Security Framework for Governmental Clouds

February 2015

enisa

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA team

Dimitra Liveri, Secure infrastructures and services Unit

Dr. M.A.C. Dekker, Secure infrastructures and services Unit

Contact

For contacting the ENISA team please use cloud.security@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

This work has been done in collaboration with Cloud Security Alliance and Technical University of Darmstadt (under the ENISA contract F-COD-14-T10), and in particular with the experts Dr. Patricia Arias (TUDA), Marina Bregu (CSA), Daniele Catteddu (CSA), Dr. Jesus Luna (CSA), Prof. Dr. Neeraj Suri (TUDA), Dr. Ruben Trapero (TUDA) .

Many special thanks to: Tony Richards: G-Cloud, Government Digital Service; Alex Zaharis: Greek research and technology network, Aleida Alcaide: Spanish ministry of finance and public administration, Mikk Lellsaar: Estonian Ministry of Economic Affairs and Communications.

We also thank the experts of the ENISA Cloud Security and Resilience expert group who provided useful comments and feedback on earlier drafts of this document: https://resilience.enisa.europa.eu/cloud-security-and-resilience

ISBN 978-92-9204-115-1 doi: 10.2824/57349

Executive summary

The idea of a central or local government leveraging the Cloud computing business model to increase the effectiveness and efficiencies of the ICT services is appealing, especially in a period of economic challenges for the European Union Member States. The concept of Governmental Cloud (Gov Cloud) has been proposed by ENISA, as well as other international agencies/public institutions since 2010-11. In the report "Security and Resilience in Governmental Clouds" and the "Good practice Guide for securely deploying Governmental Clouds" ENISA proposed, among others, the following:

"…Cloud computing service delivery model satisfies the most of the needs of public administrations, on the one hand, since it offers scalability, elasticity, high performance, resilience and security. However, many public bodies have not yet built a model for assessing their organizational risks related to security and resilience."

It also recommended that:

- *National governments should prepare a strategy on Cloud computing that takes into account the implications for security;*
- *National governments and European Union institutions to further investigate the concept of a European Governmental Cloud as a supra national virtual space where a consistent and harmonized set of rules could be applied, both in terms of legislation and security policy and where interoperability and standardization could be fostered;*
- *National governmental and Member States should foster the adoption of baseline security measures for all cloud deployment models;*

This present study builds on those conclusions and recommendations to provide formalization of a generic *security framework for governmental clouds*. The proposed security framework is based on a collection and analysis of existing Cloud computing security literature, other relevant security best practises, and on the few existing real life case studies of Governmental Clouds in Europe.

The final result is a security framework modelled into four (4) phases, nine (9) security activities and fourteen (14) steps that details the set of actions that we believe each Member States should follow for the definition and implementation of a secure Gov Cloud. The generic security framework has been empirically validated through the analysis of four (4) Gov Cloud case studies namely Estonia, Greece, Spain and UK. The real life validation of the security framework also serves the purpose of defining examples on how some EU Member States are implementing security into their Gov Cloud approaches.

As a concluding remark, we want to highlight (based on the information collected until September 2014), that very few EU Member States have currently developed approaches for Cloud computing based on a well-defined and thorough cloud security strategy (including risk profiles, classification of assets, security objectives and measures).

The objective of the proposed security framework, and the accompanying case studies, is to serve as guidance to other EU Members States towards a seamless and more secure adoption of Cloud computing.

Table of Contents

1 Introduction

The compelling business and financial benefits for adopting Cloud services, highlighted in the European Commission's European Cloud Strategy[1], have motivated a number of EU countries to develop a Cloud computing national strategy[2]. However currently not many Member States (MS) have operational governmental Cloud infrastructures supporting public administration (so called Gov Clouds). Not many public administrations are actively procuring Cloud services nor are they launching any test bed projects on Cloud computing (e.g. the European project "Cloud for Europe").

As the topic of governmental clouds constitutes ongoing exploration and development, there is naturally a conspicuous dearth of information about the experiences of such early Gov Cloud adopters, in particular related to the adopted security frameworks (including requirements, architectures, and best-practices). National experts, policy makers and other interested stakeholders often struggle to find use cases and, thus, cannot benefit from the valuable experience of well-established European Gov Cloud's. The need for detailed information related to the steps a governmental body should take to adopt Cloud services, is the starting point for this report on security frameworks for governmental clouds.

Against this background, this report compiles, analyses and makes available four (4) relevant cases studies on national Cloud security approaches (namely Estonia, Greece, Spain, and United Kingdom) in order to define a reference framework for Gov Cloud security. The contributed framework also integrates relevant findings from topical academic/practitioner literature, and aims to offer value to both the MSs that are starting to define their Cloud computing strategy, and those MSs that already have a Gov Cloud in place but want to assess it with respect to other baselines. This framework indicates the possible approaches, thus offering solutions to the governmental bodies regardless of their maturity. In this report, the technical and security aspects associated to the selected Gov Cloud use cases were analysed through four different perspectives based on a widely used security life-cycle approach (i.e., Plan-Do-Check-Act or PDCA[3]).Following this project management approach would assist in clarifying and categorising the distinct steps.

It must be noted that the framework (thus the specific steps) suggested in this report can be followed, with some minor adjustments, also from other types of cloud customers, not only public administration; however the target audience of this report frames it to focus on governmental cloud deployments.

1.1 Target audience

The results of this report, in particular the developed framework for Gov Cloud security, targets mostly national experts, governmental bodies and public administration in the EU countries interested in recommendations for defining their national Cloud security strategy, or obtaining a baseline for analysing their existing Gov Cloud deployment from the security perspectives, or to support them in filling in their procurement requirements in security.

