The Computer Journal Advance Access published November 28, 2014

doi:10.1093/comjnl/bxu141

ISGcloud: a Security Governance Framework for Cloud Computing

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

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

Security risks to organizations' information assets are hindering the development of cloud computing services. A comprehensive security governance process is needed to foster the massive adoption of cloud services and to facilitate the deployment of a security culture within any company. In this paper, we present a framework focused on the security governance of the cloud computing environment (ISGcloud), which has been built upon standards. Its principal components are based on the ISO/IEC 38500 governance standard and on the ISO/IEC 27036 outsourcing security draft. We propose a systematic collection of activities and their related tasks which detail how security governance can be deployed during the entire cloud service lifecycle. Furthermore, the whole framework is formally modelled following the SPEM 2.0 specification that provides a standardized interface with which to automate and integrate our proposed process. The theoretical definition of our proposal is also accompanied by a practical example of its application, which provides specific details of ISGcloud framework's implementation.

Keywords: information security governance; secure cloud governance; cloud computing; security governance framework; cloud lifecycle

Received 5 January 2014; revised 11 September 2014
Handling editor: David Rosado

1. INTRODUCTION

Cloud computing has emerged as an alternative with which to meet the Information Technology (IT) industry's demands for the use of computing as a utility. It has changed the way in which services are purchased and delivered as a commodity, and has the potential to transform a large part of the IT industry [1]. Cloud computing enables on-demand access to a shared pool of configurable computing resources that can be rapidly provisioned with a minimal management effort [2]. The increasing growth of Internet services and their demand for elastic resources have led this new paradigm to provide new opportunities [3, 4].

Cloud computing encompasses many technologies, and the security issues affecting any of them are therefore applicable to cloud computing [5]. Apart from the existing risks, the cloud paradigm has new risks resulting from the characteristics of its services, which need to be managed [6]. Of the new risks that have appeared in cloud environments are issues related to a wide variety of topics, such as virtualization [7], denial of service [8] or intruder detection [9, 10]. Enterprises are eager to adopt cloud computing in any of their various delivery models, but security management is necessary both to accelerate its adoption and to respond to regulatory drivers [11, 12].

The main security drawback that prevents the massive adoption of cloud computing and leads to reluctance among practitioners is the enterprise's loss of control over its information assets [13], signifying that a clear security governance strategy must be developed [14]. The cloud paradigm extends computing across corporate boundaries, which requires a governance function with active management participation [15]. The specificities of this environment lead to the need for an assurance framework that will help

organizations to deal with all aspects of security in a comprehensive manner. Security cannot be understood as single technical issues, but needs a combined approach that involves all different managerial levels [16].

An Information Security Governance (ISG) framework that tackles all the security issues in the Cloud Environment in a uniform manner is not currently available. Although there are many technological approaches that can improve cloud security, there are no comprehensive solutions at present [17]. Our previous research shows that existing efforts that attempt to deal with cloud computing security do not detail the governance aspects [18]. In this paper, we therefore propose a first approach for a security governance framework that considers the particularities of cloud deployments (ISGcloud). The ISGcloud framework compiles existing published guidance works on the field, and groups them homogeneously to provide a model that is capable of delivering an ISG process for the cloud services. ISGcloud is led by standards, signifying that its proposed activities tend towards existing security and governance standards, resulting in an alignment with actual best practices. We aim to use standards to increase the quality and reliability of the results and simplify the governance process while guaranteeing the security of the cloud service and promoting the reuse of resources [19].

The perspective followed in our approach is process oriented, thus facilitating its inclusion in any organization. In order to deploy security governance, we have chosen the model published in the ISO/IEC 38500 standard, which states that directors should perform governance by using three main processes: Evaluate, Direct and Monitor [20]. The Evaluate–Direct–Monitor cycle will therefore become a core process of our framework. We also propose the addition of a fourth process, namely Communicate, owing to the relevance of disseminating security knowledge within the organization, particularly as regards the adoption of new services such as those of cloud computing.

In addition to the four core processes highlighted, we consider that it is paramount to identify a cloud service lifecycle as part of our objective of defining an ISG deployment. Bearing this in mind, the activities included in ISGcloud can be referenced to a timeline during the service provision. The relationship between the cloud client and its provider, as with any other outsourcing service, leads to new risks throughout its lifecycle phases that must be managed in order to guarantee the service's success [21]. The ISO/IEC 27036 standard [22], despite being in its draft stage, outlines security controls to be addressed in an outsourcing lifecycle. We have adapted this standard to a generic cloud computing lifecycle in order to identify the steps in the processes.

Besides the basic definition of our ISG framework, we also provide a full model of it according to the Software and Systems Process Engineering Meta-Model Specification (SPEM) 2.0, following a standardized approach [23]. All of the activities and their related tasks are consequently formally described, signifying that ISGcloud can be easily automated or integrated with other processes. Furthermore, in order to increase the comprehension of the whole framework, we provide an imaginary example of implementation to show how the framework could be applied in a fictitious organization, and highlight some key output products of the proposed activities. An explanation is provided of both this illustrative example and ISGcloud's activities. A full practical case study is beyond the scope of this paper, since its main purpose is to introduce the principal characteristics of ISGcloud framework. However, we are also working on publishing a real case study that shows how ISGcloud has been implemented in the incipient cloud services of a public organism in Spain [24].

The framework's structure allows its integration with many existing security methodologies and supporting tools. Although some guidance is proposed to accomplish each task, the organization implementing ISGcloud should choose the one that is more suitable for their particular circumstances. Having this in mind, this paper focuses on ISGcloud's main components and leaves the details about precise methodologies or tools for future research.

The structure of this paper is as follows: Section 2 contains background information on and related work in the fields of security governance and cloud computing that have influenced our research; Section 3 provides an overview of our ISGcloud framework, describing its core processes and the proposed lifecycle of a cloud service; Section 4 presents the modelling of our proposal in relation to its activities and artefacts; Section 5 provides a detailed description of its activities and tasks; section 6 contains a example of application, in order to facilitate an understanding of its scope; finally, section 7 contains a discussion of our contribution and future work.

2. RELATED WORK

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

2.1. Information security governance

When discussing IT Governance, a key reference is Control Objectives for Information and related Technology (COBIT), which is widespread and commonly used by the IT industry [25]. COBIT is a framework for IT Governance which introduces a set of 37 processes grouped into five domains, detailing the control objectives, metrics, maturity models and other management guidelines for each of them. Although it is mainly focused on IT Governance, some of its processes are also related to ISG.

The International Organization for Standardization (ISO) has a wide portfolio of standards, some of which are dedicated

to security and governance aspects. The ISO/IEC 27001 standard is of particular interest to our objective as it is related to Information Security Management Systems, which can be used by organizations to develop and implement a framework with which to manage the security of their information assets and prepare for an independent assessment applied to the protection of their information [26]. This family of standards also includes the ISO/IEC 27014 standard, currently under development, which is intended to be a proposal for an ISG framework. Its scope includes defining ISG, thus clarifying its relationship with corporate and IT governance, and developing a framework in which to establish its objectives, principles and processes.

These two frameworks are analysed in [27], in which some other references are also considered. Of these approaches, it is worth highlighting the ISG proposal [28], which defines an information security framework, clearly distinguishing between the governance and management sides, in addition to describing the tasks, roles and responsibilities of any key individual in an organization.

The analysis performed shows that these aforementioned ISG frameworks achieve the best results when compared with a set of predefined criteria, but each of them offers a different perspective. The main drawback of using these frameworks when dealing with cloud computing security is that they have not been specifically designed for this environment, and therefore lack the particularities that arise in this situation. Nevertheless, these approaches define some important concepts that have been included in our proposal.

2.2. Security governance of cloud computing services

The special security requirements that arise when dealing with a cloud computing deployment have led to many publications that attempt to tackle these matters. Existing cloud security proposals are reviewed in [29], and the three most representative are introduced below.

The security guidance published by the Cloud Security Alliance provides practical recommendations as regards reducing the associated risks when adopting cloud computing [30]. The guidance proposes recommendations that help identify threats in the cloud context and choose the best options to mitigate vulnerabilities. Organizations using this guide must select which lines are applicable to their cloud deployment. These lines range from governance to operation issues.

A security risk assessment has been proposed by the European Network and Information Security Agency (ENISA) to provide both a framework with which to evaluate risks and security guidance for existing users [31]. This risk assessment evolves into an information assurance framework, which includes controls from the ISO 27000 family of standards.

In order to provide an understanding of cloud computing and its related risks, the Information Systems Audit and Control Association (ISACA) has been published [14]. This proposal tackles governance and security aspects separately, and contains references to additional publications in order to complement the framework.

The systematic review performed in [18] analyses all of these cloud security proposals together with other literature publications. The results of this comparison show many lacks in existing frameworks as regards the comprehensive embracement of security governance in cloud computing environments. These gaps can be presented in three groups: The Adaptation of policies and processes, Control and audit, and Service level agreement (SLA).

With regard to the Policy and Process Adaptation criterion, the ISG frameworks do not include matters concerning policy documentation procedures, the security awareness and training of all the organization's users, and the communication of security management goals and principles within the organization.

In relation to the Control and Audit group, the topics that are not covered in the proposals analysed are the regular measurement and reporting of progress and detected issues, procedures for monitoring compliance with regulatory requirements, internal policies and technical standards, and the definition of metrics with which to evaluate the security of services.

With regard to the SLA criterion, the review recommends a more active involvement between the client and the cloud provider by developing bilateral processes within both organizations and not relying solely on the contractual terms, in an attempt to improve participants' implications in the cloud service.

In addition to the highlighted lacks, the aforementioned cloud security frameworks focus primarily on the definition of processes and recommendations, i.e. what to do, and seldom offer guidance on the most adequate means for an organization to adopt those processes, or the relationship between them, i.e. how to do it.

2.3. Security governance processes

There are various core governance processes approaches in the literature; some ISO standards, such as the ISO/IEC 27001, propose adopting the Plan–Do–Check–Act (PDCA) process model to implement the governance of the security of information systems and networks [26]. We consider this approach and the ISO/IEC 38500 (Evaluate–Direct–Monitor) as valid and plausible, since both reflect the establishment of iterative processes that provide feedback on the activities performed. These cycles cover all the management levels (from the high strategic, through the middle tactical, to the low operational), thus allowing successful governance to be achieved.

While this cycle is more oriented towards governance, that of the PDCA is more focused on the lower management levels. However, we are aware that some organizations may have deployed the PDCA process model (or even other similar models) with the purpose of obtaining certification as regards

these ISO standards. In these cases, it is worth preserving the established process in order to gain the support of the existing organization culture, and therefore adapt our proposed security governance framework where required.

This iterative governance cycle is also similar to the COBIT 5 proposal, in which the Evaluate–Direct–Monitor cycle is intended for IT governance processes, and a Plan–Build–Run–Monitor cycle is suggested for the management areas [25].

Similar approaches with which to define these processes can also be found in the literature. For instance, in [32], the authors define a security governance framework based on the Direct–Control cycle. Upon examining this process, it was discovered that it shares many dualities with those mentioned above, as it differentiates the governance and management domains, and applies the iterative cycle to the strategic, tactical and operational levels.

The proposed ISG framework is not intended to substitute the aforementioned security approaches, but has rather been built to integrate them. ISGcloud is linked to relevant security standards and cloud governance models, signifying that it can evolve at the same pace as external references. This approach consequently guarantees any organization's alignment with standards and best practices, and can be adapted to any new requirements and restrictions that may appear in the future.

