Journal of Universal Computer Science, vol. 18, no. 6 (2012), 798-815
submitted: 15/10/11, accepted: 15/2/12, appeared: 28/3/12 © *J.UCS*

A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment

Oscar Rebollo
(Social Security IT Management, Ministry of Labour and Immigration, Madrid, Spain
orebollo@gmail.com)

Daniel Mellado
(GSyA Research Group, Department of Information Technologies and Systems
University of Castilla-La Mancha, Ciudad Real, Spain
damefe@esdebian.org)

Eduardo Fernández-Medina
(GSyA Research Group, Department of Information Technologies and Systems
University of Castilla-La Mancha, Ciudad Real, Spain
Eduardo.FdezMedina@uclm.es)

Abstract: The senior management of any enterprise that plans to start using Cloud Computing services needs to define a clear governance strategy with regard to the security of its information assets. This paper presents a systematic literature review whose objective is to seek existing Information Security Governance frameworks that may assist companies with these functions. The analysis of the frameworks extracted is complemented with a set of comparative criteria that consider the particularities of Cloud Computing when dealing with security governance issues.

Keywords: Information security governance, Cloud computing, Systematic literature review
Categories: K.6, K.6.5, C.2.4

1 Introduction

Cloud Computing can be defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [Mell (2009)]. However, a wide variety of definitions can be found, each of which highlights different relevant characteristics [Vaquero (2009)]. The Cloud Computing paradigm is receiving much attention from the Information Technology (IT) community [McKinsey (2009)], which has driven it through the top of Gartner's Hype Cycle [Gartner (2011)]. It is generally agreed that it has the potential to transform a great part of the IT industry by delivering services such as utility computing [Armbrust (2009)]. Although some of its characteristics have been defined as part of traditional technologies [Chen (2010)], it is the explosion of the Internet and the need to use elastic resources which has increased the offer of cloud services [Qian (2009)].

The Cloud Computing service model creates new risks and also new opportunities, which is the reason why Information Security is considered to be the

main drawback that could prevent organizations from adopting Cloud Computing [IDC (2009)]. As opposed to other technical security issues, the principal difference when dealing with Information Security from the cloud environment is the enterprise's loss of control or loss of governance over assets and information [Cloud Computing Use Case Discussion Group (2010)]. In order to reduce these threats, the collaboration of both cloud providers and clients is necessary, since it is an issue that cannot be tackled unilaterally [Ponemon Institute (2011)]. The ever-changing environment of Cloud Computing leads to a need for a suitable assurance framework which deals with the different levels of security and against which the cloud model can be secured [Sloan (2009); Subashini (2011)]

If enterprises are to gain benefit from the use of Cloud Computing, a clear governance strategy and management plan must be developed [ISACA (2011)]. Many aspects related to Information Security Governance (ISG) have been highlighted as action areas that companies should take into account before jumping into the cloud [World Economic Forum (2011)]. Moving into the cloud therefore requires the active involvement of the governing body of any enterprise if it is to be successful [Bisong (2011)]. Typical ISG activities such as goal setting, policy and standard development, the definition of roles and responsibilities and risk management must include special considerations when dealing with cloud technology and its providers [ISACA (2009)].

The absence of an accepted and established ISG model for the cloud environment that meets the needs of every type of cloud service provider and client hinders the implementation of these functions. We have therefore decided to perform a systematic literature review of the existing ISG frameworks that have been conceived to guarantee information assurance in the Cloud Computing environment. This paper presents the review process and the subsequent analysis of extracted data.

A systematic process has been followed in order to perform a literature review in search of ISG frameworks that have been specifically designed for the Cloud Computing paradigm, and which take into account its particularities. The objective methodology described in this paper guarantees the repeatability of the results and reduces the bias of the analysis.

The systematic literature review is followed by a data extraction process, in which the main characteristics of each ISG framework are highlighted in the light of different comparative criteria. These criteria have been defined to take into account the specific consideration of developing security governance in Cloud Computing environments. The purpose of this review is twofold: it returns existing ISG frameworks to be used by companies who wish to move into the cloud; and it permits a comparison of the different proposals in such a way that the main strengths and weaknesses are highlighted, and gaps for future research are detected.

The structure of this paper is as follows: the following section describes the systematic literature review process that has been conducted, detailing the steps involved; Section 3 presents a comparative framework in which a set of criteria related to the ISG in Cloud Computing is defined; Section 4 shows the main contributions of each ISG framework in relation to the comparative criteria; Section 5 contains the analysis results of the comparison performed; and finally, the review concludes in Section 6.

2 Review Process Description

This section describes the process followed to perform a systematic literature review using a trustworthy methodology [Kitchenham (2004)]. The basic aim of a systematic review is to compile and evaluate all the available research related to a question of interest, thus achieving unbiased, auditable and repeatable results. The review method presented in [Kitchenham (2007)] has been adapted to allow us to conduct our research in the field of Cloud Computing security governance.

