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-

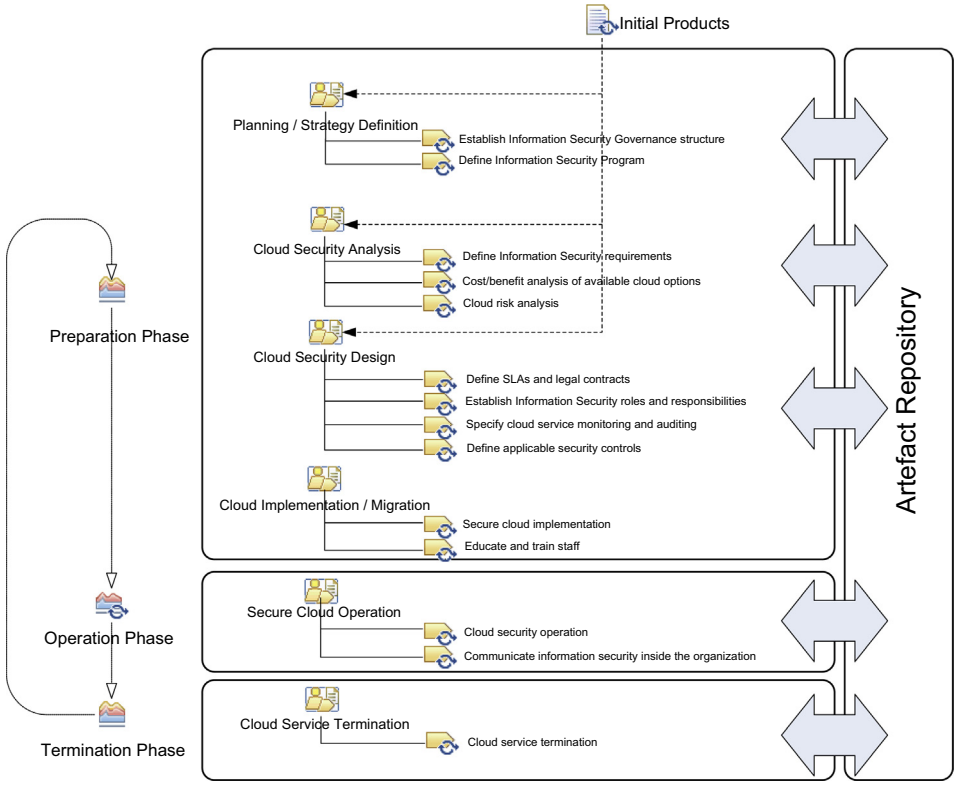

Fig. 1. ISGcloud framework.

mated and reused by external tools, we have used the SPEM specification to model ISGcloud's tasks. Each task's model includes the products used, the steps followed, the suggested guidance and the roles involved in its execution. The definition of each task's roles is important in order to being able of designating who is responsible and accountable of each task, and because not only internal roles are involved (for instance, some tasks require active involvement of the cloud provider or external auditors).

The process flow through the framework's activities is performed not only sequentially, but through iterative cycles. Each governance cycle is performed according to the previously mentioned four core processes. The results of each iteration determine whether it will be necessary to go forward or backward in the framework, signifying that artefacts are refined until the desired objectives are achieved.

The purpose of ISGcloud framework is to execute its tasks during the cloud service deployment and operation, parallel to the service's internal tasks, thus guaranteeing that a security governance structure exists around the cloud service and that all relevant aspects of security are taken into consideration.

3. Empirical evaluation design

This section contains a description of the design of our case study in order to perform an empirical evaluation of ISGcloud framework. We have followed the protocol proposed by Runeson and Höst [22], since having a standard methodology increases the opportunities of success and guarantees the process's validity. In particular, Runeson and Höst suggest translating the research objectives that have been already identified in the introduction into research questions that drive the empirical evaluation's realisation. The next step is the selection of the case and subjects which is also explained, and we finally detail the data collection procedure and explain how these data are analysed to achieve a procedure that is valid.

Following this protocol, an exploratory approach has been adopted in our empirical evaluation, thus allowing us to assess ISGcloud's performance, seek new insights and generate ideas for the framework's improvement. We also propose a flexible design, since the intrinsic characteristics of security governance encourage the handling of qualitative information and not every process can be translated into quantitative data.

The empirical evaluation's research objectives are focused on three main pillars, which can be synthesised as: cloud service security, development of a security governance structure, and the practical applicability of ISGcloud framework. These three objectives can be measured during the case study by answering the following research questions:

- Does ISGcloud lead to a secure cloud service deployment? The service's security is measured by evaluating the extent to which the organisation's security requirements are covered by the cloud provider's solution.
- How does ISGcloud favour the development of a security governance structure within the organisation that the cloud service provides coverage? Governance metrics need to be defined in order to evaluate the state of security governance inside the organisation after the service deployment, and being able to compare it with its previous situation.
- How practical and usable is the utilisation of the ISGcloud framework within an organisation? This question is measured through interviews and questionnaires to the different roles involved in the process, asking for feedback, about the easiness of the framework's application, its help and usefulness, and suggested modifications.

One of the main challenges, not only for us but for the research community as a whole, when putting a framework like ISGcloud, which comprehensively covers so many business aspects and concerns most of the existing security processes, into practice is the

difficulty to find candidate organisations willing to implement it. To overcome that challenge, in this paper we report the application of the framework to an organisation where some of the authors are currently employed. The precise nature of the cloud service is described later in the context section and, although this description may appear to be relatively modest, we consider that it is sufficiently representative to validate the practical application of ISGcloud framework and to answer the proposed research questions.

When defining the data collection procedure, the researchers' close relationship with the organisation's employees facilitated the choice of interviews as the main data collection mechanism. First degree data was thus obtained directly from the stakeholders. Upon considering the broad range of roles and people involved in the project, these interviews were planned in a semi-structured mode, in which the interview sessions are outlined in general questions and more specific subjects appear in each situation. Moreover, valuable data is obtained through direct observations of the process performance and by accessing the cloud service project documentation, both of which are required in order to fully answer our research questions.

The inherent characteristics of our empirical evaluation signify that the analysis procedure can be considered to be qualitative, although quantitative measures are collected in specific cases. In order to reduce possible bias during the analysis, it was designed as an iterative succession of steps in which conclusions were first contrasted by another researcher and then validated by the appropriate project member. The analysis was performed chronologically, following the successive development of the ISGcloud tasks and classifying the data collected in each step into the most appropriate research question.

This structured methodology has contributed to the formalism of our case study and to the validity of our results. Reliable results are consequently expected for the proposed research questions, and we have therefore been able to evaluate the suitability of ISGcloud framework in order to guarantee security governance for the cloud service selected.

4. Empirical evaluation context

This section depicts the context in which our empirical evaluation took place. We provide a description of both the organisation used to carry out our ISGcloud process and the problem that we aim to solve.

4.1. Description of the organisation

The organisation in which we decided to deploy the ISGcloud process is a Spanish public state organisation. Reasons of security and confidentiality signify that it is necessary to prevent the disclosure of relevant issues that may suppose a potential security threat to this organisation. However, we provide sufficient technical details to allow the reader to understand the organisation's context and follow the whole process.

This public organisation is responsible for providing the Spanish Social Security System with IT services, and its main function is to provide the various entities and organisations of which the State Secretariat for Social Security is formed with IT support. Its functions include systems maintenance, software development, security and IT innovation. Although it is made up of approximately 1500 employees, its services are offered to different entities signifying that its client group is made up of more than 30,000 public employees, spread over the whole country.