3. OVERVIEW OF THE FRAMEWORK

This section provides a general overview of our proposed ISGcloud framework. We describe how the process has been developed by considering the specificities of a cloud computing environment and what links to existing standards it includes. This overview of ISGcloud presents the main ideas that are subsequently developed into more detailed activities and tasks, but it is sufficient to understand the main components. This allows us to show the purpose of covering detected lacks in existing security governance approaches related to cloud computing environments, and the strong relationship that it maintains with standards throughout the entire process.

Our purpose is to develop a comprehensive security governance framework that will be suitable for cloud computing deployments. In our work, we have considered the principal contributions of the existing literature, and intend to fill the gaps detected. We additionally present our framework as a global process that provides greater details in an attempt to explain how to develop the security governance activities, in order to tackle the questions of what to do with the how to do it.

The core processes of ISGcloud are based on the ISO/IEC 38500 standard, not only because of the relevance of the standard itself, but also because of its suitability to be tailored to our needs. According to this standard, the governance cycle follows three processes: (a) Evaluate the current and future use of IT; (b) Direct preparation and implementation of plans and policies to ensure that the use of IT meets business objectives and (c) Monitor conformance to policies, and performance against the plans [20]. We additionally incorporate the Communicate process which adds the dissemination of the knowledge that is required in ISG.

From here on, we shall refer to these iterations as the Evaluate–Direct–Monitor cycle, in order to maintain a homogeneous reasoning.

Having established that the core process of our framework is to support security governance activities, it was then necessary to incorporate additional components to enable it to integrate specific activities in order to cover the particularities of a cloud computing environment. These components were selected by following the research line taken with the Evaluate–Direct–Monitor cycle and based on existing standards, in order to maintain a coherent perspective.

The process of implementing and managing ISG in cloud computing is closely bound to the service offered by the cloud provider and consequently with its lifecycle. Taking the ISO/IEC 27036 standard [22] as a basis, we propose the following generic cloud computing lifecycle: (1) Planning/Strategy Definition; (2) Cloud Security Analysis; (3) Cloud Security Design; (4) Cloud Implementation/Migration; (5) Secure Cloud Operation and (6) Cloud Service Termination.

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

The four ISG processes constitute one dimension of the ISGcloud framework, and the six activities in the cloud computing lifecycle become a second dimension. We therefore depict our framework in a bi-dimensional perspective in which the cloud services traverse the six activities containing the successive Evaluate–Direct–Monitor cycles [33].

3.1. Main characteristics

The main characteristics of ISGcloud framework are highlighted as follows

(i) Iterative processes. The framework's execution is performed through iterative cycles. The scope of each iteration ranges from a single task to the whole framework, which results in the successive refinement of the outcomes produced until the global objective is achieved.
(ii) Process reusability. The use of a model specification such as SPEM 2.0 specification [23] provides the ability to reuse the processes in other domains or contexts, which means that they may be reused in successive iterative cycles of the same cloud service or in other different service.

(iii) Product reusability. All the products created in ISGcloud's tasks are stored in an artefact repository, which facilitates their reuse in future iterative cycles. These cycles lead to a continuous improvement process, through which products are refined.
(iv) Alignment with security standards and ISG best practices. ISGcloud is aligned with widely known standards, such as ISO/IEC 27001 [26] or ISO/IEC 38500 [20], and with best practices such as COBIT 5 [25] or the Cloud Security Alliance guidelines [34].
(v) Traceability and monitoring. ISGcloud offers a set of metrics and indicators, which can be used to obtain information about the process' development in order to achieve the strategic goals. These metrics may be monitored through automatic tools, such as balanced scorecards.
(vi) Flexibility. All the activities and tasks proposed in ISGcloud can be tailored to support any Cloud Computing environment.

3.2. Participant roles

The scope of every governance process covers the whole organization, signifying that the participant roles at every managerial level need to be involved in the framework. The governance activities require the active involvement of senior officers, high executives and managers, and therefore appear along with other lower-level roles. Since senior officers are responsible for the organization's governance processes, they are involved in all the activities, signifying that they need to be informed of ISGcloud's evolution and approve the results of its tasks. The definition of the participant roles has been developed from a hierarchical organizational structure, where any of the roles may also be a user of the cloud service.

The framework's tasks are executed by following the Evaluate–Direct–Monitor cycle with the senior officers' support. These cycles are initiated in the higher levels and then traverse downwards and upwards through all the other managerial levels.

The security role has been specifically differentiated to focus on security matters. The mapping of these roles onto existing users can be very diverse, whereas various roles can be carried out by one person (i.e. senior officers and high executives) in small companies, in large companies, each role should be carried out by different people. The cloud provider role has also been included to distinguish its participation in all the activities. Depending on the cloud service offered, this role can also be subdivided into more specific subroles.

A brief description of the participant roles is shown as follows

(i) Senior officers. They are directly involved with the organization's mission and develop the main guiding strategies. This role involves different specializations, such as Chief Executive Officer (CEO), Chief Information Officer (CIO) and Chief Information Security Officer (CISO).
(ii) Business line executives. They constitute the second business level, just under the senior officers. They are responsible for translating the strategies in tactic programmes, thus defining middle term objectives.
(iii) Business line managers. They are in the lower managerial levels. They are responsible for defining short term activities and directing the operational personnel.
(iv) Human resources managers. They are responsible for personnel recruiting policies and for the development of training plans. They analyse the Communication functions in the organization, thus ensuring that the security culture achieves its objectives.
(v) IT managers. They manage both the hardware and software elements, which support the information services used by the organization. This role is mostly involved with the technical aspects of the Cloud Computing service.
(vi) Security managers. They are responsible for the various security areas (physical, logical, legal, etc.), involving both the policy definition and the verification of its compliance.
(vii) Auditors (Internal or External). They are responsible for auditing the organization's process performance. They can be internal or external to the organization, but must in both cases perform their role independently.
(viii) Operational personnel. They are in the lowest hierarchical levels. They are responsible for executing the tasks defined by upper levels.
(ix) Cloud provider. This role reflects the Cloud provider's involvement in some of the security processes, when performed within its client. In spite of being a unique role, it could be divided into various others if the Cloud Computing service requires the provider to take over different functions.

4. ISGCLOUD MODELLING

Having introduced an overview of our cloud security governance framework and its main components, this section details the modelling of both its activities and its artefacts.

In order to facilitate an understanding of the ISGcloud process, it has been formally modelled by following the SPEM specification 2.0 developed by the Object Management Group (OMG) [23]. The SPEM specification takes an object-oriented approach and uses Unified Modelling Language (UML) as a notation. It is used to define systems processes

and their components, providing the necessary concepts for their implementation and management. The SPEM model allows us to provide a standardized representation of our framework which can be easily managed by automatic electronic repositories and facilitates content reutilization by external tools. The framework is therefore supported by a standard document format which assists in its communication and dispersion to different types of organizations.

The SPEM 2.0 specification assumes an object-oriented perspective, which shares many aspects with the UML notation [35]. Its latest version has been adopted by the ISO as the ISO/IEC 19505 standard.

4.1. Activity modelling

The cloud service lifecycle introduced in the previous section was employed in the modelling of our process, resulting in six separate activities according to the SPEM nomenclature. These activities are represented in Fig. 1 using the SPEM diagram notation. The proposed activities are closely related to the outsourcing cycle presented in the ISO 27036 standard [22]. This is the basis of a general and comprehensive framework that can be tailored to provide secure governance for any cloud computing service.

There are three main phases in the service's lifecycle

(i) Preparation Phase. This covers the planning, analysis, design and implementation activities in relation to the security of the Cloud Computing service. These activities are grouped in the same phase, because its development usually takes a shorter period of time in comparison with the service's operation phase. The model allows the activities to be performed in a sequential manner, but also to step back in order to refine previously obtained results.

(ii) Operation Phase. This is focused on the secure operation of the cloud service. This phase is usually planned for a longer period, or even without a planned termination. It is developed in iterative cycles, so that ISG can be continuously guaranteed.

(iii) Termination Phase. This guarantees a secure finalization of the Cloud Computing service, which also

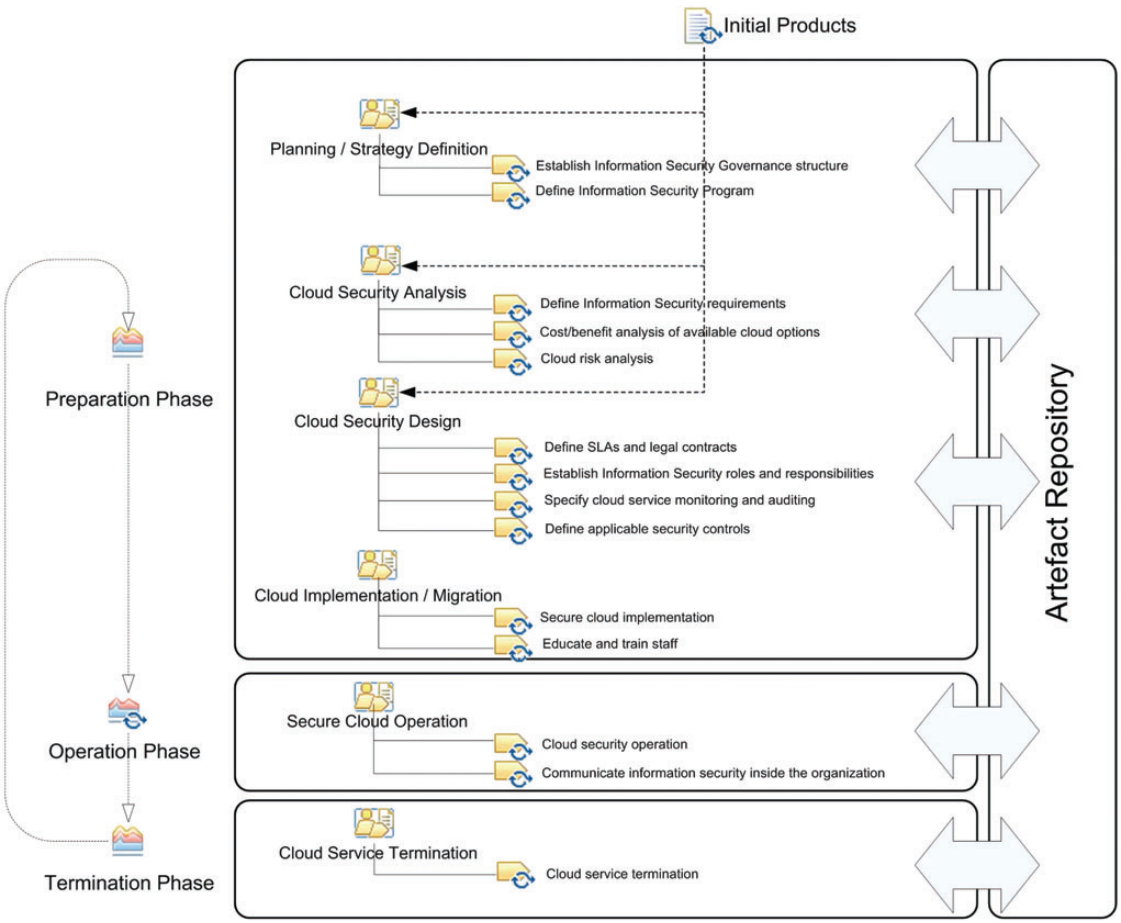

FIGURE 1. ISGcloud framework: activities and tasks.

includes its related documentation and output artefacts. These outcomes can be reused in subsequent Cloud Computing cycles.

All the model's activities should be performed iteratively, following the core principles of our framework. This feedback will allow practitioners to return to activities that have previously been accomplished with new output products that may contain additional information needed to perform another cycle. The execution of each task involves successive Evaluate–Direct–Monitor cycles to ensure that the highest levels of the organization are aware of its performance and receive feedback from the Cloud Computing service.

