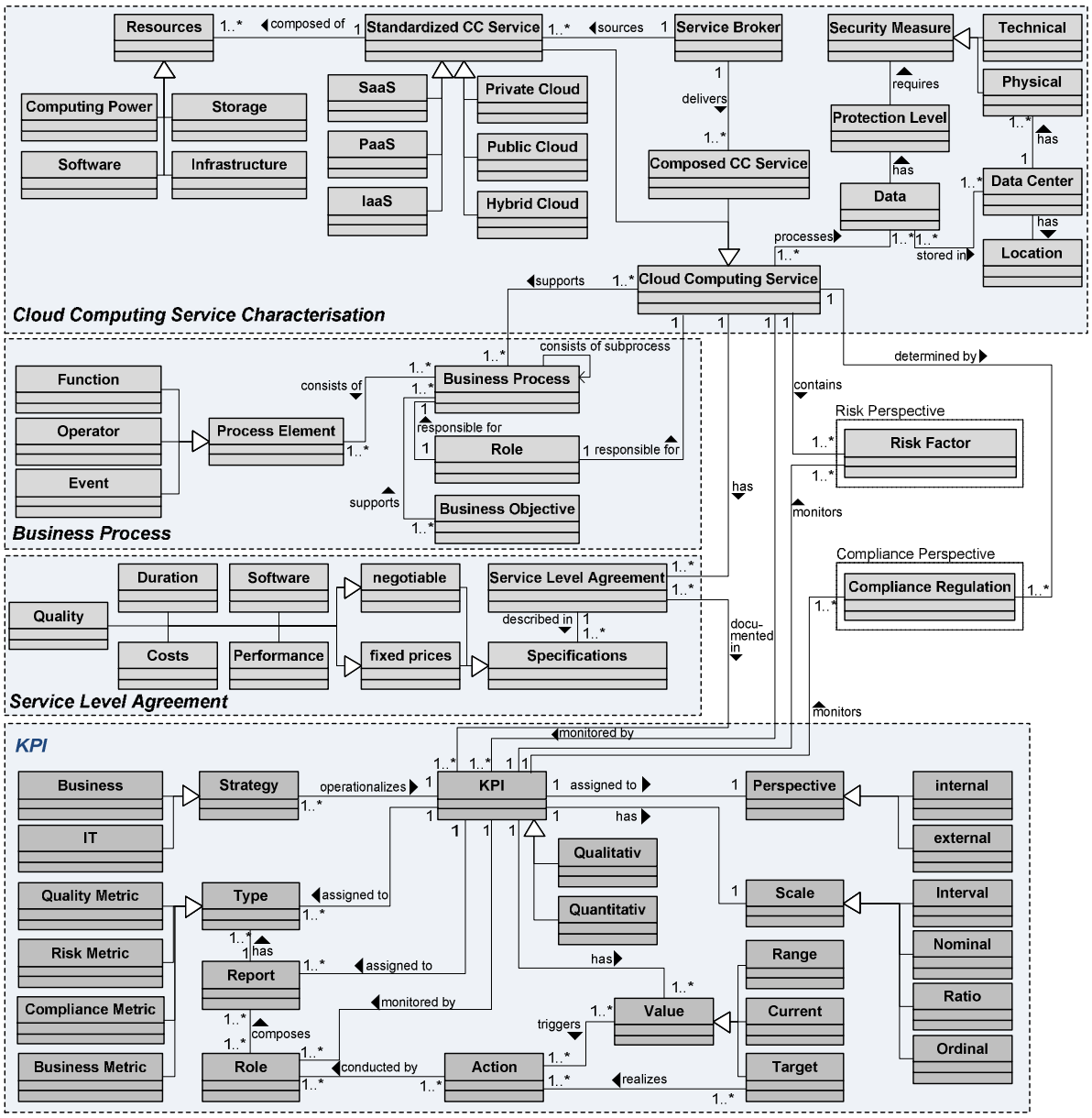

Figure 3. Cloud Computing Service and KPI Perspective

Risk and Compliance Perspective

Figure 4 depicts the risk (risk attitude, effects on assets, risk documentation and controls and general risk description) and the compliance (compliance level, audit, compliance regulation description) perspective. Risk factors are monitored by a KPI and are assigned to Cloud Computing Services and specified by compliance regulations. The decision maker has a certain risk attitude, as e. g. risk-averse, risk-neutral or risk-seeking (Bahli and Rivard, 2003) and evaluates risk factors. The probability of risk occurring can be grounded empirically by means of risk databases as e. g. the Operational Riskdata eXchange Association (ORX) (online: http://www.orx.org/) (Sackmann, Lowis and Kittel, 2009). Each identified risk factor is documented and proved by a risk audit and additional described controls (COBIT 2007). Risk factors are causing effects (described as loss) and macro effects (failure) on the business and IT of the company (Aloini, Dulmin and Mininno, 2007). Beside a risk mitigation method a risk category can be assigned to a risk factor (Iqbal and Nieves, 2007).