From the security perspective, the information held by this organisation is a critical asset not only because of its characteristics (personal data of an economic nature and health information) but also because of its quantity (information concerning every Spanish employee) and its future relevance (it contains data with which to calculate a worker's retirement, unemployment benefit or disability allowance). Each new service deployed in the organisation must consequently meet strict security measures and guarantee the security of the information it handles.

The size and complexity of this organisation also makes it suitable for developing governance policies signifying that its chief officers are able to permanently oversee every process that takes place within the entity. The fact that so many employees and direct collaborators are so spatially dispersed makes it crucial to develop a governance structure that fosters the receipt of feedback regarding almost every activity and guarantees that top strategies and directives are being followed.

A security governance framework such as ISGcloud can help this organisation to tackle security issues that may arise in the services that it provides in a comprehensive manner. This use of this framework will allow security processes to permeate the entire entity at every managerial level, thus guaranteeing alignment with the organisation's objectives.

4.2. Description of the problem

Mobile devices, such as smart-phones, tablets or laptops, are rapidly increasing their performance and achieving higher penetration rates at a fast pace. This trend is particularly relevant in the Spanish market, in which the penetration rate is higher than the European average [28,29]. These devices deliver a wide amount of capabilities, not only to individual clients, but also to the enterprise's professionals, for whom it becomes an essential tool in their everyday work.

The organisation in which our case study has been developed, is making efforts to increase the mobility of its employees. A mobility culture has become an important strategic line for its chief officers, who argue that the use of mobile devices with advanced capabilities will result in an increase in the productivity of the organisation's employees. Although such strategic boost is directed towards both internal employees (increasing their mobility tools) and external citizens (developing mobile applications in order to facilitate procedures with the Social Security), our empirical evaluation is particularly focused on the internal approach.

The development of the mobility strategic line has resulted in a variety of projects, one of which has the objective of delivering smart-phones and tablets to high and medium managerial level employees. These employees frequently make decisions to drive the organisation and direct the activities of workers at a lower level. The accuracy of these decisions usually depends on the precision of the information it is based on and on making them at the right time. These users have traditionally been granted remote access to their e-mails and some internal information, while being off the organisation's premises, but they have required a computer with an Internet connection to enable them to do so. These limitations have led to the infrequent usage of these connections, which is clearly an avoidable situation. The current distribution of smart devices attempts to solve this by allowing employees to access their e-mails and personal information from practically anywhere, thus permitting a more agile communication between users, even out of business hours.

Many of the functionalities of these devices can be securely achieved through the use of standard applications, by simply applying an adequate secure configuration. However, the organisation is extremely concerned about the potential threat of handling confidential and private information with mobile devices, as this information is leaving the organisation's premises. Bearing this in mind, additional efforts are being made to develop an appropriate

solution to the storage of confidential information that can be securely accessed by these devices. This storage cannot take place within the organisation, as it needs to be accessible from terminals that may be potentially connected anywhere, and the project leaders have therefore chosen to provide it as a cloud service. The mobile storage service is understood as a personal storage system in which each user can place his personal information and documents, and is able to access them not only from the mobile devices but from any other corporative equipment. It also allows users to share documents in a collaborative manner, and automatically performs backups, authentication and security policies, making them transparent to the users.

The storage service will be delivered as a phone application from the user point of view, and will work as a SaaS (Software As A Service) cloud service. The organisation additionally wishes the cloud operator to provide a private cloud so that it is not shared with other clients and so that an additional degree of personalisation can also be achieved. The project leaders intend to provide a service that is tailored to the organisation's needs, which constitutes a totally different approach to that offered by standard services. This cloud model also allows sufficient flexibility in order to enable the storage capacity to be increased or decreased on an on-demand basis, as the amount of potential users may change in the short term.

An overall picture of this service is shown in Fig. 2, in which the storage held by the cloud provider is accessible from both devices directly connected to the Internet and equipment located within the organisation or any of its collaborator entities. This figure also shows that all the information travels through the Internet, which is why security requirements are so important in this service design.

The size and complexity of the organisation and its client entities (the entire Social Security System) make it necessary to embrace the security policies in the corporate governance structure, and they are therefore directly supported by the chief officers and every managerial level knows its security role. This organisation has a classic governance structure, with many intermediate levels that seldom permit exceptions to the established chain of command. This is the main reason the project leaders, with the chief officers' support, are planning to extend and complement the present security governance structure in order to adapt it to recent security standards and best practices. The mobile storage service is this organisation's first step into cloud services, and it is thus an ideal chance to develop a security governance approach for this kind of services.

The organisation is structured in various divisions. Those which are most closely involved in the mobile storage project are the Production and Systems Division, which includes the Storage, Communications and Mobile Devices Departments, and the Security and Innovation Division, which includes the Security and Auditory Departments.

The users of the mobile storage service are not only employees of the organisation itself, but also many other collaborator entities that the organisation provides with IT services. In the short term, high-end smart-phones are being delivered to the chief officers and high executives of all the entities included in the Social Security System, and in the middle term it is hoped that lower managerial levels will be provided with low/middle-end terminals so that an increasing number of employees may benefit from their functionalities.

With regard to the project's complexity, the main problem is the time restriction, since the first users need to have the service operative in a period of three months, and this is another reason why it can only be offered as a cloud service, as there is no time to develop it internally.

The project's scope is clearly broader than the mere development of a security governance structure, so some details will be intentionally summarised in order to focus on the ISGcloud process. Moreover, as stated previously, some specific confidential information and data will be omitted. However, the description provided of the security governance case study will assist the reader to attain a global perspective of the ISGcloud process and contains sufficient details to allow the most important aspects of our approach to be understood.

5. ISGcloud process application

This section reviews the practical application of the ISGcloud process to the case study, providing more details on the most important tasks and aspects that may be relevant to answer the proposed research questions and to the framework's empirical evaluation.

The process described appertains to the execution of the first iteration of ISGcloud, in which the organisation chronologically follows the framework in its entire extension, as originally described

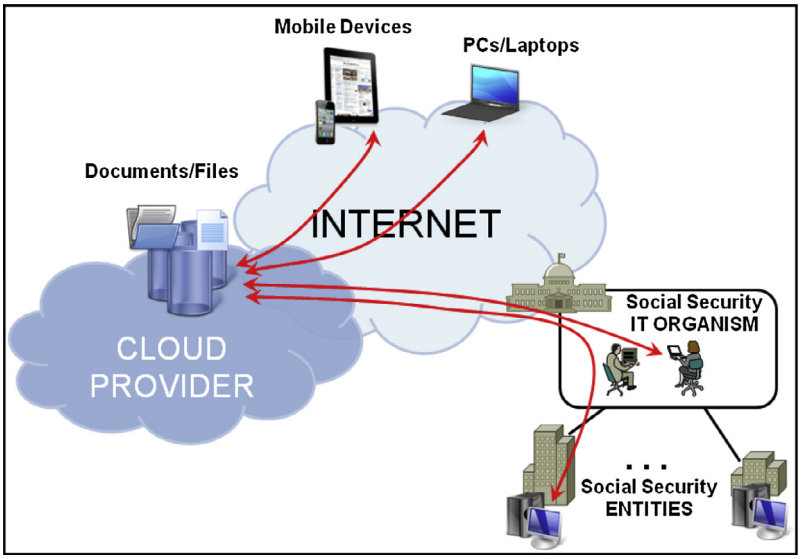

Fig. 2. Cloud storage service.

in [21]. Its purpose is to validate the proposed tasks in a real cloud service deployment, in order to adapt or modify them if necessary. Future iterations of ISGcloud in this organisation may also benefit from this work as it helps to highlight the most critical tasks or provide the organisation with more value, and facilitates the allocation of fewer resources in the remaining tasks.