However in an indirect manner, this report can be helpful for:

[1] Available online http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

[2] Available online http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds

[3] Also known as Deming cycle, PDCA is a four step management method used in business for the control and continuous improvement of processes and products. The PDCA was identified as a suitable continuous process to model information security management systems in Gov Clouds as distinct steps have to be followed and control and continuous monitoring is a notion needed in the gov cloud deployment procedure.

- EU policymakers desiring concise information about state of the art Gov Cloud security strategies from MS in order to decide on further economic, legal and technological incentives for improving the uptake of Cloud computing in the public sector.
- EU private sector, in particular small and medium-sized enterprises (SME), where more experienced studies and guidance are needed to develop the full potential of Cloud computing.
- Cloud Service Providers (CSP) and Cloud Brokers seeking further guidance related to security approaches adopted by existing MS Gov Cloud, in order to identify and better understand specific needs and requirements that might be used to better tune their existing Cloud service offerings.

1.2 Scope

This report is based on the recommendations made in the ENISA "Good practice guide on how to securely deploy governmental clouds", namely the need for a common security framework for deploying cloud services in public administration. The aim of this study is to develop a security framework. A framework is a basic structure underlying a system that is used in this case for establishing a set of general terms, concepts and practices to embed "good enough" information security in the implementation of a Gov Cloud. The framework shall serve as a reference to relevant stakeholders (cf., Section 1.1) for supporting Cloud deployments by public administrations.

1.3 Policy Context

Cloud computing drives the vast spectrum of both current and emerging applications, products and services, and is also a key technology enabler for the Future Internet. Its direct economic value to the European Union is unambiguously substantial. Cloud computing is an accepted enabler for innovation and also widely advocated as such by the European Commission (EC) in their Digital Agenda. The EC considers that Cloud computing will be a game changer in our economy and the main obstacles impeding Cloud adoption are standards, certification, data protection, interoperability, lock-in, and legal certainty[4].

In September 2012, the EC published, , the European Cloud Strategy, a policy strategy document that contains the key actions that EC policy makers have identified to support the uptake of Cloud computing in Europe. The European Cloud Strategy has two main objectives:

- Making Europe Cloud-friendly and Cloud-active.
- Connecting digital agenda initiatives.

Achieving these two objectives requires the execution of three key actions:

1. Standards and certification.
2. Safe and fair contract terms.
3. A European Cloud Partnership

This report is part of ENISA's contributions to the implementation of the European Cloud Strategy, in particular related to the development of a security framework for governmental Cloud's aimed to provide stakeholders (cf., Section 1.1) efficiency savings and take them one step closer to the "Every European Digital" goal.

[4] Warwick A. "Neelie Kroes calls for speedy EU uptake of Cloud computing". Online: http://www.computerweekly.com/news/2240114460/Neelie-Kroes-calls-for-speedy-EU-uptake-of-Cloud-computing 2012

1.4 Definitions

A standard definition for the term Gov Cloud is currently lacking. However, for the analysis presented in the rest of this document we adopt the Gov Cloud definition introduced by ENISA 2013 report, as:

- *"A Gov Cloud is an environment running services compliant with governmental and EU legislations on security, privacy and resilience (what)*
- *A Gov Cloud is a secure and trustworthy way (private Cloud or public Cloud) to run services under public body governance (how)*
- *A Gov Cloud is a deployment model to build and deliver services to state agencies (internal delivery of services), to citizens and to enterprises (external delivery of services to society) (for who)"*

An additional definition required in this report, relates to the notion of "security framework". This is as a conceptual structure intended to serve as a support or guide for the creation of a secure information system. In this document, the intention of the proposed security framework is to serve as a comprehensive guideline for the creation, deployment, assessment and improvement of a secure Gov Cloud. The proposed security framework is to be understood as a first step towards improving the European Gov Cloud landscape. Furthermore, it should be considered as the beginning of a continuous enhancement process by incorporating emerging elements, and by considering the lessons learned from its real-world application.

1.5 Methodology

The methodology to elaborate such a logic model for a security framework follows a bottom-up approach for information processing and knowledge ordering. The technical methodology focused on:

a) Defining the generic security framework based on the input collected from the analysis of available literature, and information obtained from operational Gov Clouds in European Member States. The proposed framework is based on the Plan-Do-Check-Act (PDCA) cycle. The structure of the framework is flexible enough to be extended when new use-cases will be analysed (future work).
b) Surveying and identifying four Gov Cloud use cases from MS (i.e., Estonia, Greece, Spain, and United Kingdom). The use cases were selected for being representative of Gov Cloud adoption (or mature enough) and also for their willingness to provide the required documentation to conduct the validation
c) Use case scenarios of the initially defined generic security framework through the analysis of the strategies adopted by selected case studies from the security life cycle perspective. In order to accomplish this, we identified and engaged relevant stakeholders/representatives from the selected Gov Cloud use cases through e.g., telephone interviews and email communications.

The adopted methodology allowed us to characterise the Gov Cloud use cases from different security angles (e.g. requirements, certifications, SLAs and contracts), and taking into consideration relevant security challenges (e.g., resilience, portability, continuous monitoring, and access control). This methodological approach resulted on a comprehensive analysis of selected Gov Cloud security frameworks provided as use cases, hence promoting the definition of a reference Cloud security strategy blueprint.

In summary, the core framework describes what to do when deploying secure Gov Cloud services, whereas the workflows, questionnaires and reference implementations detail how to do it. All these instruments are to be collectively used by the governmental organizations and public administrations (who), to define and implement secure Cloud-based services.

1.6 Structure

This document is organized as folllows: Section 2 details the proposed security framework for Gov Clouds, and also introduces the underlying roles and definitions. Section 3 introduces the MS use cases, and validates the proposed security framework (cf., Section 2) through the four selected Gov Cloud use cases (Estonia, Greece, Spain and United Kingdom). Section 4 summarizes the main conclusions and recommendations drawn from this report. Annexes A and B presents the full version of the questionnaires used during the interviews with the selected Gov Cloud representatives. Annex C discusses the results of our desktop research, by presenting the relevant state of the art/practice on the topic of security frameworks for Gov Clouds. Annex D contains the questionnaire template used for the interviews with the selected use cases. This questionnaire is a concrete result of the security framework presented in this report.