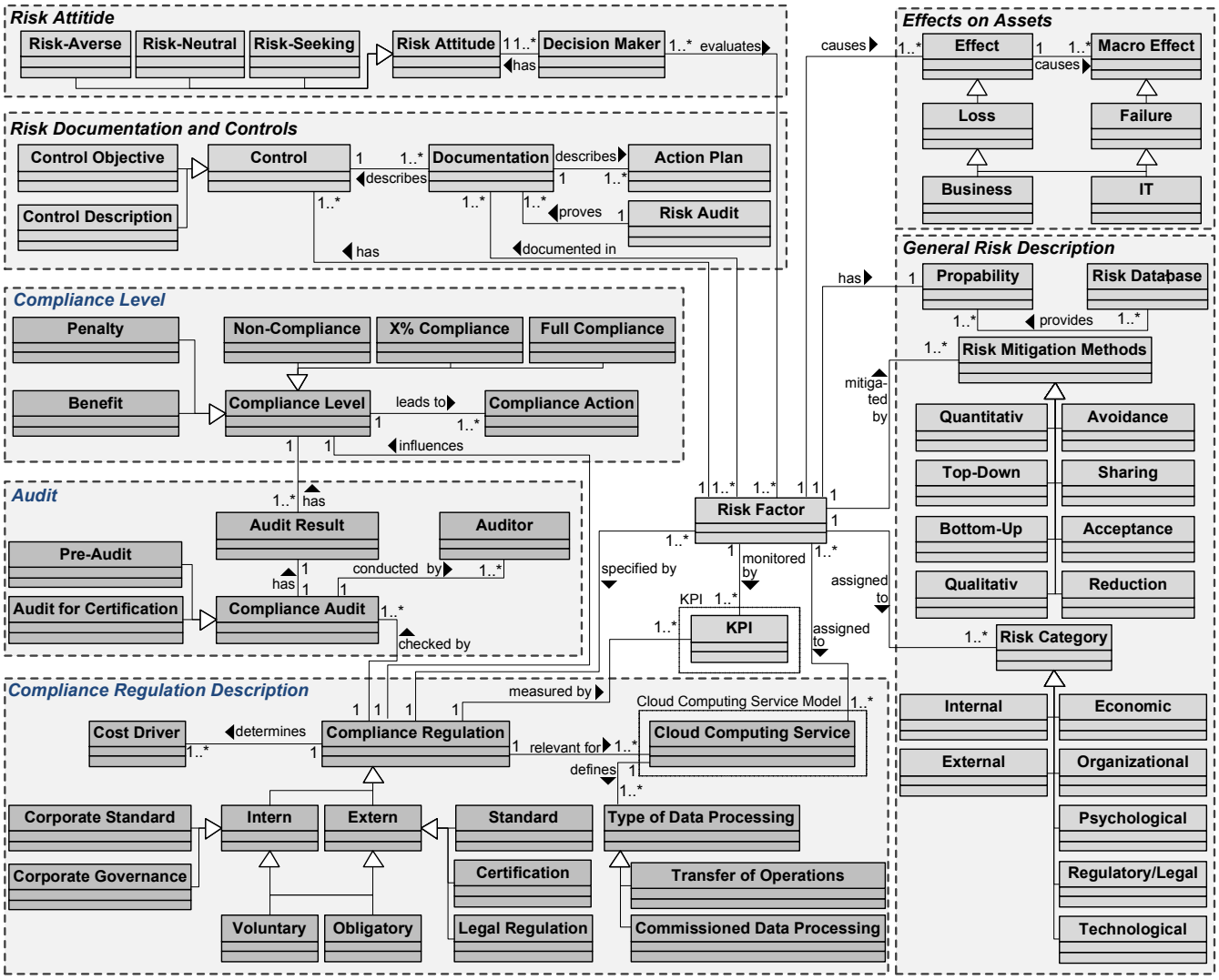

Figure 4. Risk and Compliance Perspective

Compliance with regulations and standards is a risk factor of particular significance. If a risk factor refers to a compliance regulation it is also assigned to the risk category „Regulatory/Legal“. The interconnection between the risk and compliance perspective shows that a risk factor is specified by a compliance regulation. The three central components are: compliance regulation description, compliance audit (monitoring of compliance) and compliance level (degree of compliance with a regulation). Compliance regulations can be distinguished into internal (e. g. corporate standard or governance) and external regulations (e. g. industry standard, certification or legal regulation) and can be characterized by means of voluntary or obligatory (Chaput and Ringwood, 2010). Compliance audits are conducted by external auditors, either in the form of pre-audits (friendly audits) or in order to obtain certification. We follow the research of Müller and Supatgiat (2007), who define compliance as a continuous rather than a binary phenomenon and introduce the concept of compliance levels. Müller and Supatgiat (2007) suggest a way of calculating the optimal compliance level on the basis of minimum costs and maximum profit in order to clarify where compliance (or a lack of it) leads to penalties or benefits for the company and to identify the necessary actions to be taken. Finally, what remains significant for Cloud Computing is the way of external data processing, which is in data protection acts of high importance. One can distinguish between transfer of operations and commissioned data processing.

CONCEPTUAL EVALUATION

In the literature, only few explicit evaluation approaches to reference models can be found, most of which, however, do not lead to convincing results (Frank, 2007). Therefore, we decided to follow a multi-method approach in order to ensure a thorough evaluation of our model. As a general guideline, we used the widely accepted modeling principles of Schuette and Rotthowe (1998) who emphasizes that the quality assurance of a model starts with a well-designed research process (cf. Figure 1), as well as the design and the presentation of the model itself. Adherence to these guiding principles is likely to result in a high-quality model. Our model is primarily based on the results of a systematic literature review to capture the state-of-the-art in RCM in Cloud Computing from a reliable scientific perspective. Furthermore, to integrate the practical perspective we supplemented empirical data from our database *CloudServiceMarket* (www.cloudservicemarket.info). The analysis of the Cloud Computing Services revealed new insights for our model construction and for the identification of wide spread certificates. Additionally we include best-practices and recommendations from reference models and standard giving organizations like ITIL (COBIT 2007; CSA 2011, ENISA 2009, Iqbal and Nieves, 2007, Mell and Grance, 2009).

FUTURE RESEARCH

