Introducing a Security Governance Framework for Cloud Computing

Oscar Rebollo[1], Daniel Mellado[2] and Eduardo Fernández-Medina[3]

[1]Social Security IT Management, Ministry of Labour and Immigration,
Doctor Tolosa Latour s/n, Madrid, Spain
[2]Spanish Tax Agency - Large taxpayers department - IT Auditing Unit,
Paseo de la Castellana 106, Madrid, Spain
[3]GSyA Research Group, Department of Information Technologies and Systems,
University of Castilla-La Mancha, Paseo de la Universidad 4, Ciudad Real, Spain

Abstract. The cloud computing paradigm provides a more efficient way in which to provide IT services, introducing on-demand services and flexible computing resources. The adoption of these cloud services is being hindered by the security issues that arise with this new environment. A global security solution, which deals with the specific particularities of the cloud paradigm, is therefore needed, and literature fails to report on such a solution. As a consequence, in this paper we propose a novel security governance framework focused on the cloud computing environment (ISGcloud). This framework is founded upon two main standards: on the one hand, we implement the core governance principles of the ISO/IEC 38500 governance standard; and on the other hand, we propose a cloud service lifecycle based on the ISO/IEC 27036 outsourcing security draft. The paper includes an overview of the framework and the description of a collection of activities and their related tasks.

1 Introduction

During the last few years, both 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].

However, the many benefits provided by cloud computing are also accompanied by the appearance of new risks [3], in addition to the continued presence of all the security issues that may affect its underlying technologies [4]. The independence of the cloud service delivery model signifies that security management is necessary if its adoption is to be fostered [5]. Cloud computing extends computing resources across the corporate perimeter, resulting in control being lost over its information assets. A security governance function therefore needs to be established for the management

Rebollo O., Mellado D. and Fernández-Medina E..
Introducing a Security Governance Framework for Cloud Computing.
DOI: 10.5220/0004601400240033
In *Proceedings of the 10th International Workshop on Security in Information Systems* (WOSIS-2013), pages 24-33
ISBN: 978-989-8565-64-8

levels, with a clear security strategy [6]. Regardless of the cloud model adopted, security and governance must lead and guide the adoption of cloud services [7]. Security policies and measures involve a third party when moving services to cloud computing, and this loss of control emphasizes the need for security governance within the enterprise and for the transparency of cloud providers [8, 9]. 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 [10].

An Information Security Governance (ISG) framework that tackles all the security issues in the cloud environment in a uniform manner is not currently available. Although there are many technological approaches that can improve cloud security, there are currently no comprehensive solutions [11]. Our previous research shows that existing efforts that attempt to deal with cloud computing security do not detail the governance aspects [12]. In this paper we therefore propose a first approach to a security governance framework that considers the particularities of cloud deployments (ISGcloud). The ISGcloud framework compiles existing published guidance works on the field, and groups them homogeneously to provide a model that is capable of delivering an ISG process for the cloud services. ISGcloud is led by standards, resulting in an alignment with actual best practices. With the use of standards we aim to increase the quality and reliability of the results and simplify the governance process while guaranteeing the security of the cloud service and promoting the reuse of resources [13].

The perspective followed in our approach is process oriented, thus facilitating its inclusion in any organisation. In order to deploy security governance, we have chosen the model published in the ISO/IEC 38500 standard, which states that directors should perform governance by using three main processes: Evaluate, Direct and Monitor [14]. The Evaluate-Direct-Monitor cycle will therefore become a core process of our framework. We also propose the addition of a fourth process, namely Communicate, owing to the relevance of disseminating security knowledge within the organisation, particularly as regards the adoption of new services such as those of cloud computing.

In addition to the four core processes highlighted, we consider that it is paramount to identify a cloud service lifecycle as part of our objective of defining an ISG deployment. The relationship between the cloud client and its provider, as with any other outsourcing service, leads to new risks throughout its lifecycle phases that must be managed in order to guarantee the service's success [15]. The ISO/IEC 27036 standard [16], despite being in its draft stage, outlines security controls to be addressed in an outsourcing lifecycle. We have adapted this standard to a generic cloud computing lifecycle in order to identify the steps in the processes.