ISGcloud can be tailored by the organisation to be adapted to any set of standards. This organisation, as part of the Spanish Public Administration, is subject to Spanish law, which includes legislation related to security aspects such as the Organic Law on the Protection of Personal Data and the Royal Decree regulating the National Security Framework. Besides the existing regulations, the organisation also intends to comply with international security standards.

5.1. Activity 1: planning/strategy definition

Although the organisation has established a working IT governance structure, its security governance may be considered relatively weak, as it usually relies on a few departments in the Security and Innovation Division. Bearing this in mind, the project leaders have decided to use this activity as a means to define a new security governance structure built from scratch. This new structure will be used solely in the context of the empirical evaluation, but in the future it may be contrasted with the existing one, thus allowing it to be adapted with the improvements detected.

5.1.1. Task 1A: establish information security governance structure

The security governance structure establishment first requires the identification of participant roles. The project leaders, in agreement with the chief officers, identified the main roles to be used in the ISGcloud process, which include a wide range of profiles such as senior officers, business line clients, human resources managers, IT and security managers, auditors, operators, and even cloud provider's personnel. This list of roles is complemented with a detailed description of each one's responsibilities. The profiles involved in the security governance structure are thus complete and ready to be assigned to individuals in later activities.

A security governance committee has also been created, which includes some project members and individuals from every role. This committee is in charge of supervising the security governance implantation, thus providing a certain amount of independency from the storage service deployment.

The last step in this task is to define top-level security policies as part of the security governance strategic plan. The organisation's goals and business strategy is translated into these policies. The top-level security policies related to the storage service include:

- Guaranteeing compliance with Spanish national and international regulations.
- Ensuring information access, management and retrieval.
- Participant roles must know their security responsibilities and act with due diligence.

Although it is not strictly necessary to follow this task in order to establish a security governance structure, the steps and guidance provided by ISGcloud helped the organisation to quickly identify the governance participants and to elaborate the products required in the later tasks.

One of our empirical evaluation's main objectives was being able to assess if an improvement was achieved in the organisation's security governance structure. In order to quantify this improvement, a set of ISG metrics has been developed taking into consideration the ISG goals the organisation intended to achieve. The definition of the metrics shown in Table 1 was based on strategic goals identified in governance proposals such as COBIT 5 [26].

These metrics were used to quantify the organisation's security governance structure at the beginning of the empirical evaluation, and therefore being able to compare it with the final situation achieved following ISGcloud. The metrics' results were homogenised to a uniform measure, so that results were easier to contrast and analyse. The followed methodology included the translation of these metrics to a scale ranged from 0 to 5, where 0 indicated a total absence or lack of the measured level, and 5 implied a full compliance with the metric's description. With this perspective, the metrics from all the ISG goals were merged and a unique governance measure was obtained.

After assessing the proposed governance metrics and translating their measures to a homogeneous scale, the results were weighted for each goal. Although precise information about the measures cannot be disclosed, Table 2 summarises the result of the first assessment. This result has proven very useful to evaluate ISGcloud's utility in developing a security governance structure, as we will show in the empirical evaluation's discussion.

5.1.2. Task 1B: define information security program

The organisation, as a consequence of its great concern for its information assets, had already developed a completely detailed Information Security Program. This program was structured in the following elements: security plan, security policies and procedures, and system architecture.

The aim of this ISGcloud task was to modify and complement the existing program to allow it to include security considerations as regards cloud services. As a first step, only the personal storage service is referred to, but the results obtained can be used with other cloud services with much less effort. The present economic situation has led to the need to foresee an increase in a demand for these services within this organisation, and ISGcloud has therefore introduced the foundations of the relationship between security governance and cloud services.

Taking the top-level policies defined in the previous task, the organisation proposed the overall security policies that will govern the cloud storage service. These security policies introduce the security requirements for the organisation's operation, thus ensuring the Information Security Program's alignment with the organisation's goal and strategy. This first approach to the Information Security Program was also complemented with the identification of security threats and vulnerabilities.

The Information Security Program becomes an essential element of ISGcloud, which is dynamically updated and complemented throughout the governance process. Once this task has been accomplished, the Information Security Program contains the basic foundations needed to enable the organisation to begin the security governance of the cloud service. ISGcloud then guarantees that the essential governance elements are taken into consideration so that the remaining processes can be successfully developed.

5.2. Activity 2: cloud security analysis

ISGcloud's second activity introduces a security analysis of the storage service and is divided into various tasks focused on several security aspects. Although the main steps of the tasks are executed by the project personnel in collaboration with the security managers, the chief officers must validate the results in order to maintain the governance structure defined.

5.2.1. Task 2A: define Information security requirements

The storage service's security requirements specification is intimately related to its technical specification. However, this task focuses on the security issues and will only mention technical aspects when necessary.

Table 1
Information security governance goals and related metrics.

ISG goal	Related metrics
Alignment of ISG and business strategy	Percent of enterprise processes into which ISG is integrated Frequency of ISG reporting to the executive committee Percent of business stakeholders satisfied with ISG
ISG contributes to optimal value delivery	Percent of security investments with approved benefits Level of business benefit vs. ISG investments Percent of expected value realised
Ensure security risk optimisation	Percent of enterprise risk mitigated with information security controls Frequency of security risk assessment Number of incidents that were not identified in risk assessment
Information security resources are optimised	Percent of deviation from information security budget Percent of reuse of information security solutions Percent of projects with appropriate resource allocations
Information security communication is effective	Percent of security reports that are delivered on time Number of information security training hours per staff member Percent of business stakeholders satisfied with security awareness

Table 2
Initial measurement of ISG goals.

ISG goal	Measurement	Overall score
Alignment of ISG and business strategy	1.5	2.4
ISG contributes to optimal value delivery	2	
Ensure security risk optimisation	3.5	
Information security resources are optimised	3	
Information security communication is effective	2	

Many of the security requirements of this service are imposed by Spanish regulations, to which the organisation is subject. Besides legal security requirements, it was necessary to define other kinds of security requirements for a proper design of the storage service. The following requirements were approved by the chief officers:

- Secure access: authenticate users when accessing their storage or sharing information, establish permissions so that data can only be accessed by their owners and authorised users.
- Implement security measures to prevent information leakage of stored data.
- Guarantee confidentiality and privacy of stored data and during its transfer.
- Guarantee information availability in the case of disasters or incidents on the cloud provider's premises.
- Deploy security mechanisms to prevent access to personal information when the mobile device is stolen or lost.
- Keep records/logs of storage security incidents and service use.
- Remote management of service's security.
- Allow security monitoring and auditing.
- Ensure the cloud provider personnel's compliance with security controls.
- Deploy security training plans directed towards users and technical operators.

These high-level requirements have been adequately modelled into more formal security requirements, so that they can be used to answer the empirical evaluation's research questions. The security requirements that were considered during the rest of ISGcloud process are shown in Table 3, where two hierarchical levels can be identified. The degree of these requirements' fulfilment by the implementation of the cloud service was used as a measure of the service's security. With this perspective we assess the cloud deployment's security not only based on the technical security measures implemented by the provider, but in conjunction with the extent to which the organisation's security requirements are covered and satisfied.

