View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by UEL Research Repository at University of East London

Evaluating Cloud Deployment Scenarios Based on Security and Privacy Requirements

Christos Kalloniatis, Haris Mouratidis, Shareeful Islam

Department of Cultural Technology and Communication, University of the Aegean, Mytilene, University Hill, GR-81100, Lesvos, Greece Email. chkallon@aegean.gr

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, haris@uel.ac.uk

Abstract

Migrating organisational services, data and application on the Cloud is an important strategic decision for organisations due to the large number of benefits introduced by the usage of cloud computing, such as cost reduction and on demand resources. Despite, however, of the many benefits, there are challenges and risks for cloud adaption related to (amongst others) data leakage, insecure APIs, and shared technology vulnerabilities. These challenges need to be understood and analysed in the context of an organisation's security and privacy goals and relevant cloud computing deployment models. Although, the literature provides a large number of references to works that consider cloud computing security issues, no work has been provided, to our knowledge, which supports the elicitation of security and privacy requirements and the selection of an appropriate cloud deployment model based on such requirements. This work contributes towards this gap. In particular, we propose a requirements engineering framework to support the elicitation of security and privacy requirements and the selection of an appropriate deployment model based on the elicited requirements. Our framework provides a modelling language that builds on concepts from requirements, security, privacy and cloud engineering and a systematic process. We use a real case study, based on the Greek National Gazette, to demonstrate the applicability of our work.

Keywords: cloud, cloud deployment model, security requirements, privacy requirements, cloud migration.

1. Introduction

The term "cloud computing" has positively invaded our lives providing a number of technological capabilities that have enhanced the way we perform every-day tasks. Various well known services such as email, data storage, web content management, are among the many that can be offered via a cloud environment. Although many of these services were offered, through the Internet, before the cloud era, the cloud computing environment significantly improves the degree of scalability, flexibility and resource pooling availability, therefore significantly assisting improved and efficient performance and availability [1,2].

However, the buzz that has been created in the technological world has not been transformed to the domination of the technology to the real world. One of the main issues seems to be the uncertainty and (lack of) trust of organisations and individuals about cloud computing and the (lack of) understanding of all the parameters that can affect an organisation when migrating their services and data into the cloud. A recent survey [3], conducted by a document management software company revealed that 41% of senior IT professionals don't know what cloud computing really is. From the remaining 59% of IT professionals who stated that they know what cloud computing is, 17% of them understand cloud computing to be internet-based computing while 11% believe it is a combination of internet-based computing, software as a service (SAAS), software on demand, an outsourced or managed service and a hosted software service. The remaining respondents understand cloud computing to be a mixture of the above.

Another major concern is that of security. In fact, many organisations and individuals are still avoiding cloud services mostly because they are not sure if the services provided, by different providers, are suitable for their security and privacy requirements. This is especially true for organisations since they would have to hand in highly sensitive personal and organizational data and enable running of business-critical applications into service providers over which they have no control. This introduces an extra layer of complexity on top of the expected security and privacy issues that are present in any type of software systems and services whether on the cloud or not. These concerns increase the risk factor of a potential migration to the cloud or integration of a cloud solution to an existing IT infrastructure.

The literature [2, 4, 5] has recently provided examples of research efforts that consider security and privacy within the cloud computing context. These works have mostly been focused on identifying security/privacy specific threats and vulnerabilities for the cloud, identify specific attacks to cloud infrastructure, considering specific protocols that can support security and privacy in the cloud. On the other hand, very little work, if any, has taken place in the area of security and privacy requirements elicitation and analysis for the cloud. Although, a large number of research efforts [2, 6, 7, 8, 9, 10] have been reported in the literature to deal with security and privacy requirements analysis and reasoning, but most of these work do not consider unique cloud related properties. Security and privacy in the context of cloud computing requires techniques different to those provided by the existing literature. These properties in the context cloud is different comparing the traditional IT system due to several reasons such as IT infrastructure and computational resources used by the user are owned and operated by an outside cloud provider, users data is generally stored in a multi-tenant platform that is out of user control, and a new type dependency with the unknown provider within the existing business model. It is necessary to develop techniques that identify and analyse security and privacy requirements from both user and provider perspectives and to select appropriate deployment model that aligns with the requirements focusing on the organizational needs. Techniques that will be based on appropriate modelling languages that will enable modelling of concepts that are unique in the cloud, and will support reasoning and analysis of security and privacy properties taking into account the unique characteristics of the cloud context. Our work aims to fill in this gap. In particular, we have developed a framework that supports elicitation and analysis of security and privacy requirements within a cloud computing context, and the reasoning of different cloud deployment models based on the relevant security and privacy requirements.

Section 2 presents cloud computing and it discusses security and privacy properties relate to it, focusing on cloud computing specific security and privacy properties. Section 3 presents our framework, and in particular its metamodel and process. Section 4 introduces a real case study and it demonstrates the applicability of our framework to that case study. Section 5 presents related work and Section 6 concludes the paper and points out areas for future research.

2. Cloud Computing

There is a lot of discussion and various definitions presented in the literature regarding Cloud Computing. Amongst those definition we have considered one provided by the National Institute of Standards and Technology (NIST), according to which: "*Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*.". We do not argue that this definition is better or worse than others, but we believe that this is a definition of cloud computing that is applicable within the context of our work.

2.1 Cloud Service and Deployment Models

Cloud computing is based on three fundamental models [11-13]: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Following an IaaS model, organisations outsource equipment (e.g. storage, servers, networking) to support their operations. The equipment is owned by the service provider, who is responsible for running and maintaining it. In a PaaS model, a computer platform along with deployment of associated set of software applications is provided by a service provider to an organization. In a SaaS model, service providers host applications, which are made available over the network. In the cloud, IaaS is the most basic and each higher model abstracts from the details of the lower models.

According to NIST, Cloud computing deployment models "*broadly characterize the management and disposition of computational resources for delivery of services to consumers, as well as the differentiation between classes of consumers*". In a public cloud, service providers make resources, such as applications and storage, available to the general public over the Internet. Some well-known examples of public clouds include Amazon Elastic Compute Cloud (EC2), Google AppEngine and Windows Azure Services Platform. Private clouds are employed to support services of an organization without sharing resources with any other entity. The actual infrastructure that supports the cloud could be physically located in the organisation's premises, or outside of its premises in the service providers' premise. A Community cloud runs in service of a community of organizations, having the same deployment characteristics as private clouds. A Hybrid cloud is a combination of public, private, and community clouds. Hybrid clouds leverage the capabilities of each cloud deployment model. Each part of a hybrid cloud is connected to the other by a gateway, controlling the applications and data that flow from each part to the other.

2.2 Security and Privacy in the cloud

Security and privacy issues are among the most important concerns in cloud computing, as large amounts of personal and other sensitive data are managed in the cloud. Several surveys among potential cloud adopters indicate that security and privacy is the primary concern hindering its adoption [14]. Security Company Symantec, commissioned a study for their 2011 State of the Cloud survey, to examine organizations that are adopting cloud computing. The survey found that security was considered as both the top goal and top concern by those organizations. Therefore, it is necessary to understand and analyze the relevant security and privacy issues before adopting cloud computing into existing infrastructure.

The storage of personal and sensitive information in the cloud raises concerns about the security and privacy of such information and how much the cloud can be trusted. Security and privacy in this context requires solutions very different to those provided by current research efforts and industrial practices. Solutions that will not only try to guarantee security and/or privacy from a technical point of view, but solutions that provide clear understanding of the social aspects of security and privacy and take into account, for example, organisational structures, privacy needs and appropriate laws and regulations.

In a traditional IT infrastructure set up, an organisation's infrastructure is in a known and trusted environment, being either physically located within the organization's on-premise facilities and/or directly managed by the organization. As such, the Organisation is in control of its infrastructure. When an organisation's infrastructure (wholly or partially) migrate to the cloud, that infrastructure including relevant applications and stored data are in an environment that is separated, managed and maintained externally to the organisation. Therefore, due to such scenario, the organisation loses control over all or parts of its infrastructure. As an example, consider an organisation that moves a legacy system to the cloud giving up system administrative control and processes over the networking infrastructure, including servers, access to logs, incident response and patch management. With respect to security, such scenario extends the traditional IT infrastructure security beyond the organisation's firewall, requiring consideration and review of additional attributes that include data locality, data integrity, data transfer, data privacy and recovery. As such, there are two main categories where security concerns and issues are raised: the security issues faced by the organization and the security issues faced by the cloud provider.

There is no one-size fits all approach to security as different cloud models (IaaS, PaaS and SaaS) each have different security risks. The Cloud Service Provider (CSP) and the user organization's security duties differ greatly between the cloud models. Measures must be taken to ensure that the customer organization has the same visibility and control of their applications and data in the cloud model. Furthermore, new legal and regulatory issues include regulatory compliance and auditing which further add to the complexity.

3. Incorporating security and privacy requirements in the cloud under a unified framework

3.1 Framework Modelling Language

The proposed framework consists of two main components: A modeling language and a process. The language is based on concepts from requirements engineering, and in particular of the i* [15] language, security requirements engineering, and in particular concepts from the Secure Tropos [16] language, privacy requirements engineering, and in particular from the PRiS [6,17] language, enhanced with concepts related to cloud computing. We have chosen Secure Tropos and PriS from a large number of different existing requirements engineering methodologies to develop an unified requirements engineering framework for the cloud based system. Both of the methods share similar concepts from the early stage of the development, such as actors, goals, constraints, and requirements from two different perspectives, i.e., security and privacy. In particular, Secure Tropos focuses on the elicitation and analysis of security requirements while PriS focuses specifically on the incorporation of privacy requirements in the system design process and identifies implementation techniques to support the requirements. Secure Tropos considers the social dimension of security but does not focus on privacy concept and the implementation solution of the elicited requirements. PriS contributes on this direction; in particular the method considers the privacy issues and transforms the identified requirements into the implementation solutions. Therefore, such integration allows us a framework that provides coverage from the organizational context, cloud properties, security and privacy goals and requirements to select suitable cloud deployment model to support the requirements. As a result, the framework's modeling language supports elicitation and analysis of security and privacy requirements within a cloud computing context, and a systematic way of-working for translating these requirements to select appropriate cloud deployment models. The metamodel shown in Figure 1 represents the abstract syntax of our language.