This paper is structured as follows: the following section contains related work in the fields of security governance and cloud computing that have influenced our research; Section 3 provides an overview of our ISGcloud framework, describing its core processes and the proposed lifecycle of a cloud service; Section 4 presents a detailed description of our framework's activities and tasks; finally, Section 5 contains a discussion of our contribution and future work.

2 Related Work

This section briefly summarises those proposals published in recent years whose objective is to tackle security issues from the governance perspective. We focus particularly on those dealing with cloud computing deployments.

A key reference, when discussing IT Governance, is Control Objectives for Information and related Technology (COBIT) [17]. COBIT is a framework for IT Governance which introduces a set of 37 processes grouped into five domains; detailing the control objectives, metrics, maturity models and other management guidelines for each of these processes.

The International Organisation for Standardization (ISO) has a wide portfolio of standards, some of which are dedicated to security and governance aspects. The ISO/IEC 27001 standard is of particular interest to our objective as is related to Information Security Management Systems, which can be used by organisations to develop and implement a framework for managing the security of their information assets and prepare for an independent assessment applied to the protection of their information [18].

These two frameworks are analysed in [19], in which some other references are also considered. Of these approaches it is worth highlighting the ISG proposal [20], which defines an information security framework, clearly distinguishing between the governance and management sides, in addition to describing the tasks, roles and responsibilities of any key individual in an organisation.

The main drawback of using these frameworks when dealing with cloud computing security is that they have not been specifically designed for this environment, and therefore lack the particularities that arise in this situation. The special security requirements that arise when dealing with a cloud computing deployment have led to many publications that attempt to tackle these matters. Existing cloud security proposals are reviewed in [21], and the most representative are introduced below.

The security guidance published by the Cloud Security Alliance provides practical recommendations on reducing the associated risks when adopting cloud computing [22]. The guidance proposes recommendations that help identify threats in the cloud context and choose the best options to mitigate vulnerabilities. Organisations using this guide must select which lines are applicable to their cloud deployment. These lines range from governance to operation issues.

A security risk assessment has been proposed by the European Network and Information Security Agency (ENISA) to provide both a framework to evaluate risks and security guidance for existing users [23]. The risk assessment evolves into an information assurance framework, which includes controls from the ISO 27000 family of standards.

In order to provide an understanding of cloud computing and its related risks, the Information Systems Audit and Control Association (ISACA) has published [24]. This proposal tackles governance and security aspects separately, and contains references to additional publications in order to complement the framework.

The systematic review performed in [12] analyses all of these cloud security proposals together with other literature publications. The results of this comparison show many lacks in existing frameworks as regards the comprehensive embracement of security governance in cloud computing environments.

There are various core governance processes approaches in literature; some ISO

standards, such as that of the ISO/IEC 27001, propose adopting the Plan-Do-Check-Act (PDCA) process model to implement the governance of the security of information systems and networks [18]. We consider this approach and the ISO/IEC 38500 (Evaluate-Direct-Monitor) as valid and plausible, since both reflect the establishment of iterative processes that provide feedback on the activities performed.

Similar approaches with which to define these processes can also be found in literature. For instance, in [25] the authors define a security governance framework based on the Direct-Control cycle. Upon examining this process it was discovered that it shares many dualities with the aforementioned ones, as it differentiates the governance and management domains, and applies the iterative cycle to the strategic, tactical and operational levels.

3 Overview of the ISGcloud Framework

This section provides a general overview of our proposed ISGcloud framework. We describe how the process has been developed by considering the specificities of a cloud computing environment and what links to existing standards it includes.

As previously mentioned, the core processes of ISGcloud are based on the ISO/IEC 38500 standard. According to this standard, the governance cycle follows three 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; and c) Monitor conformance to policies, and performance against the plans [14]. We additionally incorporate the Communicate process which adds the dissemination of the knowledge that is required in ISG. From here on, we shall refer to these iterations as the Evaluate-Direct-Monitor cycle.