2 State of the art in Gov Cloud activities

Previous to the design of the framework, a desk research was conducted to identify and analyse relevant work in the field of Governmental Cloud computing, since the gap analysis performed in the ENISA 2013 Gov clouds guide. This task was supported by the need to understand the following questions:

- Which is the state of deployment in various Member States (running pilots, plans, etc) since 2013?
- What are the challenges, requirements and barriers in the "cloudification" of governmental services?
- What are the state-of-the-art techniques to analyse Cloud security in governmental deployments? Is there any existing generic security framework?

This preliminary study helped in setting the basis for the rationale behind the proposed security framework. In the next paragraphs, we summarize the related work (references [29]-[42]) considering the research questions posed above.

2.1 Desk research

The work in [29] evaluates eight European countries on their use of Cloud Computing in e-Government and compares them: Austria, Denmark, Finland, France, Germany, Ireland, Spain and UK. The comparative analysis is synthetized in Table 1.

This study shows that, while the majority of countries are still in the development or planning phase, three of them -namely UK, Spain and Denmark- have already adopted Cloud Computing and hence are in an executional stage. It is to note also that, five of the eight researched countries have anchored the adoption of Cloud computing in the public sector in some kind of national strategy. Nevertheless, the full implementation of their National Cloud Computing strategy will still take another few years (conclusion derived in the ENISA 2013 guide). The most frequent planned and developed Cloud Computing deployment models amongst the evaluated countries are the private and the community Cloud. On the other hand, when comparing Cloud computing service models, 50% of the evaluated countries rely on the most common service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

The guide elaborated by the law firm Bird&Bird [30] covers the legal issues to take into account when setting up a Cloud service on a pan-European basis, including data security and data privacy regulations. The research covers twelve countries (Czech Republic, Denmark, France, Germany, Hungary, Italy, Poland, Spain, Sweden, UAE and UK) and, for each of these case studies, they include questions regarding Cloud computing usage in the public sector, such as information about operating government clouds or best practice guides for public bodies.

Gongolidis et al. [31] identified the major functional and non-functional requirements to migrate governmental applications to the Cloud. Based on the reports provided by the European Union for i2010 initiatives [32], United Nations reports for eGovernment Systems characteristics, and the Greek Interoperability Framework [34], the authors elicit the following requirements: interoperability, eAccesibility, single sign-on, transparency, scalability, adaptability, use of prototypes, availability, maintenance, and security and privacy. The paper includes also a mapping of these requirements to the different deployment models that are subject of their applicability.

Country	Cloud Computing anchored in a National Strategy	Cloud Adoption	Cloud Adoption Level	Cloud Deployment Models	Cloud Service Models	Cloud e-Government Sample Services
Austria	Yes	Planned	National Regional City	Public Cloud Private Cloud Community Cloud	IaaS PaS SaaS	Backup/Archiving Cloud Framework for e-Government applications Collaboration Suites Identity as a Service
Denmark	No	Planned Executional	Municipality	Public Cloud Private Cloud Community Cloud	SaaS	E-Mail Procurement
Finland	No	Planned				
France	Yes	Development	National	Community Cloud	IaaS	
Germany	Yes	Planned				
Ireland	Yes	Planned	National	Public Cloud Private Cloud Community Cloud	IaaS PaaS SaaS	Open Data Public Information Repositories Collaboration Suites E-Mail
Spain	No	Planned Executional	National Regional City	Public Cloud Private Cloud Community Cloud Hybrid Cloud	IaaS PaaS SaaS	E-Government Services Open Government Citizen participation E-Mail Storage/Backup Office and Collaboration
UK	Yes	Development Executional	National	Private Cloud Community Cloud	IaaS PaaS SaaS	E-Mail Office Customer Relationship Management

Table 1 Comparison of Cloud computing in e-Government across eight European countries made in [29] (for Finland and Germany no further information was available to compare them against the other countries)

Wyld [35] examines non-military uses of Cloud computing in governments across the globe (Unites States, Europe and Asia), which builds the basis of his proposed 6-step "Cloud Migration Strategy" for governmental agencies to shift to Cloud computing. In this study, as well as in a previous deeper research on Cloud for governments by the same author [36], Security and Privacy are pointed out as key requirements to enable Cloud computing migration. Furthermore, Wyld highlights the need for the development of Cloud pilots to test the utility of the technology and assess the ability to manage and bring such a project to fruition. These efforts, he remarks, should be supported—and reported within and outside the organization—so that others in IT and wider community can learn of the successes and the downsides of operating on Cloud. Thus, it will be vitally important to share both "best practices" and "lessons learned", since these demonstrations will drive the eventual acceptance and adoption of Cloud computing in governmental environments and beyond.

Tripathi and Parihar [37] provide a brief overview of e-governance challenges, categorizing them in technical, economic and social barriers. Security is again identified as a key requirement to overcome before migration of governmental services to Cloud happens.

The work carried out by Smitha et al. in [38] presents a survey on Cloud-based E-Governance systems, where E-governance is defined as "the application of information and communication technologies to exchange information between government and citizens, government and business organizations, and

between government organizations." They focus on identifying the main challenges and benefits of relying on the Cloud paradigm, pointing out again security and privacy as indispensable requirements.

Paquette et al. [39] identify the security risks involved in the governmental use of Cloud computing. The base on specific cases of the USA federal Cloud computing strategy and discuss the tangible and intangible risks associated with its use. The paper argues that a defined risk management program focused on Cloud computing is an essential part of the government IT environment. As they point out, there are risks linked to the implementation of the emerging Cloud computing paradigm, including policy changes, implementation of dynamic applications, and securing the dynamic environment. They also remark the importance of defining detailed SLAs as a mean to formalize security aspects to be covered and cope with risk.