We employ the concept of an actor to describe an entity that has strategic goals and intentions within a system or an organisational setting [15]. An actor can be an individual, a system or an organisation. An actor provides a service and requires an infrastructure. We also define a special class of an actor, a cloud actor. A cloud actor is an actor that demonstrates two unique attributes, a deployment model and a service model. We also differentiate a special class of an actor, a malicious actor. A malicious actor's intention is to introduce threats to the system, which exploit vulnerabilities. Vulnerabilities are defined as weaknesses or flaws, in terms of security and privacy. Vulnerabilities are exploited by threats, as an attack or incident within a specific context. For instance, unauthorised access to hypervisor introduces a virtual-machine escape threat [18]. This attack is associated with the computing resources on the IaaS level and may happen in all deployment models. It is worth stating that legitimate actors might unintentionally introduce vulnerabilities to a system due to failure or mistakes. Threats pose potential loss or indicate problems that can put the actor at risk. Threats can be of different types related to security and privacy, such as provider data misuse, virtual machine replication, and unavailability of data, insecure storage, and DoS. On the other hand, actors within the system environment have single or multiple goals. A Goal represents an actors' strategic interests [19]. Higher level strategic goals may be decomposed in simpler operational goals forming AND/OR goals hierarchy. Our meta-model differentiates between organizational, security and privacy goals. Examples of security goals are: Confidentiality, Integrity, Availability while for privacy goals are: Anonymity, Unlinkability and Unobservability [20-21]. These goals introduce security and privacy constraints. A constraint is used to represent a set of restrictions that do not permit specific actions to be taken, restrict the way that actions can be taken or prevent certain system objectives from being achieved [16]. Security and privacy constraints are clearly defined as separate concepts to support a clear and well-structured elicitation and analysis of security and privacy requirements. When a constraint is introduced, further analysis is required to establish if and how that constraint can be satisfied. Within the context of our metamodel, a constraint is satisfied by a measure. A measure represents a generic, implementation independent form of control that indicates how a constraint will be achieved. Measures are implemented by relevant mechanisms. A mechanism is defined as a technical solution that realizes one or more measures. Mechanisms require resources and they support services. A resource supports an infrastructure.

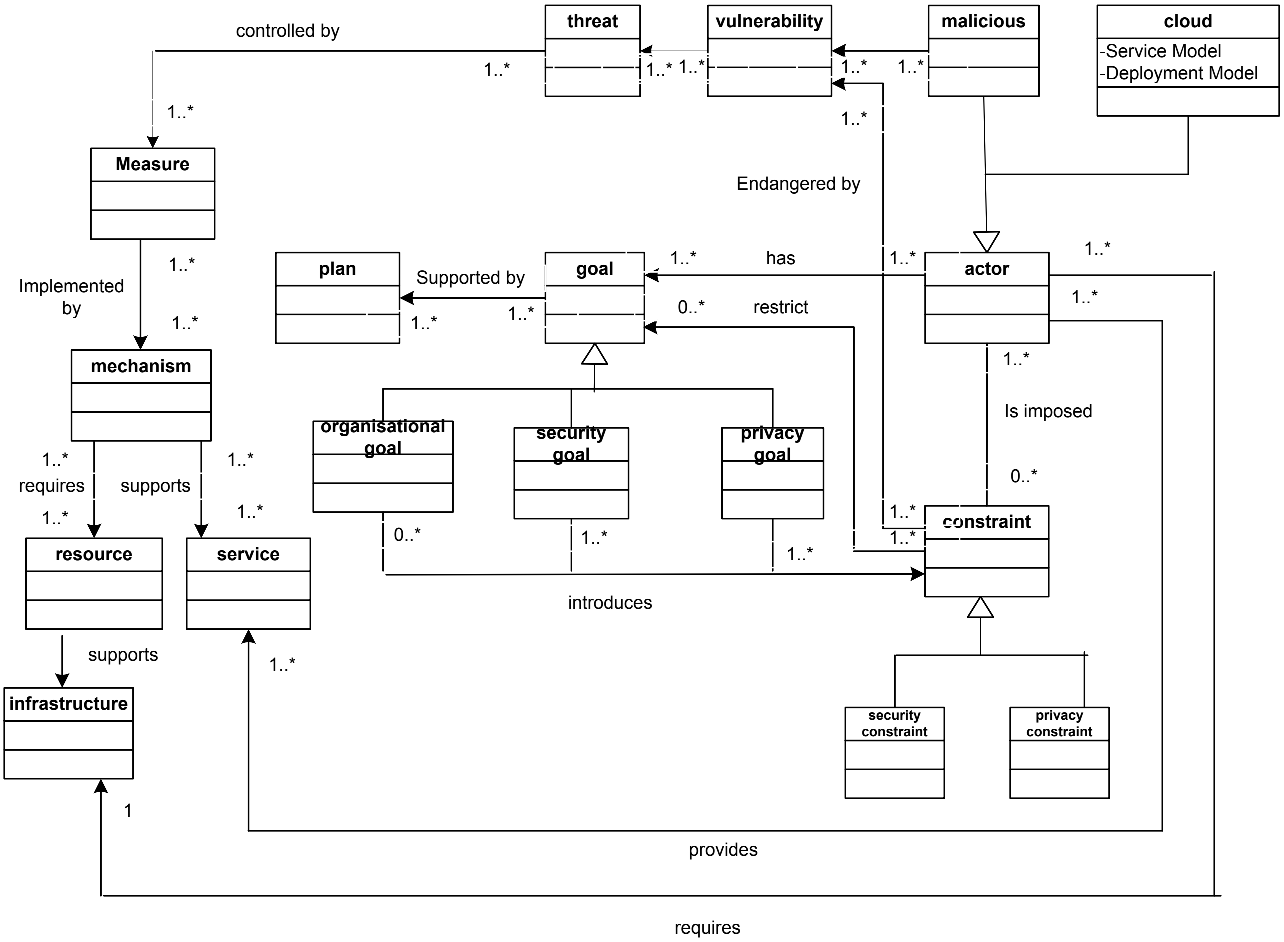
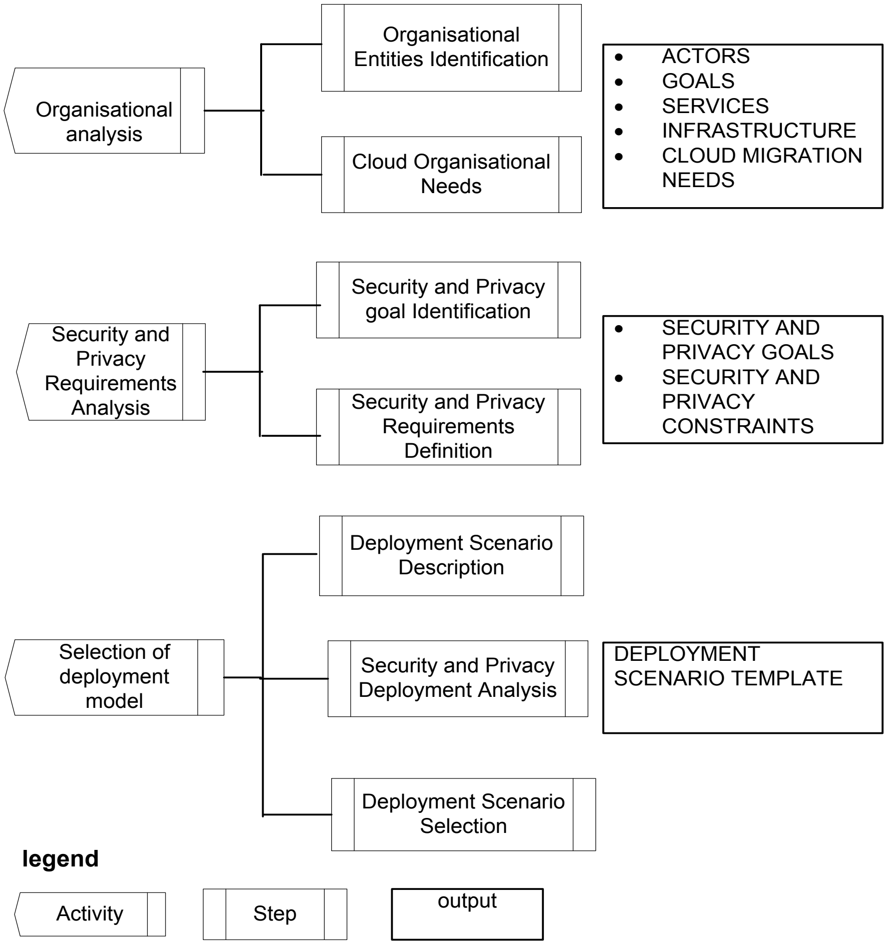


Figure 1. Metamodel for Cloud Computing Security and Privacy Concepts

3.2 The Process

We propose a process based on the underlying concepts used within the presented language. The aim of the process is to provide a structured approach for the elicitation and analysis of security and privacy requirements, and to support the selection of appropriate deployment models based on the identified requirements and relevant security and privacy mechanisms. The process assists in the understanding of specific organisational needs for cloud migration. The process consists of three iterative activities: organizational analysis, Security and Private Requirements Analysis, and selection of deployment model. Figure 2 depicts the activities and the resulting artefacts of the proposed process.



Organisational analysis
Organisational Entities Identification
Cloud Organisational Needs
ACTORS
GOALS
SERVICES
INFRASTRUCTURE
CLOUD MIGRATION NEEDS
Security and Privacy Requirements Analysis
Security and Privacy goal Identification
Security and Privacy Requirements Definition
SECURITY AND PRIVACY GOALS
SECURITY AND PRIVACY CONSTRAINTS
Selection of deployment model
Deployment Scenario Description
Security and Privacy Deployment Analysis
Deployment Scenario Selection
DEPLOYMENT SCENARIO TEMPLATE
legend
Activity
Step
output

Figure 2. Security and Privacy Requirements Engineering Process for Cloud

Activity 1: Organisational Analysis

The Organisational Analysis activity supports understanding of the organisational needs for the deployment of a cloud based infrastructure. The activity aims to identify those parts of the organisations services and processes that need to be delivered over the cloud. In doing so, the activity includes identification of key entities such as actors, goals, plans, resources, and services.

Step 1.1: Organisational Entities Identification

This step aims to understand the current organisational structure based on the identification of entities such as actors, goals, plans, resources, services and infrastructure. Such understanding introduces the foundations required for the latest activities and steps of the proposed framework.

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 email service, then an identification of entities relevant to that service would suffice. On the other hand, if a full migration is considered then the identification should include the whole of the organisation and any external entities that might affect some migration.

In our work, we consider an organisation which has a set of actors who have some common goals. These are the organisational goals that support the overall objective and business needs of the organisation. These goals can be initially high level goals that can be refined to provide more explicit goals.

Step 1.2: Cloud Organisational Needs

This step aims to identify the explicit organisational structures, services, application and data that should be deployed in the cloud. For example, going back to the email service provided as an example in the previous step, the exact details of whether the whole email service, or if just some of the applications and/or data should be deployed in the cloud should 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, an analysis takes place related to the security and privacy requirements of the organisation. We define two steps within this activity, the Security and Privacy Goal Identification and the Security and Privacy Requirements definition. The output of this activity is a set of security and privacy requirements modelled in terms of security and privacy constraints for each actor of the organisational analysis.