This iterative governance cycle is also similar to the COBIT 5 proposal, where the Evaluate-Direct-Monitor cycle is intended for IT governance processes, and a Plan-Build-Run-Monitor cycle is suggested for the management areas [17].

The process of implementing and managing ISG in cloud computing is closely bound to the service offered by the cloud provider and consequently with its lifecycle. Taking the ISO/IEC 27036 standard [16] as a basis, we propose the following generic cloud computing lifecycle: 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.

We intend to use the proposed lifecycle to develop a framework that will be suitable for all cloud deployments. Depending on the details of the cloud implementation or even on whether the cloud service is already in use, practitioners will be able to discard some of the proposed activities and tailor those remaining to their needs.

The four ISG processes constitute one dimension of the ISGcloud framework, and the six activities of the cloud computing lifecycle become a second dimension. We therefore depict our framework in a bi-dimensional perspective, in which the cloud services traverse the six activities in which successive Evaluate-Direct-Monitor cycles are held. The relationship between the core security governance cycle and the cloud lifecycle is shown in Fig. 1. The front of the triangular prism represents the four main security governance processes (Evaluate, Direct, Monitor and Communicate) that are

executed iteratively in each activity of the process. The lateral side of the prism depicts the consecutive activities of the cloud service lifecycle through which security governance is implemented.

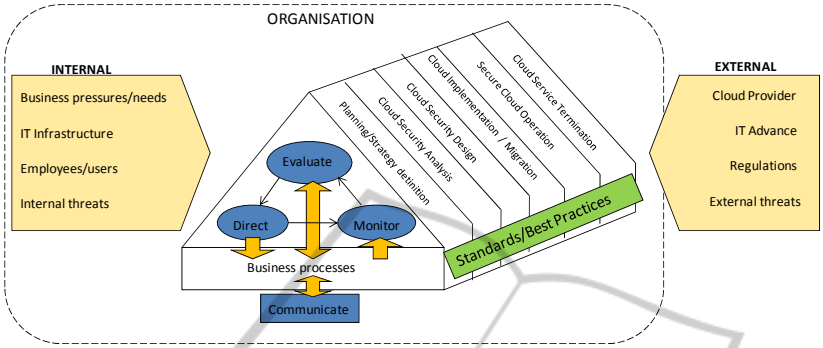

Fig. 1. Overview of the ISGcloud framework.

Surrounding the prism in Fig. 1 are some of the most relevant aspects to have influenced the security governance activities and which must therefore be considered in our framework. The left-hand side of the figure contains those issues that are internal to the organisation, while the right-hand side lists external matters. The inclusion of standards and best practices has been represented over the cloud service lifecycle in order to reflect the primordial importance of these contributions to our framework. Although we propose some relevant standards, these guidelines may already exist and be deployed within the organisation, or can be obtained from external sources.

4 ISGcloud's Activities

Having introduced the core processes of our cloud security governance framework and its main components, this section details the process structure throughout the cloud service lifecycle.

The user roles involved in the proposed framework include personnel from the whole organisation. The governance activities require the active involvement of senior officers, high executives and managers, and therefore participate along with other lower level roles. Since senior officers are responsible for the organisation's governance processes, they are involved in all the activities, signifying that they need to be informed of ISGcloud's evolution and approve the results of its tasks.

All the activities should be performed iteratively, following the core principles of our framework. This feedback will allow practitioners to return to activities that have previously been accomplished with new output products that may contain additional information to perform another cycle. The remainder of this section details the tasks proposed in each activity along with a brief description.

4.1 Activity 1: Planning /Strategy Definition

The first activity of the ISGcloud framework is designed as an introductory process to establish the foundations needed for the remaining activities.

