Future Generation Computer Systems 32 (2014) 274–281

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Towards a framework for governance architecture management in cloud environments: A semantic perspective

Knud Brandis *, Srdan Dzombeta, Knut Haufe

PERSICON Corporation, Friedrichstr. 100, 10117 Berlin, Germany

HIGHLIGHTS

- Authors introduce a model for cloud governance.
- The model serves as a holistic framework addressing governance.
- An ontology is presented that supports a semantic-based formalization of the model.

ARTICLE INFO

Article history:
Received 25 February 2013
Received in revised form
13 September 2013
Accepted 26 September 2013
Available online 18 October 2013

Keywords:
Cloud computing
Governance
Semantic technologies
Ontology
Enterprise architecture management

ABSTRACT

This article introduces a model for cloud governance with a specific focus on its semantic aspects. It considers three dominant paradigms — the business–IT alignment paradigm, the governance paradigm, and the cloud paradigm. The model can be enhanced with specific tools to serve as a holistic framework for addressing governance of both traditional and cloud-based IT environments. The proposed consideration of semantic aspects within the model can enable a more feasible application of the model in complex architectural settings — both from the point of view of architecture assessment and architecture management.

© 2013 Elsevier B.V. All rights reserved.

1. Introduction

For most organizations, information and the technology that supports this information represent their most valuable, but often most underestimated, assets. Information technology (IT) is on the one side considered the 5-th utility of an organization — next to water, electricity, gas, and telephony [1]. On the other side, its inherent complexity necessitates the introduction of various assessment, management, and governance models and thus led to the explosive growth of the discipline of information systems (IS) research during the last thirty years [2,3]. Such models aim to be both generally applicable and capable to address specific objectives, e.g., using a lifecycle model for a service-oriented architecture and addressing dependability in it [4]. The need for assurance about the value of IT, the management of IT-related risks and increased requirements for control over information are now understood as the key elements of enterprise governance [5]. Value, risk and control constitute the core of IT governance. IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives [6].

The increasing complexity of IT is twofold — IT covers more and more areas of the traditional enterprise on the one side [7] and the way how IT is provided becomes more and more complex on the other [8,9]. The regulatory demands from the different business areas have to be covered more and more by IT-based controls, and the Total Costs of Ownership (TCO) [10] of the IT services are becoming more and more crucial.

To address questions related to cost and capacity scaling, many organizations are considering driving their IT from resource-based approach to service-based approach, with the ability to scale the IT capacity according to ups and downs in demand while paying only the used IT capacity. This approach is basically known as "managed service" or "cloud computing". The concept of cloud computing embodies the utility paradigm for IT services [1]. It relies on sharing of resources to achieve coherence and economies of scale similar to a utility (like the electricity grid) over a network. The broader concept of converged infrastructure and shared services is the foundation of cloud computing. Cloud computing requires an appropriate

* Corresponding author. Tel.: +49 306881988; fax: +49 306881988.
E-mail address: KBrandis@Persicon.com (K. Brandis).

0167-739X/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.future.2013.09.022

IT governance model to ensure a secured computing environment and to comply with all relevant organizational information technology policies [11,12] and external requirements, like customer contracts, regulatory or legal aspects. As such, organizations need a set of capabilities that are essential when effectively implementing and managing cloud services, including requirement management, information security management, application lifecycle management, and risk and compliance management [13]. Data privacy is a major compliance aspect with regard to using cloud services especially in most western European countries [14].

This poses specific challenges on IT-Management and company level management. The CIO needs to consider technology, legal and economic aspects beside the business-related functionality. The company level management needs to get transparent view from company level down to technical level to assure appropriate governance level. This work proposes a conceptual model that addresses these challenges with focus on its semantic aspects. The rest of the work is structured as follows: Section 2 specifies the need for the model and frames the problem, Section 3 presents the fundamentals and state of the art research, Section 4 provides an overview of the proposed model while Section 5 focuses on the semantic aspects. Section 6 contains the discussion and Section 7 provides an outlook on our future research activities.

