Assurance of Security and Privacy Requirements for Cloud Deployment Models

Shareeful Islam, Moussa Ouedraogo, Christos Kalloniatis, Haralambos Mouratidis and Stefanos Gritzalis

Abstract—Despite of the several benefits of migrating enterprise critical assets to the Cloud, there are challenges specifically related to security and privacy. It is important that Cloud Users understand their security and privacy needs, based on their specific context and select cloud model best fit to support these needs. The literature provides works that focus on discussing security and privacy issues for cloud systems but such works do not provide a detailed methodological approach to elicit security and privacy requirements neither methods to select cloud deployment models based on satisfaction of these requirements by Cloud Service Providers. This work advances the current state of the art towards this direction. In particular, we consider requirements engineering concepts to elicit and analyze security and privacy requirements and their associated mechanisms using a conceptual framework and a systematic process. The work introduces assurance as evidence for satisfying the security and privacy requirements in terms of completeness and reportable of security incident through audit. This allows perspective cloud users to define their assurance requirements so that appropriate cloud models can be selected for a given context. To demonstrate our work, we present results from a real case study based on the Greek National Gazette.

Index Terms— Cloud Deployment, Security, Privacy, Assurance, Migration

1 Introduction

Migrating into the cloud certainly gives an organization tangible competitive advantages due to significant cost savings, improved degree of scalability, flexibility and resource pooling availability. Moreover, organizations can take advantage of Infrastructure, Platform or Software as a Service deployment models and a range of service models to choose from – Public, Private, Hybrid and Community. However, there are many uncertainties about the migration process, specifically related to the dependency of an outside provider for the existing business model, data usage and leakage, lack of understanding about the cloud, and many more [1,2,27,28].

Security and privacy are major concerns for organizations, which hinder cloud adaption as migrating into the cloud means organizations need to store their sensitive electronic assets into the providers' infrastructure [18]. Existing business applications and data are mostly controlled through the provider's infrastructure depending on the chosen model, i.e. Saas, PaaS, IaaS, on which users may not have full/any control. Users' data are generally stored in a multi-tenant platform. This scenario introduces extra security and privacy challenges comparing to the traditional computing environment. Lack of monitoring facility of user data incurs less user confidence on cloud based systems. Techniques to analyze the security and privacy issues in the context of cloud computing are different to those provided by the existing literature for traditional computing environments [17,18, 19]. It is therefore necessary to develop methods that not only identify and analyse security and privacy requirements but also provide certain assurance that these requirements are met by a specific cloud model before undertaking the migration decision. While such initiative have been put in place in for tradional IT based systems [8], the literature fails to provide evidence of a framework that fulfills that objective for cloud based services. This paper provides work towards this direction.

The novelty of the presented work is twofold. Firstly, it contributes to the current state of the art by providing a modeling framework that supports the elicitation and analysis of security and privacy needs, and a cloud migration process for the selection of an appropriate cloud model. Secondly, it introduces assurance requirements in the proposed framework and in the designed process and it examines their critical role during the migration process for the selection of the most appropriate Cloud Service Provider (CSP). Specifically, we use requirements engineering concepts such as goal, actor, security and privacy constrains, mechanisms and we introduce assurance requirement to obtain evidence for the satisfaction of the requirements through audit and transparency [12,13, 15, 20]. This allows us on one hand to identify and analyze security and privacy requirements and on the other hand to verify whether a chosen cloud deployment model addresses the identified requirements with appropriate mechanisms based on a specific organizational context. The framework includes a process with three sequential

- *Shareeful Islam is with the School of Architecture, Computing and Engineering, University of East London, Docklands Campus 4-6 University Way, E16 2RD, London UK. E-mail: shareeful@uel.ac.uk*
- *Moussa Ouedraogo is with the Luxembourg Institute of Science and Technology, L-4362,Esch-sur-Alzette, Luxembourg E-mail: moussa.ouedraogo@list.lu*
- *Christos Kalloniatis is with the Department of Cultural Technology and Communication, University of the Aegean, Mytilene, University Hill, GR-81100, Lesvos, Greece Email. chkallon@aegean.gr*
- *Haralambos Mouratidis is with the School of Computing Engineering and Mathematics, University of Brighton, Watts Building, Lewes road, Brighton BN2 4GJ. Email: h.mouratidis@brighton.ac.uk*
- *Stefanos Gritzalis is with the Department of Information and Communication Systems Engineering, University of the Aegean, 2 Palama St., Karlovassi, Samos, GR-83200, Greece,E-mail: sgritz@aegean.gr*

activities so that requirements can be extracted from real migration needs and appropriate cloud models can be selected to support these needs. We demonstrate the approach with a real case study based on the Greek National Gazette system. The results prove the efficiency of the approach on identifying respective security and privacy needs as well as the proper selection of a cloud deployment model based on these needs.

2 Related Works

This section presents a brief overview of works, presented in the literature, related to three main areas of our work, security and privacy issues, migration and audit in cloud environments.

Security, Privacy and Migration Issues in Cloud

Security and privacy issues are amongst the most important concerns in cloud computing. Several surveys among potential cloud adopters indicate that security and privacy is the primary concern hindering its adoption [1]. Cloud specific security and privacy threats such as insecure API, data leakage, insecure data deletion, session or service hijacking, malicious insiders should be controlled in a proactive way [9,18,22]. Similar to traditional computing environment, Attacks such as man-in-the middle, and Trojan are also potential attack for cloud computing [23]. These threats are due to multi-tenancy support, lack of control and secondary usage and users' universal accessibility through public network. Privacy threats differ depending on the type of cloud scenario and threats such as lack of user control, potential unauthorized secondary usage, data proliferation are more dominate in public cloud [17]. Attackers can also exploit data duplication technique to access customer data by obtaining hash code of the stored file [25]. In [26], privacy risks are considered from cloud, user, stored data and data access perspectives and highlight some mechanism for addressing the risks from these perspectives. There are works that focus on cloud migration decision. For instance a cost, benefits and risk tool is proposed by [27] to support the public IaaS cloud migration decision. Security issues are analysed for model based migrating oof a legacy system into cloud by [24]. A systematic literature review on cloud migration research is performed by [28] and results show that there is a lack of work focusing on a comprehensive decision framework for cloud migration taking into consideration requirements, feasibility study, migration strategy, execution, evaluation and cross cutting concerns. In [29], it is observed that companies wishing to migrate lack of proper ways for conducting an in-depth analysis in order to understand rationalization for migration and best possible time for migration. It is vital to understand the security, privacy, and other releated migration issues and control should be in place to address the threats and risks that arise from the issues.

Cloud Related Standards and Audit

The increasing demand of cloud computing emphasizes the ncecessity of developing standard to provide detailed guideline and recommendations for both CSP and cloud users. The National Institute of Standards and Technology (NIST) propose a standard for security, interoperability, and portability for the potential cloud adopters as target audience [5]. The standard includes a list of strategic and tactical requirements for a cost effective easy migration. The cross cutting security requirements mainly deal with identify management, security audit information, encryption, and physical security. Cloud Security Alliance (CSA) identifies sixteen control domains and provides a cloud control matrix framework by mapping it with relevant industry standards such as ISO 27001 [6]. The control matrix includes several control objectives relating to compliance and audit, data governance, security policy, access control, HR security, security management, risk management and security architecture to strength the overall information security environment of CSP. The Federal Risk and Authorization Management Program (FedRAMP) is a standardized framework for the security assessment, authorization, monitoring cloud based services and product [19]. The standard ensures that adequate security controls are in placed by the CSP to safeguard the users' migrated assets into cloud system. The framework includes a four process areas, i.e., document, assess, authorize and monitor. The potential CSP need to select, implement, and document FedRAMP security control so that an independent assessor confirm that the controls are effectively implemented for generating authorization document. Finally, a continuous monitoring needs to be taken place if the CSP is authorized by the FedRAMP.

While the efforts aboved reviewed including FedRAMP are very effective in providing support to the future cloud users, with respect to selecting a suitable and secure offering for their service migration, our contribution comes as a complementary support to companies faced with uncertainty about whch of the deployment model (private, Public, communauty or hybrid) would better suit their service, data or processes.