Although it might appear that the process is executed in a linear chain, it in fact produces its results through a sequence of iterations. Each cycle helps to refine each step in the process until appropriate results are attained. A bibliographic package is used to keep track of each iteration and to record the whole process.

2.1 Research Question

A preliminary analysis carried out in order to search for existing cloud security governance reviews showed a lack of publications dealing with these issues. Multiple Information Security frameworks exist, but few of them specify differentiating procedures for Cloud Computing environments. What is more, current Security Governance proposals seldom deal with Cloud Computing particularities. The recent wide–spread emergence of cloud deployment signifies that more in-depth research must be undertaken to identify both the differentiating security governance characteristics of Cloud Computing and what the proposals to mitigate vulnerabilities and minimize risks are.

Specifying the *research question*, which drives the systematic review methodology, is a critical step in the process. In our case, the *research question* focuses on identifying existing Information Security Governance (ISG) frameworks, initiatives and proposals that have been designed to be applied in Cloud Computing services. The scope defined is therefore twofold:

- The review is aimed at comprehensive frameworks, that is, proposals that deal with all the security aspects that may arise, from operational measures to management aspects, but particularly with the governance of information security.
- The approaches must consider the particular characteristics of Cloud Computing; only those initiatives that have been designed for the cloud model have been taken into account.

2.2 Defining the Review Protocol

A precise protocol was needed to avoid biased results in the systematic review. In this section we define the protocol followed in the literature review.

Once the research question had been settled, a set of search terms was extracted from it. These terms, or *keywords,* were used in the review to identify all the relevant initiatives that were related to the research question and to attempt to answer it. A precise definition of the research terms is vital if comprehensive results are to be achieved without overlooking important approaches.

Bearing in mind that the proposed research question embraces characteristics from different research areas, it was necessary to define the search terms in such a

way that all of them were included. Some synonyms of the terms were also included to avoid the situation of a proposal being ignored because of the different use of language. The proposed *keywords* that were used in the systematic literature review were the following:

- Cloud Security Framework
- Cloud Security
- Cloud Information Security Governance
- Cloud Computing Security Governance
- Secure Management Cloud

This set of *keywords* was used in order to attempt to compile all the initiatives related to ISG in the deployment of Cloud Computing. Since the search for these terms may have returned additional results that were not strictly related to the review's objective, selection filters were subsequently applied in order to extract the relevant studies.

The systematic literature review protocol suggests performing a preliminary search to seek existing reviews on the subject. In our case, probably because of the immaturity of the research topic, we discovered that the available resources did not contain any publications dealing with the proposed research question. The review process consequently continued to search for primary studies which contained the aforementioned *keywords*.

Selecting the *sources* in which the research will be developed is another crucial step. We therefore chose a group of databases, some of which provide their own engines to perform the searches. This choice was made by considering the general prestige of certain publications within the academic community, our previous knowledge of publications containing contents related to our research question, and sources suggested by authorities in the field. The review was therefore executed on a variety of sources, including electronic databases, search engines, journals, magazines and conference proceedings.

The *sources* chosen to perform the systematic review are listed below:

- Science Direct
- Elsevier
- Google Scholar
- IEEE
- ACM Digital Library
- University of Castilla-La Mancha Digital Library

The combination of the aforementioned search terms was applied to the sources resulting in a collection of publications, which provided a first approximation to our research question and allowed us to obtain a list of potentially relevant *primary studies*. These results then had to be filtered in order to extract those initiatives that accurately satisfied the review conditions . These proposals were narrowed down through the definition of a set of *inclusion and exclusion criteria*, which had to be objective in order to reduce the bias of the results and guarantee the repeatability of the review process.

We are dealing with a very recent and fast changing research area, and we therefore decided to restrict the time scope to the last five years. We ensured that all new initiatives were included by considering all those proposals published after 2006.

Owing to language limitations, only studies written in English were considered in this review.

One of the objectives pinpointed in this review was that of compiling comprehensive security frameworks. A further *inclusion criterion* was, therefore, to ensure that we selected proposals that dealt with as many security aspects as possible. An objective criterion was established by relying on an accepted and widespread security standard: the ISO/IEC 27000 standard family [ISO/IEC (2005)]. This standard is widely used among security professionals and includes a set of security control clauses which may serve as guidelines to achieve effective information security management. This reference was chosen because it covers a wide range of security issues, both technical and managerial, that have been agreed upon on a worldwide basis. The inclusion criterion was based on checking whether each review result tackled all the security control clauses defined in the ISO/IEC standard; if the proposal did not deal with at least half of the security control clauses in a suitable manner, it was excluded. However, if the approach covered six or more clauses out of the eleven defined in sufficient detail, it was included in the systematic literature review process.

This group of criteria was used to narrow down the initiatives obtained by the first search. In most cases, it was sufficient to contrast the title and abstract or executive summary with the proposed criteria to decide whether to include or exclude the proposal. Nevertheless, when in doubt it was, in some cases, necessary to analyze the whole text in order to make the appropriate decision.