Step 2.1 Security and Privacy Goal Identification

Once the organisational needs for cloud deployment have been identified, the next activity involves the analysis of security and privacy requirements related to the organisational cloud deployment needs. Security and privacy needs are identified based on the security and privacy goals that the organisation has. It is therefore important to fist identify the relevant security and privacy organisational goals. If the organisation has a security and privacy policy that information could be extracted from the policy. Relevant laws and regulations can also be considered to identify the set of security and privacy goals. It is important to 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 in the cloud.

Step 2.2 Security and Privacy Requirements Definition

Once the relevant security and privacy goals 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 constraints, as defined in the presented metamodel, to enable developers to adequately capture security and privacy requirements. In the context of our work a security constraint is defined as a restriction, related to security, imposed to one or more actors and which restricts the actor from performing certain actions [16]. Similarly, a privacy constraint introduces restrictions related to privacy. Security and Privacy constraints are elicited from internal to an organisation sources (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). It is important to establish the relationship between organisational goals and security/privacy constraints. In other words, it is important to know what organisational goals a security/privacy constraint is restricting. This allows us to have a clear understanding of the security and privacy constraints introduced due to specific organisational goals, and enable us to easily evaluate the organisational security and privacy constraints, in cases where organisational goals change. It is also worth noting that security and privacy constraints are the same irrespective of specific cloud deployment models since they represent security and privacy requirements. To support this step, we realise a Security and Privacy Goal Diagram based on the Secure Tropos methodology [16].

Activity 3: Selection of deployment model

The main aim of this activity is to support the selection of the appropriate deployment model for the cloud migration. The activity has three main steps: Deployment Scenario Description; Security and Privacy Deployment Analysis; Deployment Scenario Selection. To support this activity, we have developed a Deployment Model Selection template. The template, shown in appendix A, consists of two sections, which are filled in during the carried out of the activity's two first steps. Section 1 is filled in during Step 1, while section 2 is filled in during step 2. Then during step 3 an analysis of all templates is carried out to select the preferred deployment scenario. The output of this activity is a complete selection template and the decision regarding the deployment model.

Step 3.1: 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 relevant security and privacy requirements identified in the previous step. Relevant information is documented using the Deployment model selection template and in particular the following fields from Section 1:

- **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.
- **Actors Involved.** The actors involved in the specific scenario are listed.
- **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.
- **Organisational Goals.** The organisational goals identified in the previous activity, relevant to the scenario, are listed.
- **Security and Privacy Constraints.** The security and privacy constraints from the previous activity, related to the scenario, are listed.

Step 3.2: Security and Privacy Deployment Analysis

For each scenario, a security and privacy deployment analysis takes place where vulnerabilities, threats, security and privacy mechanisms, are analysed for each scenario. In particular the analysis focuses on issues related to the specific deployment model and configuration of the analysed scenario. Threats and vulnerabilities can rise from unique cloud properties such as virtualization, computational resource, and unauthorized access to instance or virtual machine running on the same physical machine considering the identified deployment scenario. Once these have been identified, relevant security and privacy mechanisms are introduced to the model to evaluate countermeasures for the identified threats and vulnerabilities. The analysis is documented through the Security and Privacy Deployment Diagram, which is added to Section 2 of the template.

Step 3.3: Deployment Scenario Selection

This final step consists of evaluating all the available templates created in the previous two steps, and selecting the preferred deployment scenario. Within the context of our work, we suggest that the selection is based on the fulfilment of each model of the relevant security and privacy requirements, i.e. how the security and privacy requirements are fulfilled by the relevant security and privacy mechanisms that are applicable to the specific deployment model. However, we understand that such simplistic evaluation might not be applicable in all cases either due to more than one scenarios fulfil their security and privacy requirements, or due to the lack of a scenario fulfilling all the relevant security and privacy requirements. In that case, a number of other criteria can be employed. Although it is outside the scope of our work to enforce the criteria and process of selecting in such cases the preferred model, criteria could include cost related criteria (for example, how much each scenario will cost to deploy), customer related criteria (for example, which scenario best fits customer expectations), resource related criteria (for example, what resources are currently available from the organisation).

4. Framework Application: The Greek National Gazette case study

The proposed framework was applied on a real case study related to analysis of the migration of some services of the Greek National Gazette (GNG) to the cloud.

Activity 1: Organisational Analysis

The first step of the first activity of the proposed framework is to analyse the organisation and identify a number of entities that are important for further analysis in the following steps and activities. The main authority of the Greek National Gazette is to publish laws and other legal decisions on the Government's Newspaper in order for these laws and decisions to be active and applicable. Besides legal decisions there are also a number of decision categories originated from the private and public sector that by law must be send for publication to the Government's Newspaper. In 2010 the National

Gazette decided to provide a service for electronic submission of the manuscripts send for publication. The whole process starts when a document is sent by a public/private sector organisation/company to the GNG. Every document that enters the National Gazette in order to be included in the Government's official Newspaper follows a specific process. The first step of this process is the categorisation and scanning of the document. Categorization is based on two criteria: the source of the document and the subject of the document. The Government Newspaper has a number of volumes, on which documents are included for publication. The proper categorisation is very important since it will determine on which volume the specific document will be published. The next step of the process involves the assignment of the unique identification number to the document. This number assists for identification and search purposes and follows the document through the rest of the respective process. If the document's source is companies from the private sector it is assigned an identification number different from those applied to document received by the public sector. Also, during this step a first electronic form of the document is registered to the NGs information system. The respective employee will enter into the system, besides the identification number, a brief description and a small summary of the document. These will be done manually from employees. In the next step of the process, the document is transformed from hard copy to electronic version (usually .DOC or .PDF formats). Usually the first scanned version requires a number of corrections. Thus, there is a recursive step between the OCR and the spelling corrections process until the document reaches its proper form and perfectly matches with the original hard copy. All this process is again conducted manually by the respective employees who constantly check every electronic version provided by the OCR, apply the corrections manually and again send it for the creation of the newer electronic version. Every electronic document which is finalised from the previous step is sent to the respective employee so as to be included in the respective issue under development based on the categorisation conducted before. The issue has a maximum number of documents that can be included but not a minimum one. For the construction of the issue a specific software tool is used which combines the available documents and organizes them in a way that the issue will be complete without redundant blank lines etc. Every issue is assigned a specific id called issue_id which includes one or more documents (each identified by its document_id). The software outputs a first draft of the issue. Its context is not always correct. Thus, qualified employees format the issue manually until it gets its final form. In this stage an integrity check of the context of the issue is also conducted for verifying that no unauthorised changes have been made on every document included for publication in the respective issue. After taking its final form the issue is signed by the general secretary of the National Gazette and is send to the Government's General Secretary for approval before proceeding for publication. The communication between the National Gazette and the Government's General Secretary is conducted by internal mail and not electronically. The specific step is fulfilled when the issue has taken the final approval and returns back to National Gazette in order to proceed with the final steps before printing. The final stage includes several sub-steps. 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. The first draft of the volume is again formatted until it reaches its final version. Before proceeding on the printing phase a final integrity check is again conducted. During this check every document included in the volume is again compared with the original hard copy versions and the final acceptance is being given. After the final acceptance a pdf file is created with a digitally unsigned version of the volume. Then the pdf file is being printed through a specific software tool and the output of this substep is the volume along with the first date of publication an its printed date. Finally, this final 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. Finally, the digitally signed version of the volume is uploaded on the National Gazette's portal with free access to all Internet users. A graphical illustration of the above process is shown in Figure 3.

Output 1: ACTORS

A number of actors can be identified by the above analysis:

- *Public Organisation Actor*, which represents any public organisation that sends documents to the GNG;
- *Private Organisation (Company)*, which represents any non-public organisational that sends documents to the GNG;
- *GNG Employee*, which represents an individual who works for the GNG. Such employees can be furthered categorised as Identification Actor (responsible for categorisation and scanning of a document), Electronic Registration Actor

(employee responsible for performing the first electronic registration of the document), Corrector Actor (employee responsible for correcting and validating the electronic version of the document against the original hard copy), Issue Editor Actor (responsible for adding documents to an issue);

- *GNG General Secretary*, who is responsible for signing GNG issues;
- *Government General Secretary*, who is responsible for approving the issues;
- *Publishing System*, which represents the information system used to support the publication process
- *General Public*, which represents any citizen wishing to access the Volumes (printed issues)