Each activity is connected to the Artefact Repository, from which it takes its input products and in which it stores its output products. We therefore provide a centralized repository that keeps records of the products used during the process. In addition to the internal artefacts, activities from the preparation phase also require initial products, which offer valuable information related to the organization but are external to ISGcloud.

Not all the tasks shown in the model are compulsory. Each organization should choose which tasks are most suitable for their necessities and which can be omitted. For instance, some tasks refer to the creation and empowerment of a security governance structure prior to the cloud service deployment, and it may not be necessary to carry these tasks out if the organization already has ISG implemented in its own processes.

In order to provide more details on the activity modelling, we have formally defined each task using the SPEM 2.0 specification. Each of the six activities that reflect the cloud service lifecycle is broken down into various tasks, and each task is defined by its related steps. The definition of each task includes the user roles that participate in its development (RoleUse), the products that serve as input or output (WorkProductUse), the steps into which the task can be divided (Step) and the standards of best practices that are suggested in the task performance (Guidance). The model structure of each task is shown in Table 1.

Each task also includes documents containing guidance that could help accomplish the task's objectives. These suggested guides are based on the standards and best practices that best match with our framework. Table 2 summarizes the most relevant references, all of which are related to either governance issues or security in cloud computing environments, and most of which have already been introduced. These auxiliary components should be considered as suggestions as to how to standardize and optimize the execution of each process, but this does not mean that organizations are forced to use them. When adapting ISGcloud to any cloud deployment, some other existing standards already used by the company may be applied, or could even be substituted for new standards that may appear in the future.

TABLE 1. ISGcloud model structure using SPEM.

Activity {kind = Phase}: *Name of the Phase*
Process: *ISGcloud*
Activity {kind = Iteration}: *Name of the iterative Activity*
TaskUse: *Name of the task*
ProcessPerformer {kind: primary}
RoleUse: *Role Name* {kind: in}
WorkDefinitionParameter {kind: in}
WorkProductUse: *Artefact name*
WorkDefinitionParameter {kind: out}
WorkProductUse: *Artefact name* {state: *state*}
Steps
Step: *Name of the step*
Guidance
Guidance {kind: type}: *Guidance name*

TABLE 2. ISGcloud's most important guidance.

Cobit
ENISA risk assurance framework
ITGI—Information Security Guidance for Boards of Directors
ISO/IEC 27001 and 27002
Cloud Security Alliance (Guidance for Critical Areas of Focus in Cloud Computing)

A sample of this modelling is shown in Table 3, in which task 2C (Cloud risk analysis) is defined using SPEM. Similar definitions have been produced with the other tasks, although they cannot be shown here owing to space restrictions.

4.2. Artefact modelling

ISGcloud framework has been designed with a process oriented perspective, signifying that its activities and tasks behave as processes that require input artefacts that are related to information security, and produce output artefacts related to the ISG objective in the Cloud Computing service. These artefacts reflect any kind of information that is related to the organization, such as security policies, organizational structure, legal contracts or security requirements.

The SPEM 2.0 specification groups all these products in the artefact category. These artefacts are essential to the processes' performance and have their own lifecycle. Each iteration and cycle allows the artefacts to be refined to evolve towards their desired ISG objective through a continuous improvement process. It is therefore important to know the state of each artefact, so that resources may be allocated in order to review tasks whose products need improvements.

All ISGcloud's artefacts are managed from an Artefact Repository. This repository acts as a document manager that supports product versioning. The repository stores and

TABLE 3. Task 2C definition using SPEM.

TaskUse: *2C Cloud risk analysis*
ProcessPerformer {kind: primary}
RoleUse: *Senior officers* {kind: in}
RoleUse: *Business line executives* {kind: in}
RoleUse: *Business line managers* {kind: in}
RoleUse: *IT managers* {kind: in}
RoleUse: *Security managers* {kind: in}
WorkDefinitionParameter {kind: in}
WorkProductUse: *Security threats and vulnerabilities*
WorkProductUse: *Security policies*
WorkProductUse: *Security requirements*
WorkProductUse: *Information Security Program*
WorkDefinitionParameter {kind: out}
WorkProductUse: *Information assets* {state: *initial draft*}
WorkProductUse: *Security threats and vulnerabilities* {state: *reviewed*}
WorkProductUse: *Risk assessment* {state: *initial draft*}
WorkProductUse: *Risk management guidelines* {state: *initial draft*}
WorkProductUse: *Risk remedial action plans* {state: *initial draft*}
Steps
Step: *2C.1 Define methodology*
Step: *2C.2 Identify information assets (particular to cloud deployment)*
Step: *2C.3 Analyze threats and vulnerabilities*
Step: *2C.4 Measure risk exposure: periodic assessment of risk impact*
Step: *2C.5 Define risk management process*
Guidance
Guidance {kind: practice}: *ENISA risk assurance framework*
Guidance {kind: practice}: *Cobit: EDM03 Ensure Risk Optimization*
Guidance {kind: practice}: *Cobit: APO12 Manage Risk*
Guidance {kind: practice}: *Cobit: BAI09 Manage Assets*

manages different versions of products, signifying that participants have access to the latest version of the product they need to handle, and can also track back to older versions and the changes among them.

The artefact modelling has been developed by creating a structure with different artefact categories, in which products can be grouped by their relationships or similarities. This structure has been designed by following the SPEM 2.0 Packet Diagram technique, in which a packet symbolizes each of the proposed artefact categories and each packet is itself formed of different artefacts.

The SPEM 2.0 specification proposes following a similar notation to that defined by UML. The following two relationships from this notation have been used:

(i) Composition relationship: this represents that an artefact is a component of a more generic artefact. It is used to reflect the breakdown of the artefacts so that it can facilitate the task's performance.
(ii) Use relationship: this represents that an artefact requires or uses another artefact, meaning that the latter must be developed beforehand if the former is to be produced.

The Artefact Modelling occurs at two levels of detail: at a first level, all the packets that belong to ISGcloud are represented, along with the main relationships among them; and at a second level, each packet is broken down into the artefacts that it contains, along with their relationships (both internal and external).

The first-level modelling is shown in Fig. 2 using a static packet diagram. Figure 2 shows the main packets identified in ISGcloud and also the dependencies among them during the ISG process.

A sample of the second-level modelling is shown in Fig. 3, which provides details of the ISG Structure Packet. This packet contains the essential artefacts needed to establish a security governance structure around the Cloud Computing service. Its main artefact is the ISG Strategic Plan, which is itself composed of the Top-level Security Policies, the ISG Organization and the Roles and Responsibilities.

A similar approach is followed with the other packets, although their second-level diagrams cannot be shown here owing to space restrictions.

5. ISGCLOUD ACTIVITIES AND TASKS

Having introduced the core processes of our cloud security governance framework and its main components, this section details the process structure throughout the cloud service lifecycle. All the activities should be performed iteratively, following the core principles of our framework. This feedback will allow practitioners to return to activities that have previously been accomplished with new output products that may contain additional information needed to perform another cycle. The remainder of this section details the tasks proposed in each activity, along with a brief description.

5.1. General structure

ISGcloud's general structure is shown in Fig. 4, which provides a summary of the activities and tasks that constitute the framework. The table also shows the steps that are involved in the execution of each task.

5.2. Activity 1: planning/strategy definition

The first activity in the ISGcloud framework is designed as an introductory process to establish the foundations needed for

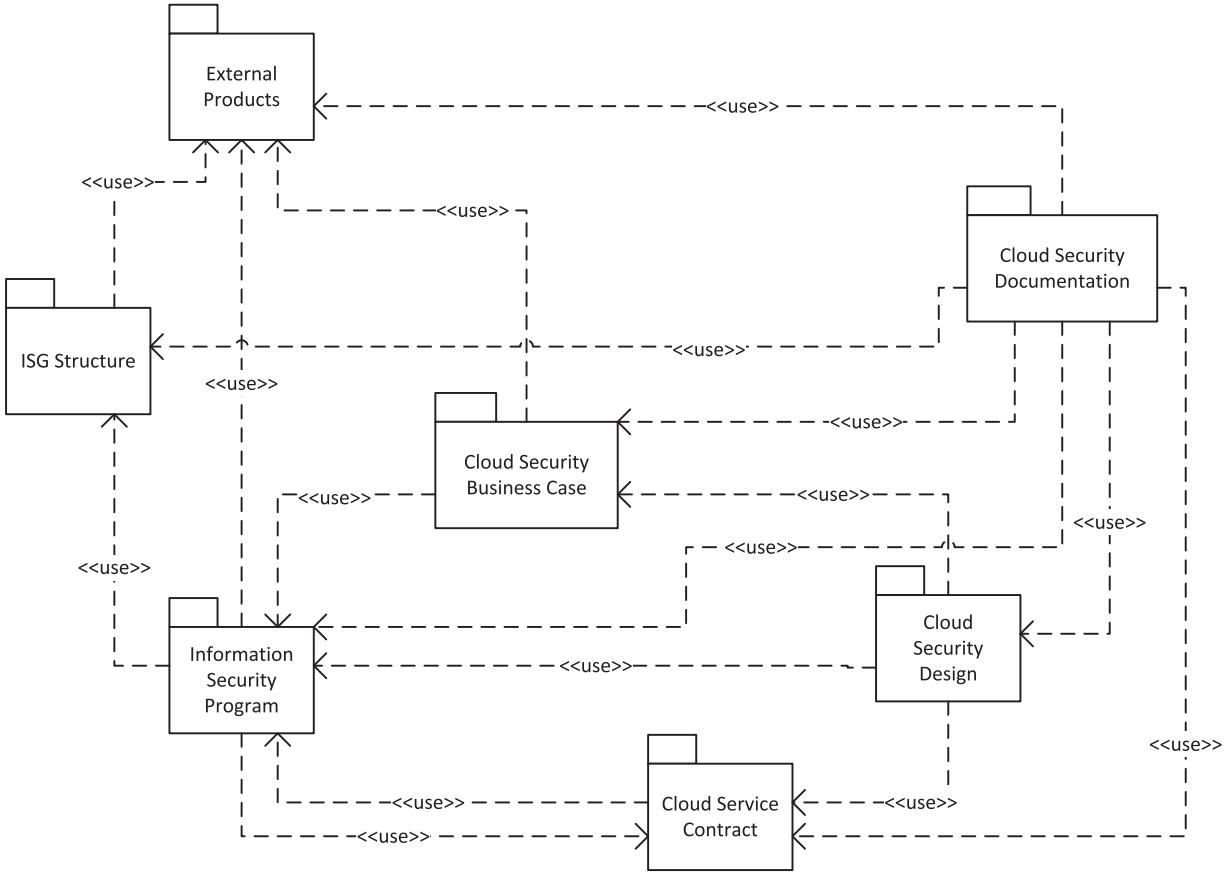

FIGURE 2. Static packet diagram.