For the further improvement and evaluation of the presented reference model, we decided to get more insights from the practitioner perspective by two different approaches. First, we are aiming to receive insights from the analysis of practitioner articles from magazines and internet articles. The huge amount of information researcher and practitioners are facing should be analyzed with the help of quantitative content analysis. In-depth content as well as sentence analyses could help to identify topic relevant news and articles, leading to insights for the reference model enhancement. The second approach follows the recommendations by Frank (2007) and aims at consulting experts by means of guided interviews. The interviews will be conducted with industry partners who have several years of experience in the field of Cloud Computing. In particular, we will apply a wide spectrum of expert knowledge for instance from the fields of law, IT service management, risk management and data center experts from both a provider and user company perspective. The main goal is to identify differences and similarities in RCM. For the technical evaluation we think about an implementation of the model in a reverse engineering tool to base our future research on the established knowledge and reduce the implementation efforts (Kollmann, Selonen, Stroulia, Systa and Zundorf, 2002).

CONCLUSIONS AND IMPLICATIONS

The reference model presented in this paper helps for RCM in Cloud Computing and to reduce the total expenditure for RCM management of Cloud Computing Services. At the same time, it improves the quality and efficiency of Cloud Computing Service Management through measurements based on KPIs and dashboards to control outsourced Cloud Computing Services. Furthermore, it provides a first generic IT artifact that helps to understand the managerial, technological and organizational challenges of Cloud Computing Services with regard to RCM issues. The model is based on a reliable basis of scientific literature and captures the current state-of-the-art in Cloud Computing management by including reference models and recommendations that support practitioners with common-practices. For the further improvement and exploration of the Cloud Computing research we see the following significant contributions the IS research community can make: Firstly, Software systems for Cloud Computing need to be developed in accordance with the most important standards and reference models. This refers to terminology, methods and processes. Moreover, it needs to be explored how software systems can be made configurable so that they can easily switch between different standards/reference models and could support the different types of Cloud Computing Services and Clouds. The developed model does not distinguish between these service and Cloud types and takes a generic approach to the topic. The main objective of the discussed model is to present a first proposal for the focused research field. Yet, the model underwent several iteration steps for improvement. While Grid Computing has been extensively driven by academia, the fields of Cloud Computing is driven and advanced by practice (Weinhardt et al., 2009). The cooperation of science and practice needs to be further promoted by applying research methods like action research or field research in order to build a bridge for knowledge exchange. In particular, in practice developed artifacts and reference models should be accompanied by research to apply validated methods and build new knowledge on the current state of research. As well, researchers can learn from Cloud Computing practice and improve existing scientific approaches.