Audits in the cloud are meant to provide a third party independent assessment of the posture of the security used by the CSP. It represents a means through which a given cloud user may be able to review and/or keep an eye on a security matter that has been to some extent devolved to a third party [2]. Because multi-tenancy allows several customers to be hosted on the same underlying infrastructure, traditional audits and reviews of a user to provide the expected level of assurance becomes less practical [3]. The SAS70 [4] was a standard audit approach for service companies to use with their customers instead of customers individually auditing the companies' services. The actual purpose of the standard was two-fold: assess the sufficiency and the effectiveness of the security controls of the CSP. The standard was superseded by SSA16, which stands for "Statement on Standards for Attestation Engagements No. 16". One core difference between the two standards rests on the fact that the evaluated company is bound to provide a written statement about the accuracy of the description of their

system and the corresponding time frame during which such an assessment has been made.

Some initiatives for monitoring and auditing the cloud have also emerged in the recent year. The authors in [7] have proposed an event-driven approach for the automated audit of cloud based services security. Dedicated algorithms for the detection of composite events (anomalies) specified by either the CSP or CSC while primitive events structure is based on XCCDF format to ensure the reuse and interoperability with some existing security audit tools. In recent years, works relating to accountability in the cloud have started to emerge. For instance, in A4CLOUD [9] project researchers are thriving to devise models that can help put in place the set of mechanisms to ensure that cloud providers are accountable for any SLA breach or a security incident that emanated a lax in their security. A federated cloud monitoring infrastructure is introduced by [21], to monitor where data is actually saved without compromising cloud isolation by collaborating among infrastructure provider, service provider and cloud consumers. As stated previously, CSA control matrix also emphasizes compliance and audit of the related objectives.

In summary, works on security and privacy issues on cloud have mostly been focused on identifying security/privacy specific threats and risks and mechanisms for controlling these risks. NIST standard provides useful security information for potential cloud users for considering cloud migration. However, it does not provide any guideline on how such requirements should be checked by the cloud users and how migration decision is supported. Moreover, it is really difficult to implement some of the requirements in real context such as sending security data to the consumer on a regular basis. Requirements relating to security audit information do not consider the transparency of data access and usage, which is critical for cloud based context and security requirements relating to disaster recovery and business continuity are not taken under consideration. CSA also provides a comprehensive up-to-date guidelines for the cloud provider overall information management system. However, very limited works have been taken in place for analysing security and privacy requirements from the organization setting and migration desire and lack of consideration to assure these requirements from the CSP perspective. Audits themselves cannot ensure the required levels of trust for an organisation that decides to move part or the whole of its resources over the cloud. Our work intends to fill the gap of the current state of the art by presenting a novel framework that combines security and privacy requirements with the assurance requirements so that appropriate cloud deployment model could be selected to support the user real migration needs. Furtheremore, this work can also complementary support the cloud standard such as FedRAMP for choosing the approipriate deployment models based on the requirements.

3 Proposed Framework

3.1 Modelling Language

The novelty of the proposed modeling language is the fact that it combines concepts from the requirements engineering, cloud computing, security, privacy and auditing domain. It uses new concepts such as cloud user, cloud service provider, audit, and mechanism, which are necessary to elicit and analysis of requirements and checks evidences to support these requirements based on organizational context. The metamodel of the language defines all concepts.

The central concept of the proposed language is that of an actor, which represents an entity that has strategic goals and intentions within a system or an organisational setting [10]. An actor can be human, a system, or an organisation. In our case, organization, cloud user and cloud service provider are three different types of actors. A cloud user actor can be individual or organization who needs cloud service and deployment model to support its specific strategic goal and intention. A cloud service provider actor has two unique properties, i.e., service and deployment model to support the cloud users. The actor organisation context considers the scope of the organizational entities such as goal, services, and infrastructure and includes migration needs into cloud that should be supported by a cloud service provider.

Vulnerabilities are defined as weaknesses or flaws existing from an actor and its surrounding environment, in terms of security and privacy. Cloud specific vulnerabilities can arise from cloud service provider's infrastructure and technology such as virtualization, data segregation, software environment, and computational resource or from the cloud user context. Vulnerabilities are exploited by threats, as an attack or incident within a specific context. The cloud specific threats can be of different types related to security and privacy, such as provider data misuse, data leakage, virtual machine (VM) replication, and unavailability of data, insecure storage, and DoS. For instance, an actor can exploit a virtualisation vulnerability to access other VM instance of same physical machine [11]. Such attack is associated with the computing resources on the IaaS level and may happen in all deployment models. Vulnerabilities and threats can pose potential security and privacy risks for the system.

Actors within the system environment have single or multiple goals based on specific roles and interest. A goal represents an actor's strategic interests [12]. Higher level strategic goals may be decomposed in simpler operational goals forming AND/OR goals hierarchy. Our language differentiates between organizational, security and privacy goals. Organisational goals represent goals that are important at organizational level and one or more actors belonging to the same organization need to fulfill. We consider cloud migration goal within the organizational goal. Security goals support security needs such as confidentiality, integrity, availability while privacy goals support privacy needs such as anonymity, pseudonymity, unlinkability and unobservability [13, 14].

These goals introduce requirements on the system that support the actor needs within the system and its surroundings [15]. Requirements are the conditions or capabilities needed within the system environment to control the actors or to fulfill the goals. When a requirement is introduced, further analysis is required to establish if and how that requirement can be satisfied. Security, privacy and assurance are three different types of requirements in our case. These requirements support the actors' security and privacy needs for the satisfaction of the goals such as requirements on confidentiality of the data at rest, requirements on integrity while data on transit, or requirements on user anonymity. Assurance requirements in the context of cloud-based systems are evidences to support the completeness and stringency of the mechanism and satisfaction of security and privacy requirements. We argue that the keys to promoting assurance in cloud based systems includes establishing the completeness of the mechanisms to fulfilling the identified requirements; and performing frequent or continuous audit to ensure such mechanisms remain in a desirable state. Similar to the security and privacy requirements, a cloud user can define their assurance needs as expectations from the cloud, such as cloud user can expect for a safe, transparent or trusted cloud.

Assurance requirements motivate an audit for collecting evidence. An audit defines mechanisms to check the completeness of requirements and associated mechanisms and identifies vulnerabilities through transparency of disclosing security incidents. Audit in a cloud infrastructure is specifically important for generating evidence related to providers' support for the effectiveness of security and privacy and compliance with other regulatory issues. In addition to conducting and reporting on audits findings, frequent and timely reports of security and privacy incidents occurring within the cloud based service to the concerned users, so that prompt action can be taken, is another salient dimension of assurance. Finally, we consider mechanism that needed to be implemented to support the identified requirements. Therefore, a mechanism is mainly defined as a technical solution to support the requirements for preventing any threats and vulnerabilities. Examples of mechanisms are data isolation, access control or provenance.

As can be seen in Fig.1, an actor has goals and security and privacy requirements support the actor's desire. Assurance requirements motivate the audit. Audit checks the completeness of requirements and mechanisms by gathering the necessary evidence to support the possible alignment between what is actually implemented as security and privacy mechanisms within a given deployment model and checks the security incident through the vulnerabilities. Note that completeness check is an offline activity that takes place with the support of some security and privacy requirements.

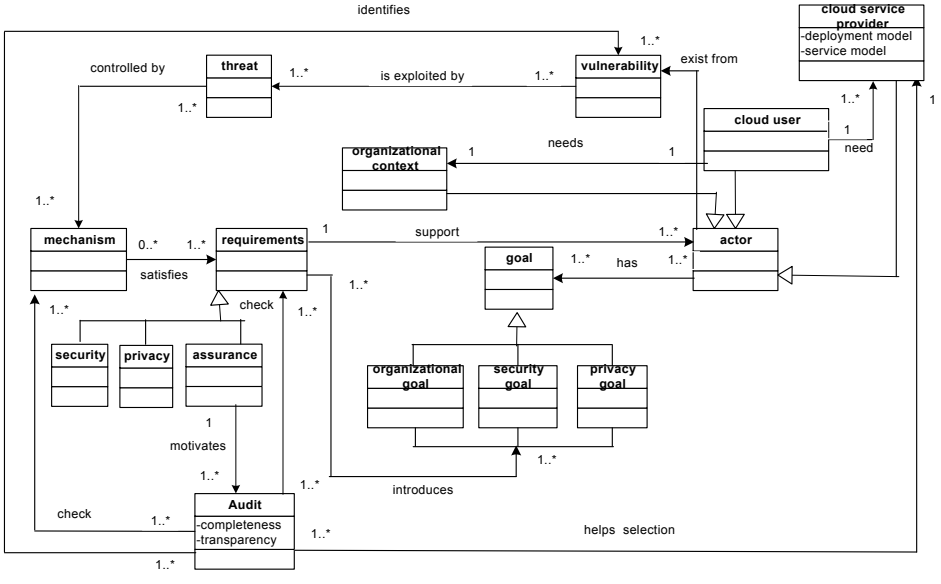

Fig 1. Conceptual Meta Model

The audit and incident report are performed based on the existing CSP available published reports and policies and during the usage of service resources. The aim is to ensure that any threats and vulnerabilities that may emerge in the future are identified and promptly addressed.