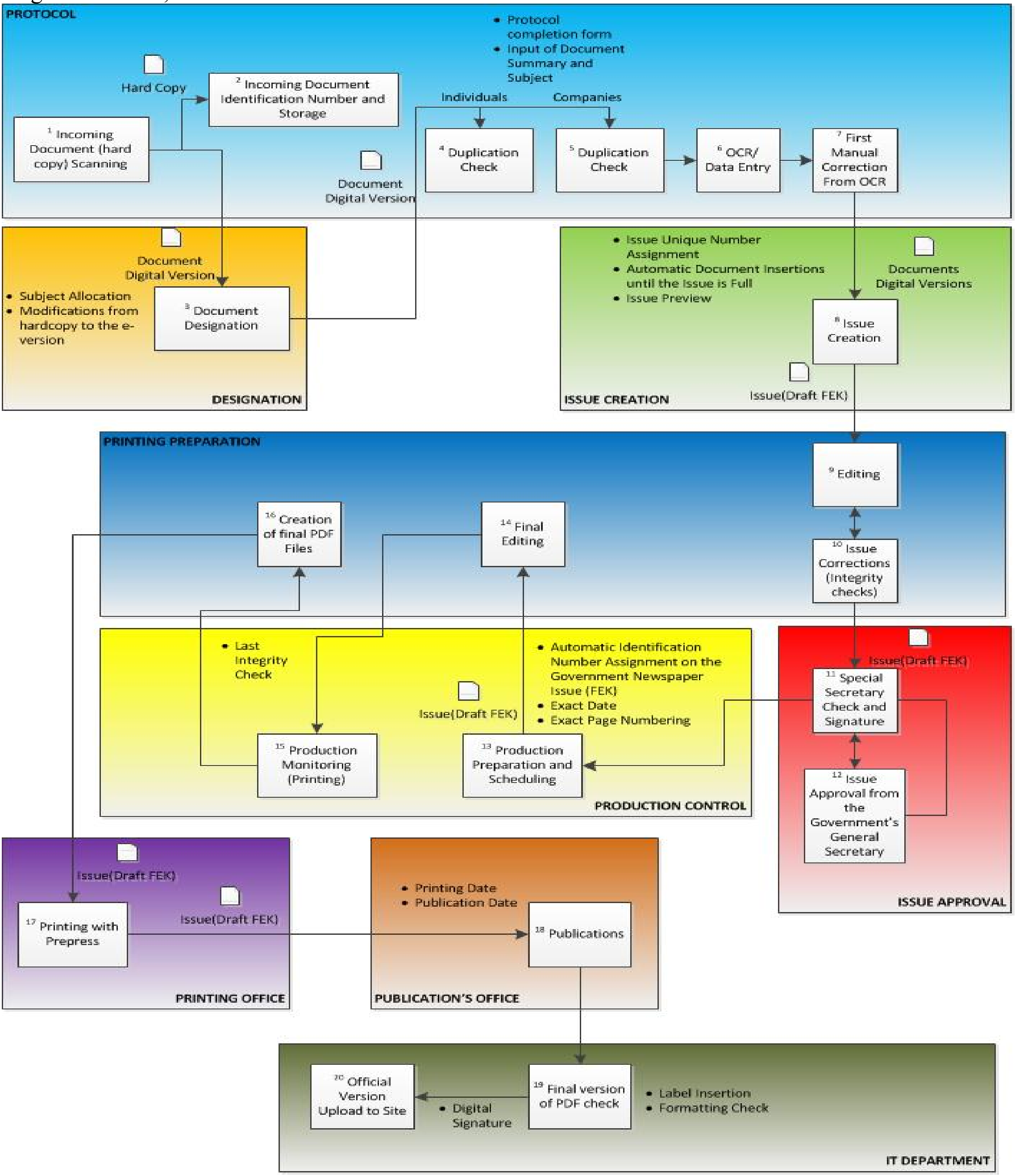

PROTOCOL
Protocol completion form
Input of Document Summary and Subject
Hard Copy
1 Incoming Document (hard copy) Scanning
2 Incoming Document Identification Number and Storage
Individuals
Companies
Document Digital Version
4 Duplication Check
5 Duplication Check
6 OCR/ Data Entry
7 First Manual Correction From OCR
DESIGNATION
Document Digital Version
Subject Allocation
Modifications from hardcopy to the e-version
3 Document Designation
ISSUE CREATION
Issue Unique Number Assignment
Automatic Document Insertions until the Issue is Full
Issue Preview
Documents Digital Versions
8 Issue Creation
Issue(Draft FEK)
PRINTING PREPARATION
9 Editing
10 Issue Corrections (Integrity checks)
14 Final Editing
16 Creation of final PDF Files
PRODUCTION CONTROL
Last Integrity Check
Automatic Identification Number Assignment on the Government Newspaper Issue (FEK)
Exact Date
Exact Page Numbering
Issue(Draft FEK)
15 Production Monitoring (Printing)
13 Production Preparation and Scheduling
ISSUE APPROVAL
Issue(Draft FEK)
11 Special Secretary Check and Signature
12 Issue Approval from the Government's General Secretary
PRINTING OFFICE
Issue(Draft FEK)
Issue(Draft FEK)
17 Printing with Prepress
PUBLICATION'S OFFICE
Printing Date
Publication Date
18 Publications
IT DEPARTMENT
20 Official Version Upload to Site
Digital Signature
19 Final version of PDF check
Label Insertion
Formatting Check

Figure 3. Description of the current administrative procedure

Output 2: GOALS

Each one of the above actors has a number of goals that they try to achieve. For the purposes of this paper we just illustrate the most basic goals of each actor. For instance the main goal of the Public Organisation Actor is to publish all the decisions that by law need to be parts of the Nations paper in order to be valid. In order to achieve that goal, a number of relevant goals can be identified. For instance, the Public Organisation Actor needs to provide the relevant documents to the Greek National Gazette. In doing so, they need to format the documents following a specific template depending on the type of document they sent. That document needs also to be approved by the Public Organisation before it is sent to the GNG. The goals of the Private Organisation actor are similar. On the other hand, 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, either from Public or Private Organisation actors, categorise the document, validate it, and publish it as part of a specific volume. Similar analysis has been employed for all the relevant actors and their main goals are shown below.

The main goal of the Identification Actor is to correctly categorise a document and scan it (in case it has send to the GNG in a hardcopy form), while the main goal of the Electronic Registration actor is to correctly check the electronic version of the document and register the document to the GNG's system. On the other hand, the main goal of the Publishing System is to support the publication process and the main goal of the General Public is to read GNG's volumes.

- *Public Organisation Actor*: Publish Decisions and Bills; Provide Document; Format Document; Approve Document.
- *Private Organisation Actor*: Publish Bills; Provide Document; Format Document; Approve Document.
- *GNG Employee*: Support the creation and publication process of every issue for the Greek Newspaper.
- *Identification Actor*: Identify Document correctly –Scan document – Categorise Document.
- *Electronic Registration Actor*: Perform first electronic registration – provide unique number.
- *Corrector Actor*: Validate textual integrity of electronic document – Conduct small corrections – Communicate with the Public/Private Organisation to verify corrections.
- *Issue Editor Actor*: Edit issue – Add documents – Ensure GNG rules regarding documents prioritisation in publishing process.
- *GNG General Secretary*: Approve GNG issues - Conduct final integrity and format checks.
- *Government General Secretary*: Approve GNG Issues for publication.
- *Publishing System*: support publication process.
- *General Public*: Read Newspaper of the Greek Government.

Output 3: SERVICES

From the above analysis we can also identify a number of services related to the GNG's publication process:

- Receive documents;
- Categorise and Identify documents;
- Transfer documents to Electronic Form (if necessary);
- Check and Validate Electronic Document against original hard copy;
- Create issue (Draft Volume);
- Publish Volume;
- Make Volume available to general public.

Output 4: INFRASTRUCTURE

To support the above services and process, the National Gazette depends on an IT infrastructure that supports the following: Automated management of the Issue & Volume Composition; Work Flow Management; Internal – Administration Services; Internet Services.

Automated management of the Issue & Volume Composition

For accomplishing these tasks a number of subsystems exist which collaborate through the use of a workflow system. These subsystems are:

- Information Collection Subsystem, which supports the collection of the document and its digital storage.
- Sorting Subsystem, which supports the identification of the document and its sorting according to a set of criteria.
- Control and Process Subsystem, which supports the correct format of the document (spelling, typos, document structure) and allocation to the correct issue.
- Volume Composition Subsystem, which controls the issue for publication and stores the issues in the appropriate folders.
- Type-Setting/Layout Subsystem, which supports the finalisation of an issue and adds relevant

typesetting details such as logos, page numbers and so on. When the Volume is ready it is automatically retrofitted to the Volume Composition System in order for the user to make any minor manual adjustments.

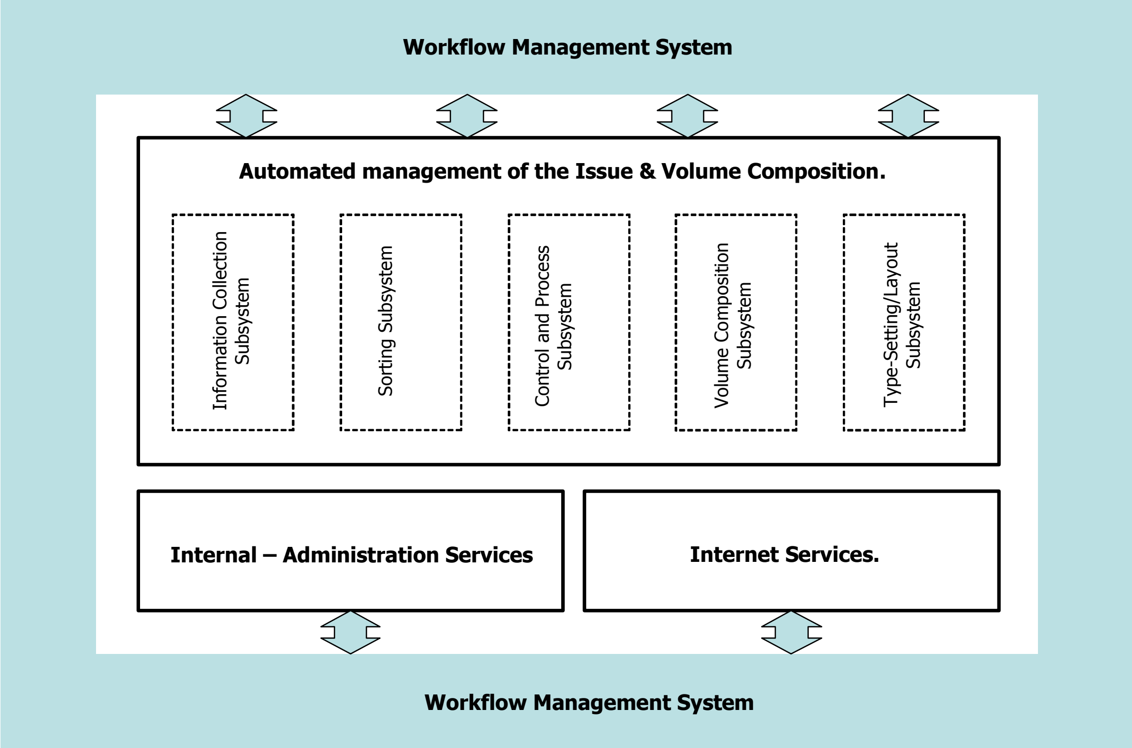

Workflow Management System
Automated management of the Issue & Volume Composition.
Information Collection Subsystem
Sorting Subsystem
Control and Process Subsystem
Volume Composition Subsystem
Type-Setting/Layout Subsystem
Internal – Administration Services
Internet Services.
Workflow Management System

Figure 4. Description of the workflow management system

The whole system records every process along with the respective stage, parameters and electronic files in an internal data base which remains active for as long as it takes in order to process the volumes of a whole academic year.

Workflow Management

This system has been developed with the Zope/Plone platform which provides proper Workflow Management System mechanisms and is responsible for the proper collaboration of the various components on the platform. The available applications are the DCWorkflow and the Openflow used for the management of static work flows and activity workflows respectively. A graphical representation is shown in Figure 4.

Internal – Administration Services

For providing these kind services to the internal users of the Information System the capabilities of the Automated management of the Issue & Volume Composition system are used along with respective query forms for conducting quick searches on old volumes and provide adequate information to citizens. Also a Report Management System is installed supported by the SQL Reporting Services tool which retrieves data from the various SQL databases located on an SQL Server and used from the National Gazette's subsystems. For developing the various reports the RDL XML-based template is used.

Internet Services

The 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. The Volume is stored in pdf and txt formats and also keywords are added for fastening and simplifying the search process. Then the Volume is digitally signed and published in the National Gazette's web site.