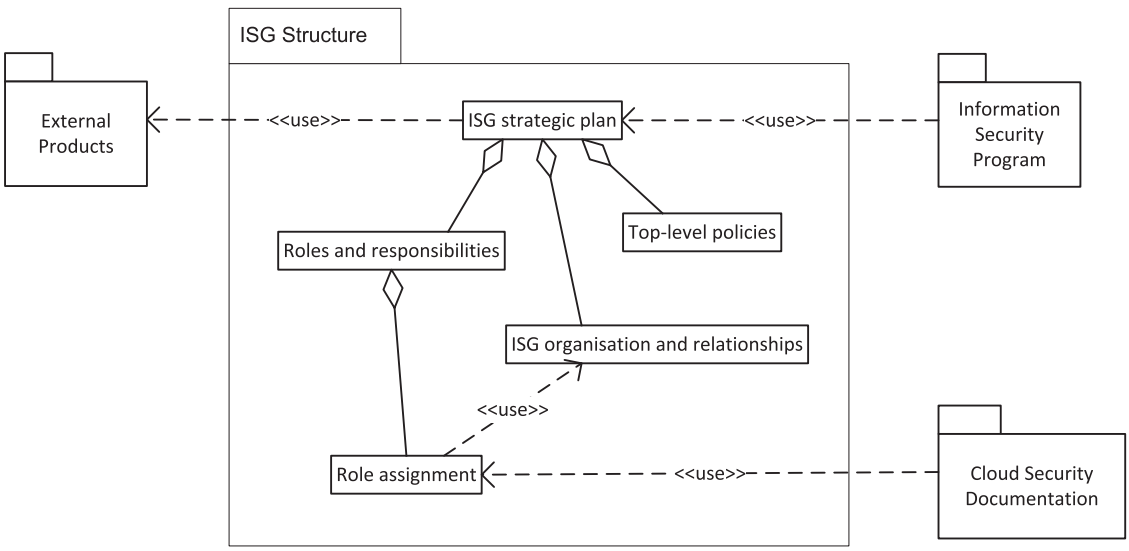

FIGURE 3. ISG structure packet detail.

Activity 1: Planning / Strategy Definition
Task 1A: Establish Information Security Governance structure
Step: 1A.1 Identify participants
Step: 1A.2 Assign roles and responsibilities
Step: 1A.3 Create teams and committees
Step: 1A.4 Indicate lines of reporting
Step: 1A.5 Develop top-level ISG policies
Step: 1A.6 Develop ISG strategic plan
Task 1B: Define Information Security Program
Step: 1B.1 Information Security Program direction
Step: 1B.2 Information Security Program vision, goals and scope
Step: 1B.3 Establish main guiding activities
Step: 1B.4 Ensure alignment of Information Security Program with mission goals and objectives
Step: 1B.5 Provide basis for measuring Information Security Program efficiency
Activity 2: Clous Security Analysis
Taslk 2A: Define Information Security requirements
Step: 2A.1 Analyze supporting standards, guidelines and procedures
Step: 2A.2 Define security requirements
Step: 2A.3 Adapt Information Security Program to the planned cloud deployment
Task 2B: Cost/benefit analysis of available cloud options
Step: 2B.1 Define comparative criteria based on requirements
Step: 2B.2 Analyze relevant approaches
Step: 2B.3 Evaluate candidate cloud providers
Step: 2B.4 Cost/benefit analysis
Step: 2B.5 Determine the operating cloud service model
Step: 2B.6 Elaborate Business case
Step: 2B.7 Ensure consistency with enterprise Information Security architecture
Task 2C: Cloud risk analysis
Step: 2C.1 Define methodology
Step: 2C.2 Identify information assets (particular to cloud deployment)
Step: 2C.3 Analyze threats and vulnerabilities
Step: 2C.4 Measure risk exposure: periodic assessment of risk impact
Step: 2C.5 Define risk management process
Activity 3: Cloud Security Design
Task 3A: Define SLAs and legal contracts
Step: 3A.1 Translate security requirements into detailed SLAs of all services
Step: 3A.2 Minimize security risks related to regulations
Step: 3A.3 Define accountability for security breach
Step: 3A.4 Periodically review of SLAs and contracts

Activity 3: Cloud Security Design (cont.)
Task 3B: Establish Information Security roles and responsibilities
Step: 3B.1 Assignment of roles, responsibilities, authority and accountability
Step: 3B.2 Assignment of ownership of information assets
Task 3C: Specify cloud service monitoring and auditing
Step: 3C.1 Define monitoring of security SLAs
Step: 3C.2 Establish processes to monitor security elements
Step: 3C.3 Design metrics of security performance
Step: 3C.4 Define service security audit process
Task 3D: Define applicable security controls
Step: 3D.1 Define security controls to the cloud deployment
Step: 3D.2 Develop Incident Response Plan
Step: 3D.3 Design Business Continuity and Disaster Recovery plans
Activity 4: Cloud Implementation / Migration
Task 4A: Secure cloud implementation
Step: 4A.1 Define additional security controls to guarantee assurance during implementation
Step: 4A.2 Define new processes or modify existing ones to include ISG
Step: 4A.3 Integration of ISG into all organisational processes
Step: 4A.4 Guarantee security on information systems acquisition
Task 4B: Educate and train staff
Step: 4B.1 Design security training plan
Step: 4B.2 Educate staff on required actions related to cloud computing
Step: 4B.3 Increase knowledge to enhance compliance. Knowledge transfer to end users.
Step: 4B.4 Train on standards, guidelines and new cloud risks
Step: 4B.5 Evaluation of training received
Activity 5: Secure Cloud Operation
Task 5A: Cloud security operation
Step 5A.1 Apply Evaluate-Direct-Monitor cycle over security processes
Step 5A.2 Periodical audits
Task 5B: Communicate information security within the organisation
Step: 5B.1 Elaborate cloud security documentation
Step: 5B.2 Communicate the importance of information security inside the organisation
Step: 5B.3 Security awareness inside the organisation
Step: 5B.4 Inform of new policies and procedures
Activity 6: Cloud Service Termination
Task 6A: Cloud service termination
Step: 6A.1 Ensure secure data retrieval from cloud provider (or transfer to other provider)
Step: 6A.2 Verify application of termination policies on cloud provider
Step: 6A.3 Document the service termination

FIGURE 4. General structure of ISGcloud's activities and tasks.

the remaining activities. Its main objectives are to establish a security governance structure within the organization and to provide an Information Security Program that defines the boundaries in which the following activities take place. It therefore focuses on security and governance issues, and leaves the linking with cloud computing services to later phases. These objectives are successfully attained by carrying out the two tasks identified in this activity.

This activity is composed of two tasks, as shown in Fig. 5, each of which is focused in one of the two objectives of the activity. The roles involved in its performance are chosen from the higher managerial levels, including senior officers, business executives and security and IT managers.

The initial effort of tailoring the framework to each situation is particularly relevant in this first activity. An organization that has already implemented a security governance framework can take advantage of it and substitute any of the ISGcloud steps for its own established governance processes. However, we recommend checking the definition of the two tasks included in this activity and their output products in order to guarantee that similar artefacts are produced, even if the process followed differs from that proposed. The consistency between our cloud security framework and the processes implemented within the organization is therefore guaranteed in subsequent activities.

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

Task 1B: *Define Information Security Program*. Once an effective governance structure and top-level security policies have been defined, then an Information Security Program must be developed. This program consists of a series of activities that support the enterprise risk management plan and result in the development of the security strategy and policies [36]. This task must be performed coordinately by IT and security managers and senior officers, in order to guarantee that the security program is aligned with the business objectives.

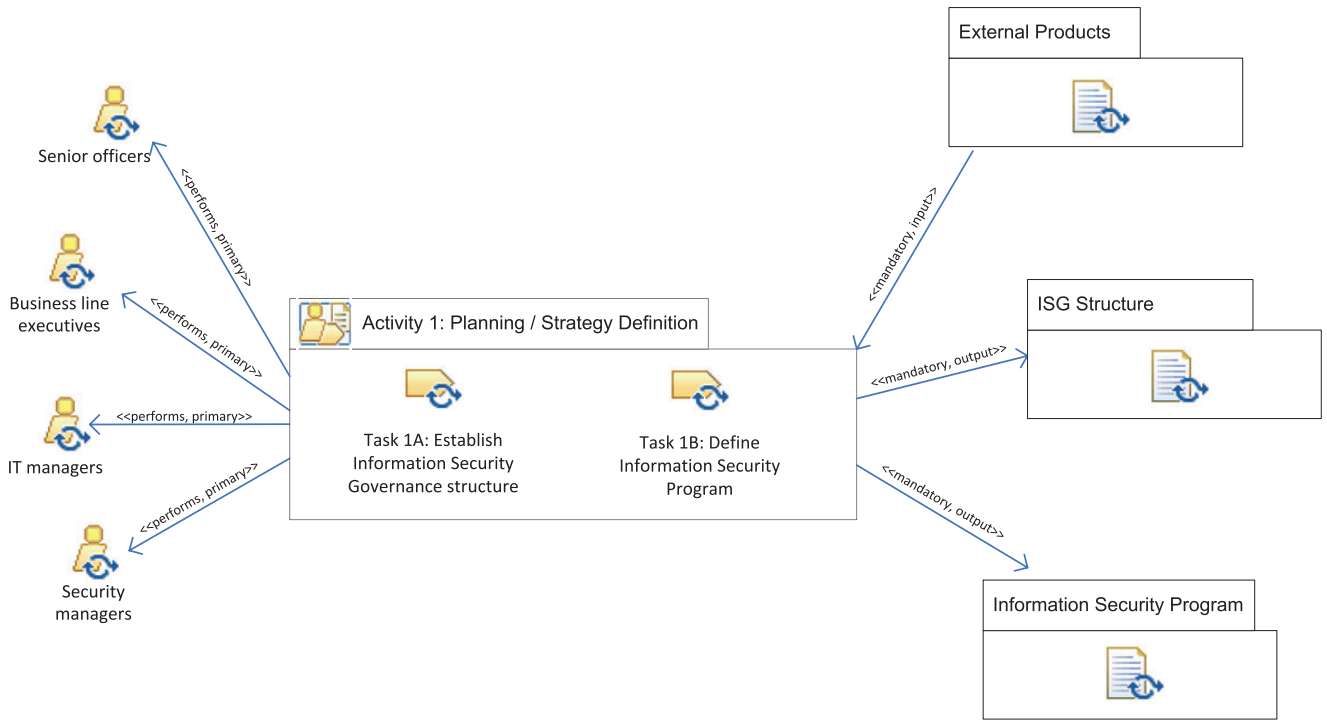

FIGURE 5. Activity 1: tasks, roles and artefact's packets.

5.3. Activity 2: cloud security analysis

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

(i) security requirements analysis,
(ii) cost/benefit analysis of available cloud options and
(iii) cloud risk analysis.

Figure 6 contains the main components of this activity. The activity is divided into three tasks, each of which is focused on the different analyses proposed.

This activity is performed by the highest roles in the organization, together with some management roles.

Although each of the three tasks can be executed separately, all of them are related as part of the same Evaluate–Direct–Monitor cycle. It may therefore be necessary to perform consecutive iterations of the three tasks of which this activity is composed in order to achieve the desired results. Even also, the results of each of these tasks may drive to changes in the other two ones.

The outcomes of these analyses are crucial to the choice of the cloud service and its associated security governance.

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

Task 2B: *Cost/benefit analysis of available cloud options*. Once the security requirements and security policies have been defined, the organization needs to evaluate the cloud options that are available for the services being deployed. This evaluation is performed in this task through cost/benefit analyses that include the cost of effective governance to manage risk and ensure regulatory compliance [37] and the value added by the cloud service. These analyses must include security considerations regarding the degree of fulfilment of the security requirements by the different candidate cloud providers in relation to the cloud service model chosen. Although it is an early estimation, the business case provides a first economic approach as regards the organization's cloud service security prospects.