3.2 Process

In order to allow for the systematic elicitation of security and privacy requirements, along with evidence to support their satisfaction through assurance activities, we have tailored a process based on the underlying concepts depicted in Fig.1 and discussed in the previous section. Ultimately, such a process will have the metric to assist in the selection of the appropriate deployment models that satisfies at best the security and privacy expectation of the cloud consumer. In particular, the process supports the understanding of specific organisational needs for cloud migration and consists of three iterative activities: organizational analysis, security and privacy requirements analysis, and finally, security and privacy assurance analysis. Fig. 2 depicts the activities, steps, and the resulting artefacts of the proposed process using OMG stan-

dard Software & Systems Process Engineering Metamodel (SPEM) version 2.0. SPEM allows creating a flexible process model as well as supports a concrete description of the process.

Activity 1: Define Organisational Context

This activity initiates the whole process by identifying relevant cloud user organizational entities, security and privacy goals and cloud migration needs. Organizational senior executives/business managers' active involvement is necessary for performing the steps within the activity.

Step1.1: Organisational Entities Identification

This step aims to understand the current organisational structure based on the identification of entities such as actors, organizational goals, plans, and resources. It is important to note that the extent of the identification of entities depends on the extent to which the organisation aims to consider migration to the cloud. For example, if only one service of the organisation is considered for migration, for instance the data storage service, then identification of entities relevant to that service would suffice. On the other hand, if a full migration is considered then the identification should include all organsation's entities both internal and external that might affect the migration.

Step1.2: Security and Privacy Goal Identification

Once the organisational entities for cloud deployment have been identified, the next activity involves the analysis of security and privacy needs related to the organisational cloud deployment needs. Security and privacy needs are identified based on the security and privacy goals that the organisation has. Security and privacy policies are very important for the goal identification. Relevant laws and regulations can also be considered to support identification of security and privacy goals. Note that the aim is not to "blindly" use any security and privacy goal that the literature has captured but to identify those that are relevant to the organisational parts that are considered for deployment to the cloud.

Step 1.3: Cloud Organisational Needs

This step aims to identify explicit organisational structures, services, application and data that should be deployed in the cloud. For example, if a data storage service is to be migrated, the exact details of whether the whole data of a specific application or just fragments of data should be deployed in the cloud will be identified at this step. To support such identification, the organisation needs to consider how such deployment would affect the organisation internally, for example whether existing policies, roles and responsibilities and the organisation's business strategy would need to be modified; how such change might affect (positively or negatively) customer handling and customer services; and develop a clear understanding of the benefits and limitations of such deployment.

Activity 2: Security and Privacy Requirements Analysis

During this activity, the identification and analysis of the respective organisation's security and privacy requirements is conducted. Security manager and internal audit (if any) are mainly involved for this activity. Two steps and two respective outcomes are defined, the Security and Privacy requirement identification and deployment scenario description.

Step 2.1: Security and Privacy Requirements Identification

Once the relevant security and privacy goals and cloud migration needs have been identified, an elicitation and analysis process for security and privacy requirements is employed. We base our analysis on the concepts of security and privacy requirements, defined in the presented metamodel, to enable developers to adequately capture security and privacy requirements. Security and privacy requirements are elicited considering organisation entities such as organisation goal, actors, cloud migration needs, threats and vulnerabilities. Moreover, organisational specific document such as organisational policies, goals, and business processes, external sources (such as laws and regulations, possible external threats identified), and relevant technological restrictions based on the technology used (such as constraints that might be unique for cloud computing environments) can also be used to elicit the requirements. The identified requirements are analysed based on the potential threats and vulnerabilities of the CSP surface and its surrounding environment. Therefore, this step also includes identification of threats and vulnerabilities to analyse the requirements for further refinement. It is also worth noting that security and privacy requirements are the same irrespective of specific cloud deployment models.

Step 2.2: Deployment Scenario Description

During this step, a deployment scenario is identified and described. The description is based on information related to the deployment model to be used, the hosting model, the relevant services and resources to be deployed along with the available security and privacy mechanisms. Relevant information is documented using the deployment model selection template:

a) *Deployment Scenario Type*. A specific type of deployment model is identified. In particular, the following deployment models can be selected: Private, Public, Hybrid, and Community.

b) *Actors Involved*. The specific actors such as cloud user and CSP involved in the specific scenario are listed.

c) *Hosting Type*. The hosting type is specified. Options include: On-premises, where the cloud is hosted within the Organisational firewall; Third-party location, where the cloud is hosted outside the Organisational firewall.

d) *Organisational and Migration Goals*. The organisational and migration goals identified in the previous activity, relevant to the scenario, are listed.

e) *Security and Privacy Requirements*. The identified requirements from the previous step that are relevant for the scenario context add in the template.

f) *Security and Privacy Mechanisms*. The mechanism identification takes as input the security and privacy requirements and possible vulnerabilities and threats defined in the previous activity. The associate mechanisms available for a given deployment scenario and those security and privacy requirements of the cloud user addressed are mapped. Note that, some mechanisms support both secu-

rity and privacy requirements such as access control where as others are specifically designed for security or privacy requirements such as VM anonymizer to support anonymity of user activity in the cloud. The outcome of the mapping between security and privacy requirements and the mechanisms available for each deployment is fundamental for undertaking the security and privacy assurance analysis following.

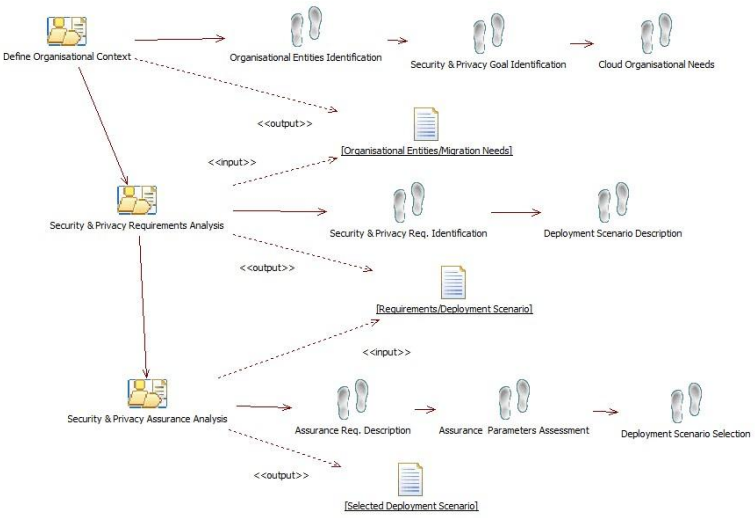

Fig. 2. Proposed Process

Activity 3: Security and Privacy Assurance Analysis

This final activity aims to obtain evidence for the completeness of requirements to align with the assurance needs and select the appropriate deployment for the identified context. Mainly security manager, auditor and CSP involvement are necessary for performing the steps within this activity. However, senior executives should also be involved for undertaking the final deployment scenario selection.