In this task, ISGcloud goes into the governance process in greater depth, bridging it with the security requirements definition. This is the path which allows security strategies and policies to become a secure service operation. ISGcloud framework also supports the alignment of the security governance process with chosen standards and provides sufficient flexibility to be able to adapt to them.

5.2.2. Task 2B: analysis of available cloud options

The security requirements identified, along with some other restrictions in the contracting procedures that are imposed on the organisation by Spanish regulations, narrowed down the cloud provider candidates that could be chosen to provide the storage service. Existing alternatives were analysed in this task from various perspectives in order to evaluate their security. This analysis complements others that may be performed in other departments, such as those of a technical or economical nature. The eventual choice must consider all these analyses and adequately ponder the security weight. Nevertheless, ISGcloud focuses on security aspects, although it does not guarantee that the best option is chosen from the point of view of security.

With regard to the aforementioned restrictions, the Innovation Department stated that there were only two available cloud providers for the storage solution. Owing to reasons of confidentiality, these alternatives will be referred to as Solution A and Solution B. The comparison of these alternatives necessitated the definition of a group of criteria that would evaluate the different aspects of ISG. Taking advantage of the security requirements that were defined in the previous task, the same requirements were used as comparative criteria to select the cloud provider whose security solution is best aligned with the organisation's needs.

The project members, in collaboration with the security managers, proceeded to evaluate all these criteria. The assessment was performed using a three point scale with the following weights:

- The provider has no provision to support the requirement: a 0 is allocated.
- The provider has limited or partial provision to support the requirement: a 1 is allocated.
- The provider has fully tested provision to support the requirement: a 2 is allocated.

The information for this evaluation was gathered from public statements related to both alternatives and from preliminary commercial encounters, in which some insights into security details were collected. Nevertheless, it is important to highlight that some specific criteria were difficult to evaluate due to the lack of appropriate information and, therefore, the project members acknowledged that the final security of the service's implementation might be different from the this task's estimations.

Table 3
Security requirements.

Security requirements	
1. Authentication	2. Confidentiality
1.1. User identification	2.1. Data isolation
1.2. Management of user's certificates	2.2. Anonymisation
3. Integrity	4. Availability
3.1. Encryption	4.1. Data recovery
3.2. Remote device management	4.2. Fault tolerance
3.3. Data backup	4.3. Data location
5. Transparency	6. Auditability
5.1. Incident reporting	6.1. Coverage
5.2. Data monitoring	6.2. Independence of verification
5.3. Service interoperability	6.3. SLA enforcement

The security analysis supported other additional information that the chief officers may have received, which eventually led them to choose the service named Solution A for deployment. Table 4 contains a summary of the allocated weights to each security requirements, along with the overall security score of each cloud service's alternative. Although the approach can support the allocation of different powers to weight each security requirement, in the presented case study the organisation decided to allocate the same weight for all.

In this task, ISGcloud helped by analysing the various cloud service alternatives by identifying comparative criteria related to their security governance. Although, the framework cannot guarantee that the most secure alternative is chosen, since this decision involves far more considerations, it ensures that their security aspects are evaluated in alignment with the organisation's Information Security Program.

5.2.3. Task 2C: cloud risk analysis

The second ISGcloud activity includes a security risk analysis of the cloud storage service, which was performed by the security department and project members. Following ISGcloud suggestions, the organisation decided to use ENISA's Risk Assurance Framework [30] to support this analysis.

The first step involved identifying the information assets related to this service and the threats that might have an impact upon them. The service's purpose is to store and share private documentation, and this personal information is therefore the main asset. In addition to personal information, other tangible and intangible assets were also identified.

Once the information assets and potential threats have been identified, the risk assessment was performed in order to evaluate the exposure to risks. The risk quantification was used to develop risk management guidelines in order to reduce the most threatening ones to acceptable tolerance levels. ISGcloud introduces the risk analysis into the governance process. A periodic assessment must be performed, which is validated by the chief officers. In successive Evaluate-Direct-Monitor cycles, directors receive information about risk exposure and its time evolution or tendency.

Table 4
Cloud service alternatives' weights.

Security requirement	Solution A weight	Solution B weight
1. Authentication	1	1
2. Confidentiality	1	2
3. Integrity	2	1
4. Availability	2	2
5. Transparency	1	0
6. Auditability	2	1
Overall score	1.5	1.2

The risk analysis' results were also used to quantify some of the governance metrics defined in the first activity. The outcomes of each iteration were utilised in order to have the governance indicators updated during the empirical evaluation.

With ISGcloud support, the risk analysis becomes a dynamic process that is closely linked to the other activities. It must be updated throughout the storage service lifecycle with the active involvement of the organisation's directors, who in this case have decided to perform the risk assessment at least twice a year since the threats and vulnerabilities identified may alter in the near future.

5.3. Activity 3: cloud security design

The third activity of ISGcloud involves the security design tasks. This design must be performed in co-ordination with the technical and organisational designs, thus allowing a comprehensive solution to be deployed. The tasks proposed by ISGcloud guarantee the alignment of the resulting design with the security governance structure.

5.3.1. Task 3A: define SLAs and legal contracts

The Service Level Agreements are a key element of the governance structure. They reflect the rules that drive the service relationship between the cloud provider and the organisation. Among other aspects, appropriate clauses are introduced in order to fulfil security requirements and achieve successful security governance.

The development of the storage service has been tailored to the organisation's needs, signifying that its SLAs do not contain as many standardised clauses as other public cloud services. However, it was necessary for the legal department to review both the preliminary and the tailored clauses in order to give its approval.

Following a similar approach to that of the security requirements identification, the organisation first defined security clauses related to legal regulations. Once the organisation had dealt with legal clauses, the other security requirements were translated into more technical security clauses. These forced the cloud provider to comply with a set of requirements that would guarantee their security governance. The SLAs also include penalty clauses to avoid the situation of the cloud provider not following the bilateral contract.

The outcomes of this task were relevant to the empirical evaluation because an appropriate SLA definition would result in improvements of the cloud service's security, measured through the previous security requirements' metrics, and also would reflect into higher scores of the security governance indicators.

The chief officers oversaw the definition of the SLAs, as this represents a key piece of the governance cycle. ISGcloud helped with this task in order to define the foundations of the legal relationship between the organisation and the cloud provider. This task is of paramount importance for both the governance of the cloud service and for the security auditing that takes place in later phases of the cycle.

5.3.2. Task 3B: establish information security roles and responsibilities

According to the ISGcloud framework, this task is focused on the assignment of security roles and responsibilities to specific employees and on the definition of ownership of the information assets.

On the one hand, the roles involved in the storage service security were initially defined in task 1A, during the definition of the security governance structure, along with the responsibilities of

each one. These roles were assigned to specific people from both the organisation and the cloud provider, and their responsibilities were explained to them. On the other hand, the information assets affected by this project were identified in the risk analysis in task 2C. Similarly to the security roles, these assets were linked to specific individuals.

Although this ISGcloud task may appear to be quite simple, it is very important that roles and information assets were adequately assigned in order to establish the security governance structure and to develop adapted training plans in later activities.

5.3.3. Task 3C: specify cloud service monitoring and auditing

This task defines the service monitoring that will be performed, which constitutes a fundamental part of the three steps governance cycle. The design results will clearly determine how the Monitor and even part of the Evaluate processes of the Evaluate-Direct-Monitor cycle take place during the operation steps.

