Information and Software Technology 58 (2015) 44–57

Contents lists available at ScienceDirect

Information and Software Technology

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

Empirical evaluation of a cloud computing information security governance framework

Oscar Rebollo [a,*], Daniel Mellado [b], Eduardo Fernández-Medina [c], Haralambos Mouratidis [d]

[a] Social Security IT Management, Ministry of Labour and Social Security, Doctor Tolosa Latour s/n, 28041 Madrid, Spain
[b] Spanish Tax Agency, Large Taxpayers Department, IT Auditing Unit, Paseo de la Castellana 106, 28046 Madrid, Spain
[c] GSyA Research Group, Department of Information Technologies and Systems, University of Castilla-La Mancha, Paseo de la Universidad 4, 13071 Ciudad Real, Spain
[d] Secure and Dependable Software Systems Research Cluster, School of Computing, Engineering and Mathematics, University of Brighton, Watts Building, Lewes Road, BN2 4GJ Brighton, United Kingdom

ARTICLE INFO

Article history:
Received 17 October 2013
Received in revised form 24 September 2014
Accepted 5 October 2014
Available online 14 October 2014

Keywords:
Information security governance
Case study
Cloud computing
Security governance framework
Cloud lifecycle

ABSTRACT

Context: Cloud computing is a thriving paradigm that supports an efficient way to provide IT services by introducing on-demand services and flexible computing resources. However, significant adoption of cloud services is being hindered by security issues that are inherent to this new paradigm. In previous work, we have proposed ISGcloud, a security governance framework to tackle cloud security matters in a comprehensive manner whilst being aligned with an enterprise's strategy.
Objective: Although a significant body of literature has started to build up related to security aspects of cloud computing, the literature fails to report on evidence and real applications of security governance frameworks designed for cloud computing environments. This paper introduces a detailed application of ISGCloud into a real life case study of a Spanish public organisation, which utilises a cloud storage service in a critical security deployment.
Method: The empirical evaluation has followed a formal process, which includes the definition of research questions previously to the framework's application. We describe ISGcloud process and attempt to answer these questions gathering results through direct observation and from interviews with related personnel.
Results: The novelty of the paper is twofold: on the one hand, it presents one of the first applications, in the literature, of a cloud security governance framework to a real-life case study along with an empirical evaluation of the framework that proves its validity; on the other hand, it demonstrates the usefulness of the framework and its impact to the organisation.
Conclusion: As discussed on the paper, the application of ISGCloud has resulted in the organisation in question achieving its security governance objectives, minimising the security risks of its storage service and increasing security awareness among its users.

1. Introduction

During the last few years, organisations and individuals have started paying attention to the explosive growth and adoption of cloud computing services. This new paradigm encompasses access to a shared pool of computing resources that can be rapidly provisioned and released with minimal management effort [1]. Users may benefit from the flexibility and elasticity of on-demand cloud services, especially at present when economic restrictions require IT departments to achieve more objectives with less resources. When these kinds of services are aligned with well-defined strategic initiatives and objectives, they make valuable contributions to an enterprise [2]. Enterprises using cloud computing for their businesses report economic savings of up to 30%, along with other related benefits such as more effective mobile working, higher productivity or the standardization of processes [3].

However, the many benefits provided by cloud computing are also accompanied by the introduction of new risks [4], in addition to the continued presence of all the security issues that may affect its underlying technologies [5]. Organisations have these services at their disposal but cannot disregard their security requirements [6]. The independence of the cloud service delivery model signifies that security management is necessary if its adoption is to be

* Corresponding author. Tel.: +34 913902883; fax: +34 914698477.
E-mail addresses: orebollo@gmail.com (O. Rebollo), damefe@esdebian.org (D. Mellado), Eduardo.FdezMedina@uclm.es (E. Fernández-Medina), h.mouratidis@brighton.ac.uk (H. Mouratidis).

http://dx.doi.org/10.1016/j.infsof.2014.10.003
0950-5849/

fostered [7]. Cloud computing extends computing resources across the corporate perimeter, resulting in control being lost over its information assets. Organisations outsourcing strategic IT projects face a high degree of risk, which needs to be mitigated in order to guarantee their service's assurance [8]. The selection of adequate security controls and the optimal risk treatment are some of the main problems within the scope of IT security, which usually rely on international assurance standards [9,10].

An information security governance (ISG) function therefore needs to be established for the management levels, with a clear security strategy [11]. Regardless of the cloud model adopted, security and governance must lead and guide the adoption of cloud services [12]. Security policies and measures involve a third party when moving services to cloud computing, and this loss of control emphasises the need for security governance within the enterprise and for the transparency of cloud providers [13,14]. Security governance, as part of the company's corporate governance, is the most suitable path by which to gain control of security processes and guarantee an alignment with business strategies [15]. Information security policy compliance requires active governance enforcement with adequate controls over the organisation's personnel [16]. Such security compliance is a major issue in many organisations, as it involves dealing with an increasing number of diverse compliance sources and needs to be implemented within an enterprise-wide scope [17].