When external users are demanding data from the system the Plone Database which has the original data creates replicas with metadata on properly designed databases used specifically for the fast response to the demanding users. These databases serve both the internal and external zones of the system.

A graphical representation of the whole National Gazette's IT architecture is shown in Figure 5.

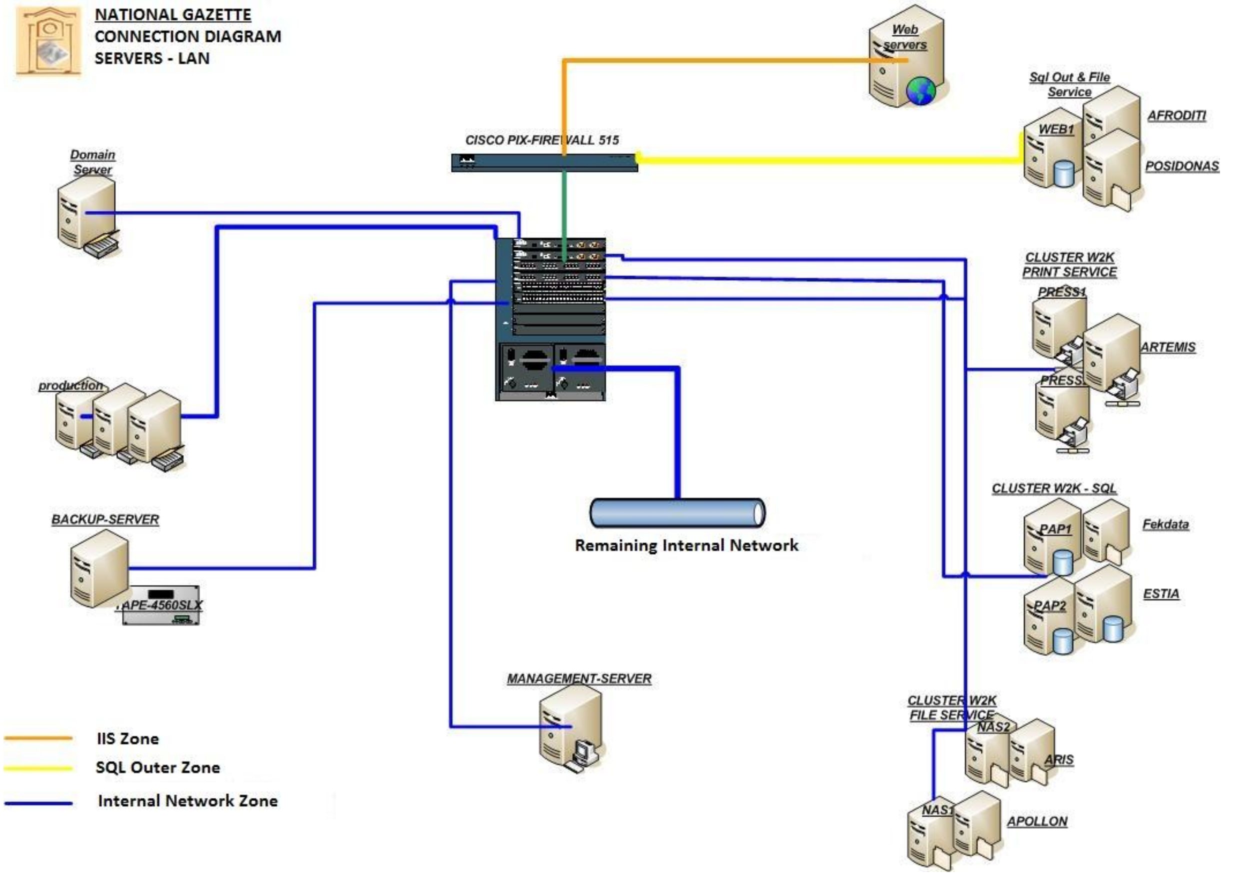


Figure 5. National Gazette's IT architecture

Output 5: CLOUD MIGRATION NEEDS

Following our framework, the second step of activity 1 aims to identify those services that need to be migrated to the cloud. In the case of the GNG, during our project, a decision was made to analyse those services that are considered external to the publication process, i.e. the Receipt of the Documents and 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 of the GNG, since these are the main external services of the GNG providing support for the Public and Private Organisations and the Greek 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 for serving the public and private organisations. The demands on Infrastructure and machine capabilities change on a monthly basis since the publishing needs of the government and the organisations increase dramatically. Current infrastructure will fail to serve the correct and proper documents' reception. Migrating this service on the cloud will solve the infrastructure limitations, sources' constraints and backup issues with much lesser cost that the one needed for the GNG in order to be equipped with new infrastructure. Regarding the second service the reasons of migration are similar. 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 thus saving money and time.

Activity 2: Security and privacy requirements analysis

Output 1: SECURITY AND PRIVACY GOALS

As discussed in the previous section, the second activity of our framework aims to identify and analyse relevant security and privacy requirements.

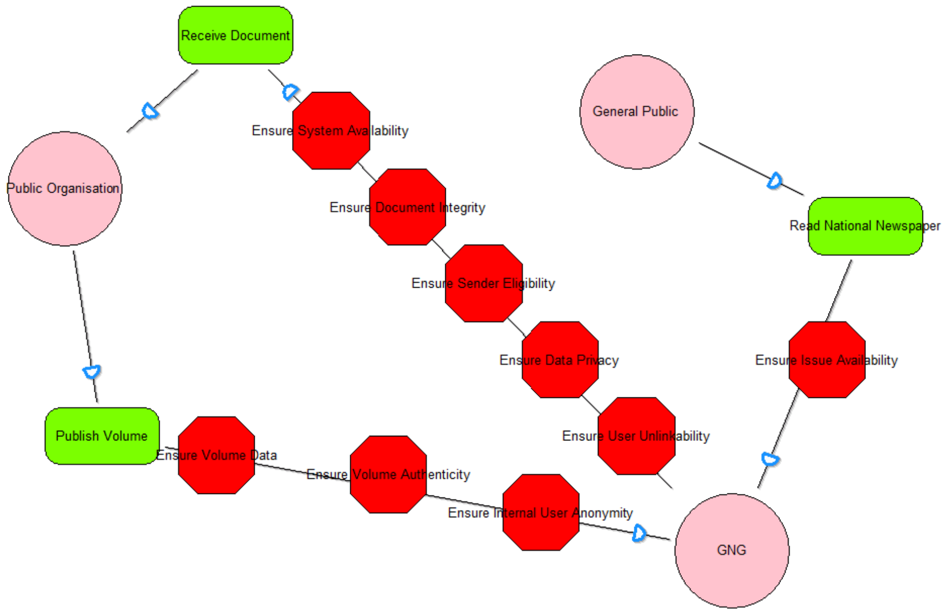
The first step of this activity aims to identify the relevant security and privacy goals. For the GNG case study and relevant to the two identified services we have identified the following security and privacy goals: Confidentiality, Integrity and Availability (Security Goals) and Anonymity, Data Privacy and Unlikability (Privacy Goals).

The Confidentiality goal is mandatory in order to ensure external's user eligibility. Integrity is of vital importance as well since it must be ensured that non – authorised alterations of the documents, issues and volumes are allowed. Availability will ensure that the system will provide the proper mechanisms in order to be able to accept documents for publications as well as provide the published volumes to the Greek Citizens.

Ensuring anonymity of GNG's internal users is also important since the published volumes should not include any identifiable information of the users that worked in the publication process. The volumes should only be signed by the General Secretary and the respective politicians regarding the published documents in each volume. Data Privacy ensures that the private identifiable information of the external users that send documents to the GNG are safely stored along with the requested document and are conformed to the respective EU regulations regarding data manipulation and storage. Finally, unlinkability between the GNG and the external users should be realised when GNG authorisation system sends the authentication means to the external users in order to gain access to the submission system.

Output 2: SECURITY AND PRIVACY CONSTRAINTS

The next step according to the proposed framework is to identify and analyse relevant security and privacy requirements. As discussed in the previous section, in the context of our work we represent security and privacy requirements in the form of security and privacy constraints. We focus our analysis in two services as discussed above and to assist with the analysis we employ the Enhanced Security Actor Diagram from the Secure Tropos methodology. As indicated above, the GNG depends on the Public Organisation Actor to receive the document to be published. On the other hand, the Public Organisation Actor depends on the GNG actor to publish the document. Both these dependencies introduce a number of security and privacy constraints as shown in Figure 6. For example, the Receive Document dependency introduces the following constraints, i.e. Ensure System Availability, Ensure Document Integrity, Ensure Sender Eligibility, Ensure data privacy and Ensure User Unlinkability when providing authentication means to eligible users. On the other hand, the Publish Volume dependency introduces the following constraints, i.e. Ensure Volume Integrity, Ensure Volume Authenticity and Ensure Internal User Anonymity. There is also a dependency between the General Public Actor and the GNG, read National dependency, which introduces one more constraint, i.e. Ensure Issue Availability.


Receive Document
General Public
Ensure System Availability
Public Organisation
Ensure Document Integrity
Read National Newspaper
Ensure Sender Eligibility
Ensure Data Privacy
Ensure Issue Availability
Publish Volume
Ensure User Unlinkability
Ensure Volume Data
Ensure Volume Authenticity
Ensure Internal User Anonymity
GNG

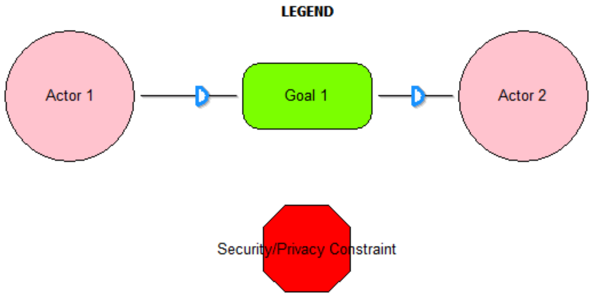


Figure 6. Security and Privacy Constraints for the GNG

Activity 3: Selection of deployment model

According to the framework, the next activity involves the selection of the deployment model. In doing so, three different steps need to be followed. The first is related to the identification and description of relevant deployment scenarios. Once the scenarios to be considered have been defined, and documented in Section 1 of the relevant template, the next step involves the analysis of each one of these scenarios in terms of vulnerabilities, threats and security and privacy mechanisms. The Security and Privacy Deployment Diagram is used for that analysis and the resulting diagram is added to Section 2 of the template. The third and final step involves the deployment scenario selection.