Task 2C: *Cloud risk analysis*. The third analysis included in this activity is a cloud security risk analysis. The objective of

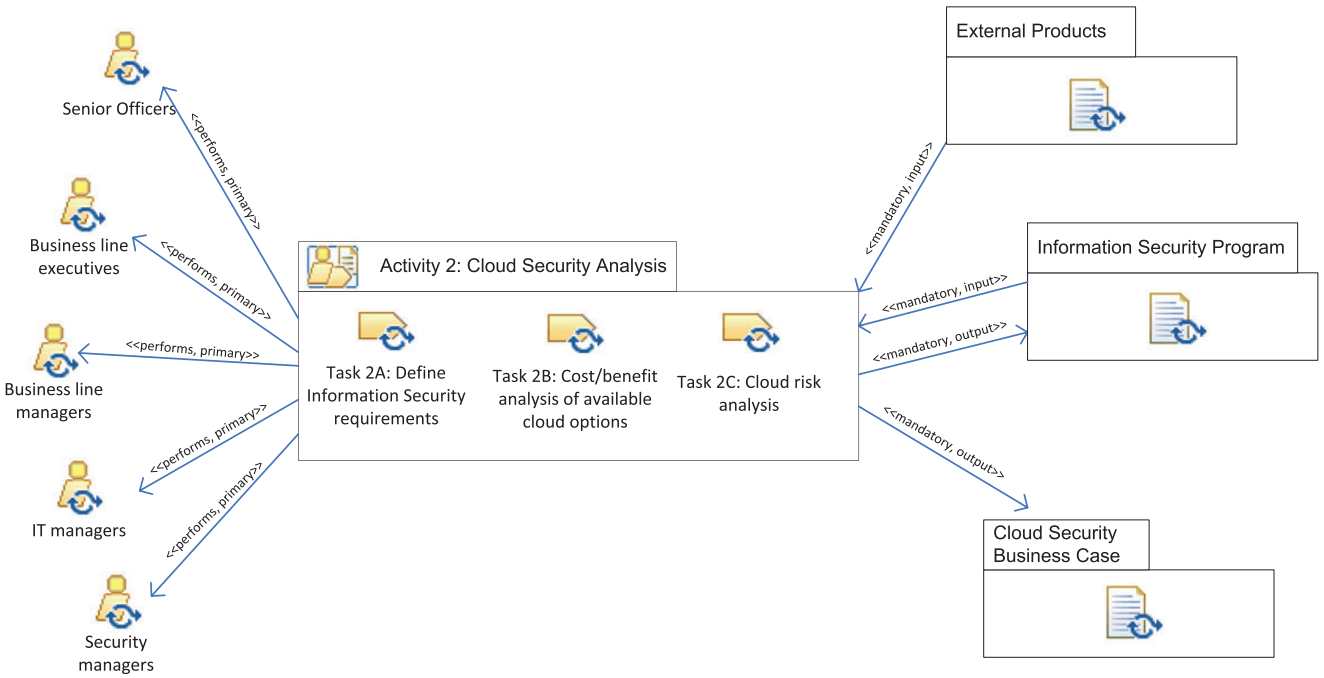

FIGURE 6. Activity 2: tasks, roles and artefact's packets.

this task is to provide an understanding of the cloud service security risks identified and to define management processes for these risks. Like any risk assessment, this includes the identification of the information assets with their related threats and vulnerabilities, and the definition of procedures to manage the risks and counteract them. We recommend using the Information assurance framework defined in [31] by ENISA, which assists in following these steps.

5.4. Activity 3: cloud security design

The objective of ISGcloud's third activity is to provide a comprehensive design of the security governance that will be implemented together with the cloud service. This activity in itself constitutes an Evaluate–Direct–Monitor cycle, since an iterative execution is recommended for the development of a satisfactory design result.

This activity consists of four tasks, as shown in Fig. 7, which also depicts the participant roles and the packets involved.

Because of the differentiating characteristics of cloud services, there is a task that focuses on designing the contractual relationship between the organization and the cloud provider and defining the SLAs. The remaining tasks have more in common with other security processes and involve a detailed specification of security controls and security roles, and the definition of how the organization intends to monitor and audit the cloud service's security.

When starting this activity, we suppose that the cloud service has been selected from the previous activity, and the cloud provider role can therefore be incorporated in order to participate in the tasks. This role is mostly related to designing the relationship processes between the organization and the cloud provider, which is then translated into the SLAs desired.

This activity is performed in parallel with other stages of the cloud service lifecycle, such as the solution's technical design, the service procurement or contract signing. These stages must also be considered by the organization but are out of ISGcloud's scope.

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

Task 3B: *Establish Information Security roles and responsibilities*. The security design requires a detailed establishment of responsibilities within the organization. This assignment depends to a great extent on the governance structure defined in the first activity. This task demands an identification of the

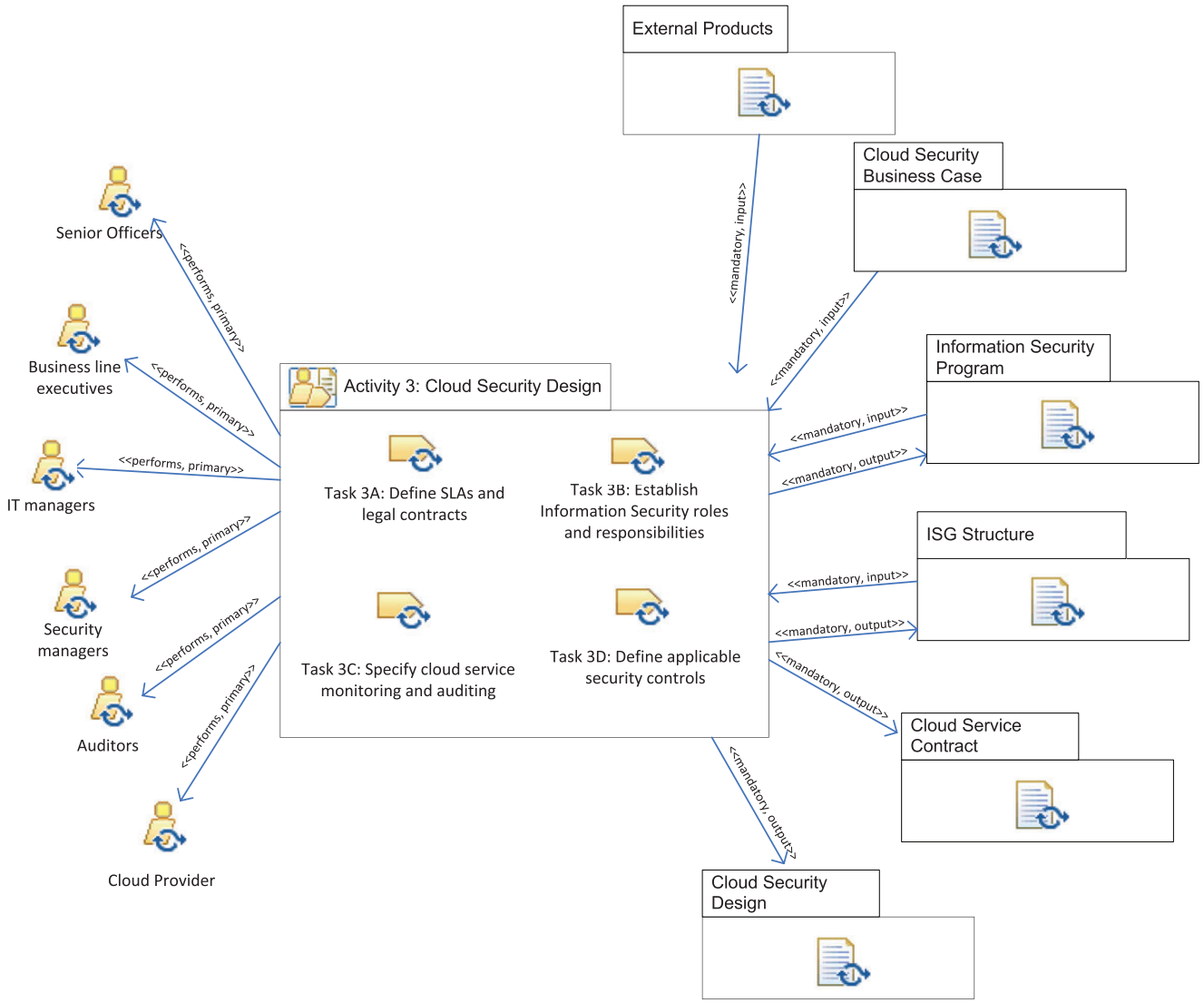

FIGURE 7. Activity 3: tasks, roles and artefact's packets.

information assets, in order to define the ownership and responsibility of each one.

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

Task 3D: *Define applicable security controls*. The last task in the design activity is focused on defining the security controls. Based on the risk analysis, the organization must develop the security measures that it will apply both during the cloud service operation and also in cases of incidents or major disasters. This task can be performed by following any of the existing security standards, such as ISO/IEC 27001 [26]. This task is executed coordinately between the client organization and the cloud provider: the user identifies the security controls that are needed in order to fulfil its security requirements, and the provider designs the implementation of the controls on the cloud service.

5.5. Activity 4: cloud implementation/migration

Once the security design has been completed, then the cloud service implementation takes place. The objective of this activity is to provide the organization with a secure service implementation, governed by the Evaluate–Direct–Monitor cycle, whereas all the organization's members are adequately instructed as to their security functions, as part of the Communicate process.

The execution of this activity varies depending on whether the cloud service implemented has been previously used in the organization or whether it is a migration from one cloud provider to another. Here are some of the most common scenarios

(i) The service does not exist previously. The project involves a new service that the organization has not yet developed and will be provided via a cloud computing implementation.
(ii) The service is offered internally. The organization already provides the service in its own infrastructure. This scenario involves a migration from the organization's internal premises to an external cloud provider.
(iii) The service is offered externally. The organization already provides the service via an external provider. This scenario involves a migration from the former provider to a new cloud provider.

Each of these scenarios may involve adjustments being made to this activity's tasks or to some of their steps. ISGcloud offers a broad scope, signifying that it is able to include any of them. Service implementation terminology will be used in the remainder of this paper, although references may also be made to a migration. The two tasks that are proposed in this activity are shown in Fig. 8, along with the participant roles and artefact packets involved in its execution.

This activity's tasks are focused on deploying the security controls required to guarantee a secure cloud service implementation and on providing personnel with the security training related to it.

These tasks are performed in parallel with other technical and organizational stages of the cloud service implementation, which also need to be taken into consideration by the organization.