2. The need for a holistic governance architecture model

The cloud paradigm is increasingly becoming mainstream and is considered as a major research topic in computing science. Correspondingly, "cloud computing" is becoming a buzzword in the industry [15]. The popularity of digital devices and the ubiquitous use of the Internet lead to a constantly growing demand for cloud computing [16]. Cloud computing denotes both the applications delivered as services over the Internet and the hardware and software systems within the data centers which provide those services [17]. Cloud computing enables large economies-of-scale in IT provision, but it also faces a number of challenges [18]. Benefits that are mostly associated with it include fast deployment, pay-per-use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attacks, low-cost disaster recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services [19]. Thus, moving to cloud services makes users more efficient, facilitates collaboration with their co-operators, and helps users to have seamless access to other digital devices [20]. Moreover, cloud computing enables the optimization of resources [21]. However, cloud applications, like any other disruptive technology, present also many practical problems [22]. In other words, the cloud computing service model creates new risks in the computing industry scenario [23]. Typical risk issues are related to the maintenance of high service availability, the provision of end-to-end secure solutions as well as the management of longer-standing service workflows [24]. Cloud storage is an example of a foundational cloud service, which allows data owners to move data from their local computing systems to the cloud [25] and organizations are becoming more and more aware of its advantages [26]. Moving data into the cloud offers great convenience to users, since users do not need to care about the complexities of direct hardware management of storage infrastructures [27]. Despite of the advantages, this new paradigm of data storage service introduces several security challenges, which have to be addressed — confidentiality, integrity and data availability issues [28]. Traditionally, security issues with respect to data are the domain of IT governance. As already mentioned, cloud services rely often on shared infrastructure. In many cases, competitors are using the same cloud infrastructure. To provide cloud-based, meaning based on shared infrastructure, IT services in compliant and assured manner, the CIO needs to establish appropriate IT governance. IT governance addresses the following focus areas:

- Strategic alignment,
- Value delivery,
- Risk management,
- Resource management, and
- Performance measurement [6].

In order to fulfill these IT governance focus areas in a cloud-based environment, an organization needs a complete overview of all kind of objects from different areas, like own technology (servers, switches, software, etc.), own infrastructure (buildings, rooms, AC systems, energy supping units, racks, etc.), and organization (organizational units, providers, contracts, service level agreements, persons, roles and responsibilities, data, etc.) and their relationships between each other as well as the interdependencies between all of them. In the area of information systems research and also in management science it is a common approach to aim to establish a model that can represent fairly accurate a specific problem area and to then use the model in order to provide relevant recommendations. A model that aspires to capture the complexity of modern IT and information management should apply a holistic view and in the same time build on existing best practices in the specific areas (e.g., legal, economics and technology).

The envisioned model should consider the following aspects:

- a mid-size organization typically has 5.000 to 10.000 technical and infrastructural objects,
- the model should be able to provide information with regard to object ownership also considering higher level objects that have a relation to it (e.g., the data item X is part of document Y which is owned by department Z), and
- the model should also provide information about relevant regulatory and compliance requirements and thereby consider a multi-faceted view (e.g., regulatory requirements may depend on legal entity of service provider, location of particular infrastructural item, characteristics of the data item, ownership of the data item).

3. Research foundations

This section presents the needed definitions and concepts in the areas of cloud governance and enterprise architecture management.

3.1. Cloud governance

The paradigm of extending traditional IT governance to cloud computing is denoted as cloud governance [9]. There are emerging approaches to establish methodologies for cloud governance where two main directions are becoming clearer. On the one side, there are approaches that consider cloud providers similar to common service providers and aim to introduce approaches from the area of provider governance in these areas. Of particular interest here is the specific role of cloud brokers and whether they can attain a role similar to the role of trusted mediators in other markets for complex goods or services (e.g., real estate, stock exchanges). A study in 2011 [9] demonstrated that organizations are increasingly expecting such governance services from cloud brokers. A more practical implication of this approach is the trend to require typical service provider certifications such as SSAE-16 (formerly SAS-70) from cloud service providers.

On the other side we can observe rather incremental approaches that aim to enhance traditional IT governance and make it "cloud-aware". An example for such an approach proposes to extend traditional IT governance frameworks such as ITIL and CoBIT using governance for service-oriented architectures (SOA) as a bridge [29].

Download English Version:

https://daneshyari.com/en/article/6873612

Download Persian Version:

https://daneshyari.com/article/6873612

Daneshyari.com