Step 3.1: Assurance Requirements Description

During this step, assurance needs are defined based on the identified security and privacy requirements and mechanisms to satisfy these requirements. In particular, cloud users should define the level of security and privacy requirement she would like to fulfill, the level for audit she will wish to perform on the delocalized service and finally if she requires to be notified in case of incident at the CSP's infrastructure. An assurance requirement can thus be expressed as the triplet (Completeness, Auditable, Reportable) as shown below in an XML format:

```
<Completeness>..<\Completeness>
 <Auditability>..<\Auditability>
  <Reportable>..<\Reportable>
```

Step 3.2: Assurance Parameters Assessment

This step assesses the assurance parameters by collecting the evidence from the CSP resources. Therefore, the requirements are checked for completeness and relevancy for a specific cloud model. Evidence of completeness can be gathered through an audit conducted by (on behalf) of the user or through such certification as CSA STAR achieved by the CSP. Given that different types of cloud deployment model provide different security levels, decision to adopt either of these models should be done through due consideration of the user's assurance requirements. Assessment of completeness involves verifying whether all or most of the security and privacy requirements are addressed by existing mechanisms within the various cloud deployment scenarios proposed. Such an evaluation will use the information emanating the first two steps of the second activity. After such an evaluation the following assessment results can be attained (also shown in Table 1): a) *SA_COM.1:* None of the key security and privacy requirements are met by the security mechanisms available for the deployment model, b) *SA_COM.2*: The key security and privacy requirements are only partially observed by the security of the deployment model. And c) *SA_COM.3:* All the key security and privacy requirements are fulfilled by the security of the deployment model. Alternatively, the above specified levels can be defined in the following way:

Let:

f_i: a key functionality of the security mechanism

h_j: A verified functionality of the security mechanism during the verification

N: the number of key functionalities

N′: the number of functionalities verified

F: the set of key security requirements defined in a reference (standard, regulation, or other policies relevant to the CSC).

$$F: (f_i)_{1 \le i \le N}$$

H: the set of security requirements covered by the CSP's security controls.

$$H: (h_j)_{1 \le j \le N}{}'$$

Similar to the Completeness check, the audit further includes auditable metrics for assessing the model. The importance of this feature lies on its potential to allow one to get information on the status of the security and privacy but also drive the revision of them in view of addressing potential vulnerabilities that may emerge with time. A

cloud service, which security verification process is assessed at Level 5 (SA_AUD.5), provides enough guarantees of independent opinion about the status of the security it claims.

Completeness capability levels	Completeness Capabilities definition	Short Description: What portion of the key security requirements is covered by the CSP's security?
SA_COM.1	$\{ A\_j, h_j \notin F,\ 1 \le j \le N' \}$	**None**
SA_COM.2	$\{ \exists i,\ f_i \notin H, 1 \le i \le N$	**Partial**
SA_COM.3	$\{ \_ j , h_j \in H, F \subset H$, and $1 \le j \le N'\}$	**All (Complete)**

Table.1 Description of the Completeness metric

Moreover, the conducted verification is comprehensive enough to reflect the true posture of the security and privacy and the timely manner in which the existing vulnerabilities are detected, allows for corrective actions to be promptly applied. At Levels 3 and 4 (SA_AUD.3 and SA_AUD.4), though the verification can be conducted by an independent third party that follows a well-structured process, there is an element of caution as not all relevant parts of the security and/or privacy are probed. The lack of a structured approach cumulated with the lack of an independent third party review of the security and privacy, make the lowest levels 1 and 2 (SA_AUD.1 and AU_AUD.2), not conducive of some good practices.

The above audit levels are matched to a set of minimum requirements needed to satisfy them, for the auditability metric as shown in the matrix below. In another word, *an audit V satisfies auditability level k if all the parameters (Coverage, depth, rigor and independent verification) capabilities for V are greater or equal to the corresponding parameters for k. Alternatively, V will be assessed at level (k - 1).* Table 2 provides the minimal requirement for achieving each auditability level.

Class	Quality Family and Meaning	SA_AUD				
		1	2	3	4	5
QAM: Security verification process Quality Metrics	**QAM_COV: Coverage.** Larger coverage of the verified security mechanism provides more confidence on the results about its status.	1	2	2	2	3
	QAM_DPT: Depth. A detailed verification of the security mechanism will decrease the likelihood of undiscovered errors.	1	2	2	3	4
	QAM_RIG: Rigour. The more structured the evaluation of the deployed security mechanism, the more reliable the outcome of the verification.	1	2	2	3	3
	QAM_IND: Independence of verification. Verification performed by a third party evaluator or a software tool provides more assurance.	1	1	2	2	3

Table 2- The auditability metric levels and associated components

Such requirements for auditability are based upon:

a) *The Coverage of the verification:* Coverage is defined as the extent to which the set of functionalities of a security mechanism that are relevant to the security of the CSC (hereafter referred to as the key functionalities) can be vetted during the verification. The coverage family is composed of three ordinal levels, which are formally described are provided below. The coverage family of the auditable metric bears some similarity with the completeness metric previously discussed. Though, the actual scope of application differs between the two metrics. Indeed, while the completeness metric is used for determining how much of the requirements specified in a standard, regulation or policy are carried out by the CSP, the coverage metric helps to determine whether functionalities of the security mechanism, considered as paramount in the protection of the cloud service, have been probed. The same applies for privacy mechanism respectively. Table 3 provides the formal definition associated to the coverage capability.

Let *F: the set of key functionalities of a security mechanism defined in its documentation,*

H: the set of functionalities verified during the verification

f_i*: a key functionality of the security mechanism*

h_j*: A verified functionality of the security mechanism during the verification*

N: the number of key functionalities

N': the number of functionalities verified during the verification

$H: \{ h_j \}_{1 \le j \le N'}$

$F: \{ f_i \}_{1 \le i \le N}$

Coverage capability levels	Coverage Capabilities definition	Short Description: What portion of the key functions is covered by the verification?
QAM_COV.1	$\{ \forall j, h_j \notin F,\ 1 \le j \le N' \}$	**None**
QAM_COV.2	$\{ \exists i,\ f_i \notin H, 1 \le I \le N \}$	**Some**
QAM_COV.3	$\{ \forall j , h_j \in H, F \subset H$, and $1 \le j \le N'\}$	**All**

Table 3 formal definition associated to the coverage capability.

b) *Depth of the Verification*: The Depth metric is a finer refinement of the Coverage metric as it helps frame the extent in which a key functionality of a verified security mechanism is probed. Each of the key functionalities of a security mechanism has security properties that should be observed for the mechanism to fulfil that function. For instance, a firewall traffic filtering function would require a stringent set up of properties relating to packets that can or cannot get in or out of the system perimeter. Similarly, the auditing function of the firewall would require properties for recording any violation or attempted violation of the rules set.

Unlike the coverage metric, which has been subdivided into 3 capability levels, the depth metric involves four capabilities levels. One of the reason this occurs is that although the key functionalities of a verified security mechanism are often known, lower level properties which condition the well functioning of the latter may not be known in entirely by those conducting the verification. A formal documentation, which provides a comprehensive description of the mechanism, is often needed.

The key functionalities F can now be represented as:

$$F: \{ f_i(p_{i,1}p_{i,2} ..p_{i,k}) \}_{1\le i\le N}$$

Subsequently the set of key properties for a security or privacy mechanism with "N" key functionalities having each a "K" variable number of key properties is represented as:

$$P: \{p_{ij},\ 1\le i \le N,\ 1\le j \le K\}$$

Although the key functionalities of a mechanism are generally known by the user or security expert as per its nature, the level of details regarding the atomic properties inherent to its well-functioning may not all be known to the user or the security expert. Consequently the existence of a "formal document" detailing the key properties of the mechanism, either security or privacy, plays a major role in the elucidation of the depth family. We therefore define the following predicates DOCUMENT (D) to signify that the set of properties are clearly defined in a formal document.

Let Q: {qm,n} 1≤m≤N, 1≤n≤Z, be the set of properties verified for the mechanism during a verification process. The depth capabilities are defined in Table 4

Depth capabilities levels	Depth Capabilities definition	Description: What portion of the known key properties of the SM is verified?
QAM_DPT.1	{ ¬DOCUMENT (D), ∃ (m, n) $q_{m,n} \in Q$}	**Unknown**
QAM_DPT.2	{DOCUMENT (D), ∀ (m, n) $q_{m,n} \notin P$}	**None**
QAM_DPT.3	{ DOCUMENT (D), ∃ (i, j) $p_{i,j} \notin Q$}	**Some**
QAM_DPT.4	{DOCUMENT (D), ∀ $p_{i,j} \in P$, ∀ $q_{m,n} \in Q$, $P \subset Q$}	**All**

Table 4- Formal definition of the Depth

c) *Rigour of the verification*: Rigour of verification refers to the maturity of the verification process, i.e. whether it follows a systematic process and how sophisticated the means of verification is. Reliance on a mature process for the verification is relevant for a comprehensive verification that cannot always be guaranteed when relying solely on the individual expertise of those conducting the verification. Three levels for the rigour metric have been defined as depicted in the table 5 below.