The survey carried out in [39] is centered on the analysis of the readiness (i.e., maturity state) of E-government Information systems (EGIS) and Cloud Computing. The study concludes that e-government readiness is a major concern, and that currently there is little availability of comprehensive assessment methods for e-government readiness and most of the assessment frameworks are varied in terms of philosophies, objectives, methodologies, approaches, and results. As a guide for future work, the paper proposes a new framework with the aim to provide a modeling and analysis method to guide the assessment of EGIS systems migration readiness. The framework considers four dimensions, namely: Technical, Organizational, Stakeholders and Environment and Society. Security and privacy are to be considered as key components of the identified assessment dimensions.

Finally, a close related work is the "Analysis of Cloud best practices and pilots for the public sector" [40] published in 2013 by the European commission. This report aims at analysing the current national initiatives for the deployment of clouds in the public sector in ten Member States, and the methodological approach builds on interviews and desk research. The study concludes that so far, in the analysed Member States (Austria, Belgium, Denmark, France, Germany, Italy, the Netherlands, Portugal, Spain, and United Kingdom), the deployment of Cloud in the public sector (at the national level) is at a very early stage. The Member States have taken very different approaches regarding Cloud in terms of applications covered (citizen-type, employee-type, vertical, critical, sensitive), type of infrastructure (public Cloud versus private Cloud), relationships with e-government applications (development from scratch or just migration of existing applications), or global policy. Thise analysis is centered around the kind of deployment models, general features and existing barriers; but there is no assessment with regard to security.

2.2 Findings and conclusions

In summary, after studying the state-of-the art, we can conclude that:

- The state of deployment of Governmental Cloud computing is in general at a very early stage. Not many changes have been noted since the ENISA 2013 study[5] that presented cloud adoption levels in the EU. The changes are depicted in the image below. The information on this diagram is based on the desk research and only discusses 13 countries of the EU (based on information from the desk research).
- Security and privacy issues are considered as key factors to take into account for migration, and at the same time are the main barriers for adoption. Protection of sensitive data is still an issue seeking solution, spanning from the SLA provisions to the actual technological mechanisms i.e encryption etc. Even though most countries recognize the benefits from

[5] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds/at_download/fullReport

adopting a business model like cloud (scalability, resilience, portability), they are reluctant to take the next step and migrate services to the cloud.

- There is a clear need for Cloud pilots (like Cloud4Europe project) and prototypes in order to test the utility of the technology. There is also a need for best practices and success stories to be disseminated in the EU public administration community. Furthermore, it is crucial to report these efforts within and outside the organizations so that it raises awareness among the broad IT community of the actual advantages and the disadvantages of operating in the clouds[6].
- The main security challenges, requirements and barriers in the cloudification of governmental services are related to: data protection and compliance, interoperability and data portability, identity and access management, auditing, adaptability and availability, as well as risk management and detailed security SLA formalization.
- There are no current studies that comprehensively analyse the security frameworks of currently running or planned governmental Cloud deployments. Hence, there are no guidelines to define a generic security framework that allows to assess and benchmark Gov Cloud security.

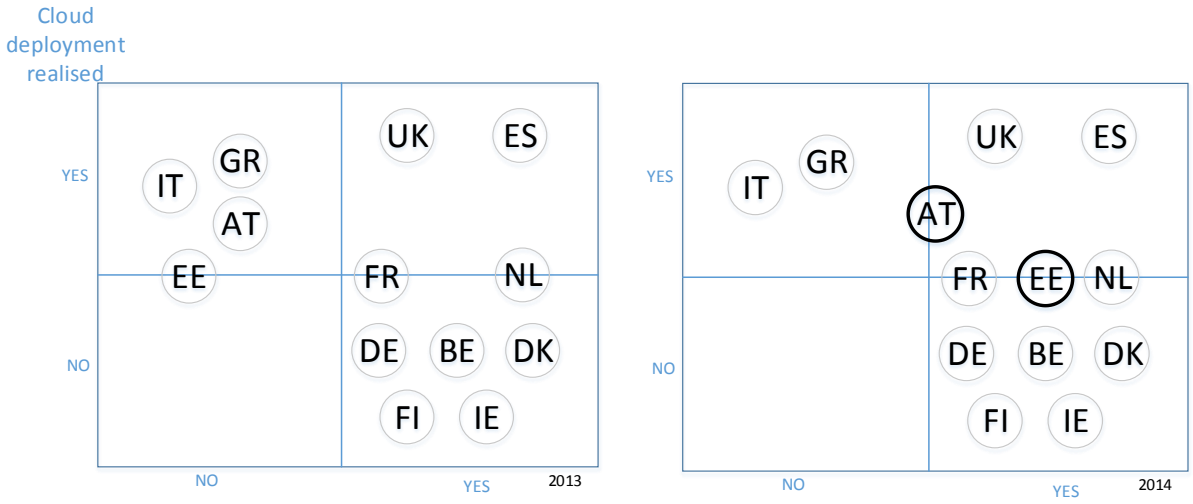


Figure 1 Cloud adoption in 13 countries in the EU during 2013-2014

The identified challenges, barriers and requirements are placed as input to model the structure of the proposed generic security framework. It is to mention that this work builds on two previous ENISA studies: the first one[7] was centered on defining a decision-making model to be used by senior management to determine how operational, legal and information security requirements, can drive the identification of the Gov Cloud architectural solution that best suits the needs of their organization. The second work [42] performs a gap analysis the Member States based on the government Cloud infrastructures and underlines the diversity of Cloud adoption in the public sector in Europe and the need of a common framework.