Task 1A: Establish Information Security Governance Structure. Given the importance of security governance, the intention of this task is to introduce ISG into the organisation's culture. Senior officers and high executives, who have knowledge of the company's structure, mission and goals, are in charge of identifying the participants, grouping them in teams by affinity and assigning their responsibilities. The governance process involves the whole organisation, signifying that the relationships among the different management levels and the reporting lines need to be clearly defined. This task comes up with the ISG strategic plan that covers all these issues and includes the top-level policies concerning security governance.

Task 1B: Define Information Security Program. Once an effective governance structure and top-level security policies have been defined, then an Information Security Program must be developed. This program consists of a series of activities that support the enterprise risk management plan and result in the development of the security strategy and policies [26]. This task must be performed co-ordinately by IT and security managers and senior officers, in order to guarantee that the security program is aligned with the business objectives.

4.2 Activity 2: Cloud Security Analysis

The second activity focuses on performing various analyses related to the security of the cloud service. These analyses are developed according to the governance structure and the Information Security Program elaborated in the former activity.

Task 2A: Define Information Security Requirements. The first task in this activity has the objective of translating the strategic security policies and high level threats defined with the security program into more detailed requirements. Ensuring a complete alignment with the organisation's mission, the goals are translated into security requirements. This task requires a previous evaluation of existing standards and guidelines that are suitable for the organisation. When defining these requirements it is important to start considering the cloud service that the organisation intends to implement and its related deployment. Hence it is in this step when the ISGcloud framework begins its relationship with the cloud computing environment.

Task 2B: Cost/benefit Analysis of Available Cloud Options. Once the security requirements and security policies have been defined, the organisation needs to evaluate the cloud options that are available for the services being deployed. This evaluation is performed in this task through cost/benefit analyses that include the cost of effective governance to manage risk and ensure regulatory compliance [27] and the value added by the cloud service. These analyses must include security considerations of the different candidate cloud providers in relation to the cloud service model chosen. Although it is an early estimation, the business case provides a first economic approach as regards the organisation's cloud service security prospects.

Task 2C: Cloud Risk Analysis. The third analysis included in this activity is a cloud

security risk analysis. The objective of this task is to provide an understanding of the cloud service security risks identified and to define management processes for these risks. Like any risk assessment, this includes the identification of the information assets with their related threats and vulnerabilities, and the definition of procedures to manage the risk and counteract them. We recommend using the Information assurance framework defined in [23] by ENISA, which assists in following these steps.

4.3 Activity 3: Cloud Security Design

The objective of ISGcloud's third activity is to provide a comprehensive design of the security governance that will be implemented together with the cloud service.

Task 3A: Define SLAs and legal contracts. Like any outsourcing service, cloud computing services need adequate service level agreements (SLAs) to be properly managed. Successful security governance is achieved through an appropriate translation of the organisation's security requirements into agreements with its cloud provider in order to manage and minimise risks. These agreements should include not only legal clauses, but also a complete group of security measures, which will be the starting point for the subsequent audit and monitoring tasks. SLAs, as part of the iterative governance cycle, must be periodically reviewed with the purpose of modifying detected lacks and improving the cloud service's security management.

Task 3B: Establish Information Security Roles and Responsibilities. The security design requires a detailed establishment of responsibilities within the organisation. This assignment depends to a great extent on the governance structure defined in the first activity. This task demands an identification of the information assets, in order to define the ownership and responsibility of each one.

Task 3C: Specify Cloud Service Monitoring and Auditing. This is a key task in the security design as it specifies the conditions under which the cloud service will be monitored. The organisation defines the processes and metrics needed to perform security audits based on the previously defined SLAs. The results of this activity determine how the Monitor and Evaluate processes of the iterative cycle will be executed in the operation activities.

Task 3D: Define Applicable Security Controls. The last task in the design activity is focused on defining the security controls. Based on the risk analysis, the organisation must develop the security measures that it will apply both during the cloud service operation and also in cases of incidents or major disasters. This task can be performed by following any of the existing security standards, such as ISO/IEC 27001 [18].

4.4 Activity 4: Cloud Implementation / Migration

Once the security design has been completed, then the cloud service implementation takes place. The execution of this activity varies depending on whether the cloud service implemented has been previously used in the organisation or whether it is a migration from one cloud provider to another.