Rigour capabilities levels	Rigour Capabilities definition	Rigour capabilities description:
QAM_RIG.1	The verification is undertaken without following a systematic procedure.	**Informal**
QAM_RIG.2	Semi-structure verification: A clear verification procedure exists for the verification but the means of verification is informal (e.g. Manual)	**Semi formal**
QAM_RIG.3	The verification process is structured and follows the requirements within a verification documentation or a standard; and is performed by a software tool, formal verification means etc.	**Formal**

Table 5. The levels for the Rigour capability

d) *Independence of verification*: Verification performed by a third-party evaluator, or software tool provides more assurance than a self-assessment does. Indeed, conducting some assessments of a security or privacy mechanism is a very relevant task in the management of security, but more so when the goal is to sway a client on the adequacy of one's security and privacy. Three levels of capabilities exist for the independence of verification metric. To help elucidate the different capability levels for the QAM_IND family, let us consider the following:

I_d: The set of individuals who participated in deploying the security mechanism

I_v: The set of individuals who verify the security mechanism

$I_{v,i}(q_{m,n})$: Individual "$I_{v,i}$" verifies property n for functionality m ($q_{m,n}$ having been defined in the coverage section)

Based on the above, independence of verification is here defined as the intersection between the set of individuals who were involved in the mechanism's deployment and those undertaking the verification i.e. QAM_IND: Id ∩ Iv. The capabilities for the QAM_IND family are as shown in Table 6.

After completeness and auditability assessment, the final part of assurance assessing is through reporting of security and privacy information and incidents to the CSC, pertains to the level of transparency offered by the CSP. Two levels have been defined in relation to this metric.

Independence capabilities levels	Independence of verification's Capabilities definition	Verification process description
QAM_IND.1	{∀ m, ∀n, ∀ i ; $I_{v,i}(q_{m,n}) \Longrightarrow I_{v,i} \in I_d$} $I_v = I_d$ $I_v \cap I_d = I_v = I_d$	**Self-assessment**
QAM_IND.2	{∀ m,∀n, ∃ i $I_{v,i}(q_{m,n}) \Longrightarrow I_{v,i} \in I_d$} $(I_v \cap I_d) = I \subset I_d$	**Partially**
QAM_IND.3	{∀ m, ∀n, ∀i , $I_{v,i}(q_{m,n}) \Longrightarrow I_{v,i} \notin I_d$} $I_v \cap I_d = \emptyset$.	**Totally**

Table 6. Formal definition of the Independence of Verification

The first of such levels, SA_REP.1, depicts a cloud whereby; no information on the security is actually communicated to the users, a case of non-transparency.

The second level SA_REP.2 relates to a cloud service said to be transparent security or privacy wise, as the relevant information relating the security and privacy is shared with each of its CSC depending on the contractual clause between the two. Detailed information on both the Audit and the Reporting metrics can be found in [2].

The table 7 summarises potential assurance requirements from cloud users using the three criteria, along with the denomination for cloud services depending on the results on the values for assurance parameters. Trusted cloud is the most desirable once with the highest level of completeness, auditable and reportable. However, in many cases it is hard to achieve. User can also desires to have a safe, auditable or transparent cloud and not desire unsafe or non-transparent cloud.

Step 3.3: Deployment Scenario Selection

In this step, we will seek to leverage on that body of information for making an informed choice of a cloud deployment model. Four cases can be envisaged based on the requirements for SA defined in table 8. Note that, we consider the first four requirements as the realistic to be

Completeness (C)	Auditable (A)	REportable (RE)	CLOUD SERVICE DENOMINATION
3	X	X	SAFE CLOUD
X	5	X	AUDITABLE & ADAPTIVE
X	X	2	TRANSPARENT
3	5	2	TRUSTED CLOUD
1OR2	X	X	UNSAFE CLOUD
X	1 OR 2	X	SELF_ASSESSED CLOUD
X	3 OR 4	X	INDEPENDENT BUT INCOMPLETELY ASSESSED CLOUD
X	X	1	NON-TRANSPARENT CLOUD
Legend: X	Any Assessed value for the criterion		

Table 7. CSC's assurance requirements and denomination for cloud services

CSC ASSURANCE REQUIREMENT			CLOUD DEPLOYMENT MODEL		
Completeness C	Auditable A	REportable RE	Private	Community	Public
3	--	--	OK	OK	OK
--	5	--	OK	OK	--
--	--	2	OK	OK	--
3	5	2	OK	OK	--

Table 8. Matching CSCs' assurance requirements with cloud deployment models

expressed by a cloud user while seeking to make a decision about choosing cloud deployment scenario. As such, if the cloud user requirements for assurance points focus on "safe cloud", private or community could be the most suitable one. In particular, such requirement can be best supported by the private or community cloud setting given the involvement of the user in its adaption actions and operation of the migrated entities. Nonetheless, a public cloud that could demonstrate fulfilment of such requirement through its certification or through other relevant evidence can still be a solution to the user.

The same applies for assurance requirement that indicates the need for a "Reportable cloud". Indeed, the ideal deployment model would be either a private or community cloud. However, should a pubic cloud owner, under legal clauses with the user, agree to inform the latter of any security incident on the infrastructure that may have replication on the user's application, processes or data, a public cloud deployment can still be envisaged. But in real cases there are examples that highlight the fact that CSPs are generally very reluctant to provide an accurate picture about incidents involving their infrastructure. Users requiring a "trusted cloud" a private or community cloud deployment model is advocated as this could provide the environment for audits, selection of controls that meet all salient security and privacy requirements and the ultimate awareness of the CSC in the event of a security breach. Table 8 summarises the matching cloud user assurance requirements with deployment models. Although the individual assurance parameters can suffice to form a judgement on deployment scenario type, we could image a situation whereby a set of security and privacy requirements set by the user through the provided activity of the process requires some trade off before decision making. Importantly the cloud model will be considered against traditional ones only when the benefit (including security and privacy) overweight the alternatives. As such in the event that no deployment has been considered as adequate for a given company, the implication is that there is no urgency for a quick migration to the cloud.

4 Case Study

We have applied our work on a case study along with action research to demonstrate the applicability of the proposed framework. Action research makes an effort to provide practical value of real subject problems while simultaneously contributing to the acquisition of new theoretical knowledge [16]. The framework is applied on a real study context of the Greek National Gazette (GNG). The main aim of this study is to determine the applicability of the framework in a real organizational context.

4.1 Study context

The main authority of the GNG is to publish laws and other legal decisions on the Greek Government's Newspaper in order for these laws and decisions to be active and applicable. In 2010, the National Gazette decided to provide a service for electronic submission of the manuscripts sent for publication. The whole process starts when a document is sent by a public/private sector organisation/company to the GNG.

The first step of this process is the categorisation and scanning of the document. The next involves the assignment of the unique ID to the document depending on private or public sector organisation and registers to the National Gazette's (NG) information system by transforming from hard copy to electronic version (usually .DOC formats). Every electronic document is going to be included in the respective issue under development based on the categorisation conducted before. With the use of specific software all available documents are combined and a draft issue is exported. Qualified employees format the issue manually until it gets its final form. In this stage an integrity check of issue's content is also conducted for verifying that no unauthorised changes have been made on every document included for publication in the respective issue. Then, the issue is signed by the general secretary of the NG and is send to the Government's General Secretary for approval before proceeding for publication. When the issue is approved for publication a new identification number is assigned on the issue, which basically stops being an issue and becomes a paper volume with a specific volume_id along with a date and the number of pages the specific volume is formed of. Before proceeding on the printing phase a final integrity check is again conducted. After the final acceptance a pdf file is created with a digitally unsigned version of the volume. Finally, this version is again checked for any mistakes in the context or the format of the text and after that it is formatted

with the respective logos and labels and is digitally signed by using RSA 128 bits algorithm, forming the final version of the document. Finally, the digitally signed version of the volume is uploaded on the National Gazette's portal with free access to all Internet users.

4.2 Introduction of the process

Activity 1: Define Organisational Context

The first step of the first activity is to analyse the organisation and identify the entities involved in the migration services.

ACTORS

We consider GNG as an organizational actor and several stakeholders are potential cloud user actors. These are: *a) Public/Private Organisation Actor*, which represents any public or private organisation that sends documents to the GNG; b) *GNG Employee*, which represents an individual who works for the GNG, including the General Secretary, who is responsible for signing GNG issues; c) *Government General Secretary*, who is responsible for approving the issues; d) *Publishing System*, which represents the information system used to support the publication process; e) *General Public*, which represents any citizen wishing to access the Volumes (printed issues).