[6] As stated in [36] "it will be vitally important to share both "best practices" and "lessons learned", since these demonstrations will drive the eventual acceptance and adoption of Cloud computing in governmental environments and beyond."

[7] http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds

3 Security Framework for Governmental Clouds

Based on input collected during the desk research and some preliminary interviews, a logic model for a security framework for governmental clouds was sketched including the specific activities and steps. In addition to that, a description of the different roles of the involved parties (cloud customer, cloud provider, citizens, so on) is included and their responsibilities/involvement to each of the phases of the lifecycle is defined.

3.1 Roles

The (common) relevant roles found in the definition and implementation of the analysed Gov Cloud use cases explained below:

- **Cloud Owner** relates to the organization that legally owns the Gov Cloud and defines policies and requirements.
  Example: the Greek Research and Technology Network S.A. (GRNET S.A.) provides Cloud services to the academic and research community in the case of the Greek Gov Cloud (Okeanos and ViMa)[8].

- **Cloud Service Provider (CSP)** is the organization that provides Cloud services to the Gov Cloud and takes responsibility for making them available to the Cloud Customers. Provision of services is defined according to the requirements specified by the Cloud Owner, and usually described on Service Level Agreements (SLA) and other contracts. CSP's might own and/or manage the IT infrastructure (IaaS), platform (PaaS) and applications (SaaS) that are made available to Cloud Customers, or provide applications (PaaS or SaaS) on top of an infrastructure and/platform fully managed by the Cloud Owner.
  Example: in the Spanish Gov Cloud the Cloud Owner also provides Cloud services[9] , whereas in the case of U.K. the Cloud services are provided by accredited public CSP's[10].

- **Cloud Customer** is the organization/public administration using the Cloud services provided by the CSP through the Cloud Owner.
  Example: in Spain the Gov Cloud offers services to the Spanish Public Administration e.g., the @firma platform for e-certificate validation.

Finally, it should be emphasized that different roles may be adopted at the same time by the same entity, for example the Spanish Public Administration owns and provisions Cloud services through the SARA[11] network (owner and provider). In the same context, the role of the customer and the owner can be filled by one authority i.e. a governmental authority that want to provide cloud services for internal communication to its staff.

We explain in each security step of the lifecycle how these different stakeholders are involved, what are their specific roles based on the three definitions presented above, and finally which their responsibilities are. The roles are depicted below:

[8] More information can be found on Section 4.1.1.
[9] cf., Section 4.1.3
[10] cf., Section 4.1.4
[11] SARA is an acronym that in English stands for "Spanish Public Administrations Network".

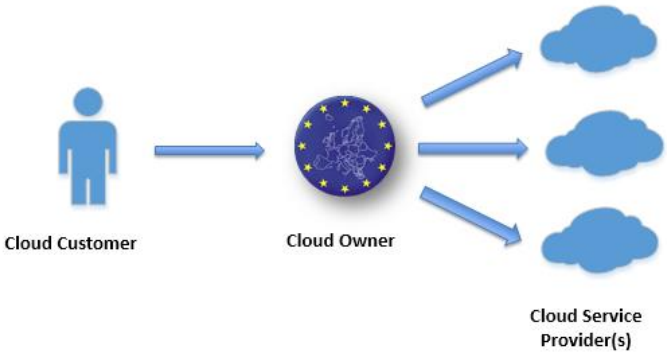


Figure 2. Gov Cloud roles.

3.2 Logic Model

Based on the preliminary analysis of the state of the art and use cases presented in this document, together with the feedback obtained from the individual interviews, the Plan-Do-Check-Act (PDCA)[12] was identified as a suitable continuous process to model information security management systems in Gov Clouds. In consequence, the PDCA cycle leads to the definition of the proposed security framework for governmental Clouds presented in this report. This model is very often adopted in information security as it clearly identifies the individual steps of a process and it includes the notion on evaluation (check) and adjustment/update (act) which is very important in all network and information security aspects. It has to be noted that this Framework should be part of a greater plan the governmental bodies will design for procuring cloud services; this Framework covers the security perspective of the decision.

The PDCA model (also called "Deming cycle") encompasses the following phases:

1. **Plan**: This phase focuses on setting policies along with a strategy for implementing controls to achieve security objectives.
2. **Do:** This phase involves implementing and operating the controls, i.e., controls are executed in the DO Phase.
3. **Check:** This phase is focused on the review and evaluation of the performance (efficiency and effectiveness) of the system. Tests are performed to ensure that controls are operating as intended and meet objectives.
4. **Act:** This phase involves the remediation to deficiencies or gaps identified in the CHECK Phase. Changes are made to improve the approach or when necessary to bring the system back to the planned performance.

Our study identified these phases as the general steps a governmental agency/public administration typically follows to deploy a secure service in the Cloud.

Each phase of the cycle is sub-divided into a number of sample tasks/actions that are considered to be necessary to reflect the specific needs and requirements of a country's public administration. The conclusion to these phases was based on the desk research conducted and initial input from the existing gov cloud deployments. The list of tasks identified and suggested is not meant to be considered as exhaustive; the framework is flexible enough to accommodate more or less requirements and can be adjusted accordingly. The different tasks proposed for each stage, together with their inputs and outputs, are detailed in the next sections. For all the phases we provide examples

[12] http://kaizensite.com/learninglean/wp-content/uploads/2012/09/Evolution-of-PDCA.pdf,

to support the factuality of this framework, back to back with the existing Gov Cloud implementations. Additionally, for each phase, a template is provided (cf., Annex C) to identify the security-related information that must be collected and used by the governmental agency during the PDCA cycle.