Task 4A: Secure Cloud Implementation. This task focuses on the security during the service implementation and the parallel modification of the organisational security processes. Additional security controls are needed in the migration, some of which will depend on the type of cloud deployment. Along with the service implementation, the organisation's processes are adapted to the newly designed specification.

Task 4B: Educate and Train Staff. The extension of the cloud service security issues within the organisation is a key governance process. Although the Communicate process should have increased the security awareness in previous activities, it is in this task in which a global training plan is developed, and each member of the staff is educated according to his/her participation in the cloud service.

4.5 Activity 5: Secure Cloud Operation

The fifth activity of ISGcloud is devoted to the cloud service operation. The previous activities can be considered as time delimited, but it is generally difficult to fix time limits to the operation since it usually has an indefinite duration. This is why the proposed core iterative cycle is especially relevant in this activity.

Task 5A: Cloud Security Operation. The security operation task reflects the successive iterations of the governance cycle. This cycle requires a precise design of the processes, so that every participant can play their defined role. The continuous improvement process may produce modifications to products from previous activities, such as the Information Security Program or the Risk Analysis. If so, it may be interesting to revisit previous activities, even while the cloud service is operating. Successful security governance not only requires regular service measurement, but also an adequate prioritization of the programs and regular reporting of security issues, which may include recommendations for corrective and preventive actions.

Task 5B: Communicate Information Security within the Organisation. This task reflects the continuous communication process that takes place within the organisation to maintain security awareness and permit the extension of new policies. Although this task could also be included in the previous one (Cloud security operation), the differences between the Communicate process and the Evaluate-Direct-Monitor cycle suggest this separation, in a more illustrative and understandable manner.

4.6 Activity 6: Cloud Service Termination

The objective of the last activity is to provide the service termination with security.

Task 6A: Cloud Service Termination. This task includes the steps needed to guarantee a secure service termination and information retrieval from the cloud provider, whether the service is transferred to another provider or is finally discarded. The main outputs of this task are the security reports that contain the knowledge gained by the organisation, which can be reused in successive security governance iterations.

5 Conclusions

Several research efforts concerning cloud services' security have been published, but we have spotted a lack of a security governance framework that takes into account the particularities of cloud computing. The main contribution of this work is the proposal of a comprehensive ISG framework (ISGcloud) that is intimately linked with the cloud service lifecycle. The objective of ISGcloud framework is to provide practitioners with a systematic approach that can be easily followed to guarantee successful security governance, independently of the type of cloud deployment.

In order to being able to understand the framework, we have introduced a brief description of ISGcloud's activities and tasks. However, we are aware that more detail is needed before our proposal is put into practice. We plan to continue our research expanding the proposed tasks, so that each one identifies its involved steps, the user roles that participate in its execution, its input and output products, and proposed guidance documents that may help to achieve its objectives. Our future research should allow us to provide a structured process approach that facilitates its integration with other organisational processes and its reusability, which may be modelled following the Software & Systems Process Engineering Meta-Model Specification (SPEM) [28]. Following this line, we plan to complement the SPEM definition of the framework's activities with a supporting tool, such as EPF Composer.

Furthermore, we intend to be able to carry out a practical utilizacion of ISGcloud framework in a real life scenario, so that our theoretical research is put into practice to evaluate and validate its utility. We shall continue to validate our proposal by contacting candidate organisations that intend to develop cloud services or have already deployed them, and are interested in security governance issues related to the cloud environment.

Acknowledgements

This research is part of the following projects: MEDUSAS (IDI-20090557), financed by the Centre for Industrial Technological Development (CDTI), ORIGIN (IDI-2010043(1-5)) financed by the CDTI and the FEDER, SERENIDAD (PEII11-037-7035) financed by the "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla- La Mancha" (Spain) and FEDER, and SIGMA-CC (TIN2012-36904) and GEODAS (TIN2012-37493-C03-01) financed by the "Ministerio de Economía y Competitividad" (Spain).