The quality assessment of the selection of publications performed was conducted in the aforementioned multistage process. As previously stated, the systematic review was executed iteratively, signifying that the results were analyzed after each cycle to confirm whether we were heading in the right direction.

2.3 Data Extraction and Synthesis

The purpose of our systematic literature review was to compile all the ISG frameworks related to Cloud Computing in order to be able to analyze and compare them. Although the initial selection performed by the proposed process was used as a basis, it was still necessary to define a comparative environment which would lay the foundations for the subsequent analysis. The *data extraction* process provided a better understanding of the actual relevance of each proposal.

The *comparative framework*, which is detailed in the following section, shows the various items of information that were extracted from each initiative. This resulted in data extraction forms that were filled in for each proposal.

Although it would have been possible for the review process to end with the extraction of data from the selected initiatives on the basis of the criteria defined in the comparative framework, we continued with the process, using these data to obtain information about each proposal and synthesizing it. We therefore came closer to the objective of gaining knowledge about the strengths and weaknesses of existing ISG frameworks in the research area of Cloud Computing.

The data synthesis led to a descriptive summary of the characteristics of each initiative, and it was therefore possible to complete existing gaps and to discover which desirable features were required.

3 Comparative Framework

In this section, we introduce a *comparative framework* of Information Security Governance for its application to Cloud Computing initiatives. It was not our intention to define a universal framework which could be applied to every security proposal in general, but rather a set of conceptual references that would permit an objective comparison of the systematic review results.

This framework unites features from different research areas, such as Information Security, Cloud Computing and Information Technology (IT) Governance. In order to simplify the comparative criteria, the most relevant aspects of each field are described below in order to extract the differentiating characteristics on which our comparison is based. We therefore focus on the specificities that arise in the overlapping of these areas and not on well known general matters.

The utility of this comparative framework lies in the fact that it provides precise criteria with which to undertake the data extraction from the security proposals. The comparison of various initiatives on the basis of specific concepts provides more intuitive results.

3.1 Introduction to Information Security Governance

Information Security Governance (ISG) consists of the leadership, organizational structures and processes that safeguard information inside an organization [ITGI (2006)]. More specifically, it is considered to be the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk [Bowen (2006)].

The above definitions, along with others that can be found in literature, allow us to conclude that ISG is directly related to three research subjects: Information Technology Governance, Corporate Governance and Information Security. Although this is studied in a Cloud Computing environment, this relationship must be born in mind if we are to be able to distinguish and disaggregate the different components of which it is made up.

The comparative analysis performed in [Rebollo (2011b)] reviews a wide variety of existing ISG frameworks in the light of these three domains. The analysis results show that although each framework attempts to deal with ISG in a comprehensive manner, some aspects are tackled in more depth than others. Matters such as Risk Management, Strategic Alignment or Process Management are considered in sufficient detail by almost all of the proposals, but other issues such as Value Delivery through IT or Control and Accountability are considered less frequently.

When transposing these security frameworks for their deployment in Cloud Computing, the same precautions must be taken. More importantly, the loss of control which is inherent in Cloud Computing must be compensated for with additional security controls to reduce vulnerability. Different criteria from the domains that shape ISG will therefore be extracted when defining the *comparative framework* of our systematic review.

From the same previous study we can also learn that, globally speaking, two of the ISG frameworks analyzed achieve the best results in the completeness ranking, but each of them offers a different perspective: the IT Governance Institute proposal [ITGI (2007)] is mainly focused on IT Governance, and ISO/IEC standards [ISO/IEC (2005)] deal principally with aspects of Information Security. These two references were used in our systematic review in the process of defining the *comparative framework*.

3.2 Overview of Information Security in Cloud Computing

The Cloud Computing environment has led to the emergence of new security risks owing to the process modification it prompts within the client organization. It additionally modifies existing old risks whose threats and vulnerabilities need to be re-evaluated [Jericho Forum (2009)]. The Information Security of cloud services shares many similarities with the traditional IT services deployed in a company, but it also has sufficient specificities that are worth consideration.

As with any new technology, Cloud Computing creates new risks and opportunities. Moving services or applications to the cloud may generate new opportunities for the business, its security and its IT departments owing to the re-architecting of applications, but this simultaneously creates threats to security [Cloud Security Alliance (2009)]. When customers move their data or applications to the cloud, the processes of implementing and enforcing security policies change to involve a third party. The enterprise's loss of control emphasizes the need for special requirements from cloud service providers (i.e. transparency, accountability…).

The comparative review of cloud security proposals developed in [Rebollo (2011a)] analyzes existing Information Security frameworks that have been specifically designed for the Cloud Computing environment. This comparison is performed using the eleven security control clauses from the ISO/IEC 27002 standard as evaluation criteria. Some other criteria are also introduced to evaluate cloud particular conditions such as the alignment between client IT security policies and cloud provider implementation, and liability, which reflects the relationship of responsibility between the cloud customer, the provider and applicable laws.