Task 4A: *Secure cloud implementation*. This task focuses on the security during the service implementation and the

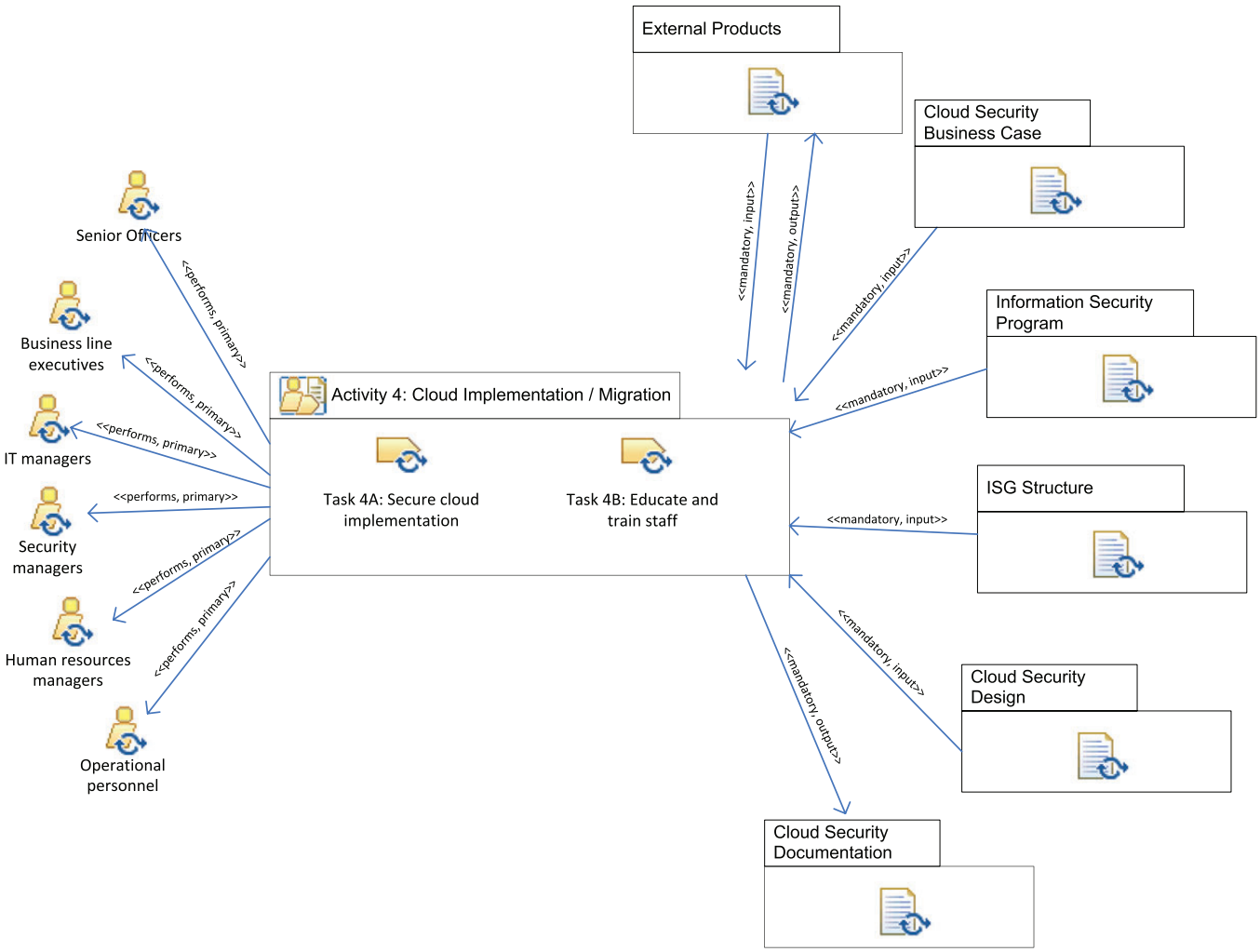

FIGURE 8. Activity 4: tasks, roles and artefact's packets.

parallel modification of the organizational security processes. Additional security controls are needed in the migration, some of which will depend on the type of cloud deployment. Along with the service implementation, the organization's processes are adapted to the newly designed specification.

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

5.6. Activity 5: secure cloud operation

The fifth activity of ISGcloud is devoted to the cloud service operation. The previous activities can be considered as time delimited, but it is generally difficult to fix time limits to the operation since it usually has an indefinite duration. It is for this reason that the proposed core Evaluate–Direct–Monitor iterative cycle is especially relevant in this activity. These processes take place continuously until a decision is made to terminate the cloud service. The framework thus guarantees the active security governance of the organization's services.

Figure 9 shows the two tasks of which this activity is composed.

The first task in this activity is focused on maintaining the security level required during the operation stage, whereas the second task considers the organization's security communication process.

It is worth highlighting that all the participant roles defined by ISGcloud are involved in this activity. This is explained because all of them need to participate, in some way or other, in the security governance structure that has been implemented around the cloud service.

Task 5A: *Cloud security operation*. The security operation task reflects the successive iterations of the governance cycle. This cycle requires a precise design of the processes, so that all participants can play their defined role. The continuous improvement process may lead to modifications to products from previous activities, such as the Information Security Program or the Risk Analysis. If so, it may be interesting to revisit previous activities, even while the cloud service is operating. Successful security governance not only

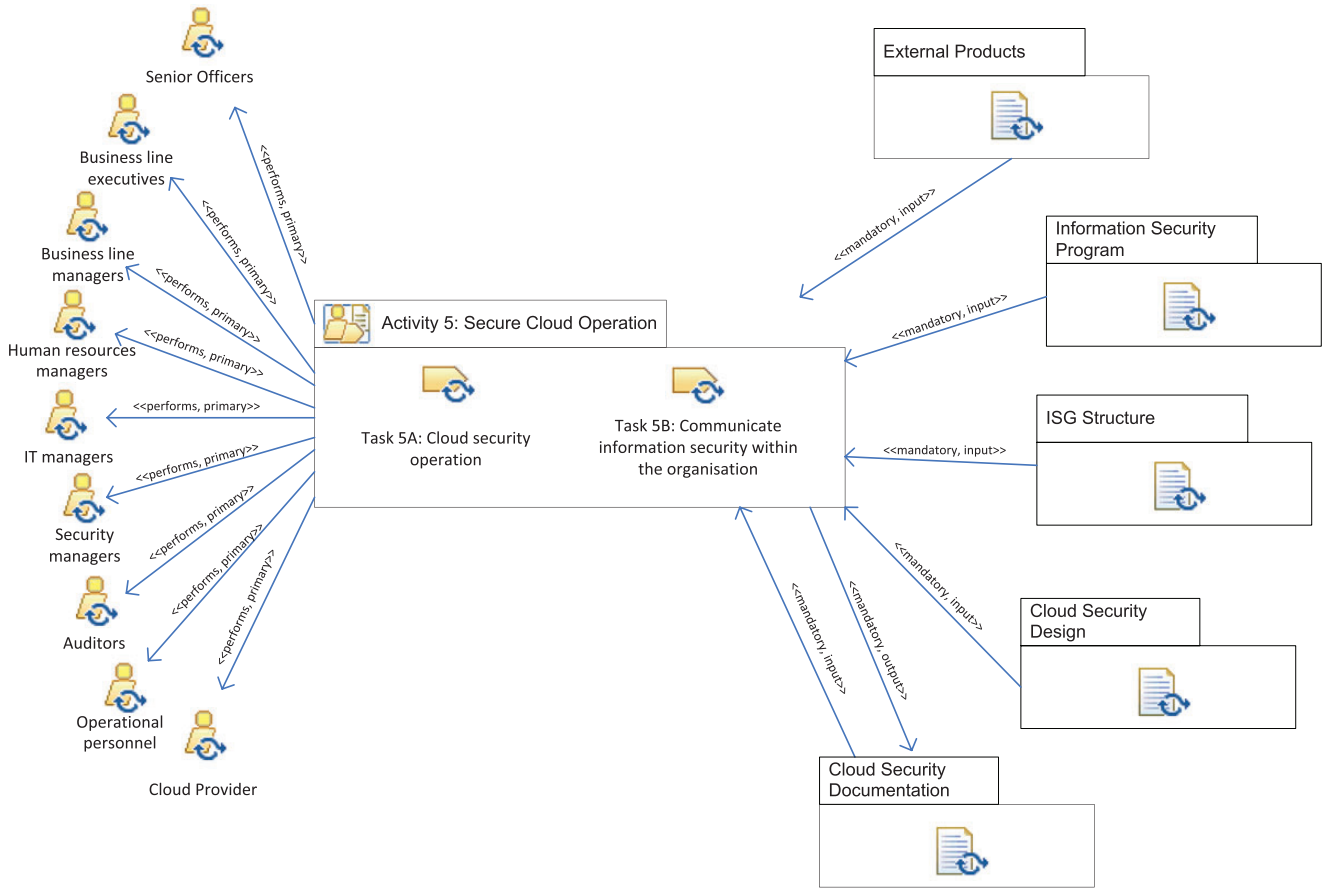

FIGURE 9. Activity 5: tasks, roles and artefact's packets.

requires regular service measurement, but also an adequate prioritization of the programmes and the regular reporting of security issues, which may include recommendations for corrective and preventive actions.

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

5.7. Activity 6: cloud service termination

The objective of the last activity is to provide the service termination with security. Bearing in mind that security governance is a continuous process that does not conclude with the end of the service, this final activity facilitates the basis for new security governance cycles. The organization can take advantage of the knowledge obtained and lessons learned for the security of future services.

This activity contains one task, as shown in Fig. 10.

This activity is performed by the higher managerial roles, and involves finishing the relationship with the cloud provider.

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

6. EXAMPLE OF APPLICATION

We have developed a simple example of application in order to illustrate the modelling of ISGcloud's activities. Our main purpose is to provide an additional understanding of our framework, but this may also serve to partially validate its practical applicability. Although our research is performed theoretically, we propose useful examples that provide an overview of how our approach might be implemented in an organization that is planning to deploy cloud services. These examples are useful to help understand the objectives of the proposed activities and their related tasks, and also provide a practical insight into the sample products involved.

We propose using a fictitious middle-size organization devoted to healthcare services, which owns several businesses located in different towns in the same regional area. The core services of the organization are formed of general practitioners and doctors in various specialities, but there are also other supporting and paramedic staff. This company owns

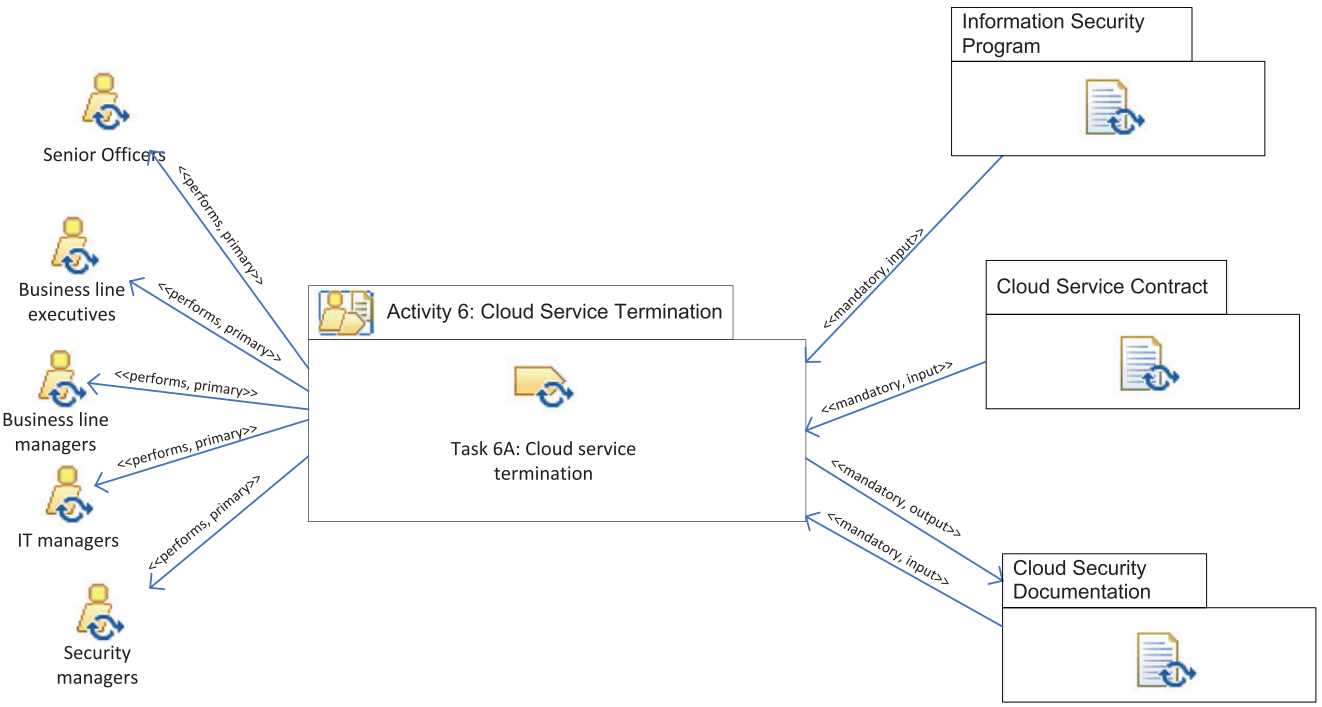

FIGURE 10. Activity 6: tasks, roles and artefact's packets.

an obsolete e-mail platform which is used to allow its personnel to communicate when following patients' medical histories in different specialities, or to solve professional questions among doctors. The e-mail platform is run on its premises in a rented building in which the IT department has its data centre. The platform hardware was amortized many years ago, and is now starting to limit the deployment of new software versions that provide the new functionalities required. The IT managers are therefore suggesting that senior officers should invest in an outsourcing plan in order to move the e-mail service to the cloud computing environment, whereas the security department is attempting to promote a security culture within the company.