The objective of the storage service monitoring was twofold: to measure the compliance with the SLAs defined and to evaluate the service's security evolution. From the complete list of contracted SLAs, the organisation identified those that were suitable and representative for monitoring. In order to complete the security monitoring, every item must include its correlative threshold so that an alarm can be triggered in case of its being surpassed. Initial thresholds were reviewed in successive iterations so that alerts received comply with the security requirements.

When defining the auditing processes, the organisation specified both the elements that needed to be evaluated and the periodicity during which the audit should take place. These security audits were initially performed by internal employees from the organisation's Audit Department, working independently, but in the future they might be outsourced to an external third party.

From the empirical evaluation's perspective, it was crucial to include into the service monitoring those items that had been previously identified as security governance metrics. As a result, a kind of scorecard was developed that summarised the metrics' evolution during the empirical evaluation.

With the use of this task ISGcloud supports the introduction of the cloud service monitoring and audits into the organisation's internal processes. The framework leads to a secure service deployment and to the ability to monitor its security throughout the entire service lifecycle.

5.3.4. Task 3D: define applicable security controls

The objective of the last design task is to define the security controls to be deployed in the storage service. The term security control is employed in a broad sense as a synonym for safeguard or countermeasure, resulting in a means to manage risks including policies, procedures or practices [31].

The organisation took the previous activity's analyses in order to define the security controls to be deployed both within the organisation itself and by the storage provider. The security department's intention was to follow the guidelines provided in ISO/IEC 27002 when defining the security controls, but to also translate them to the cloud service with the adequate considerations. However, the list of specified controls was not limited to the standard's clauses.

The security controls were mainly aimed at satisfying the security requirements and improving ISG inside the organisation. The fulfilment degree of this objective will be discussed later, along with the analysis of the empirical evaluation's achievements.

This task concludes the security design activity. With it, ISGcloud guarantees that, even in the first iteration, every security aspect is taken in consideration and included in the cloud service design. Most of the steps developed are involved with the Direct and Monitor phases of the governance cycle, but they are prepared in order to be able to execute the Evaluate phase when the service operation takes place.

5.4. Activity 4: cloud implementation/migration

Having designed the security, along with the completion of the storage service design, then the service implementation stage begins. ISGcloud divides this activity into two tasks related to the underlying governance processes; the first task establishes the foundations in order to introduce the Evaluate-Direct-Monitor process into the organisation's security, while the second focuses on the Communication process by spreading security knowledge among the organisation's employees.

5.4.1. Task 4A: secure cloud implementation

The implementation of the storage service, from the users' perspective, involved adjusting the configuration options on their mobile devices and also installing new applications and components. Implementation instructions were also developed so that users could have guidance during the process.

Apart from the service deployment, this task also included the integration of security governance into all the organisation's processes. Existing routine procedures were reviewed in order to incorporate designed security controls and participate in the governance cycle. New processes have also been defined in order to fulfil the security requirements and controls designed in previous activities. The organisation's chief officers supervised the adoption of these new processes so that the security governance structure proposed by ISGcloud could be deployed.

The assessment of this task's execution under the empirical evaluation's research questions was performed by gathering feedback from various participant roles. Some interviews were programmed during this activity, and also direct opinions could be received thanks to the close cooperation with some project members.

Following ISGcloud support, there is assurance that the previously designed security controls and their correlative processes are systematically deployed. The implementation of the storage service therefore guarantees its compliance with security and its embracement within the organisation's security governance structure.

5.4.2. Task 4B: educate and train staff

The Communicate security governance process starts to play a critical role from this point on owing to the fact that the widespread nature of both the general security culture and specific cloud service security issues is a key governance success factor. Although previous activities may have contributed towards disseminating some of these security issues, it is in this task that the process reaches its peak state in order to increase the organisation's security awareness.

The Human Resources department developed a security training plan in collaboration with the security governance committee. This development considered the various roles involved in the cloud service by identifying the security knowledge that each user must attain. Apart from the storage service's users, all other project participants were instructed with the security matters that they must know according to their participant role in the storage service.

Following this task, ISGcloud allows a functional Communicate process to be deployed that is intimately related to the more general Evaluate-Direct-Monitor cycle of the security governance structure. Security awareness thus spreads naturally within the organisation, and is integrated into the organisation's operational processes.

5.5. Activity 5: secure cloud operation

ISGcloud proposes dividing the service operation activity into two tasks, similar to the implementation activity approach. As a result, the first task focuses on performing successive iterations of the security governance cycle, while the second concentrates on the Communicate core governance process.

5.5.1. Task 5A: cloud security operation

This task has the purpose of ensuring that all previously made efforts as regards designing and implementing security governance processes are effectively executed through the proposed Evaluate-Direct-Monitor cycle. Some of the previous tasks' results which this operation stage benefits are as follows:

- Every participant satisfies his responsibilities and carries his assigned role out.
- Cloud service's processes include security controls, which are aligned with the organisation's policies and strategies.
- Monitoring and audit procedures are implemented in order to evaluate service's security.
- Communication channels are established between the organisation and the cloud provider.

Following ISGcloud, the organisation's chief officers obtained adequate feedback about the security processes' performance, which was summarised for them so that deviations could be detected and appropriate decisions be made. In order to facilitate the data collection during successive governance cycle iterations, it was important to perform the previously designed monitoring and audit processes correctly. Table 5 shows a sample of some security processes that were executed during this operation task, and how successive ISG iterations produced modifications and improvements in them.

With this task, ISGcloud's guidance helped the organisation to translate all the outputs into operative processes. The security governance structure, including critical issues such as SLA monitoring, organisation's processes adaptation or security monitoring, could therefore be comprehensively driven into operation. What is more, all the efforts made in operating the new storage service could be taken advantage of in the future if new cloud services are adopted by the organisation.

5.5.2. Task 5B: communicate information security inside the organisation

This task focuses on the Communicate governance process, contributing to the spreading and maintenance of the security culture within the organisation. Its objective is therefore twofold: ensuring that the storage service users are permanently aware of security, and deploying mechanisms to facilitate the spreading of new security policies or modifications to procedures.

The organisation, following ISGcloud's proposal, included the security operation documentation in this task. This process had its starting point in all the documentation generated in previous activities and basically involved completing and complementing it with the operation's progress. This security information about the storage service was held in a project repository, thus permitting service users to be granted access according to their roles.

Having access to available documentation is not sufficient for an effective security governance Communicate process. The organisation has therefore developed various wide-spreading actions, which were focused on communicating the importance of information security in all processes. Some of these actions were the following ones:

- Provide users with additional training sessions, following the cloud service's training program.
- Schedule periodical conferences and reports about the most relevant security aspects.
- Develop additional security documentation, which is addressed to some users with specific requirements.

With this task, ISGcloud framework guarantees that a successful Communicate process is deployed in the organisation, and that it is completely aligned and interlinked with the iterative Evaluate-Direct-Monitor cycle as part of the same security governance structure. This ensures a comprehensive consistency with other governance elements, such as security roles and processes.

The empirical evaluation finishes with the first iterations of this task and the previous one. Although the cloud service will continue to be provided, having achieved the secure operation activity we have gathered enough information to address the research questions.

Table 5
Sample of security processes during service operation.