Output 1: DEPLOYMENT SCENARIO TEMPLATE

For the purposes of this paper we have decided to illustrate two different scenarios. Scenario 1 is based on a Public Cloud Deployment model, related to the receive document organisational goal of the Greek National Gazette. The relevant, to that goal, actors are the Public Organisation and the Private Organisation. Our analysis in the previous activity has concluded that relevant to the Receive Document goal, the GNG has a number of security and privacy constraints such as Ensure System Availability, Ensure Document Integrity, Ensure Sender Eligibility, Ensure Data Privacy and Ensure User Unlinkability when providing authentication means to eligible users. Moreover, for the purposes of this scenario we consider that the hosting of the cloud will be on a third party-location. Section 1 of the template in appendix B illustrates the details of Scenario 1, while in Section 2 of that template, the security and privacy deployment analysis is illustrated with the aid of the Security and Privacy Deployment Diagram (SPDD).

Security and Privacy Deployment Diagram (SPDD), shown also in Figure 10 for clarity, shows the GNG public cloud actor along with the various security and privacy constraints, vulnerabilities, threats, security and privacy features and security and privacy mechanisms related to the main goal of the scenario, i.e. Receive Document. In particular, The Receive Document goal is restricted by five different security and privacy constraints as discussed above. For the purposes of this paper, and to keep the analysis to a reasonably easy to understand level, we only illustrate in the template the analysis of three of them, i.e. Ensure System Availability, Ensure Document Integrity and Ensure User Unlinkability. The Ensure System Availability security constraint is endangered by the Cloud Server Operation vulnerability, which can be exploited by the Cloud Lack of Recovery and Cloud Long Term Viability threats. The former threat can be controlled by the Data Recovery security feature, while the latter threat can be controlled by the Data Synchronisation and Failure Reporting security features. A number of security mechanisms have been identified that implement these security features. For example, Data Synchronisation can be implemented by ACID (Atomicity, consistency, isolation, durability) properties mechanism or BASC (Basically Available, Soft State, Eventual Consistency) properties mechanism. Similarly, the Ensure User Unlinkability privacy constraint is endangered by two vulnerabilities, i.e. Plain Text transmission and Eavesdropping of data lines. These two vulnerabilities can be exploited by the Credential Linkage threat (the former vulnerability), and the Identity Disclosure threat (the latter vulnerability). Both threats can be controlled by the Anonymous Communication privacy feature, which can be implemented with a number of different privacy mechanisms such as Onion routing, Tor Architecture, Pseudonimisation, and VM Anonymity. Similar analysis is shown for the Ensure Document Integrity security constraint.

Scenario 2 is based on a Private Cloud Deployment model, related to the same goal as scenario 1, i.e. the Receive Document organisational goal. Because of that, this scenario has the same actors, and security and privacy constraints as Scenario 1 but a different hosting type model, i.e. the cloud is hosted on-premises.

Appendix C illustrates the template of scenario 2. Our Analysis, as also shown in appendix C, illustrated that there are a number of common vulnerabilities, threats and security mechanisms on both scenarios. However, the private cloud scenario introduces some differences in terms of the vulnerabilities and the threats. In particular, Private clouds usually lead to an explosion in the number of VMs in existence, since organisations usually develop libraries of VMs to support quick deployment of new services. As a result, some VMs are created but never used or are used for a while and then go for a significant amount of time without usage. As such they might develop, due to the lack of application of routine software updates, critical vulnerabilities. As such, attackers can exploit that vulnerability by identifying insecure VMs. An important security measure related to that is the ability to monitor VM activity in order to identify abandoned VMs. Security mechanisms related to that are usually monitoring of log files and monitoring of user access records. Another vulnerability that is usually most commonly found in a private cloud is Personally Identifiable Information (PII). Organisations are more willing to store personal identifiable information (such as personnel records) to a cloud model they have control. However, that creates threats related to Identity Disclosure and Credential Linkage.

As discussed in the previous section, once we have analysed all the different scenarios, the next step of the proposed framework is the selection of the appropriate deployment scenario. Looking at the two scenarios analysed above, it is important to note that there is no much difference in terms of the satisfaction of the related security and privacy requirements. In both deployment scenarios, the security and privacy requirements are endangered by quite few vulnerabilities, which in turn can be exploited by a rather large number of threats. Similarly, in both scenarios all threats can be mitigated using appropriate security and privacy features and relevant security and privacy mechanisms. So from that point of view, there are not much differences between the two scenarios. However, our analysis pointed out a fundamental difference. In the case of private cloud, a large number of vulnerabilities are related to malicious insiders such as Hijacking, and vulnerabilities related to the administration of the organisational data and resources, such as Abandoned VMs and Personally Identifiable Information. Our discussion with the relevant software engineers from the GNG indicated that these are vulnerabilities for which action can be easier taken than vulnerabilities where the GNG has no control of. Moreover, although for a large number of security and privacy mechanisms are the same in both scenarios, the staff from GNG believe it is better to have control of the implementation of these mechanisms rather than depend on third party providers. As such, the selected scenario between the two presented in Scenario 2, i.e. the private deployment scenario.

5. Related Work

There are a number of works that have already contributed requirements engineering method for security and privacy for the development of software systems. Mouratidis & Giorgini [16] propose Secure Tropos, an extension of Tropos methodology with the concepts of secure dependency, goal, plan, resource and constraint. The approach supports the analysis of security from the Requirements Engineering phase. Houmb et al. introduce the SecReq approach to elicit, analyse the trace the security requirements from requirements engineering phase to design [7]. A misuse case driven approach is used to establish visual links between use cases and misuse cases for eliciting security requirements at an early stage of the development [9]. PriS is a requirements engineering method that incorporates privacy requirements as organisational goals that need to be satisfied and adopts the use of privacy process patterns as a way to: (a) describe the effect of privacy requirements on business processes; and (b) facilitate the identification of the system architecture that best supports the privacy-related business processes [6, 17]. Islam et al. use natural language patterns with Hohfeld legal taxonomy to extract security requirements from laws and combine them with the ISO/IEC policies and finally trace the identified requirements into the secure system design [21,23]. Four methodological activities are used to evaluate existing security and privacy requirements for legal compliance [24]. The approach in particular prioritises the requirements and establishes traceability links from requirements to legal texts. A model based process is proposed to support security and privacy requirements engineering using a set of concepts such as goal, actor, constraint, and threat [8].

On the other hand, there are works that focus on the security and privacy issues of the cloud computing domain. Mulazzani et al. [25] demonstrate that attackers can exploit data duplication technique to access customer data by obtaining hash code of the stored file. A decision support tool based on cost and benefits and risk is proposed for the public IaaS cloud migration [10]. The cost modelling tool enables users to model IT infrastructure using UML. A goal-drivel approach is introduced to analyse security and privacy risks of cloud based system [2]. Goals, threats and risks are consider from three main components data, service/application, and technical and organisational measure. Some works identify the security and privacy threats. For instance, Pearson identify that privacy threats differ depending on the type of cloud scenario and lack of user control, potential unauthorized secondary usage, data proliferation are more dominate in public cloud [4]. Side-channel attack can instantiate new VMs of a target virtual machine so that the new VM can potentially monitor the cache hosted on the same physical machine [18]. There are four possible places where faults can occur in cloud computing: provider-inner, provider-across, provider user and user-across [5]. It is necessary to address any fault arising from these places within the cloud infrastructure.

The presented works are important and provide solid contribution for understanding security and privacy issues of the system context. However none of the above works focuses on defining a framework to support elicitation and analysis of security and privacy requirements and the selection of an appropriate cloud deployment model based on these requirements. Our work fills that gap.

6. Conclusions

Before migrating their services, data and applications to the cloud, organisations need to understand and control the issues that could pose any potential risks of using the Cloud. Security and privacy issues and threats and vulnerabilities can be different for different cloud deployment models. Moreover, organisations might have different security and privacy requirements from a cloud based system.

In this paper, we have demonstrated a framework that provides a language and a process to support the selection of cloud deployment models based on an organisations security and privacy requirements. We have integrated Secure Tropos and PriS to develop the security and privacy requirements engineering method for the cloud. The application of our work to a real case study has been very promising. The case study results identified a list of security and privacy requirements and two different deployment scenario that are relevant for the organizational context. However, there is more work that needs to be done. Our overall aim is to provide a complete framework that will support organisations in understanding the risks and challenges with respect to security and privacy of migrating their operations to the cloud. In doing so, we believe it is important to develop automated mechanisms and tools to support organisations to analyse their security and privacy requirements and perform a full risk analysis of a potential cloud migration. Our future work will be dedicated towards that aim.

References

[1] Microsoft Technical report: Privacy in the cloud computing era, a Microsoft perspective, November 2009, Microsoft Corp, Redmond, USA

[2]Islam, S., Mouratidis, H., & Weippl, E. (2012b). A Goal-driven Risk Management Approach to Support Security and Privacy Analysis of Cloud-based System, Book chapter Security Engineering for Cloud Computing: Approaches and Tools, IGI global publication.

[3] Version One Survey Results: Cloud Confusion amongst IT Professionals, 24 June 2009, http://www.versionone.co.uk/news/cloud-of-confusion-amongst-it-professionals.php

[4]Pearson, S., & Benameur, A. (2010). 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.

[5] Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding Cloud Computing Vulnerabilities, IEEE Security & Privacy Magazine, Vol. 9(2), pp. 50-57.

[6] Kalloniatis, C., Kavakli, E. and Gritzalis, S. (2008), “Addressing privacy requirements in system design: The PriS method”, Requirements Engineering, 13(3): 241-255.

[7]Houmb, S. H., Islam, S., Knauss, E., Jürjens, J., & Schneider, K. (2010), Eliciting Security Requirements and Tracing them to Design: An Integration of Common Criteria, Heuristics, and UMLsec. Requirements Engineering Journal, 15(1):63–93, March. Springer-Verlag

[8]Islam, S. , Mouratidis, H., Kalloniatis, C. , Hudic, A. , & Zechner, L., (2012a). Model Based Process to Support Security and Privacy Requirements Engineering, International Journal of Secure Software Engineering (IJSSE), Vol. 3, issue 3, September, IGI global publication.

[9]Sindre, G., Opdahl, A. L. (2005). Eliciting security requirements with misuse cases, Requirements Engineering Journal, 10(1): 34–44.

[10] Khajeh-Hosseini, A. , Sommerville , I. , Bogaerts, J. , & Teregowda, P.(2011). Decision Support Tools for Cloud Migration in the Enterprise.

In proceeding of IEEE 4th International Conference on Cloud Computing. IEEE Computer Society.

[11] Baburajan, Rajani, The Rising Cloud Storage Market Opportunity Strengthens Vendors, infoTECH, August 24, 2011". It.tmcnet.com. 2011-08-24. Retrieved 2011-12-02

[12] Kerravala, Zeus, Yankee Group, Migrating to the cloud is dependent infrastructure, Tech Target. Convergedinfrastructure.com. Retrieved 2011-12-02.