Having defined a possible context, we shall now depict how this organization could take advantage of the ISGcloud framework to guarantee the security governance of its cloud e-mail service. An overview of the task development will be provided for illustrative purposes, but most of the complexity and formality associated with the framework are intentionally omitted. We focus on the key roles and artefacts of which a good practical approximation to our process is composed, and ignore other secondary elements. The results of this example can be easily extrapolated to any other organization, independently of the cloud service it plans to implement.

The transition of this organization is depicted in Fig. 11, in which the e-mail service migrates from a self provided basis to a cloud service. The e-mail cloud provider is represented as an independent entity, thus constituting a public cloud that it available to any customer via the Internet. Figure 11 also reflects the governance structure led by the ISG committee, with members of all the relevant departments, which drives the secure service transition fostering the security governance process.

Let us suppose that our sample organization has no previous experience of governance processes, and that its CEO is responsible for identifying relevant participants in every department and assigning their corresponding roles. *Task 1A* (*Establish Information Security Governance structure*) begins with the creation of an ISG committee consisting of members of all the participant roles, which coordinates the steps of this activity and is responsible for the establishment of a security governance structure. This committee translates the business objectives into the following top-level security policies

(i) Information handled according to national regulations.
(ii) Guarantees of patient privacy.
(iii) Adequate information access, management and retrieval.

The organization decides that this committee will supervise all the remaining tasks during the cloud service lifecycle and will be responsible for their performance.

The sample organization owns an outdated security program that needs to be rewritten and updated with the policies that were newly defined during *Task 1B* (*Define Information Security Program*), which include

(i) Authentication of accesses to the mail service.
(ii) Integrity and confidentiality of stored information.
(iii) Adequate service availability.

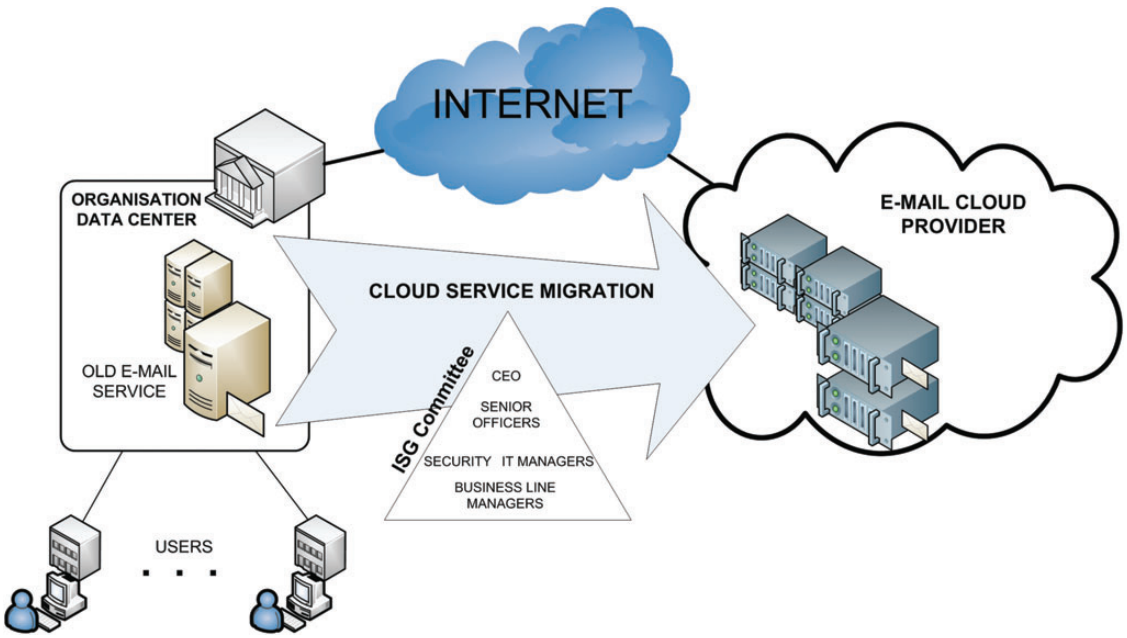

FIGURE 11. ISGcloud applied to e-mail service migration.

New metrics are also defined to measure the security program

(i) Reports of security breaches.
(ii) Number of procedures aligned with the security program.
(iii) Security processes performance.

The IT and security managers agree with senior officers that their future service strategy will be based on cloud computing, and that this project may therefore serve to check the validity of the ISG framework and be used to begin developing a governance culture within the company.

The sample organization starts the analysis activity with *Task 2A* (*Define information Security requirements*), during which the ISG committee analyses the security requirements for the cloud service. The organization is highly concerned about how the security breaches may damage the company's image, and this is therefore reflected in the e-mail platform requirements. Some of the more relevant requirements are as follows

(i) Secure access to information and e-mails, which includes authentication and permission authorization.
(ii) Cloud provider handles incidents and guarantees service availability.
(iii) Security reports are updated regularly.
(iv) Automatic security monitoring.

In order to improve the organization's image from the point of view of its patients, security managers are seeking access to security certifications, such as those that will comply with the ISO/IEC standards. They therefore decide to follow the family of ISO/IEC 27000 standards throughout the entire project, wherever it is possible to adapt its security controls and processes.

The security requirements obtained in the previous task are used along with other technical and business requirements and additional considerations to compile cloud provider candidates that are capable of contracting the e-mail service. The execution of *Task 2B* (*Cost/benefit analysis of available cloud options*) leads to an analysis of the cloud providers identified in collaboration with the financial department. Some common expenditures and savings are estimated for each cloud alternative (i.e. savings on hardware and software acquisition; freeing space in a rented data centre building), whereas others are particular to each provider (i.e. cost per e-mail address or cost per disk space). The results of these analyses are expressed in the business case with reference to the cloud provider chosen, which results in the e-mail platform being provided as Software-as-a-Service in a public cloud.

The second ISGcloud activity ends with the risk analysis, which is performed with the participation of the security department and the ISG committee in *Task 2C* (*Cloud risk analysis*). The organization decides to follow the ENISA risk assurance framework [31] to identify possible risks that may affect their information assets. This guide helps us to identify threats and vulnerabilities and to elaborate risk management plans. Table 4 shows a sample of some assets and their corresponding threats.

TABLE 4. Assets and threats sample.

Asset	Threat
Personal information	Service unavailability
	Non authorized access
	Data leak or loss
	Inappropriate backup management
Provider Infrastructure	Intruders
	Malicious insider
	Natural disasters
Reputation	Revealing security incidents
SLA	Contract breach
	Bankruptcy of cloud provider
	Security regulation changes

Although the analysis activity is performed by considering the e-mail cloud service, most of its products can be reused in future iterations of the Evaluate–Direct–Monitor cycle. If this project is successful, the organization plans to migrate more services to the cloud, so this acquired knowledge will facilitate the participants' development tasks in future iterations.

Once the best cloud provider candidate has been chosen, the security design activity begins in conjunction with the contract signing. Personnel from the cloud provider therefore participate in both this activity and subsequent ones. A provider's project leader is designated as an interlocutor with the organization's ISG committee, and also controls some of the key resources concerning the security issues of the e-mail service. Although the SLA development takes place outside the framework, the ISG committee must review its clauses in *Task 3A* (*Define SLAs and legal contracts*) and possibly incorporate additional ones in order to cover security requirements. Some of the security SLAs are

(i) Use strong encoding on information stored by the cloud provider.
(ii) Cloud provider cannot use information for other purposes.
(iii) Ensure that regional regulation of personal information is covered.
(iv) Destroy information after service finalization.

Some penalizations are also agreed on to compensate any security incidents caused by the provider (i.e. security breaches or unauthorized use of personal information have an economic penalization, which is proportional to the incident degree).

When defining security responsibility, the sample organization is responsible for the e-mail security and the

cloud provider is accountable for the security implementation. The incipient governance structure started previously is detailed in *Task 3B* (*Establish Information Security roles and responsibilities*) by designating the ownership of information assets within the organization (i.e. users are responsible for information attached to their e-mails or system administrators are responsible for maintaining a disaster recovery backup), and the cloud provider is also included (i.e. the provider's operator is responsible for communicating security incidents).

The Evaluate–Direct–Monitor cycle requires the organization to define the service monitoring that will be performed in *Task 3C* (*Specify cloud service monitoring and auditing*). The e-mail provider facilitates its clients with a tool for automated monitoring that allows the platform's state to be consulted and the receipt of real-time alerts. This tool is managed by the organization's IT department, which includes its use in their daily operation processes. Security thresholds are also defined for the measures performed

(i) Number of failed attempts to log in.
(ii) Percentage of storage space available.
(iii) Information volume sent outside the organization.

Aligned with the organization's purpose of achieving a security certification, the ISG committee decides to hire external auditors to perform periodical evaluations by a third party. The organization defines auditing processes which provide more detailed information than the daily monitoring (i.e. a monthly check that information stored by the provider is securely encoded and periodical access to the audit log).

The security design concludes in *Task 3D* (*Define applicable security controls*), in which the organization details the security controls that are to be applied on the e-mail platform in order to minimize the previously detected risks and threats. The ISG committee decides to follow the security controls identified in the ISO/IEC 27001 standard and adapts them to the cloud service. Table 5 shows a sample of how each control objective from the standard is translated into a security control. Disaster recovery plans are also developed to guarantee business continuity and minimize the impact of a major incident (i.e. daily backups of cloud provider data will be obtained and stored on separate premises).

The organization decides to migrate its old e-mail information to the cloud provider, so that historic documents can be shared on the same platform, signifying that a migration plan needs to be provided by the IT department, as the e-mail service cannot be implemented out of the box. In order to guarantee this activity's security, *Task 4A* (*Secure cloud implementation*) suggests defining additional security controls for the e-mail migration (i.e. additional encoding to the transferred data until it is stored in the cloud provider). The ISG committee verifies that organizational processes are modified to include security governance tasks or even that new ones are established. Some of these processes are

(i) User authorization [existing process]: the organization defines the management of digital certificates that are assigned to mail users. Automatic triggers are developed so that if a user leaves the organization, his certificate is revoked.
(ii) Operation monitoring [existing process]: existing monitoring processes are adapted in order to include new security policies and guarantee compliance with the security program.
(iii) Incident reporting [new process]: new incident reporting channels are established between the organization and the cloud provider.
(iv) Mail security auditory [new process]: periodic auditory processes are defined, so that relevant security controls can be analysed.

During the migration activity in our example, a training plan is developed in *Task 4B* (*Educate and train staff*), so that at the same time as users are instructed on the new e-mail application they learn the new security measures that must be taken into account. This plan includes different perspectives according to the roles that exist within the organization (i.e. e-mail users learn the secure use of passwords to access the application; system administrators learn how to perform monitoring with automated tools).