Security process	ISG iteration results
Physical and environmental security	Strengthen cloud provider's perimeter security as a consequence of some failures
Incident management	Users are provided with mobile tools that allow reporting and managing their security incidents from their devices
Human resources security	Reinforce security training, especially on some roles where lacks are detected
Access and identity management	Force users to employ more secure passwords when using their devices and update them regularly, so that risks are reduced when mobile devices are lost or stolen
Legal requirements	Adapt some SLA clauses due to a regulation change about personal data protection

6. Empirical evaluation results

The development of the empirical evaluation introduced herein has allowed us to put ISGcloud framework into practice in a real life environment. With this work we have validated both the framework's overall performance and the suitability of the proposed tasks and activities. The entire framework has permitted a security governance structure to be established within the organisation which, although at an incipient stage, guarantees that security will be handled adequately in both the newly adopted cloud services and in possible future ones. The empirical evaluation represents the process's first iteration within the organisation and, despite being unable to obtain long-term conclusions, we consider it sufficient to have attained representative results as regards the research questions.

Having introduced the methodological approach, we shall now analyse the results according to each of the proposed research questions. A structural and analytical answer to the questions is therefore provided, thus validating our research objectives. A summary of lessons identified and lessons learned is also presented in this section.

6.1. Does ISGcloud lead to a secure cloud service deployment?

ISGcloud has helped the organisation to tackle security matters from two points of view: a traditional security perspective, of which the Security Department had more knowledge; and a comprehensive security governance approach, in which the organisation had a larger field for learning and adapting.

Some ISGcloud tasks, such as those related to the storage service risk assessment (task 2C), the design of security controls (task 3D), or the processes' auditory (task 3C), belong to the traditional security perspective. These tasks made slight improvements in order to adapt classical methodologies to the cloud environment. The organisation already had previous knowledge of these kinds of activities, and it was therefore quite straight forward to adapt them to the particularities of the cloud storage service, thanks to ISGcloud's guidance.

However, it was in the remaining tasks that our framework achieved its main objectives and contributed towards the establishment of a security governance structure around the cloud service – an issue that is considered in the following research question. This has proved to be particularly relevant in tasks 1A and 1B.

The wide spreading of a security culture was one of the most noticeable achievements of ISGcloud, which not only drove a secure service deployment with the cloud storage's case study, but facilitated security assurance in the organisation's future cloud services. Tasks 4B and 5B contributed essentially to this objective. Project leaders reported that most cloud service's users gained additional security knowledge during the process, which resulted in adopting better security practices and increasing their security awareness. This improved security culture may also help future iterations of ISGcloud framework, even when dealing with other cloud services.

One of this research question's objectives was to measure the security of the new storage service. In order to be able of quantifying it, we are using the security requirements defined by the organisation in task 2A. Assessing the fulfilment degree of these requirements and assigning weights to each of them allowed us to obtain a measure of the service's security. This result complements our qualitative analysis and other subjective perceptions about the service that were gathered during the project's development.

The security measurement has been performed similarly to the cloud provider analysis described in task 2B; that is, we used a three point scale with a weight of 0 if the provider has no support for the requirement, a weight of 1 if the provider has limited or partial support for the requirement, and a weight of 2 if the provider has full support for the requirement. Table 6 contains a summary of the allocated weights for every security requirement and the resulting score.

Following this methodology, the empirical evaluation of the cloud service's security throws an overall score of 1.6 out of 2. These means that following ISGcloud framework the organisation has achieved about 80% of its security requirements. This analysis also serves to identify those requirements that are more weakly supported, so that the continuous ISG process allows improving the cloud service's security.

Besides, a comparison between these weights and those allocated during the cloud provider selection, there are slight differences in the scores. The main reason of this divergence is that the initial weights were based on prospects about the expected security and these ones take into account the real implementation.

Table 6
Storage service security's weights.

Security requirement	Allocated weight
1. Authentication	1.5
2. Confidentiality	1
3. Integrity	1.7
4. Availability	2
5. Transparency	1.3
6. Auditability	2
Overall score	1.6

6.2. How does ISGcloud favour the development of a security governance structure within the organisation that the cloud service provides coverage?

Although the organisation had already established a security governance structure, this could really be considered as incipient in comparison to the situation achieved after the case study's development. Some governance characteristics were previously deployed, such as a security strategy, or reporting lines, but these were insufficient when dealing with cloud services. After ISGcloud's first iteration, the organisation has at its disposal not only a comprehensive security governance structure, but one that is adapted and prepared to embrace future cloud services.

From the governance perspective, the following security elements can be highlighted, which show the interweaving of the cloud storage service with the governance structure:

- *Security SLAs (task 3A)*: the restrictions imposed by the Spanish public contract law forced the organisation to carefully determine the contract's content, since this implied a long term service period during which it was quite difficult to alter the terms accorded. This conditioning has led the project to make special efforts to analyse the cloud service's security implications and to translate them to contract terms and SLAs.
- *Security processes (task 4A and 5A)*: when discussing security processes, the organisation has been able to re-design its internal processes during the project so that they were adapted to a much broader scope and absorbed into the security governance structure, and to define new processes that drove the relationship and operations with the cloud provider.
- *Security roles and training (task 3B)*: the identification and individualisation of the personnel roles involved in the empirical evaluation has allowed the organisation to personalise its security governance deployment. The cloud provider's inclusion as a role in the process and the delivery of training sessions adapted to each role permitted a clear assignment of responsibility as regards the cloud service's information actives.
- *Security assessment (task 3C)*: one key governance element introduced by ISGcloud was a continuous monitoring cycle that was evaluated through metrics and security audits of relevant processes. After the empirical evaluation's execution, the organisation now has at its disposal a complete set of information sources from which senior officers and lower managerial levels may collect adequate information for their duties.

Furthermore, it was also possible to quantify the improvement achieved in the ISG structure thanks to ISGcloud framework. Using the governance goals and metrics previously defined in task 1A, it was possible to measure its state once the security operation activity has been reached. Following the same methodology, Table 7 shows the measurement of each governance goal and the overall score.

Comparing this result with the initial measurement performed at the project's beginning, the ISG structure has improved from a 2.4 score to a 3.8 out of 5, which means an improvement of nearly 60% in our proposed governance criteria. Apart from validating the benefits for the organisation in terms of its governance structure, these metrics also served as a continuous scorecard for chief officers, who were able to periodically assess the progress made on the cloud service's security.

6.3. How practical and usable is the utilisation of the ISGcloud framework within an organisation?

The empirical evaluation performed has provided a relevant opportunity to evaluate the benefits of applying ISGcloud frame-

Table 7
Final measurement of ISG goals.

ISG goal	Measurement	Overall score
Alignment of ISG and business strategy	4.3	3.8
ISG contributes to optimal value delivery	3	
Ensure security risk optimisation	4.7	
Information security resources are optimised	3.3	
Information security communication is effective	3.7	

work in a real life environment. From a formal perspective, ISGcloud is structured by following general and well known project stages, signifying that its integration into the organisation's storage service project has been performed without many difficulties. This intuitive ease of application is translated into a very soft learning curve, which signifies that even the organisation's non-security experts have been able to fully understand ISGcloud's implications and become rapidly involved in the project.

ISGcloud's integration with widely known security standards and best practices has also been a key factor in the project's success, as it has allowed the Security Department to maintain the standards and references which they are familiar with. In this respect, our framework has proved to have a high degree of flexibility, since it is capable of adapting itself to practically any existing security proposal.

A set of interviews were programmed during the empirical evaluation's process to obtain information about the user's perception. People from all the roles involved in the project were asked to offer their opinion with the purpose of giving a precise answer to this research question. They were asked about the easiness of the framework's application, its help and usefulness, and what modifications they could suggest. During the first three ISGcloud's activities only some project members were interviewed, but many more users were included in the questionnaires during the implementation and operation activities.