REFERENCES

Ahlemann, F., and Riempp, G. (2008) RefModPM: A Conceptual Reference Model for Project Management Information Systems, *Wirtschaftsinformatik*, 50, 2, 88-97.

Aloini, D., Dulmin, R., and Mininno, V. (2007) Risk management in ERP project introduction: Review of the literature, *Information & Management*, 44, 6, 547-567.

Anstett, T., Karastoyanova, D., Leymann, F., Mietzner, R., Monakova, G., Schleicher, D., and Strauch, S. (2009) MC-Cube: Mastering Customizable Compliance in the Cloud, in *Proceedings of the 7th International Joint Conference on Service Oriented Computing*, 592-606.

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

Bahli, B., and Rivard, S. (2003) The information technology outsourcing risk: a transaction cost and agency theory-based perspective, *Journal of Information Technology*, 18, 3, 211-221.

Brandic, I., Dustdar, S., Anstett, T., Schumm, D., Leymann, F., and Konrad, R. (2010) Compliant Cloud Computing (C3): Architecture and Language Support for User-Driven Compliance Management in Clouds, in *Proceedings of the 3rd International Conference on Cloud Computing*, IEEE, 244-251.

Braun, C., and Winter, R. (2005) A Comprehensive Enterprise Architecture Metamodel and Its Implementation Using a Metamodeling Platform, in Ulrich Frank (Eds.) *Proceedings of the 2nd International Workshop on Enterprise Modelling and Information Systems Architectures*, Gesellschaft für Informatik, 64-79.

Brocke, J. vom (2007) Construction Concepts for Reference Models, Reusing Information Models by Aggregation, Specialisation, Instantiation, and Analogy, in *Reference Modelling for Business Systems Analysis*, IDEA, 47-75.

Brocke, J. vom, Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., and Cleven, A. (2009) Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process, in *Proceedings of the European Conference on Information Systems*, Verona, Italy.

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., and Brandic, I. (2009) Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, *Future Generation Computer Systems*, 25, 6, 599-616.

Chaput, S.R., and Ringwood, K. (2010) Cloud Compliance: A Framework for Using Cloud Computing in a Regulated World, in Nick Antonopoulos and Lee Gillam (Eds.) *Cloud Computing Principles Systems and Applications*, Springer, 241-255.

Chen, H.-M. (2008) Towards Service Engineering: Service Orientation and Business-IT Alignment, in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences HICSS 2008*, IEEE, 114-114.

COBIT (2007) COBIT 4.1 - Control Objectives for Information and related Technology, ITGI – IT Governance Institute.

CSA (2011) Cloud Security Alliance GRC Stack, Cloud Security Alliance.

Durkee, D. (2010) Why cloud computing will never be free, *Communications of the ACM*, 53, 5, 62.

ENISA (2009) Cloud Computing: Benefits, risks and recommendations for information security, ENISA.

Frank, U. (2007) Evaluation of Reference Models, in Peter Fettke and Peter Loos (Eds.) *Reference Modeling for Business Systems Analysis*, IDEA, 118-139.

Gagliardi, F., and Muscella, S. (2010) Cloud Computing – Data Confidentiality and Interoperability Challenges, in Nick Antonopoulos and Lee Gillam (Eds.) *Cloud Computing Principles Systems and Applications Computer Communications and Networks*, Springer, 257-270.

Govindarajan, A., and Lakshmanan, G. (2010) Overview of Cloud Standards, in N Antonopoulos and L Gillam (Eds.) *Cloud Computing Principles Systems and Applications*, Springer, 77-89.

Guo, Z., Song, M., and Song, J. (2010) A Governance Model for Cloud Computing, in *Proceedings of the International Conference on Management and Service Science*, IEEE, 3759-3764.

Heinle, C., and Strebel, J. (2010) IaaS Adoption Determinants in Enterprises, in R. Altmann, J.; Rana, O. F.; Buyya (Eds.) *GECON 2010, LCNS*, Springer, 93–104.