Analysis results show that cloud specific criteria and those that gather traditional security issues, which are usually related to a technical point of view, are widely taken into account in the proposals studied. Of these criteria, the following can be highlighted: Access Control, Communications and Operations Management, Physical and Environmental Security, and Compliance. However, aspects related to organizational management are less frequently considered. These are Security Policy, Asset Management and Human Resources Security.

Upon summarizing these results we can conclude that existing cloud security frameworks are more focused on systems and physical security, that is, they highlight traditional and well known security aspects. Nevertheless, security governance, high level organizational processes, and related security subjects that have gained importance in the last few years, are not dealt with in such great depth in these proposals. There is thus an obvious need for research to continue in these fields.

The conclusions extracted from this comparative review may also be used to take advantage of our systematic literature review by obtaining valuable information for the early stages of the process defined. As a reference for the definition of the

comparative framework, the cloud security proposals that achieve the best marks are those developed by the Cloud Security Alliance (CSA) and the European Network and Information Security Agency (ENISA).

3.3 Definition of the ISG Comparative Framework

The *comparative framework* defined in this systematic literature review was used to perform the data extraction of the selected primary studies. As stated previously, it is not our intention to develop a holistic comparison of ISG proposals, and the scope is therefore limited, in a more practical manner, to a set of differentiating features that are suitable for the Cloud Computing area, thus providing more valuable results. Security aspects that are well known by the academic community and taken into account in most of the approaches are not dealt with in our comparison, and we simply focus on the relevant aspects that arise in the confluence of these research fields. The ideas gathered about ISG and Information Security in Cloud Computing were used as a basis from which to extract these differentiating characteristics and define the criteria to be used in the comparison.

With regard to the two studies introduced previously, we shall now highlight some of the results concerning the deficiencies identified in existing security frameworks. In [Rebollo (2011b)] we can observe that current ISG proposals show lacks in matters such as Value Delivery through IT or Control and Accountability, while in [Rebollo (2011a)] we learn that the security topics that are least frequently considered in existing cloud security approaches are Security Policy, Asset Management and Human Resources Security. Upon uniting these topics it is possible to observe certain similarities, and it seems that all of them belong to the overlapping area of all the aforementioned research fields involved in this review. This area, despite appearing to be relatively diffuse, is the main objective of our comparative framework, and contains the necessary elements that prevent the loss of security governance caused by the outsourcing of services to a third party.

A Cloud Computing ISG function requires active reinforcement of those governance aspects that may compromise an enterprise's security, and result in an increase in vulnerability as a result of the new relationship between the company and the cloud provider. This new relationship needs additional resources so that both the cloud client and the provider can trust each other as regards the services contracted. According to the analysis shown above, and to our preliminary research, the criteria that represent the most relevant characteristics, which may differentiate ISG frameworks in a Cloud Computing deployment, are supported by three pillars: *Policies and Processes Adaptation* (PPA), *Control and Audit* (CA), and *Service Level Agreements* (SLA). The description of these three criteria, which are intimately related, is shown as follows.

Whenever a company decides to use Cloud Computing services, its managers need to make additional efforts as regards redefining the processes affected. The security ambit is no exception, and security policies therefore need to be re-evaluated according to the cloud paradigm. Information Security Governance processes developed in the organization should result in security collaboration programs between customers and providers to achieve agreed goals [Cloud Security Alliance (2009)]. *Policies and Processes Adaptation* reflects these modifications which involve the whole organization from the governance organs to the working staff,

owing to the fact that processes that have traditionally taken place in the company or even in a department, are now driven by the cloud provider. We have included topics such as the redefinition of roles, the modification of Information Security policies to ensure strategic alignment with the business, the implementation of new security processes and procedures in order to achieve the company's goals, the optimization of security investments that deliver business value through IT, the risk management of both traditional and emerging threats, and the management of identities in this criterion.

Enterprises need to be able to control these new processes, which run out of the company's boundaries into the cloud provider. Similarly, as with traditional procedures, control points and periodical checking are recommendable, and have the added difficulty of involving a third party. The *Control and Audit* criterion embraces the additional security controls that should be established owing to the new cloud relationship. It includes a definition of new security controls, the specification of security metrics for evaluation, performance management by monitoring security strategies and processes, the provision of tools that allow cloud provider logs to be accessed, and new auditory functions that allow the client organization to audit and evaluate the services provided by the cloud by monitoring its levels.

The two aforementioned criteria are glued together with the SLA signature. This agreement reflects the commercial relationship between the cloud client and the provider. The SLA is a tool that permits customers to specify the security requirements they expect during the provision of the service, and should offer a commitment to provide the security services required on the part of the cloud provider [ISACA (2009)]. The governance body of the company must be aware that, although it is possible to delegate the responsibility of some processes or operations to the cloud provider, its own accountability cannot be transferred. It is thus of paramount importance to guarantee that the SLAs include all the security aspects that the organization wishes to control. The *Service Level Agreement* criterion contains issues such as the precise limitation of responsibilities between the cloud client and the provider, the definition of security accountability of every role in the company, the establishment of compliance requirements and controls that will periodically be held to evaluate the service, the clarification of legal concerns such as applicable law in the case of a trial, whose jurisdiction involves stored data, or whether the cloud provider can sub-contract services to another provider, and possible penalties for infractions on both sides. It is worth noting that the non-fulfilment of the SLAs is a security risk in itself, and must also be evaluated.