A summary of the interview's results about some questions is shown in Fig. 3. These graphics show that 54% of the interviewees considered that it was easy or very easy to learn the framework, while 23% valued it as difficult or very difficult. The main difficulty reported by this group was that the framework used a technical language, which may be a drawback for non-security experts. When questioned about the utility of ISGcloud, 69% of the interviewees thought it was useful or very useful, whereas only 12% ranked it as useless or very useless. The most frequent answer on this question was that the classification of ISGcloud's activities through the cloud service life cycle helped to understand which tasks were the most important in each stage.

Additionally, people were asked to offer their opinions about possible modifications or suggestions to improve the whole process. The issues that were more frequently answered among interviewees were those related with a lack of supporting tools to follow the cloud service's deployment. The project leaders made efforts to analyse and evaluate various tools in order to select those that best suit them. Having identified this issue, we can now complement our research with an analysis of existing tools and suggest those that can be most easily tailored to ISGcloud and support our framework's purpose. ISGcloud's scope is so broad and comprehensive that we have not been able to develop an automatic tool that could support the whole framework. However, this matter will be taken into account for future work.

6.4. Other lessons learned

In addition to answering the pre-arranged research questions shown above, the execution of the empirical evaluation has also provided valuable information with which to validate the performance of ISGcloud framework and to identify issues that demand additional research efforts.

Among the lessons learned, we could highlight the introduction of additional governance metrics in all ISGcloud's tasks. During the empirical evaluation's planning, the project leaders realised that the framework only provided feedback of its performance to senior officers during particular tasks. Considering the information flow's relevance as regards keeping higher managerial levels aware of the project's progress, it has been necessary to insert new performance metrics in every task. These metrics facilitate the execution of consecutive Evaluate-Direct-Monitor cycles and allow a permanent oversight of the cloud service deployment, which constitutes a core piece of our security governance framework.

Throughout the empirical evaluation's progress, we have also identified that the project's members made greater efforts in the first three activities. The strategic planning, security analysis and security design of the cloud services have involved considerably more time consuming tasks. This behaviour may be attributed to the novelty of the cloud storage service in the organisation and the precautions that needed to be taken to guarantee its security. However, these ISGcloud activities will be explored in greater depth in order to provide more details with which to facilitate their execution.

7. Related work

This section discusses related work in the field of the information security governance of cloud services. This relatively new research area has arisen from the merging of security governance and cloud security research fields, and we will therefore discuss existing work in both areas.

On the one hand, when dealing with information security governance, most approaches originate from the IT governance field. One of the most representative references is therefore Control Objectives for Information and related Technology (COBIT) [26], which has introduced a set of 37 IT governance processes, some

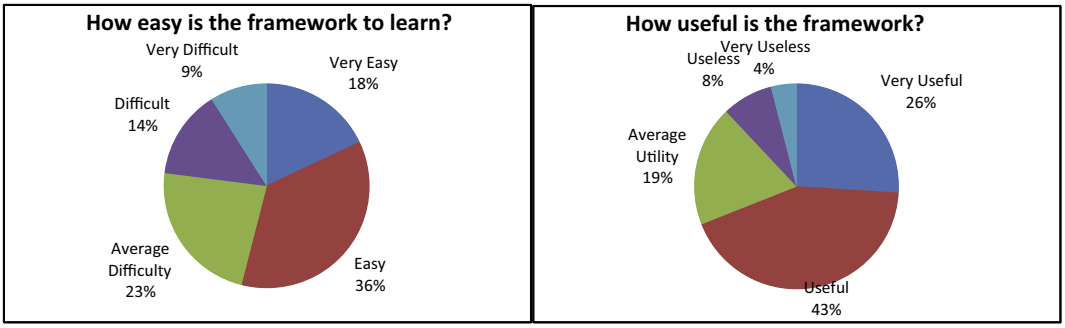

Fig. 3. Caption of interview's results.

of which can also be applied to security governance. The International Organisation for Standardization (ISO) has also developed some standards for these fields. Those which are most closely related to our research are: the ISO/IEC 27001 standard [31], which is devoted to Information Security Management Systems; the ISO/IEC 27014 [32], which is currently under development and whose intention is to define a security governance framework; and the ISO/IEC 38500 [25], which provides a framework for IT governance. The security governance framework proposed by Von Solms in [33], which distinguishes between governance and management sides, is also relevant to our purpose.

All of these security governance references share some commonalities and each one has particular strengths and weaknesses, as shown in our previous research [34]. They have not been specifically designed to be applied to cloud computing services, signifying that many difficulties arise when attempting to integrate them into this new environment.

On the other hand, there are many publications regarding cloud computing security but most of them are focused on specific security issues (i.e., privacy, trust [35], certificate authentication [36] or virtual machine security) rather than adopting a broader scope [37]. Nevertheless, we shall present those works that offer a comprehensive security solution to cloud services, and are closer to our approach. The security guidance elaborated by the Cloud Security Alliance [38] provides practical recommendations in order to identify security threats in cloud computing and develop measures to minimise risks. The Information Systems Audit and Control Association (ISACA) has published IT Control Objectives for Cloud Computing [39], in which they propose adapting existing governance frameworks to the cloud environment, differentiating between the aspects of security and governance. A Cloud Computing Security Risk Assessment has also been published by the European network and Information Security Agency (ENISA) [30], which provides guidance with which to evaluate risks in a cloud deployment and includes security recommendations. Another risk assessment tool has been proposed as QUIRC (A Quantitative Impact and Risk Assessment Framework for Cloud Security) [40], where authors measure cloud risks using six security objectives. The ISO is even working on the ISO/IEC 27036 standard [41], whose objective is to provide security for cloud services throughout their lifecycle. There are also some approaches that try to widespread trust in cloud services such as the TrustCloud framework [42], which addresses accountability in cloud computing via technical and policy-based approaches.

All of these cloud security proposals offer a particular perspective when dealing with security issues, but none of them considers holistically security governance aspects. The systematic review of cloud security governance approaches performed in [19] shows the principal lacks identified in each work in relation to certain comparative criteria. Our ISGcloud framework, upon which this paper's empirical evaluation is based, differs from these approaches in a twofold sense: it deals comprehensively with security governance in cloud services in an all-inclusive scope, and it offers practical guidance on how to perform the security activities, not just explaining what to do as in the aforementioned works.

8. Conclusions

Although the research community is aware of the importance of introducing cloud service security into the enterprises' governance structures, there seems to be a lack of such a structured approach. Neither academic literature nor the security industry has provided a security governance framework that is suitable for cloud computing services. We have proposed ISGcloud in order to fill this gap by providing a process oriented framework which guides users through the steps of developing a security governance structure around a cloud deployment and is based on the cloud service's lifecycle. Our framework provides a comprehensive and flexible approach that may be tailored to a wide variety of organisations and cloud service models.

The practical empirical evaluation presented in this paper has served to obtain valuable information about ISGcloud's performance. We have validated its utility in achieving the security governance objectives and its capability to be integrated into the cloud service project without many difficulties. Thanks to our framework, a Spanish organisation has been able to introduce a security culture in all its internal processes, which not only guarantees that its cloud storage service is operated with adequate security, but also establishes the governance foundations for future services. However, this empirical evaluation has also shown certain limitations of ISGcloud, some of which have led to corrections with which to improve it, and others of which have been left for a later analysis since they require more in-depth research.