In table 2 we present an overview of our security framework based on the PDCA lifecycle:

Lifecycle Phase	Security Activity	Security Steps	Example[13]
PLAN *This phase focuses on setting policies, a strategy for implementing controls to achieve security objectives*	Risk Profiling	Identify services to "*cloudify*"	The UK's Gov Cloud defines three categories (Official, Secret, Top Secret), to profile the risk associated with the assets to "cloudify".
		Select relevant Security Dimensions[14]	
		Evaluate individual impact to dimensions	
		Determine global Risk Profile	
	Architectural Model	Decide on the deployment-Service Model[15]	Surveyed Gov Cloud's do not define specific security criteria for selecting the deployment model.
	Security & Privacy requirements	Establish Security Requirements	The Greek Gov Cloud defines a set of baseline requirements for CSP's.
DO *This phase involves implementing and operating the controls, i.e., controls are executed in the DO Phase*	Security Controls	Selection of security controls	Not a common approach (none of the surveyed Gov Clouds define baseline controls based on the selected service/deployment model.
	Implementation, Deployment & Accreditation	Formalization and implementation of the selected security controls	The Spanish Gov Cloud defines self-assessment as an option for ex ante verification.
		ex ante verification of suitability of the Cloud service to provide a sufficient level of assurance	
		Start service execution	
CHECK *This phase is focused on the review and evaluation of the performance (efficiency and effectiveness) of the system. Tests are performed to ensure that*	Log/Monitoring	Periodically check that security controls are in place and being followed	The Spanish Gov Cloud has deployed a set of tailored tools for monitoring the implemented security controls.

[13] Further details in Section 4.
[14] Security dimensions are the aspects of information security that combined offer a completely secure solution; the basics are availability, integrity and confidentiality however the list has been updated the last few years (privacy,
[15] Deployment model: public, private, community cloud

Lifecycle Phase	Security Activity	Security Steps	Example[13]
controls are operating as intended and meet objectives	**Audit**	Verification that the defined / contracted levels of security are fulfilled	The UK Gov Cloud performs annual audits through accredited consultants.
ACT *This phase involves the remediation of deficiencies or gaps identified in the CHECK Phase. Changes are made where necessary to bring the system back to the planned performance.*	**Changes Management**	Implementation of remedies and improvement to the security framework / approach	The Greek Gov Cloud detects and reacts to SLA violation in an ad-hoc manner.
	Exit Management	Contract termination, return of data to customer and data deletion	Cloud Customers can request deletion of their data from the Greek Gov Cloud on termination of contract.

Table 2 Overview of the logic model

Let see now in detail the specific phases:

3.2.1 PLAN Phase

When taking the decision of moving a service to the Cloud, the first critical step is planning. From a security point of view, planning involves the definition of a risk profile and the identification of security requirements. Thus, the final goal of the PLAN phase is to design a security programme built on risk analysis. The tasks or activities to be carried out in the PLAN phase are shown in the flow diagram in Figure 3.

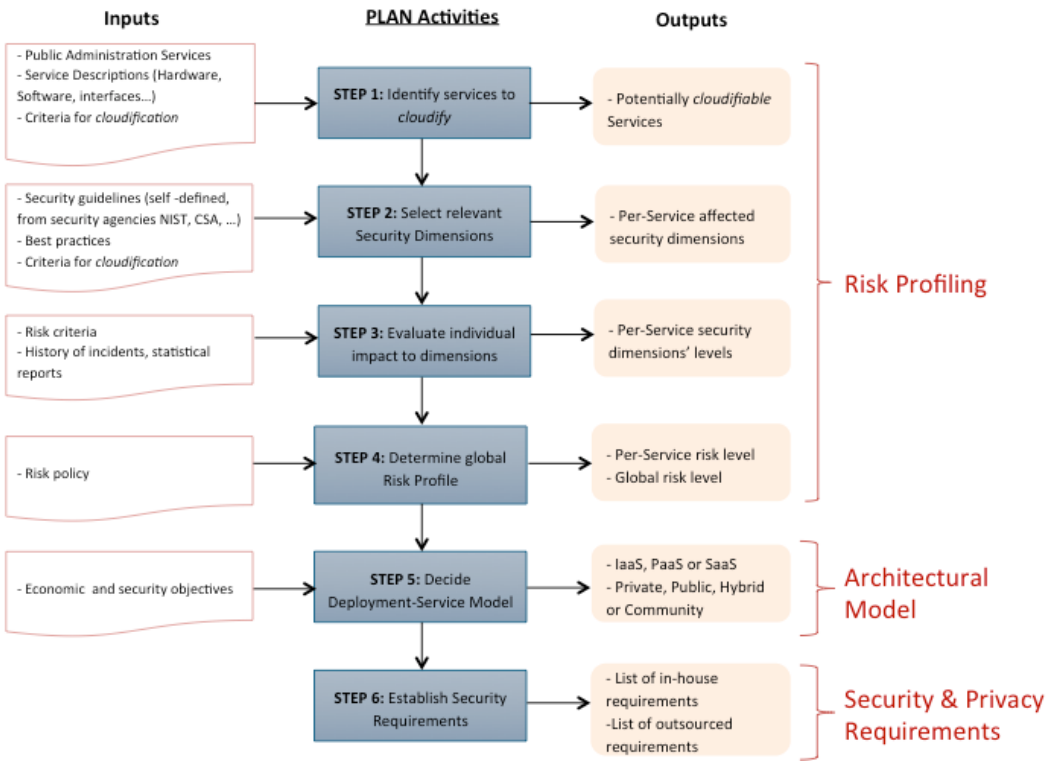


Figure 3. PLAN Phase workflow: activities, inputs and outputs.

The first part of the planning requires the Gov Cloud Customer to categorize its assets depending on the criticality of the services provided and the information handled. The selection of an asset category is based on risk, which implies considering the impact and the probability (potential loss) that an adverse event affecting the security of the information or systems would have on the organization. For example, the data managed by a governmental healthcare service are more sensitive and require stricter security measures than a service for consulting traffic information.