TABLE 5. Sample of security controls.

ISO/IEC 27002 Control Objective	*Security Control*
Security policy	Internal communication of the information security program and security policies
Organization of information security	ISG committee meets monthly to review iterations of ISG cycles
Asset Management	Information assets are classified into three levels of confidentiality
	Documents are labelled so that different security controls can me applied
Human resources security	Mail users are given clear security instructions about their responsibilities
	Develop security training program
Physical and environmental security	Avoid storing confidential information in untrusted clients
	Delegate data centre's security on the cloud provider

TABLE 6. 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
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 and update them regularly
Legal requirements	Adapt some SLA clauses due to a regulation change

Throughout the service contract period, when the e-mail service migration has finished, our sample organization performs iterative Evaluate–Direct–Monitor cycles of *Task 5A* (*Cloud security operation*) with participants from corporate governance to operator users. Each of them plays his/her assigned role and follows the approved security policies. The security department effectuates continuous monitoring (i.e. secure user identification or ensuring that the computers accessing the application are virus free) and reviews the external auditors' monthly reports. The ISG committee is responsible for ensuring that every organizational department follows the newly defined security processes. Table 6 shows a sample of how ISG iterations produce modifications on security processes.

In parallel with the e-mail service operation, the sample organization develops *Task 5B* (*Communicate information security within the organization*) and prepares periodic widespread activities to maintain an active security culture. Human resources managers have detected a high rotation of doctors in some specialities, and they therefore inform the ISG committee, so that documentation to instruct newcomers on the e-mail security measures can be elaborated. The committee is also responsible for maintaining the Artefact Repository, including the security reports produced, and ensuring that every department updates its products.

Now that the service operation has finished, our sample organization is satisfied with the cloud service performance, but wishes to change its cloud provider, because some security breaches have occurred and they have not received the desirable incident response. Before the end of the contract, the ISG committee compiles the relevant documentation of all the activities, and in *Task 6A* (*Cloud service termination*), a termination report is developed with useful information for successive iterations. Taking advantage of the ISG structure established, some of the initial tasks from the next cycle are greatly simplified. The committee therefore decides to jump to the analysis tasks (second activity) and evaluate new cloud providers by additionally considering the newly discovered risks.

7. CONCLUSIONS

Cloud computing environments, like other outsourcing approaches, provide their client organizations with great benefits, but also lead to new organizational risks. These new threats need to be managed from the corporate governance level in order to achieve a security culture within the organization, thus guaranteeing risk minimization. Security governance therefore becomes a process of paramount importance, which is desirable for cloud client organizations if they intend to maintain control over cloud services [38].

Although several publications and standards concerning the security governance and cloud security fields exist, we have detected that there is no security governance framework that adequately deals with the particularities of cloud computing. The main contribution of this work is the proposal for a comprehensive ISG framework (ISGcloud) that is intimately linked with the cloud service lifecycle. The objective of ISGcloud framework is to provide practitioners with a systematic approach that can be easily followed to guarantee successful security governance, independently of the type of cloud deployment. Furthermore, it is based on security standards and published guidelines, so that existing efforts on ISG can be reused and tailored to each organization's needs.

The proposed process is founded atop of two principal standards. On the one hand, it considers four core governance processes inspired on the principles of the ISO/IEC 38500 standard (ISO/IEC, 2008): Evaluate, Direct, Monitor and Communicate. These processes are related in an iterative cycle which guarantees that security governance spreads throughout the entire organization. ISGcloud also takes into account the successive stages of the cloud service lifecycle that have been adapted from the ISO/IEC 27036 standard [22]. The ISG process is therefore divided into various activities that take place throughout the proposed cloud lifecycle.

The ISGcloud framework presented has been modelled by following the SPEM Specification [23]. This modelling allows us to provide a structured process approach that facilitates its integration with other organizational processes and its reusability. In this paper, we have included the formal definition of the ISGcloud activities and the tasks into which each activity is disaggregated. The formal definition of each task is composed of the participant roles involved in the task, the products that are expected as inputs and the resulting outputs, the steps identified to perform the task and the guidelines that can be used to help during the task development. With the proposed guidelines, we establish linking points to external standards, into which practitioners can insert the suggested standard or any other known guide. As a result, we present an open framework that can be integrated into any organization, regardless of whether it has previously developed ISG processes. If the

organization has a working security governance structure, it can also take advantage of our framework in order to successfully adapt it to the cloud services.

Although we have accompanied the definition of the activities with an example of how ISGcloud should be utilized in a fictitious organization, we plan to continue our research with a real case study. We shall continue to validate our proposal by contacting candidate organizations that intend to develop cloud services or have already deployed them, and are interested in security governance issues related to the cloud environment. By deploying our process in a real organization, we expect to gain feedback about its usability and practicality in a real cloud service. We are also working on extending the structure of the framework so that more details will be provided during the development of each task, and its components will be expanded so that we can facilitate its adoption by organizations that have no previous experience in the field. Following this line, we plan to complement the SPEM definition of the framework's activities with a supporting tool, such as EPF Composer. Such a tool would be compatible with our formal modelling and would provide automation and graphical support when developing our framework and implementing it in a real organization. Finally, it is possible to customize ISGcloud to particular organizations, such as small and medium enterprises that may wish to adopt it but lack the resources of big companies.

FUNDING

This work is partially supported by R&D project GEODAS (TIN2012-37493-C03-01) and SIGMA-CC (TIN2012-36904), funded by Ministry of Economy and Competitiveness and the Regional Development Fund, FEDER.

REFERENCES

[1] Armbrust, M. et al. (2009) *Above the Clouds: A Berkeley View of Cloud Computing*. University of California, Berkeley. UCB/EECS-2009-28.

[2] Mell, P. and Grance, T. (2011) *The NIST Definition of Cloud Computing. SP 800-145*. National Institute of Standards and Technology (NIST).

[3] Gartner. (2011) *Gartner's hype cycle special report for 2011*. http://www.gartner.com/newsroom/id/1763814.

[4] Chen, Y., Paxson, V. and Katz, R.H. (2010) *What's New About Cloud Computing Security?* University of California, Berkeley. UCB/EECS-2010-5.

[5] Hamlen, K., Kantarcioglu, M., Khan, L. and Thuraisingham, B. (2010) Security issues for cloud computing. *Int. J. Inf. Secur. Priv.* **4**, 39–51.

[6] Jericho Forum. (2009) *Cloud cube model: selecting cloud formations for secure collaboration*. http://opengroup.org/jericho/cloud_cube_model_v1.0.pdf.

[7] Lombardi, F. and Di Pietro, R. (2011) Secure virtualization for cloud computing. *J. Netw. Comput. Appl.* **34**, 1113–1122.

[8] Chonka, A., Xiang, Y., Zhou, W. and Bonti, A. (2011) Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *J. Netw. Comput. Appl.* **34**, 1097–1107.

[9] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A. and Rajarajan, M. (2013) A survey of intrusion detection techniques in Cloud. *J. Netw. Comput. Appl.* **36**, 42–57.

[10] Patel, A., Taghavi, M., Bakhtiyari, K. and Celestino, J. (2013) An intrusion detection and prevention system in cloud computing: a systematic review. *J. Netw. Comput. Appl.* **36**, 25–41.

[11] Subashini, S. and Kavitha, V. (2011) A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl.* **34**, 1–11.

[12] Muñoz, A., Gonzalez, J. and Maña, A. (2012) A performance-oriented monitoring system for security properties in cloud computing applications. *Comput. J.* **55**, 979–994.

[13] Wood, T., Ramakrishnan, K.K., Shenoy, P. and Merwe, J.V.d. (2012) Enterprise-ready virtual cloud pools: vision, opportunities and challenges. *Comput. J.* **55**, 995–1004.

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

[15] Bisong, A. and Rahman, S.S.M. (2011) An overview of the security concerns in enterprise cloud computing. *Int. J. Netw. Secur. Appl.* **3**, 30–45.

[16] Sood, S.K. (2012) A combined approach to ensure data security in cloud computing. *J. Netw. Comput. Appl.* **35**, 1831–1838.

[17] Rong, C., Nguyen, S.T. and Jaatun, M.G. (2013) Beyond lightning: a survey on security challenges in cloud computing. *Comput. Electr. Eng.* **39**, 47–54.

[18] Rebollo, O., Mellado, D. and Fernández-Medina, E. (2012) A systematic review of information security governance frameworks in the cloud computing environment. *J. Univers. Comput. Sci.* **18**(6, Special Issue on Security in Information Systems), 798–815.

[19] Fung, A.R.-W., Farn, K.-J. and Lin, A.C. (2003) Paper: a study on the certification of the information security management systems. *Comput. Stand. Interfaces* **25**, 447–461.

[20] ISO/IEC 38500. (2008) *ISO/IEC 38500:2008 Corporate governance of information technology*. ISO/IEC.

[21] Chou, D.C. and Chou, A.Y. (2009) Information systems outsourcing life cycle and risks analysis. *Comput. Stand. Interfaces* **31**, 1036–1043.

[22] ISO/IEC 27036. (draft) *ISO/IEC 27036 - IT Security - Security techniques - Information security for supplier relationships*. ISO/IEC.

[23] OMG. (2008) *Software & systems process engineering metamodel specification v.2.0*. http://www.omg.org/spec/SPEM.

[24] Rebollo, O., Mellado, D., Fernandez-Medina, E. and Mouratidis, H. (2015) Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*. 58, 44–57.

[25] ITGI. (2012) *Control Objectives for Information and related Technology (COBIT 5)*. ISACA.

[26] ISO/IEC 27001. (2005) *ISO/IEC 27001:2005 Information Technology - Security Techniques - Information Security Management Systems - Requirements*. ISO/IEC.

[27] Rebollo, O., Mellado, D., Sánchez, L.E. and Fernández-Medina, E. (2011) Comparative Analysis of Information Security Governance Frameworks: A Public Sector Approach. *Proc. 11th European Conf. on eGovernment—ECEG 2011*, Ljubljana, Slovenia.

[28] Solms, S.H.v. and Solms, R.v. (2009) *Information Security Governance*. Springer.

[29] Rebollo, O., Mellado, D. and Fernández-Medina, E. (2011) A Comparative Review of Cloud Security Proposals with ISO/IEC 27002. *Proc. 8th Int. Workshop on Security in Information Systems—WOSIS 2011*, Beijing, China.

[30] Cloud Security Alliance. (2009) *Security Guidance for Critical Areas of Focus in Cloud Computing v2.1*. Cloud Security Alliance.

[31] Catteddu, D. and Hogben, G. (2009) *Cloud Computing Security Risk Assessment - Benefits, Risks and Recommendations for Information Security*. European Network and Information Security Agency (ENISA).

[32] Solms, R.v. and Solms, S.H.B.v. (2006) Information security governance: a model based on the direct–control cycle. *Comput. Secur.* **25**, 408–412.

[33] Rebollo, O., Mellado, D. and Fernández-Medina, E. (2013) Introducing a security governance framework for cloud computing. *Proc. 10th Int. Workshop on Security in Information Systems—WOSIS 2013*, Angers, France.

[34] Cloud Security Alliance. (2011) *Security Guidance for Critical Areas of Focus in Cloud Computing V3*. Cloud Security Alliance.

[35] OMG. (2012) *Unified modeling language 2.4.1*. http://www.omg.org/spec/UML.

[36] Allen, J.H. and Westby, J.R. (2007) *Governing for Enterprise Security Implementation Guide*. Software Engineering Institute - CERT.

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

[38] Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. and Molina, J. (2009) Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. *Proc. ACM Workshop on Cloud Computing Security*, Chicago, IL, USA, 85–90.