This paper's results represent the first wave of information that we have been able to collect from the case study. The security governance structure deployed is based on long term processes, and the cloud service's lifecycle is also expected to be in operation for at least a few years; we therefore expect to continue holding regular tracking meetings in order to receive more feedback about the project. We hope to gain additional knowledge about the future performance of our framework and to acquire a wider perspective of the results.

Future work will focus on improving ISGcloud framework in relation to the limitations identified, and to other possible drawbacks that may also emerge. We plan to research the details of the framework's tasks and steps in greater depth, especially those that this case study has highlighted as needing more effort on the part of the organisation. We are additionally working to review existing tools that could be used to support our process and also be included in the framework guidelines.

Acknowledgements

This research has been funded by the SERENIDAD project (Consejería de Educación, Ciencia y Cultura de la Junta de Comunidades de Castilla La Mancha and Fondo Europeo de Desarrollo Regional FEDER, PEII11-0327-7035) and by the SIGMA-CC project (Ministerio de Economía y Competitividad and Fondo Europeo de Desarrollo Regional FEDER, TIN2012-36904).

References

[1] P. Mell, T. Grance, The NIST definition of cloud computing, in: SP 800-145, National Institute of Standards and Technology, 2011.
[2] Gartner, Gartner's Hype Cycle for Cloud Computing, 2012.
[3] D. Bradshaw, G. Folco, G. Cattaneo, M. Kolding, Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take, 2012.
[4] Y. Chen, V. Paxson, R.H. Katz, What's New About Cloud Computing Security?, University of California, Berkeley, 2010
[5] K. Hamlen, M. Kantarcioglu, L. Khan, B. Thuraisingham, Security issues for cloud computing, Int. J. Inform. Secur. Priv. 4 (2010) 39–51.
[6] D. Mellado, E. Fernández-Medina, M. Piattini, Security requirements engineering framework for software product lines, Inf. Softw. Technol. 52 (2010) 1094–1117.
[7] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (2011) 1–11.
[8] J.M. Verner, L.M. Abdullah, Exploratory case study research: outsourced project failure, Inf. Softw. Technol. 54 (2011) 866–886.
[9] A.J. Varela-Vaca, R.M. Gasca, Towards the automatic and optimal selection of risk treatments for business processes using a constraint programming approach, Inf. Softw. Technol. 55 (2013) 1948–1973.
[10] P.J. Graydon, T.P. Kelly, Using argumentation to evaluate software assurance standards, Inf. Softw. Technol. 55 (2013) 1551–1562.

[11] A. Bisong, S.S.M. Rahman, An overview of the security concerns in enterprise cloud computing, Int. J. Netw. Secur. Appl. (IJNSA) 3 (2011) 30–45.
[12] Avanade, Global Survey: Has Cloud Computing Matured? Third Annual Report, June 2011.
[13] D.G. Rosado, R. Gómez, D. Mellado, E. Fernández-Medina, Security analysis in the migration to cloud environments, Fut. Intern. 4 (2012) 469–487.
[14] Y. Zhu, H. Hu, G.-J. Ahn, S.S. Yau, Efficient audit service outsourcing for data integrity in clouds, J. Syst. Softw. 85 (2012) 1083–1095.
[15] D. Mellado, L.E. Sánchez, E. Fernández-Medina, M. Piattini, IT Security Governance Innovations: Theory and Research, IGI Global, USA, 2012.
[16] Y. Chen, K.R. Ramamurthy, K.-W. Wen, Organizations' information security policy compliance. Stick or carrot approach?, J Manage. Inform. Syst. 29 (2013) 157–188.
[17] H. Tran, U. Zdun, T.i. Holmes, E. Oberortner, E. Mulo, S. Dustdar, Compliance in service-oriented architectures: a model-driven and view-based approach, Inf. Softw. Technol. 54 (2012) 531–552.
[18] C. Rong, S.T. Nguyen, M.G. Jaatun, Beyond lightning: a survey on security challenges in cloud computing, Comput. Electr. Eng. 39 (2013) 47–54.
[19] O. Rebollo, D. Mellado, E. Fernández-Medina, A systematic review of information security governance frameworks in the cloud computing environment, J. Univ. Comput. Sci. 18 (2012) 798–815.
[20] D.G. Rosado, E. Fernández-Medina, J. López, M. Piattini, Analysis of secure mobile grid systems: a systematic approach, Inf. Softw. Technol. 52 (2010) 517–536.
[21] O. Rebollo, D. Mellado, E. Fernández-Medina, Introducing a security governance framework for cloud computing, in: Proceedings of the 10th International Workshop on Security in Information Systems (WOSIS), Angers, France, 2013, pp. 24–33.
[22] P. Runeson, M. Höst, Guidelines for conducting and reporting case study research in software engineering, Empir. Softw. Eng. 14 (2009) 131–164.
[23] European Commission, Unleashing the Potential of Cloud Computing in Europe, 2012.
[24] V. Kundra, Federal Cloud Computing Strategy, 2011.
[25] ISO/IEC, ISO/IEC 38500:2008 Corporate Governance of Information Technology, 2008.
[26] ITGI, Control Objectives for Information and Related Technology (COBIT 5), 2012.
[27] OMG, Software & Systems Process Engineering Meta-Model Specification v.2.0, 2008. <http://www.omg.org/spec/SPEM>.
[28] Fundacion Telefonica, La Sociedad de la Informacion en España 2011, 2012.
[29] Pew Research Center, Global Digital Communication: Texting, Social Networking Popular Worldwide, 2011.
[30] D. Catteddu, G. Hogben, Cloud Computing Security Risk Assessment – Benefits, Risks and Recommendations for Information Security, European Network and Information Security Agency (ENISA), 2009.
[31] ISO/IEC, ISO/IEC 27001:2005 Information Technology – Security Techniques – Information Security Management Systems – Requirements, 2005.
[32] ISO/IEC, ISO/IEC 27014 Information Technology—Security Techniques—Governance of Information Security, Draft.
[33] S.H.v. Solms, R.v. Solms, Information Security Governance, Springer, 2009.
[34] O. Rebollo, D. Mellado, L.E. Sánchez, E. Fernández-Medina, Comparative analysis of information security governance frameworks: a public sector approach, in: The Proceedings of the 11th European Conference on eGovernment – ECEG 2011, Ljubljana, Slovenia, 2011, pp. 482–490.
[35] I.M. Abbadi, A framework for establishing trust in Cloud provenance, Int. J. Inf. Secur. (2012) 1–18.
[36] J. Crampton, H.W. Lim, K.G. Paterson, G. Price, User-friendly and certificate-free grid security infrastructure, Int. J. Inf. Secur. 10 (2011) 137–153.
[37] O. Rebollo, D. Mellado, E. Fernández-Medina, A comparative review of cloud security proposals with ISO/IEC 27002, in: Proceedings of the 8th International Workshop on Security in Information Systems – WOSIS 2011, Beijing, China, 2011, pp. 3–12.
[38] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, 2009.
[39] ISACA, IT Control Objectives for Cloud Computing, 2011.
[40] P. Saripalli, B. Walters, QUIRC: a quantitative impact and risk assessment framework for cloud security, in: IEEE CLOUD, IEEE, 2010, pp. 280–288.
[41] ISO/IEC, ISO/IEC 27036 – IT Security – Security Techniques – Information Security for Supplier Relationships, Draft.
[42] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, B.-S. Lee, TrustCloud: a framework for accountability and trust in cloud computing, in: IEEE Services, IEEE, 2011, pp. 584–588.