This process of categorization is called "***Risk Profiling***" and involves Steps 1 to 4 in the flow diagram shown before. Its input is the set of assets of the customer, and the output is a category or risk profile. The steps needed to obtain a risk profile are:

1. Select the set of services (and associated assets) likely to be moved to the Cloud;
2. Select the security dimensions/properties that are relevant for each considered service (e.g. C-I-A: Confidentiality, Integrity and Availability);
3. Evaluate the potential impact to the organization of a threat exploiting a vulnerability and its likelihood to happen (i.e., impact assessment);
4. Determine the risk category of the service under evaluation;
5. Determine the overall risk profile.

During the risk profiling process, multiple information sources are utilized including risk policies, security guidelines, best practice documents, etc.

Example: During the risk profiling process the UK's Gov Cloud defines three categories (Official, Secret, Top Secret), to profile the risk associated with the assets to "cloudify" these are based on the criticality of the information and systems.

After determining the risk profile, the organization should decide on the architecture. This task, called "***Architectural Model***", encompasses Step 5 in the PLAN workflow, and implies the selection of:

1. A deployment model: Private, Public, Hybrid or Community.
2. A service model: IaaS, PaaS, or SaaS

It is worth noting that boundaries of responsibilities between the Gov Cloud customer and CSP vary significantly depending on the selected service model, being bare minimum in IaaS and more CSP responsibilities in SaaS models[16].

Public organizations must explicitly address compliance to security requirements depending on whether the Gov Cloud infrastructure is property of and/or is administered by a third party, or it is owned by the organization itself. If the public administration is also the Gov Cloud owner, then the verification of adequacy and also the fulfilment of security norms is a specific task for this organization to perform. However, if a third party owns the infrastructure then compliance requirements must also be addressed by it.

Another aspect of the deployment-service model is subcontracting. The public administration should consider if it allows the CSP to subcontract the provided Cloud service. An example would be the case of a public SaaS provider which computing/storage infrastructure is subcontracted to another public CSP that offers IaaS. This is called supply chain phenomenon and is very important in cloud offerings that all compliance, service level obligations and responsibilities should narrow down to the vendors

[16] Refer to diagram in the ENISA SME security guide

and subcontractors in the supply chain. In summary, the decision of the architectural model serves to distinguish which security requirements will be under the CSP's responsibility, and which ones are going to be managed by the customer.

Note: The step of choosing the architectural model doesn't exist in the studies Gov Cloud structures in EU, however it is an important intermediate decision that can deliver clearer results as input for the next steps i.e. according to the requirements (performance and security) in service the Cloud owner should decide on the most cost-efficient and lean cloud solution.

Thus, the governmental organization must identify the list of security requirements associated to its risk profile, which will be materialized in the DO Phase. This is the last step of the PLAN Phase, called "***Security and Privacy Requirements***", and Step 6 of the workflow contemplates it.

The security and privacy requirements should be categorized (e.g. technical, operational, legal, and others), and organized according to the actor responsible of fulfilling them (e.g., in-house vs. outsourced requirements).

Example: The Greek Gov Cloud defines a set of baseline requirements for CSP's based on national ICT requirements on security and on national law (data protection and privacy requirements).

What do the different actors have to do in the PLAN phase: a summary of the activities to be performed by each role during the PLAN phase is presented below.

VO:	Activity
Cloud Customer	All six activities comprising the PLAN stage.
Cloud Owner	Might support Cloud Customers during the different steps comprising the PLAN stage. For example, providing information related to the supported deployment/service models (Step 5). If the cloud owner is also the cloud customer then should take all the steps of the PLAN phase.
Cloud Service Provider	Usually the potential providers are not involved in this phase. However the provider might provide information about own resources/services to fine-tune elicited security and privacy requirements.

Table 3. PLAN: roles and activities.

3.2.2 DO Phase

The DO phase includes the implementation of the specific security controls or security measures that are required to fulfil the security requirements elicited during the PLAN stage. Based on the results of the PLAN phase, the identification of the risk profile for each asset category along with the selection of the most suitable service and deployment model, the public administration will proceed to implement the appropriate security measures. The tasks or activities to be carried out during the DO phase are shown in Figure 4.

As shown there, the initial inputs are both (a) the list of in-house security requirements, and (b) the list of requirements to be outsourced to the CSP. The workflow is composed of two major activities:

1. "**Security Controls**": This task is the first step for this phase and consists of selecting the appropriate security controls, which are capable of fulfilling the security requirements elicited in the PLAN phase.

   Note: The step of designating security requirements to security controls doesn't exist in the already studied Gov Cloud structures in EU, however it is an important intermediate decision that can deliver clearer results as input for the next steps i.e. specific controls can make easier for the provider to understand the needs of the customer.

2. "**Implementation, Deployment and Accreditation**": This task, which involves Steps 2, 3 and 4, implies the actual formalization and implementation of the selected security controls, as well as starting the operation of the Gov Cloud service. In-house controls are to be described in a local policy document, whereas outsourced controls are usually formalized in a SLA (or some other class of contract). This task also contemplates the *ex-ante* verification or accreditation to assess the suitability of a CSP to provide a "good enough" level of assurance within the Gov Cloud.

Example: In the Spanish Gov Cloud the roles of each actor are identified (client, provider), and the policy is applied accordingly. The segregation of roles in the scheme is decided by the stakeholders in collaboration, according to the law provisions.