[13] Voorsluys, William; Broberg, James; Buyya, Rajkumar . Introduction to Cloud Computing. In R. Buyya, J. Broberg, A.Goscinski. Cloud Computing: Principles and Paradigms. 2011. New York, USA: Wiley Press. pp. 1–44. ISBN 978-0-470-88799-8.

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

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

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

[17] Kavakli, E., Gritzalis, S and Kalloniatis, C. (2007), "Protecting Privacy in System Design: The Electronic Voting Case", Transforming Government: People, Process and Policy, 1(4): 307-332.

[18] Gong, C., Liu, J., Zhang, Q., and Chen, H. & Gong, Z. (2010). The Characteristics of Cloud Computing, Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, IEEE Computer Society Washington, DC, USA.

[19] H. Mouratidis, C. Kalloniatis, S. Islam, M. P. Huget, S. Gritzalis (2012) "Aligning Security and Privacy to support the development of Secure Information Systems, Journal of Universal Computer Science

[20]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

[21]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

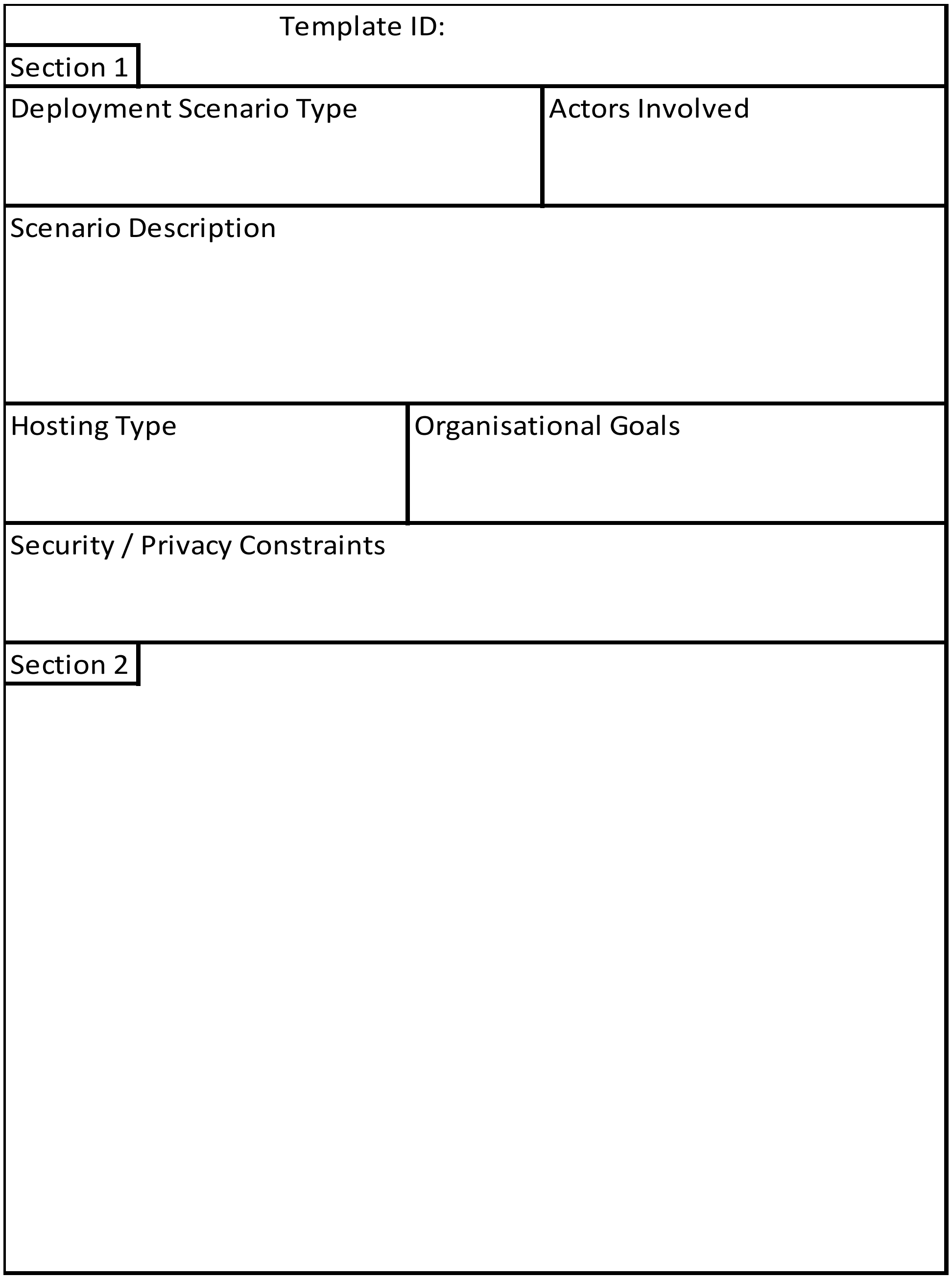
[22] Islam, S., Mouratidis, H. and Jürjens, J.(2011), "A Framework to Support Alignment of Secure Software Engineering with Legal Regulations", Journal of Software and Systems Modeling (SoSyM), Theme Section on Non-Functional System Properties in Domain-Specific Modeling Languages (NFPinDSML), Springer-Verlag.

[23]Islam, S., Mouratidis, H., & Wagner, S.(2010). Toward a framework to elicit and manage security and privacy requirements from laws and regulation, In Proceeding of Requirements Engineering: Foundation for Software Quality(REFSQ), Lecture Notes in Computer Science, Volume 6182/2010, pp.255-261.

[24]Massey, A.K., Otto, P. N., Hayward, L. J. and Antón, A. I., (2010). Evaluating existing security and privacy requirements for legal compliance, Requirements Engineering Journal, Vol 15(1), Springer-Verlag.

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

Appendix A
Cloud Deployment Scenario Template



Template ID:	
Section 1	
Deployment Scenario Type	Actors Involved
Scenario Description	
Hosting Type	Organisational Goals
Security / Privacy Constraints	
Section 2	

Appendix B
Public Cloud Deployment Scenario for GNG

Template ID: **01**

Section 1

Deployment Scenario Type
Public Cloud

Actors Involved
Public Organisation
Private Organisation

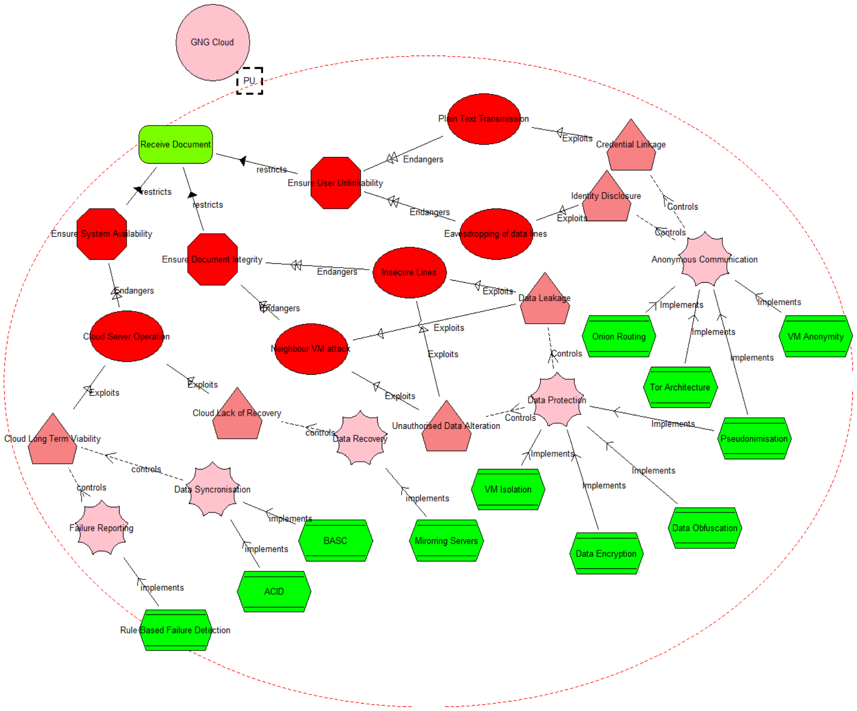
Scenario Description
This Scenario is based on a Public Cloud Deployment model, related to the Receive Document organisational goal of the Greek National Gazette. The GNG depends on Public and Private Organisations to receive the document.