The *comparative framework* which is composed of these three criteria will be taken as a reference to extract information about how each ISG approach deals with these matters. These objective criteria guarantee that the results of our systematic literature review will provide a comprehensive overview of the actual state of ISG proposals in Cloud Computing.

4 ISG Frameworks Data Extraction

This section contains a summary of the information extracted from each of the ISG frameworks found by our systematic review process. A brief description of each

proposal is provided, along with the most relevant aspects related to the three comparative criteria defined in the previous section.

4.1 Cloud Computing: Benefits, risks and recommendations for information security

Description. The European Network and Information Security Agency (ENISA) has published a guide [Catteddu (2009)] which assesses the security risks and benefits of using Cloud Computing, and provides security guidance for potential and existing users. This guide reviews technical and legal risks, along with policy and organizational issues. Of these, the Loss of Governance stands out, and reflects the loss of control when services are outsourced to a third party. These risks are used as a starting point for the introduction of an information assurance framework, which is based on the controls from the ISO 27000 family.

PPA. The loss of control and governance could lead to the impossibility of complying with the security requirements, a lack of confidentiality, integrity and availability of data, and a deterioration of performance and quality of service. This framework proposes guidance questions with which to perform the process adaptation, most of which are related to personnel and operational security and to the supply-chain assurance.

CA. Although the authors state that the ISG instruments should be used to keep watch on common practices among cloud providers in order to avoid severe impacts being made on the organization's strategy, this guidance does not provide detailed recommendations with regard to the Cloud and Audit function.

SLA. Cloud Computing generates new legal risks such as those resulting from changes in jurisdiction when the client does not control where its applications or data reside. ENISA offers a list of areas that should be included in legal agreements which includes data protection and transfer, confidentiality, intellectual property or limitation of liability. The authors state that the SLAs should offer a commitment to provide the required security services on the part of the cloud provider.

4.2 Cloud Cube Model

The Cloud Cube Model proposed in [Jericho Forum (2009)] identifies criteria with which to differentiate cloud formations from each other and their provision scheme. The model's objective is to assist in determining which cloud formation is best suited to the business' needs, along with enabling secure operation through the chosen option. The Jericho Forum's model proposes the development of a Collaboration Oriented Architecture (COA) to assure secure business in de-perimeterised environments. The COA framework [Jericho Forum (2008)] includes a set of guidelines with which to guarantee secure interaction between users and end systems located in different security domains.

PPA. Business processes need to be redefined so that they can operate across and between multiple organizations. The authors therefore ensure that COA-compliant architectures permit that the way in which organizations do business changes, whilst managing information risks to an acceptable level. They also identify key lifetime management processes that need to be mastered if reliable transformations are to be achieved.

CA. Audit information needs to be of adequate quality if it is to meet the needs of each collaborating organization, and a driving principle in audits on COA-compliant architectures is, therefore, transparency between partners. This framework thus provides recommendations for the audit and compliance areas.

SLA. This architecture recognises among its principles the importance of compliance with legal and contractual requirements. Participating parties can thus resolve conflicts through enforcement mechanisms. However, limited recommendations are offered in this criterion.

4.3 Cloud Security and Privacy

Description. The authors of the book [Mather (2009)] propose an introductory view to a variety of security issues related to Cloud Computing, so that users can be confident of dealing with the most important concerns.

PPA. From the ISG perspective, the cloud service provider and its customer have to manage various processes, such as Managing identity, Defining service requirements, Monitoring service levels, Providing assurance in internal controls, Managing incident response, or Developing a business continuity program. The role of IT departments will change to become more like that of managers of the IT services provided, since the operations are transferred from the customer to the cloud provider.

CA. The authors highlight the importance of audit and compliance functions, particularly in Cloud Computing environments owing to its outsourcing nature. A whole chapter is dedicated to these ISG issues, and provides implementation recommendations. A different perspective is offered since greater emphasis is placed on the cloud provider than on the client organization.

SLA. The book is scattered with recommendations about topics that should be included in the SLAs, but this criteria is not dealt with at the same depth as in the previous frameworks. The authors advise a review of the standard SLAs since they usually lack the desirable transparency.

4.4 IT Control Objectives for Cloud Computing

Description. The Information Systems Audit and Control Association (ISACA) has recently published [ISACA (2011)] with the purpose of providing an understanding of Cloud Computing and identifying its related risks. This framework deals with governance, security and assurance aspects separately. The proposal contains references to other additional ISACA papers in order for it to be complemented with governance criteria.