Helmbrecht, U. (2010) Data protection and legal compliance in cloud computing, *Datenschutz und Datensicherheit - DuD*, 34, 8, 554-556.

Iqbal, M., and Nieves, M. (2007) IT Infrastructure Library V3 - Service Strategy, Office of Government Commerce.

Kamara, S., and Lauter, K. (2010) Cryptographic Cloud Storage, *Proceedings of the 1st Workshop on RealLife Cryptographic Protocols and Standardization*, 1-14.

Khajeh-Hosseini, A., Sommerville, I., and Sriram, I. (2010) Research Challenges for Enterprise Cloud Computing,

Kollmann, R., Selonen, P., Stroulia, E., Systa, T., and Zundorf, A. (2002) A study on the current state of the art in tool-supported UML-based static reverse engineering, in Liz Burd and Arie Van Deursen (Eds.) *Proceedings of the Ninth Working Conference on Reverse Engineering*, IEEE, 22-32.

Martens, B., Pöppelbuß, J., and Teuteberg, F. (2011) Understanding the Cloud Computing Ecosystem: Results from a Quantitative Content Analysis, in *Proceedings of the 10th International Conference on Wirtschaftsinformatik*, Zürich.

Martens, B., and Teuteberg, F. (2009) Why Risk Management Matters in IT Outsourcing - A Systematic Literature Review and Elements of a Research Agenda, in *Proceedings of the 17th European Conference on Information Systems*, Italy.

Matthews, J., Garfinkel, T., Hoff, C., and Wheeler, J. (2009) Virtual machine contracts for datacenter and cloud computing environments, *Proceedings of the 1st workshop on Automated control for datacenters and clouds ACDC 09*, 25-30.

Mei, L., Chan, W.K., and Tse, T.H. (2008) A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues, in *Proceedings of the IEEE Asia-Pacific Services Computing Conference*, Yilan, 464-469.

Mell, P., and Grance, T. (2009) NIST Definition of Cloud Computing, Gaithersburg, USA.

Müller, P., and Supatgiat, C. (2007) A quantitative optimization model for dynamic risk-based compliance management, *IBM Journal of Research and Development*, 51, 3/4, 295-307.

Onwubiko, C. (2010) Security Issues to Cloud Computing, in Nick Antonopoulos and Lee Gillam (Eds.) *Cloud Computing*, London, 271-288.

Pearson, S. (2009) Taking Account of Privacy when Designing Cloud Computing Services, in *Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing*, 44-52.

Pring, B., Brown, R.H., Frank, A., Hayward, S., and Leong, L. (2009) Sizing the Cloud, Understanding the Opportunities in Cloud Services, Gartner.

Racz, N., Weippl, E., and Seufert, A. (2010) A Frame of Reference for Research of Integrated Governance , Risk & Compliance, in *Proceedings of the 11th IFIP TC 6/TC 11 International Conference*, 107-116.

Rosemann, M., and Van Der Aalst, W.M.P. (2007) A configurable reference modelling language, *Information Systems Journal*, 32, 1, 1-23.

Sackmann, S., Lowis, L., and Kittel, K. (2009) Selecting Services in Business Process Execution – A Risk-based Approach, in *Proceedings of the 9th International Conference on Wirtschaftsinformatik*, Vienna, 357-366.

Schuette, R., and Rotthowe, T. (1998) The Guidelines of Modeling - An Approach to Enhance the Quality in Information Models, in Tok Wang Ling, Sudha Ram, and Mong Li Lee (Eds.) *Proceedings of the 17th International Conference on Conceptual Modeling*, Springer, 240-254.

Talukder, A.K., Zimmerman, L., and Prahalad, H.A. (2010) Cloud Economics: Principles, Costs, and Benefits, in Nick Antonopoulos and Lee Gillam (Eds.) *Cloud Computing: Principles, Systems and Applications*, Springer-Verlag London, 343-360.

Webster, J., and Watson, R.T. (2002) Analyzing the past to prepare for the future: Writing a literature review, *MIS Quarterly*, 26, 2, xiii-xxiii.

Weill, P., and Ross, J.W. (2004) IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press.

Weinhardt, C., Anandasivam, A., Blau, B., Borissov, N., Meinl, T., Michalk, W., and Stößer, J. (2009) Cloud Computing – A Classification, Business Models, and Research Directions, *Business & Information Systems Engineering*, 1, 5, 391-399.

Yunis, M.M. (2009) A 'cloud-free' security model for cloud computing, *International Journal of Services and Standards*, 5, 4, 354-375.