Existing literature offers both security governance frameworks and security solutions for cloud computing, but additional research efforts are needed to tackle security challenges [18]. Our previous research shows that existing proposals dealing with cloud computing security have shortcomings regarding to their compliance with governance aspects [19]. Such systems have clear differentiating features, which suggests the need for adapted security management methodologies [20]. We have therefore proposed ISGcloud, a framework based on security guidelines and standards that can be adopted by any organisation that wishes to develop a security governance structure, thus providing its cloud services with coverage [21]. Our approach is process oriented, which facilitates its inclusion in internal processes, and details security activities and tasks that can be applied during the cloud service lifecycle.

This paper contains the practical utilisation of ISGcloud framework in a real life scenario. The purpose of this empirical evaluation is to put our theoretical research into practice in order to evaluate and validate its utility. The literature fails to report on empirical case studies of security governance frameworks designed for cloud computing services, so the main novelty of this paper is that it introduces a real life practical application of our proposed framework. Along with the description of the process, this paper also contains the empirical evaluation of the framework's validity, analysing its usefulness in a real situation.

Our objective with this empirical evaluation is twofold: to evaluate the benefits and possible draw-backs of using the ISGcloud framework in order to continue improving it; and to validate whether the cloud service's security achieves its desired level and whether a security governance structure is developed around it. The empirical evaluation was conducted by following a structured methodology [22], signifying that unbiased results were obtained and that it is easy to follow the way in which these results are reported. The characteristics of our research permit the use of a flexible design to treat the qualitative data obtained during the application of ISGcloud.

The empirical evaluation took place in a public organisation, which provides IT services to the Spanish Social Security System. This organisation was planning its first steps into cloud computing and ISGcloud was used to cover its security aspects. This case is particularly relevant because public organisations are subject to regulations that make information security a critical issue, and the launching of cloud services in these organisations serves as a tool to allow the adoption of cloud by citizens and enterprises to be fostered. International institutions are promoting the secure use of cloud services by public administrations; for instance, the European Commission has identified the key areas of cloud computing in which action is needed, which includes contractual security problems or confusion concerning applicable standards [23]. The adoption of cloud solutions by government agencies requires that its internal processes be redefined and translated into agreements with the cloud provider [24], aspects that are dealt with by ISGcloud and discussed in this paper.

The remainder of the paper is structured as follows: Section 2 provides a brief overview of the ISGcloud framework, explaining its principal activities; Section 3 presents the empirical evaluation design and it details the methodology followed. An introduction to the context is provided in Section 4, including a description of the organisation and the problem that the cloud service aims to solve; Section 5 details the application of the framework to the case study; Section 6 highlights the results obtained in our research; Section 7 shows related work in this research area; and the paper concludes in Section 8.

2. Overview of ISGcloud framework

The overview shown in this section is a summary of our previous work [21], where a deeper explanation of ISGcloud framework can be found, providing more details of its activities and artefacts.

ISGcloud framework is process oriented and is based on a set of activities, which provide a structured means of developing a security governance structure supporting a cloud computing service. These activities are closely related to the cloud service lifecycle that we have adopted which is based on 6 stages: 1. Planning/Strategy Definition; 2. Cloud Security Analysis; 3. Cloud Security Design; 4. Cloud Implementation/Migration; 5. Secure Cloud Operation; and 6. Cloud Service Termination.

During the whole process, the framework maintains a continuous security governance approach, being aligned with existing proposals such as ISO/IEC 38500 standard [25] or COBIT 5 [26]. Using a similar perspective as these proposals, ISGcloud includes four core governance processes: (a) evaluate the current and future use of IT; (b) direct preparation and implementation of plans and policies to ensure that the use of IT meets business objectives; (c) monitor conformance to policies, and performance against the plans; and (d) communicate the knowledge and policies that are required in ISG.

All the activities proposed during the cloud service lifecycle are divided into their correlative tasks, which are themselves formed of detailed steps. This way, ISGcloud offers a precise description of activities that should be overtaken to guarantee security governance of the cloud service. Organisations willing to implement the framework have at their disposal a number of issues, which must be taken into consideration in order to provide appropriate assurance. ISGcloud's tasks also include numerous references to existing guidance and support of security standards that may be used in order to facilitate its implementation and performance.

Each task is related to an artefact repository from which the necessary inputs are taken and its outputs are delivered. This repository contains security models and products that are incrementally developed and refined until the objectives defined are achieved. The artefact repository therefore acts as a document manager that stores and manages different versions of products.

A general overview of our framework's activities and tasks is represented in Fig. 1, using the Software & Systems Process Engineering Metamodel (SPEM) diagram notation [27].

In order to facilitate the understanding of our framework and to provide a standardised representation of it, which can be auto-