ORGANIZATIONAL GOALS

We focus on the goals based on the specific actor's interest as shown in the following bullet points: *a) Public/private Organisation Actor:* Publish Decisions and Bills; Provide Document; Format Document; Approve Document. *b) GNG Employee*: Support the creation and publication process of every issue for the Greek Newspaper and approve GNG issues by conducting final integrity and format checks. *c) Government General Secretary:* Approve GNG Issues for publication. *d) Publishing System:* support publication process. *e) General Public:* Read Newspaper of the Greek Government.

For instance the main goal of the Publishing System is to support the publication process. In supporting that goal, the Publishing System actor has to receive the document, categorise the document, validate it, and publish it as part of a specific volume.

SERVICES

From the above analysis we can also identify a number of services related to the GNG's publication process: *a) Receive documents, b) Categorise and Identify documents, c) Transfer documents to Electronic Form (if necessary), d) Check and Validate Electronic Document, e) Create issue (Draft Volume), f) Publish Volume and g) Make Volume available to general public.*

INFRASTRUCTURE

The GNG IT infrastructure supports the following: Automated management of the Issue & Volume Composition; Work Flow Management; Internal – Administration Services; Internet Services. Workflow Management developed with the Zone/ platform and is responsible for the proper collaboration of the various components on the platform. Internet service is based on Adobe InDesign software is being used in order to automatically create the final electronic version of the Volume after it has been printed in its final form

SECURITY & PRIVACY GOALS

To support the organizational goals identified previously, the main security goals identified are *Confidentiality, Integrity and Availability. Preservation* of integrity is vital since any unauthorised alterations on the articles may create great law gaps in Greek Government since any article published in the NG's paper is immediately applicable from any third party in Greece. So integrity of the published articles is of vital importance in National Gazette. For the same reasons *availability* of the online services is also important since all Greek citizens, companies, public services etc should be able to download at any time the current legislation and all the respective decisions published in the NG's paper. Finally, *confidentiality* should also be protected for the NG's users as well as for the published documents.

Regarding privacy, the goal identified was *unlinkability* goal. Specifically, users accessing and downloading volumes should maintain their privacy regarding the volumes they are interested in and thus unlinkability between the users and the downloaded volumes should be satisfied in the NG's online system.

CLOUD ORGANISATIONAL NEEDS

The potential services that could be migrated to the cloud and respective migration goals are given below:

Migrated services: Receipt of the Documents, the Publication of the Volume. Migrating these services to the cloud is important and necessary since these services are the most demanding and vital services. Through these services GNG supports public and private organizations and the citizens, while the rest of the services are mostly internal services regarding the publication of the documents. Currently, receiving the documents is based on a server that has to be active constantly, which creates many threats since it is a single point failure for the GNG.

Migration goal: in-house maintenance constraints and cost reduction. The demands on infrastructure and machine capabilities change on a monthly basis since the publishing needs of the government and the organizations increase dramatically. Due to the Greek financial crisis the available government funding for maintaining these services in house and covering the respective operational costs lowers on a monthly basis. Current infrastructure will fail to serve the correct and proper documents' reception. Migrating these services on the cloud will solve the infrastructure limitations, sources' constraints and backup issues with much lesser cost that the one needed for the GNG for that. Volumes' availability will be better ensured in a cloud context rather than on dedicated servers that have specific processing capabilities and might introduce restrictions on simultaneous access from specific number of citizens. Cloud can offer combined infrastructures, on demand increase or decrease of the space and process sources depending on the time period without the GNG to be forced to buy new costly infrastructure.

Activity 2: Security and Privacy Requirements Analysis

The first step focuses on identifying security and privacy requirements based on the organizational identified entities from previous activity and these requirements pose restriction to achieve the security and privacy goals. There are dependencies among the Public Organisation Actor and GNG actors to the services chosen for this case study. For demonstration simplicity, we will concentrate on one, most representative dependency between the Public Organisation Actor and the GNG which is the *receive document for publication.* Of course the identified dependencies further extend with the cloud provider. Based on the conceptual model described above for every dependency a number of potential threats are identified like a) *Unauthorized modification by GNG employee, b) Unavailability of a specific article from the National Gazette, c) Interception of data in transitd) Insecure storage and e) Lack of control*

Finally, the analysis on this step ends up with the introduction of the respective security and privacy requirements for the dependency *Receive document for publication*.

Identified Security and Privacy Requirements

R1: The system shall check that only legitimate user can send the document; R2: The received document shall not alter without any approval from the legitimate sender; R3: Users of the service shall be unlikable so that public and private organization actor cannot identify the specific GNG employee responsible for handling the receive volume.; R4: The system shall be available to receive any document for the Gazette.; R5: The received document shall only be access by the GNG employee; R6: The system shall provide accountability/ audit support to the users submitted document for the publication; R7: A secure communication shall established between GNG user and CSP

Suggested Deployment Scenario Description

For better describing and presenting the attributes of the deployment scenario, we have introduced a deployment scenario template. Specifically, the template includes information about the proposed scenario type, respective actors, services, organisational goals, cloud migration goals, analytical description of the scenario, the respective security and privacy requirements as well as the security and privacy mechanisms that can assist in the realization of these requirements. For the specific case and based on the nature of the security and privacy requirements we examined and analysed two scenarios, migration on a public cloud and a community cloud. The analysis of every scenario is presented on figures 3 and 4 respectively. The deployment scenario templates are also very useful for the linkage with the assurance activity since the mechanisms proposed in every scenario are useful for checking the assurance of the requirements and every mechanisms itself. Comparing these two scenarios, community cloud benefits features from the public cloud and at the same time provides added level of security and privacy similar to private cloud. We consider on premises community cloud and user can deploy own mechanism for the security and privacy protection such as preference for data security. Two deployment alternatives are being contemplated by GNG. Public cloud is one of the options for GNG for the outsourcing of its service as well as data. The mechanisms for the public cloud are: *P1: VM anonymity; P2: Encryption of data at rest; P3: Access control; P4: Rule based failure detection; P5: Mirroring server for back up; P6: Onion routing; P7: VM isolation; P8: Data obfuscation; P9: provenance; P10: Secure communication protocols.*

In case of community cloud, the infrastructure itself belongs to the community of the consortium organizations as cloud users that are using the infrastructure; the consortium leverages the expertise of a security firm that is entrusted with the safe and secure usages of the deployed services. Therefore, the appointed security firm entitled to conduct audits of the underlining security to verify its stringency and compliance with their respective regulators. Furthermore, each organization of the consortium can commission what the firm allows. Each user can deploy its own mechanism for the protection. One related to a private/community cloud deployment model which, in addition to being restricted to a number of organizations of the same typology, features a number of security mechanisms including: *C1: Data encryption; C2: Identity and access management; C3: Back up servers; C4: VM introspection; C5: Data anonomisation and pseudonimisation; C6: user preference for data security; C7: Integrity data checks; C8: security audit in user's VM env; C9: Secure isolated channel*

Activity 3: Security and Privacy Assurance Analysis

- **Assurance Requirements**

It is imperative for the GNG that all of the security and privacy requirements listed be met by any deployment solution. Rather than taking the word of the infrastructure owner for security and privacy, the GNG would like to perform some frequent audits for satisfying the requirement of the regulators but also ensuring the readiness of security of its service.

Deployment Scenario	
Scenario Type: Public cloud **Service**: Receive document	**Actors**: Cloud user(Public and private organization, GNG employee)
Hosting Type: Third party location	**Organisational goal:** Availability of receive document service
Cloud migration goals: Resolve in house infrastructure & maintenance constraints and back up issues, cost reduction	
Scenario description: One of the main services of GNG , receive document, decided to migrate into cloud. This migration shall be able to address various in house limitations. This scenario consider the public cloud model with hosting in third party location. Therefore, access control, back up and integrity of the received document are important for this scenario context.	
Security and privacy requirements: • The system shall check that only legitimate user can send the document • The received document shall not alter without any approval from the legitimate sender • Users of the service shall be unlinakble so that public and privacy organization actor can not identify the specific GNG employee responsible for handling the receive volume. • The system shall be available to receive any document for the Gazette. • The received document shall only be access by the GNG employee • The system shall provide accountability/audit support to the users submitted document for the publication • A secure communication shall be established between GNG user and CSP	
Security and privacy mechanism: • VM anonymity • Encrypt receive data • Access control • Rule based failure detection • Mirroring server for backup • Onion routing • VM isolation • Data obfuscation • Provenance • Secure communication protocol	

Fig 3: Scenario description for public cloud

Therefore, GNG would like to ensure its choice of deployment model meets the characteristics of a trusted cloud as an assurance requirement thus based on table 7 a cloud deployment for which the level of completeness,

auditability and reportable will be respectively 3,5 and 2. Besides the need to have its security and privacy requirements met within the outsourced environment the GNG is also inclined to solutions with lesser cost and more flexibility in the management but these are considered secondary compared to security and privacy issue.