PPA. Typical Governance activities such as goal setting, policy development, and risk management must be considered in this new environment. Changes must therefore be made to ensure that performance objectives are met and that business and technology are strategically aligned. The authors propose adapting CobIT [ITGI (2007)] to handle cloud related processes.

CA. An audit and assurance program is provided in [ISACA (2010)] to be used in a Cloud Computing environment, which includes an enterprise risk management framework to identify security risks and mitigate vulnerabilities. The governance of this risk management can be performed by using the ISACA's Risk IT framework.

SLA. ISACA states that the SLA is the most effective tool an enterprise can use to ensure adequate protection. It must contain clear requirements as regards handling, usage, storage and availability of information, and specific rights for an external audit.

4.5 Security Guidance for Critical Areas of Focus in Cloud Computing

Description. The Cloud Security Alliance (CSA) has published guidelines on different security issues related to Cloud Computing. The guide [Cloud Security Alliance (2009)] has a section which deals with Governing in the Cloud, whose second domain is dedicated to Governance and Enterprise Risk Management. The proposed guidelines are not compulsory and may not all be applicable to every cloud deployment, but help to identify threats in the cloud context and to choose the best options by which to mitigate vulnerabilities.

PPA. The CSA's guidelines propose that any ISG processes developed within the organization should result in security collaboration programs between customers and providers to achieve agreed goals. The service model may adjust the defined roles and responsibilities in collaborative information security governance and risk management processes. User organizations should review ISG structure and processes, and assess the provider's security processes and capabilities for sufficiency and consistency with their own.

CA. The provider's security processes and controls should be assessed and audited, although traditional assessment approaches may not be available and new audit techniques may be defined. Organizations need to understand their cloud provider's ability to produce the evidence required for the compliance evaluations, and should assume the role of bridging the gap between the cloud provider and the third party auditor. Moreover, the provider's information security controls should be demonstrably risk-based and clearly support the client's processes.

SLA. Among the ISG recommendations provided by the CSA, high emphasis is placed on defining metrics and standards for measuring the performance of information security, which should be auditable and be documented on the contracts. As part of the legal issues, the CSA distinguishes between functional, jurisdictional, and contractual dimensions.

4.6 Security and Control in the Cloud

Description. [Julisch (2010)] proposes expanding the concept of an Information Security Management System (ISMS) from ISO/IEC 27001 to a virtual ISMS. An ISMS includes the set of processes and policies used by an organization to implement, operate and monitor information security; and a virtual ISMS extends this concept to services that are outsourced to cloud providers. By following this standard, the Plan-Do-Check-Act (PDCA) cycle is adapted to the virtual ISMS, the planning and control steps being the most relevant when dealing with cloud services.

PPA. The authors adopt the iterative PDCA cycle to define, implement and review the organization's internal processes. Continuous iterations are used to refine the processes in order to achieve their control objectives.

CA. Most of the Control functions take place in the Check phase of the cycle. The paper focuses on the cloud provider side, where there is more space for further

improvement, particularly in defining the type of monitoring provided, and the procedures followed to perform third party audits.

SLA. This paper analyzes public cloud's SLAs and concludes that they tend to protect cloud providers with small penalties in comparison to the risk that is transferred. Each iteration of the PDCA cycle should include the possibility of modifying existing SLAs if new improvements are made or necessities change.

5 Comparison of ISG Frameworks

In this section we summarise the main contributions of each ISG Framework analyzed in our systematic literature review in the light of the proposed comparative criteria. The differentiating characteristics of each proposal are therefore highlighted so that both cloud clients and providers may easily distinguish which one suits their own necessities for successful security governance. This analysis also includes the subjects that are not tackled in the ISG proposals and the gaps that we believe need to be filled.

Table 1 shows the main concepts included in each ISG Framework in relation to the three cloud governance comparative criteria (*Policies and Processes Adaptation*, *Control and Audit*, and *Service Level Agreement*).

In addition to presenting the main contributions, the table also shows an 'X' whenever a criterion is insufficiently developed and lacks are evident. An '(*)' is used to indicate the cases in which the subjects are dealt with in an external source that is different to the reference analyzed in our systematic literature review, but belongs to or is related to the same ISG framework.

Generally speaking, a first glance at the table shows that most of the ISG approaches offer recommendations or advice to cover the fields of the proposed criteria. A more precise definition of procedures and tools should therefore be provided in order to facilitate the security governance development. A more detailed concreteness of activities and tasks would be desirable for the implementation phases.

In the few cases in which processes are outlined, the authors follow the widely known Plan-Do-Check-Act (PDCA) cycle suggested in popular security standards such as ISO/IEC 27001 [ISO/IEC (2005)]. This perspective has also been adopted by later studies such as that of [Miller (2009)] in which more details are provided about each of the PDCA cycle steps with the aim of adapting the security governance to the Cloud Computing environment.