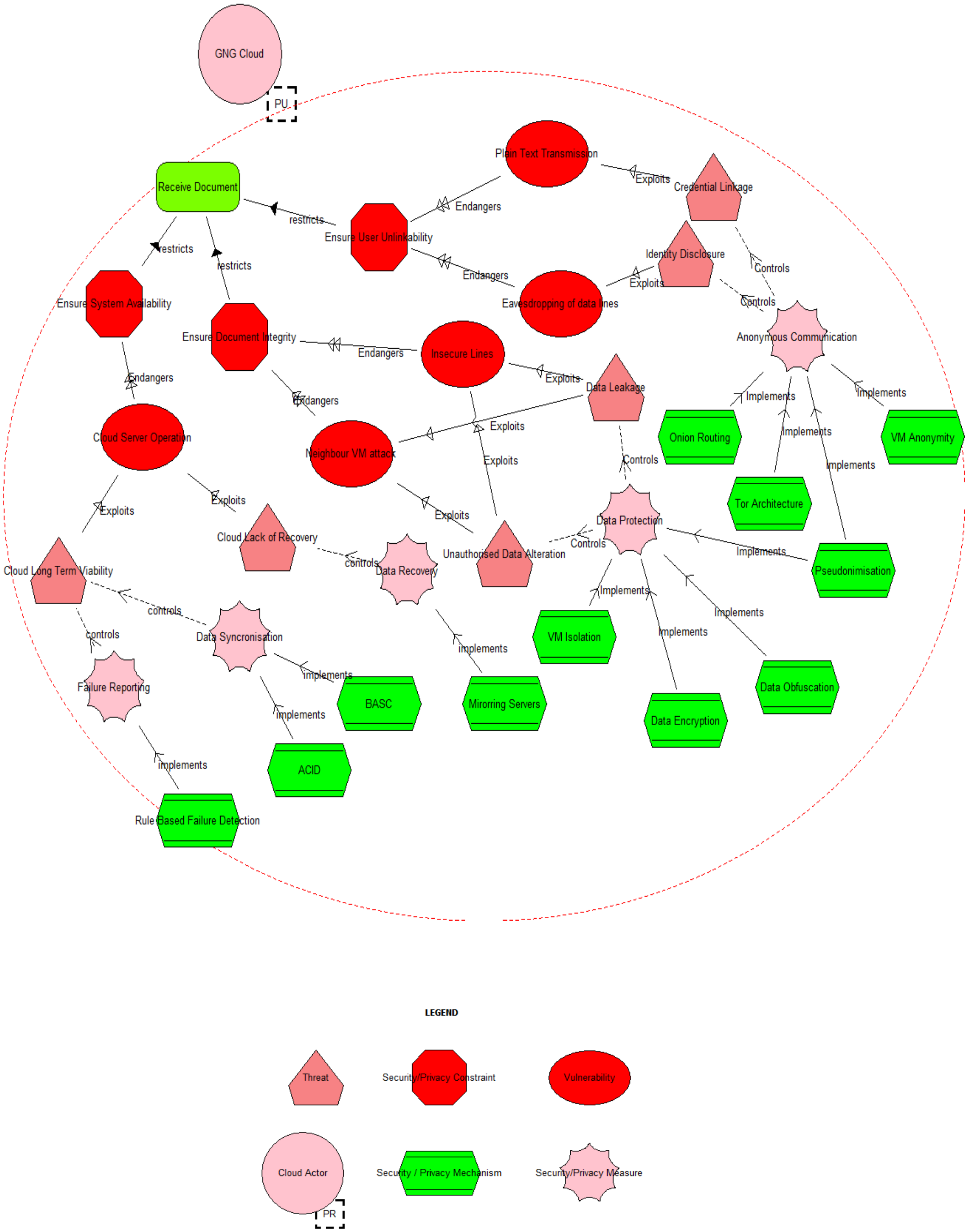
Hosting Type
Third-Party Location

Organisational Goals
Receive Document

Security / Privacy Constraints
Ensure System Availability, Ensure Document Integrity
Ensure Sender Eligibility, Ensure Data Privacy, Ensure User Unlinkability

Section 2




GNG Cloud
PU
Receive Document
Plain Text Transmission
Credential Linkage
Exploits
Endangers
restricts
Ensure User Unlinkability
Identity Disclosure
Controls
restricts
restricts
Endangers
Exploits
Ensure System Availability
Ensure Document Integrity
Eavesdropping of data lines
Controls
Anonymous Communication
Endangers
Insecure Lines
Endangers
Exploits
Data Leakage
Implements
Implements
Endangers
Exploits
Onion Routing
VM Anonymity
Cloud Server Operation
Neighbour VM attack
Implements
Exploits
Controls
Implements
Tor Architecture
Exploits
Exploits
Exploits
Data Protection
Cloud Lack of Recovery
Controls
controls
Unauthorised Data Alteration
Implements
Cloud Long Term Viability
Data Recovery
Pseudonimisation
Implements
controls
Implements
VM Isolation
controls
Data Syncronisation
implements
Implements
Failure Reporting
implements
Data Obfuscation
BASC
Mirorring Servers
Data Encryption
implements
ACID
implements
Rule Based Failure Detection
LEGEND
Threat
Security/Privacy Constraint
Vulnerability
Cloud Actor
PR
Security / Privacy Mechanism
Security/Privacy Measure

Appendix C
Private Cloud Deployment Scenario for GNG

Template ID: **02**

Section 1

Deployment Scenario Type
Private Cloud

Actors Involved
Public Organisation
Private Organisation

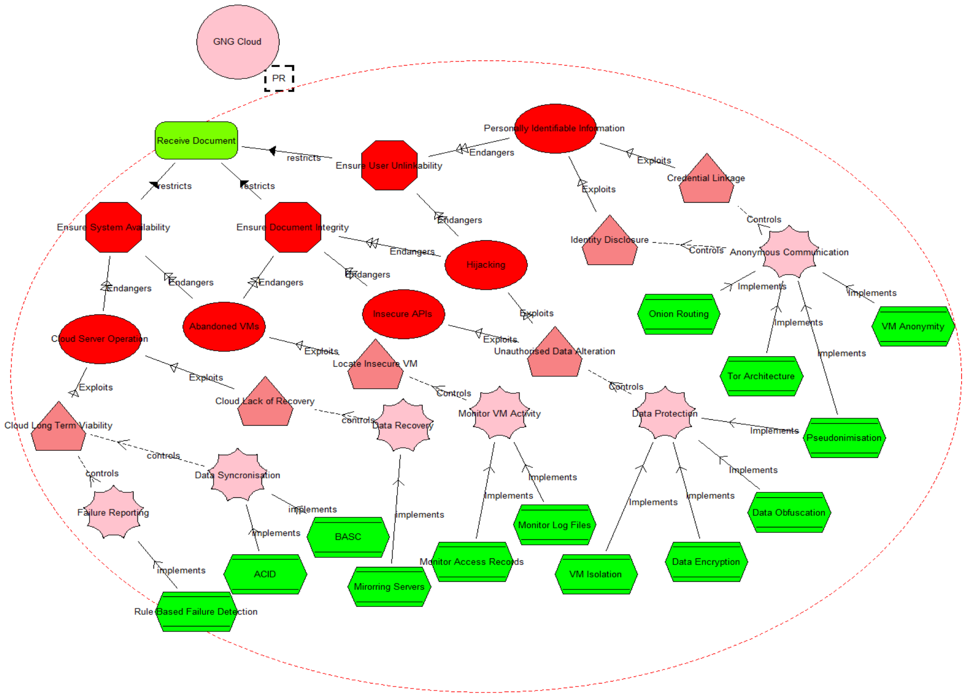
Scenario Description
This Scenario is based on a Private Cloud Deployment model, related to the Receive Document organisational goal of the Greek National Gazette. The GNG depends on Public and Private Organisations to receive the document.

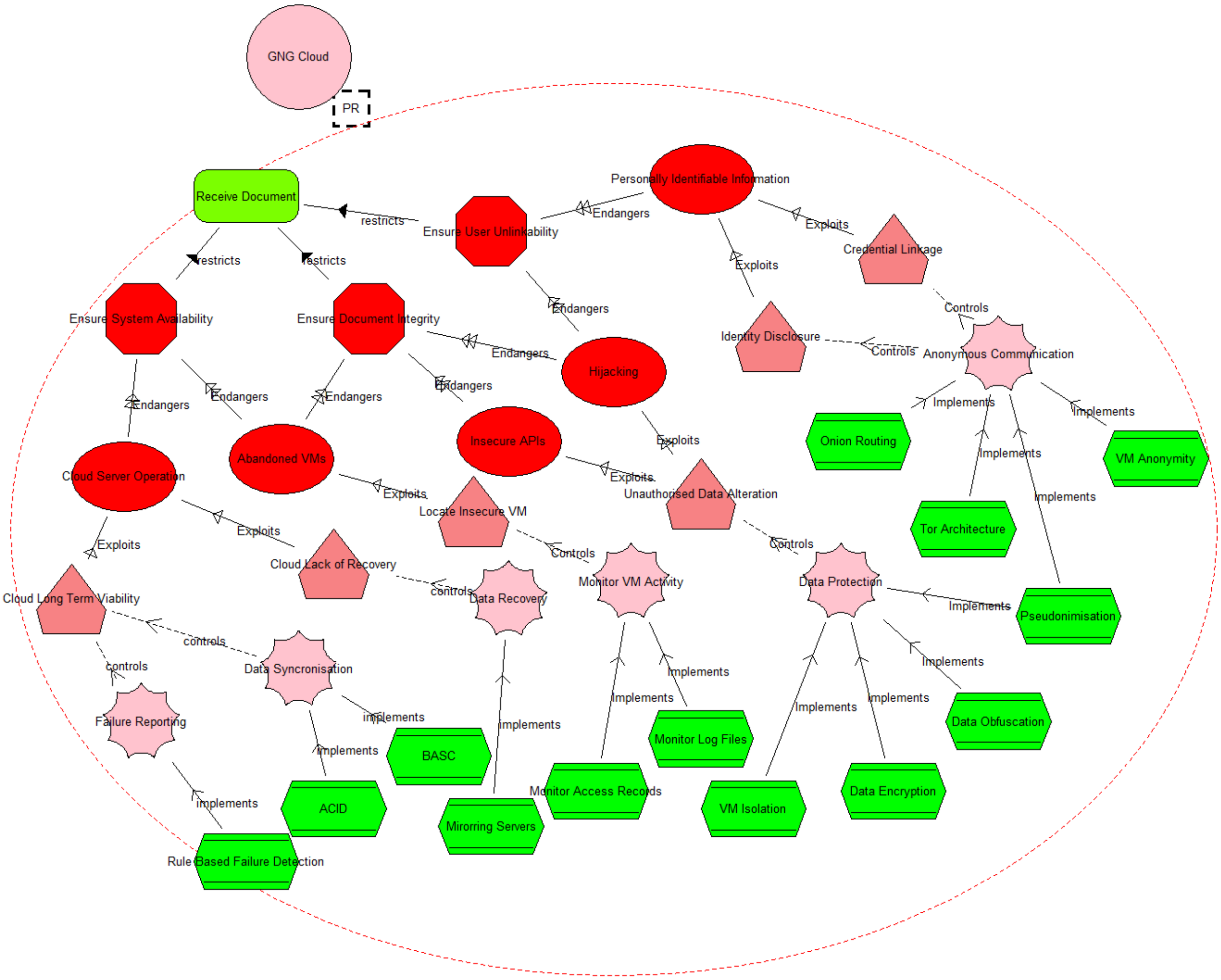
Hosting Type
On-premise Location

Organisational Goals
Receive Document

Security / Privacy Constraints
Ensure System Availability, Ensure Document Integrity
Ensure Sender Eligibility, Ensure Data Privacy, Ensure User Unlinkability

Section 2




GNG Cloud
PR
Receive Document
restricts
Ensure User Unlinkability
Endangers
Personally Identifiable Information
Exploits
Credential Linkage
restricts
restricts
Ensure System Availability
Ensure Document Integrity
Endangers
Exploits
Identity Disclosure
Controls
Controls
Anonymous Communication
Endangers
Hijacking
Endangers
Endangers
Endangers
Endangers
Implements
Implements
Onion Routing
Cloud Server Operation
Abandoned VMs
Insecure APIs
Exploits
Implements
VM Anonymity
Exploits
Exploits
Locate Insecure VM
Unauthorised Data Alteration
Tor Architecture
Implements
Exploits
Cloud Lack of Recovery
Controls
Controls
Exploits
controls
Data Recovery
Monitor VM Activity
Data Protection
Implements
Pseudonimisation
Cloud Long Term Viability
controls
Data Syncronisation
Implements
controls
Implements
Implements
Failure Reporting
implements
implements
Implements
Implements
Data Obfuscation
Implements
Monitor Log Files
BASC
ACID
implements
Monitor Access Records
VM Isolation
Data Encryption
Mirorring Servers
Rule Based Failure Detection