- **Assurance parameters assessment**

In this step, initially, we consider the assessment of the completeness of the available mechanisms for both deployment scenarios with respect to the specified security and privacy requirements. Hence we proceed with mapping the identified security and privacy requirements with the mechanisms for each of the two deployment scenarios. Results are presented on table 9. The analysis of the security and privacy requirements and the deployment scenarios reveals that both the community and public cloud satisfy the completeness metric.

Deployment Scenario

Scenario Type: Community cloud **Service**: Receive document	**Actors**: Public and private organization, GNG employee
Hosting Type: On premise location	**Organisational goal:** Availability of receive document service

Cloud migration goals: Resolve in house infrastructure constraints and back up issues, cost reduction

Scenario description: One of the main services of GNG , receive document, decided to migrate into cloud. This migration shall be able to address various in house limitations. This scenario consider the public cloud model with hosting in third party location. Therefore, access control, back up and integrity of the received document are important for this scenario context.

Security and privacy requirements:

- The system shall check that only legitimate user can send the document
- The received document shall not alter without any approval from the legitimate sender
- Users of the service shall be unlinakble so that public and privacy organization actor can not identify the specific GNG employee responsible for handling the receive volume.
- The system shall be available to receive any document for the Gazette.
- The received document shall only be access by the GNG employee
- The system shall provide accountability/audit support to the users submitted document for the publication
- A secure communication shall be established between GNG user and CSP

Security and privacy mechanism:

- Data encryption
- Identity and access management
- Back up servers
- VM introspection
- Data anonomisation and pseudonimisation
- user preference for data security
- Integrity data checks
- security audit in user's VM env.
- Secure isolated channel

Fig 4. Scenario description for community cloud

Security & Privacy Requirements	Related mechanisms	
	Public Cloud	Community Cloud
R1	P3	C6,C2
R2	P2,P3,P7	C1,C2, C6,C7
R3	P6,P8	C2,C5
R4	P5	C3
R5	P3	C2
R6	P9	C8
R7	P10	C9

Table 9. Mapping requirements and deployment scenarios security

Based on the analysis and definition provided in Step 3.2 of Activity 3 regarding the auditability, the community cloud in these instances offers more assurance since all aspects of the security and privacy are linked to the hired environment and to the infrastructure that support the service can be vetted by independent auditor, i.e., SA_AUD.5 In contrast the level of auditability that can be achieved for the public cloud would be between SA_AUD.3 and SA_AUD.4 at best. This is because although independent audits are possible they remain restricted to the GNG's VMs when some of the security posture of the latter depend on security controls that are beyond the VMs boundary. Furthermore the community cloud offers a rule based failure detection that can be customized according to GNG needs for flagging and reporting anomalies events that may be of relevance to the well function of its document service.

- **Selecting the most adequate deployment scenario**

Amongst the criteria for the selection of the deployment model as specified by GNG were the completeness of the security and privacy concerns; the conduct of third party audits on the security of the infrastructure owner and, frequent reports of security incidents relevant to its activity. The analysis conducted using the assurance approach demonstrate that the community cloud is more appropriate to the GNG needs given the completeness, auditability and reporting of incidents and anomalies can be met at the highest levels thus making that deployment a trusted cloud as described in table 7. With respect to cost, the expenditure that may be linked to the community cloud was expected to be higher than that of the public cloud though we did not engage in such an analysis given the most salient criteria of selection were security and privacy.

4.3 Discussion

Greek National Gazette is a large public government organisation that faces real operational problems and the need for migrating specific services into the cloud is of vital importance for its future operational continuity. Thus, this framework was applied on the right time in the GNG since the organisation was seeking a solution on real issues that have been an obstacle on its daily operational activities and were adding more effort and cost to an already problematic and hard environment. Therefore, the framework is implemented and actively supports the GNG.

The combination of security and privacy requirements along with assurance requirements on a cloud migration process was firstly presented and the successful application for the authors was a critical step for its viability and future development. Due to limited space only two deployment scenarios where presented. However, it is clear that the framework depending on the security and privacy requirements examined and the assurance requirements that the user places and the cloud models react play a critical role on the deployment model. Selecetion of private or community clouds as the more safe clouds cannot be made a priori as an obvious solution since the satisfaction of assurance requirements combined with security and privacy may lead to other models offering solutions closer to users' needs.

The proposed activities on the specific case study reasonably benefit the GNG to identify the requirements and end up with the selection of the most appropriate deployment model based on its current organizational needs. This led up to a direct assessment of the proposed model, which ended up successfully based on the results

described above. The main observation is the justification of the proposed research that assurance parameters are effective in the selection process of a cloud provider when individuals or companies wish to migrate part or the whole set of services to the cloud.

Through the case study it became obvious that security and privacy goals derived initially from the organisation and its operational environment and also from the respective CSP are critical to determine the migration decision. Especially in the GNG where security and privacy requirements need to be fulfilled and due to the governmental nature of the services, the GNG officers do wish to have the ability to assess the cloud provider before they decide to migrate their data and services into the cloud. Therefore the framework provides an early understanding of the necessity of migration, the security and privacy issues and the threats that support the informed decision making process for the selection of the adequate cloud deployment model. We also recommended the GNG employees to be trained with the cloud technologies so that cloud adaption actions and operation actions can be performed properly. The artefacts of the activities within the process followed in this paper were discussed with the National Gazette's officers and they were accepted especially because of the set of factors that were taken under consideration before the final decision was taken. The artefacts were also understandable to support the real needs.

5 CONCLUSIONS

Cloud migration is one of the most important concerns nowadays for both private and public organisations since due to the recent financial situations every organisation is aiming on cost reductions without losing efficiency and service quality. However, before migrating services, data or infrastructure into the cloud, it is necessary to realise and understand the migration needs and risks that cloud migration hinders. These risks vary among organisations especially due to the variability of information as well as the type of cloud services each organization wishes to use. Finally, the selection of the respective cloud model that will be adopted plays an important role on the potential risks that the organization might face as well. Thus, the role of security and privacy are very important for an organization to decide which cloud solution fits best its needs and requirements.

In this paper, a framework for supporting the elicitation and analysis of organisation's security and privacy needs and assurance to support these needs are presented. The aim of the framework is to assist organisations in selecting the most appropriate cloud model based on their security and privacy needs. We consider security and privacy requirements engineering concepts for the proper elicitation and analysis of the requirements and include assurance requirements for verifying the fulfillness of the requirements using completeness, auditable and reportable metrics. By quantifying the fulfillness of every suggested cloud model it is easier and more efficient to suggest the solution that should fit on the specific organisation's context and security and privacy goals. Finally, the applicability of the proposed framework was demonstrated on a real case scenario. The study results show that the approach supports the understanding of security and privacy requirements from the studied organisational context and identifies possible deployment scenarios so that appropriate decision can be taken. The assurance confirms which deployment model is suitable for the context. We plan to develop tool support to automate the elicitation and assurance activity. We would also like to focus on in-depth analysis of business issues and existing CSP offers.

ACKNOWLEDGEMENT

The work was partly supported by the national fund of research of the Grand Duchy of Luxembourg (FNR) SAINTS project, grants number C12/IS/3988336 and Austrian Science Fund (FWF) project no. P26289-N23.