With regard to the *Policies and Processes Adaptation* criterion, the ISG frameworks recommendations deal principally with processes management, the redefinition of organizational roles and, to a much lesser extent, with IT alignment with the business. Other subjects within this criterion that are not mentioned and which should be included are as follows: the cost/benefit analysis of effective governance, the communication of security management goals and principles in the organization, policy documentation procedures, and the security awareness and training of all the organization's users.

ISG Framework	Policies and Processes Adaptation	Control and Audit	Service Level Agreement
Cloud Computing: Benefits, risks and recommendations for information security (ENISA)	- Recommendations and check-list questions to provide assurance	X	- Legal and contractual recommendations
Cloud Cube Model	- Collaboration Lifecycle Management processes (person, risk, information, device and enterprise relationships) (*)	- Audit and Compliance from Collaboration Oriented Architecture (*)	X
Cloud Security and Privacy	- Proccesses management - Adapt security management standards (ITIL, ISO 27001)	- Cloud provider audit recommendations	X
IT Control Objectives for Cloud Computing (ISACA)	- Adjust the way business processes are handled - IT alignment with the business - CobIT (*)	- Audit and Assurance Program, tool (*) - Risk IT (*) - Val IT (*)	- Requirements for business continuity and disaster recovery - Rights for third party audits
Security Guidance for Critical Areas of Focus in Cloud Computing (CSA)	- Collaboration programs - Redefine roles and responsibilities	- CloudAudit (*)	- Common Assurance Maturity Model (*) - Legal recommendations (functional, jurisdictional and contractual)
Security and Control in the Cloud	- PDCA cycle to refine processes	- PDCA cycle for Control functions	- PDCA cycle with dynamic contractual changes

Table 1: Comparison of Cloud Computing ISG Frameworks with the defined criteria

In relation to the *Control and Audit* criterion, ISG frameworks recommend different kinds of audit tools which attempt to adapt their functions to the

particularities of the outsourcing inherent to Cloud Computing deployments. However, most of these tools are provided by external documents, which do not necessarily detail how to perform these audits or adapt them to the cloud environment. Some other ISG control topics that are not included and should also be mastered by the proposals analyzed are: the regular measurement and reporting of progress and detected issues, procedures for monitoring the compliance with regulatory requirements, internal policies and technical standards, the definition of metrics to evaluate services, and how logs are stored and accessed by third parties.

Finally, of the ISG frameworks analysed, the *Service Level Agreement* criterion is that which appears to be most diffused. Although most of the proposals include legal and contractual recommendations to be followed when redacting SLAs, more emphasis should be placed on the development of bilateral agreements, and not only on unilateral agreements. The development of SLAs involves certain particularities that can only be solved at a local or regional level, but common practices that are spread over the reviewed frameworks should be gathered together and standardized. No company's security can rely solely on contractual controls and the subsequent judicial procedures, and the SLAs must therefore reflect the fact that ISG needs to be coordinated between both the cloud user and the provider. Apart from the terms and conditions that are recommended by most ISG frameworks, we consider that the SLAs should include both the processes and the controls defined by the two aforementioned criteria and agreed between the provider and the client; more active implication in the cloud service may thus be achieved among participants. Another activity that should be taken into account is the benchmarking of SLAs, considering the involvement of senior management in order to allow the measurement and comparison of different providers.

Comparison results show that most of the ISG frameworks reviewed deal partially with all the proposed cloud security criteria, but that additional efforts should be made to fill the gaps detected. In order to achieve a comprehensive ISG approach that is suitable for a Cloud Computing environment, the highlighted lacks could be reviewed and mastered previous to the service deployment. Each of the three criteria includes important issues that have not been tackled by the ISG frameworks analyzed, and that must be assured by both cloud clients and providers. These detected issues will serve as foundations in order for us to continue our research in this area.

6 Conclusions and Perspectives

The great importance that Cloud Computing is attaining among IT professionals and the imperious necessities of some organizations to jump into the cloud signifies that the Information Security of this new paradigm is becoming a top research priority. The governance functions of the cloud model mean that the procedures and activities of both cloud clients and providers must be adapted, and both operational staff and senior management must be involved in this process.

This paper contributes to the security governance of Cloud Computing environments in two major aspects: on the one hand, a systematic literature review is conducted to extract, from a variety of academic sources, existing ISG frameworks that are suitable for application in Cloud Computing deployments; on the other hand, a comparative framework is defined whose criteria facilitate the analysis and

comparison of the former ISG frameworks, focusing on the main particularities of the cloud model.

Although the comparative analysis shows that current ISG frameworks deal with most of the proposed criteria to some extent, gaps have been detected that must be filled. New research lines are open to investigate the reviewed proposals in order to fill the gaps. Our future research will benefit from the comparison performed, since it highlights the desirable features of security governance in Cloud Computing. If we are to develop a comprehensive cloud ISG framework, we must consider every aspect pinpointed in this review. We are currently researching this field in depth with the intention of solving the deficiencies found in the process adaptation, audit and SLAs criteria.