References

1. Mell, P., Grance, T.: The NIST Definition of Cloud Computing. SP 800-145. National Institute of Standards and Technology (NIST) (2011)
2. Gartner: Gartner's Hype Cycle for Cloud Computing. (2012)
3. Chen, Y., Paxson, V., Katz, R.H.: What's New About Cloud Computing Security? University of California, Berkeley (2010)

4. Hamlen, K., Kantarcioglu, M., Khan, L., Thuraisingham, B.: Security Issues for Cloud Computing. International Journal of Information Security and Privacy 4 (2010) 39-51
5. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34 (2011) 1-11
6. Bisong, A., Rahman, S.S.M.: An overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications (IJNSA) 3 (2011) 30-45
7. Avanade: Global Survey: Has Cloud Computing Matured? Third Annual Report , June 2011 (2011)
8. Rosado, D.G., Gómez, R., Mellado, D., Fernández-Medina, E.: Security Analysis in the Migration to Cloud Environments. Future Internet 4 (2012) 469-487
9. Zhu, Y., Hu, H., Ahn, G.-J., Yau, S. S.: Efficient audit service outsourcing for data integrity in clouds. Journal of Systems and Software 85 (2012) 1083–1095
10. Mellado, D., Sánchez, L.E., Fernández-Medina, E., Piattini, M.: IT Security Governance Innovations:Theory and Research. IGI Global, USA (2012)
11. Rong, C., Nguyen, S.T., Jaatun, M. G.: Beyond lightning: A survey on security challenges in cloud computing. Computers and Electrical Engineering 39 (2013) 47-54
12. Rebollo, O., Mellado, D., Fernández-Medina, E.: A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. Journal of Universal Computer Science 18 (2012) 798-815
13. Fung, A.R.-W., Farn, K.-J., Lin, A. C.: Paper: a study on the certification of the information security management systems. Computer Standards & Interfaces 25 (2003) 447-461
14. ISO/IEC: ISO/IEC 38500:2008 Corporate governance of information technology (2008)
15. Chou, D.C., Chou, A.Y.: Information systems outsourcing life cycle and risks analysis. Computer Standards & Interfaces 31 (2009) 1036–1043
16. ISO/IEC: ISO/IEC 27036 - IT Security - Security techniques - Information security for supplier relationships (draft)
17. ITGI: Control Objectives for Information and related Technology (COBIT 5) (2012)
18. ISO/IEC: ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements (2005)
19. Rebollo, O., Mellado, D., Sánchez, L.E., Fernández-Medina, E.: Comparative Analysis of Information Security Governance Frameworks: A Public Sector Approach. The Proceedings of the11th European Conference on eGovernment – ECEG 2011, Ljubljana, Slovenia (2011) 482-490
20. Solms, S.H.v., Solms, R.v.: Information Security Governance. Springer (2009)
21. Rebollo, O., Mellado, D., Fernández-Medina, E.: A Comparative Review of Cloud Security Proposals with ISO/IEC 27002. Proceedings of the 8th International Workshop on Security in Information Systems - WOSIS 2011, Beijing, China (2011) 3-12
22. Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V3. (2011)
23. Catteddu, D., Hogben, G.: Cloud Computing Security Risk Assessment - Benefits, risks and recommendations for information security. European Network and Information Security Agency (ENISA) (2009)
24. ISACA: IT Control Objectives for Cloud Computing. (2011)
25. Solms, R.v., Solms, S. H. B.v.: Information Security Governance: A model based on the Direct–Control Cycle. Computers & Security 25 (2006) 408-412
26. Allen, J.H., Westby, J. R.: Governing for Enterprise Security Implementation Guide. Software Engineering Institute - CERT (2007)
27. Miller, J., Candler, L., Wald, H.: Information Security Governance - Government Considerations for the Cloud Computing Environment. Booz Allen Hamilton (2009)
28. OMG: Software & Systems Process Engineering Meta-Model Specification v.2.0. http://www.omg.org/spec/SPEM (2008)