REFERENCES

[1] P.J. Bruening, and B.C. Treacy "Privacy & Security Law Report: Privacy", Security Issues Raised by Cloud Computing. The Bureau of National Affairs, 2009

[2] M. Ouedraogo and H. Mouratidis "Selecting a cloud service provider in the age of cybercrime", Computers & Security, Special issue on Cybercrime in the Digital Economy, vol.38, pp.3-13, Elsevier, 2013

[3] P.G. Dorey and A. Leite "Commentary: Cloud computing – A security problem or solution?" Information Security Technical Report, vol. 16, no. 3-4, pp. 89-96, Elsevier, 2011

[4] AICPA "Statement on Auditing Standards (SAS) n°70", from http://sas70.com/sas70_overview.html, 2012

[5] NIST, US Government Cloud Computing Technology Roadmap Volume II Release 1.0 (Draft), Useful Information for Cloud Adopters, November 2011

[6] CSA, Cloud Controls Matrix V.3.0.1, 2014 ,https://cloudsecurityalliance.org/research/ccm/

[7] M. Ouedraogo, E. Dubois, D. Khadraoui, S. Poggi and B. Chenal "Adopting an Agent and Event Driven Approach for Enabling Mutual Auditability and Security Transparency in Cloud Based Services, In Proceeding of CLOSER 2015

[8] M. Ouedraogo, D. Khadraoui, B. Rémont, E. Dubois, H. Mouratidis: Deployment of a Security Assurance Monitoring Framework for Telecommunication Service Infrastructures on a VoIP Service. In Proceedings of NTMS 2008: P1-5

[9] M. Theoharidou, N. Papanikolaou, S. Pearson and D. Gritzalis, " Privacy Risk, Security, Accountability in the Cloud" proceedings of IEEE International Conference on Cloud Computing Technology and Science, 2013

[10] E. Yu "Modelling Strategic Relationships for Process Reengineering", Ph.D. thesis, Department of Computer Science, University of Toronto, Canada, 1995

[11] B. Grobauer, T. Walloschek and E. Stocker "Understanding Cloud Computing Vulnerabilities", IEEE Security & Privacy Magazine, vol. 9, No. 2, pp. 50-57, 2011

[12] H. Mouratidis, C. Kalloniatis, S. Islam, M. P. Huget, S. Gritzalis "Aligning Security and Privacy to support the development of Secure Information Systems, Journal of Universal Computer Science, vol. 18, no. 9, pp. 1608-1627, 2012

[13] C. Kalloniatis, E. Kavakli, S. Gritzalis, "Dealing with Privacy Issues during the System Design Process", Proceedings of the ISSPIT'05 5th IEEE International Symposium on Signal Processing and Information Technology, pp.546-551, D. Serpanos et al. (Eds.), December 2005, Athens, Greece, IEEE CPS Conference Publishing Services, 2005

[14] C. Kalloniatis, E. Kavakli, S. Gritzalis, "Methods for Designing Privacy Aware Information Systems: A review", Proceedings of the PCI 2009 13th Pan-Hellenic Conference on Informatics, pp.185-194, V. Chrysikopoulos, N. Alexandris, C. Douligeris, S. Sioutas (Eds.), September 2009, Corfu, Greece, IEEE CPS Conference Publishing Services, 2009

[15] H. Mouratidis and P. Giorgini, "Secure Tropos: A Security-Oriented Extension Of The Tropos Methodology", International Journal of Software Engineering and Knowledge Engineering, World Scientific Publishing Company, 2006

[16] R.M. Davison, M.G. Martinsons, N. Kock, Principles of canonical action research, Information Systems Journal 14 (2004) 65–86

[17] S. Pearson, & A. Benameur. Privacy, Security and Trust Issues Arising from Cloud Computing, 2nd IEEE International Conference on Cloud Computing Technology and Science, pp 693 – 702, UK. IEEE Computer Society, 2010.

[18] C. Kalloniatis, H. Mouratidis, M. Vassilisc, S. Islam, S. Gritzalis, E. Kavaklif, Towards the design of secure and privacy-oriented Information Systems in the Cloud: Identifying the major concepts, Computer Standards & Interfaces , Vol 36, Issue 4, june 2014, Elsevier

[19] FedRAMP, Security assessment process, https://www.fedramp.gov/resources/documents/

[20] M. Ouedraogo, C.T. Kuo , S. Tjoa, D. Preston, E. Dubois, P. Simoes and T. Cruz (2014)Keeping an Eye on Your Security Through Assurance Indicator, In proceeding of SECRYPT 2014.

[21] P. Massonet, S. Naqvi, C. Ponsard, J. Latanicki, B. Rochwerger, M. Villari: A Monitoring and Audit Logging Architecture for Data Location Compliance in Federated Cloud Infrastructures. In Proceeding of 2011 IEEE International Parallel & Distributed Processing Symposium, 2011

[22] H. Takabi, J. Joshi, & G. Ahn, G. Security and Privacy Challenges in Cloud Computing Environments, IEEE Computer And Reliability Societies, November/December. IEEE Computer Society,2010.

[23] M. Gregg,"10 security concerns for cloud computing", GlobalKnowledge Training LLC, 2010, http://viewer.media.bitpipe.com/1078177630_947/1268847180_5/WP_VI_10SecurityConcernsCloudComputing.pdf.

[24] D.G. Rosado, R. Gomez, D. Mellado, & E. Fernández-Medina, E. Security Analysis in the Migration to Cloud Environments, Future Internet,4(2).2012

[25] M. Mulazzani, S. Schrittwieser, M. Leithner, M. Huber, M. & E. Weippl Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space. Proceedings of Usenix Security,2011.

[26] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proc. of VLDB, Vienna, Austria, Sep. 2007.

[27] A. Khajeh-Hosseini, I. Sommerville, J. Bogaerts, and P. Teregowda. Decision support tools for cloud migration in the enterprise, IEEE International Conference on Cloud Computing, pages 541-548. IEEE, 2011.

[28] P. Jamshidi, A. Ahmad, C. Pahl, Cloud Migration Research: A Systematic Review, , IEEE Transactions on Cloud Computing , Vol 1, Issue 2, July-December, 2013

[29] M. Klems, J. Nimis, S. TaiDo, Clouds Compute? A Framework for Estimating the Value of Cloud Computing ,Designing E-Business Systems. Markets, Services, and Networks, Lecture Notes in Business Information Processing Volume 22, 2009, pp 110-123,2009

Shareeful Islam Dr. Shareeful Islam is currently working at the School of Architecture, Computing and Engineering (ACE), University of East London, UK. He was awarded his PhD from Technische Universität München, Germany and M.Sc. in Information Communication System Security from the KTH, Sweden and M.Sc. in CS and B.Sc. (Hons) in APE from the University of Dhaka, Bangladesh. He is a Fellow of the British Higher Education Academy (HEA) and has published more than 40 referred papers in high-quality journals and international conferences. He participated in EU, industry, KTP projects. His research interests and fields of expertise are risk management, requirements engineering, security, privacy, trust, and cloud computing.

Moussa Ouedraogo Dr. Moussa Ouedraogo is a researcher at the Luxembourg Institute of Science and Technology. He holds a PhD degree from the University of East London (UK) and has been involved in numerous national and European research projects tackling the issue of security. His research interest focuses on security assurance, security monitoring and automated security audits.

Christos Kalloniatis Dr. Christos Kalloniatis is an Assistant Professor at the Department of Cultural Technology and Communication, University of the Aegean where he also serves as a member of Cultural Informatics Laboratory (CiLab). He received his PhD from the same department and holds an M.Sc. from the Department of Computer Science, Univeristy of Essex. His research is focused on the design of secure and privacy-aware information systems and services both in traditional and cloud oriented environments. He has served as a program committee member in several International Conferences and as a reviewer in many International Journals. He is a member of Greek Computer Society.

Haralambos Mouratidis Haralambos Mouratidis is Professor at the School of Computing Engineering and Mathematics, University of Brighton. He holds a B.Eng. (Hons) from the University of Wales, Swansea (UK), and a M.Sc. and PhD from the University of Sheffield (UK). He is also a Fellow of the Higher Education Academy (HEA) and a Professional Member of the British Computer Society (BCS). His research interests lie in the area of secure software systems engineering, requirements engineering, information systems development and agent oriented software engineering. He has published more than 100 papers and he has secured funding as Principal Investigator from national – Engineering and Physical Sciences Research Council, Royal Academy of Engineering, Technology Strategy Board (TSB) - and international – European Union- funding bodies.

Stefanos Gritzalis Prof. Stefanos Gritzalis is the Director of the Lab. of Information and Communication Systems Security (Info-Sec-Lab), University of the Aegean, Greece. He holds a BSc in Physics, an MSc in Electronic Automation, and a PhD in Information and Communications Security from University of Athens, Greece. He has been involved in several national and EU funded R&D projects. His published scientific work includes 30 books or book chapters, 100 journals and 135 international refereed conference and workshop papers. He has acted as Guest Editor in 30 journal special issues, and has been involved in more than 30 international conferences and workshops. He is an Editor-in-Chief or Editor or Editorial Board member for 20 journals and a Reviewer for more than 50 journals. He has supervised 12 PhD dissertations and acts as President-Elect of the AIS - Hellenic Chapter, Member of the ACM, the IEEE.