Acknowledgements

This research is part of the following projects: MEDUSAS (IDI-20090557) and ORIGIN (IDI-2010043(1-5), financed by the Centre for Industrial Technological Development (CDTI) and the FEDER, MAGO-PEGASO (TIN2009-13718-C02-01) awarded by the Spanish Ministry for Science and Technology and SERENIDAD (PEII11-0327-7035) and SISTEMAS (PII2I09-0150-3135) financed by the Council of Education and Science of the Castilla-La Mancha Regional Government.

References

[Armbrust (2009)] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. "Above the Clouds: A Berkeley view of Cloud Computing", University of California, Berkeley (2009).

[Bisong (2011)] Bisong, A. and Rahman, S. S. M. "An overview of the Security Concerns in Enterprise Cloud Computing." International Journal of Network Security & Its Applications (IJNSA) 3(1): 30-45 (2011).

[Bowen (2006)] Bowen, P., Hash, J. and Wilson, M. "Information Security Governance". Information Security Handbook: A Guide for Managers, National Institute of Standards and Technology: 2-19 (2006).

[Catteddu (2009)] Catteddu, D. and Hogben, G. "Cloud Computing Security Risk Assessment - Benefits, risks and recommendations for information security", European Network and Information Security Agency (ENISA) (2009).

[Cloud Computing Use Case Discussion Group (2010)] Cloud Computing Use Case Discussion Group. "Cloud Computing Use Cases White Paper v4.0, http://cloudusecases.org/." (2010).

[Cloud Security Alliance (2009)] Cloud Security Alliance. "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1." (2009).

[Chen (2010)] Chen, Y., Paxson, V. and Katz, R. H. "What's New About Cloud Computing Security?", University of California, Berkeley (2010).

[Gartner (2011)] Gartner. "Gartner's Hype Cycle Special Report for 2011." (2011).

[IDC (2009)] IDC. "IDC IT Cloud Services Survey: Top Benefits and Challenges." (2009).

[ISACA (2009)] ISACA. "Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives", (2009).

[ISACA (2010)] ISACA. "Cloud Computing Management Audit/Assurance Program" (2010).

[ISACA (2011)] ISACA. "IT Control Objectives for Cloud Computing." (2011).

[ISO/IEC (2005)] ISO/IEC. "ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements.", (2005).

[ITGI (2006)] ITGI. "Information Security Governance: Guidance for Boards of Directors and Executive Management (2nd Edition)" (2006).

[ITGI (2007)] ITGI. "Control Objectives for Information and related Technology (COBIT 4.1)" (2007).

[Jericho Forum (2008)] Jericho Forum. "Collaboration Oriented Architecture, http://www.opengroup.org/jericho/publications.htm." (2008).

[Jericho Forum (2009)] Jericho Forum. "Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration." (2009).

[Julisch (2010)] Julisch, K. and Hall, M. "Security and Control in the Cloud." Information Security Journal: A Global Perspective 19(6): 299-309 (2010).

[Kitchenham (2004)] Kitchenham, B. "Procedures for Perfoming Systematic Review", Australia, Joint Technical Report, Software Engineering Group, Departement of Computer Scinece Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd. (2004).

[Kitchenham (2007)] Kitchenham, B. and Charters, S. "Guideline for performing Systematic Literature Reviews in Software Engineering. Version 2.3", University of Keele (Software Engineering Group, School of Computer Science and Mathematics) and Durham (Department of Conputer Science) (2007).

[Mather (2009)] Mather, T., Kumaraswamy, S. and Latif, S. "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'Reilly (2009).

[McKinsey (2009)] McKinsey. "Clearing the air on cloud computing." (2009).

[Mell (2009)] Mell, P. and Grance, T. "The NIST Definition of Cloud Computing v15", National Institute of Standards and Technology (NIST) (2009).

[Miller (2009)] Miller, J., Candler, L. and Wald, H. "Information Security Governance - Government Considerations for the Cloud Computing Environment", Booz Allen Hamilton (2009).

[Ponemon Institute (2011)] Ponemon Institute. "Security of Cloud Computing Providers Study", (2011).

[Qian (2009)] Qian, L., Luo, Z., Du, Y. and Guo, L. "Cloud Computing: An Overview." Proceedings of the 1st International Conference on Cloud Computing: 626-631 (2009).

[Rebollo (2011a)] Rebollo, O., Mellado, D. and 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 (2011a).

[Rebollo (2011b)] Rebollo, O., Mellado, D., Sánchez, L. E. and Fernández-Medina, E. "Comparative Analysis of Information Security Governance Frameworks: A Public Sector

Approach", 11th European Conference on eGovernment – ECEG 2011, Ljubljana, Slovenia (2011b).

[Sloan (2009)] Sloan, K. "Security in a virtualised world." Network Security(8): 15-18 (2009).

[Subashini (2011)] Subashini, S. and Kavitha, V. "A survey on security issues in service delivery models of cloud computing." Journal of Network and Computer Applications 34(1): 1-11 (2011).

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

[World Economic Forum (2011)] World Economic Forum. "Advancing Cloud Computing: What to do now?" (2011).