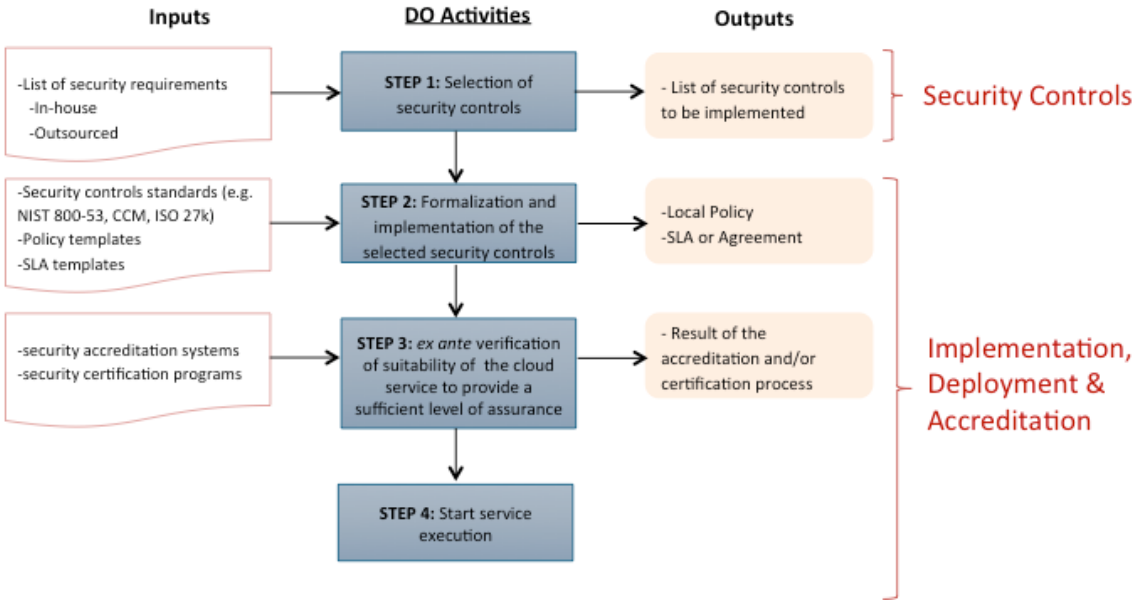


Figure 4. DO Phase workflow: activities, inputs and outputs.

After the activities described above are completed the Cloud service shifts to an operational state, and its correct implementation (from the security point of view) is assessed during the CHECK Phase.

What do the different actors have to do in the DO phase: a summary of the activities to be performed by each role during the DO phase is presented below.

Gov Cloud Role	Activity
Cloud Customer	Perform all four activities for those requirements to be fulfilled in-house.
Cloud Owner	Mostly in charge of Step 3 (e.g., accreditation of CSP's), although could also have responsibility for establishing policies and SLA's (Step 2).
Cloud Service Provider	Fulfilment of outsourced security controls (Steps 1 and 2), procedures for accreditation on the Gov Cloud (Step 3), and operation of the service (Step 4).

Table 4. PLAN: roles and activities.

3.2.3 CHECK Phase

During the CHECK phase the deployed security controls are monitored to verify both their effectiveness and efficiency. Consequently, the CHECK phase involves two activities:

1. "**Log/Monitoring**", which involves the monitoring of activities and evidences for further analysis and reporting (Step 1).

Example: In Estonia they follow an approach of continuous monitoring and logs are kept only for specific services.

2. "**Audit**", which performs periodic/continuous checks based on the monitored data to assess if the security controls fulfil the security levels agreed on the SLA's and contracts (Step 2).

Example: In Spain they perform internally an audit every two years, and in some extraordinary cases they perform ad hoc targeted audits. Audit team is created ad hoc and is comprised by internal or/and external personnel, supervised by an audit leader. The audit team members have to prove accreditation and/or experience in regard to information systems and security, and a confidentiality agreement must be signed before the audit.

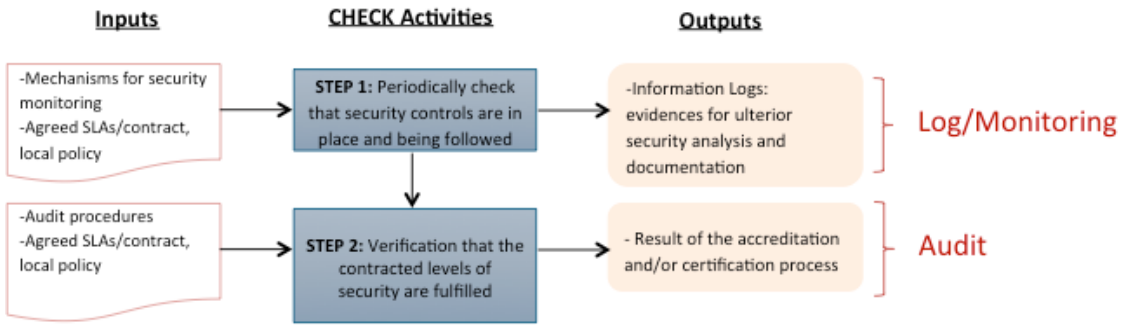


Figure 5. CHECK Phase workflow: activities, inputs and outputs.

The CHECK phase might involve some level of automation to monitor the implemented controls, although the Gov Cloud owner/CSP might also take into account that some of the security controls usually require humans (e.g., auditors) for the assessment process. If a monitored value deviates (beyond a threshold) from the agreed objective, then the ACT phase is triggered.

What do the different actors have to do in the CHECK phase: a summary of the activities to be performed by each role during the CHECK phase is presented below.

Gov Cloud Role	Activity
Cloud Customer	Might receive the outputs from both Step 1 and Step 2 (for outsourced services). In-house services should implement both Steps 1 and 2.
Cloud Owner	Mostly in charge of Step 2, although Step 1 is also in scope depending on the responsibility shared with the CSP.
Cloud Service Provider	Responsible for Step 1 and also involved in Step 2 (along with the Cloud Owner).

Table 5. CHECK: roles and activities.

3.2.4 ACT Phase

The ACT Phase, summarized by the workflow shown in Figure 6, involves the actions to be taken when the activities deployed on the CHECK Phase (for continuously monitoring and testing the security of the system) detect an anomalous event (e.g. a violation of the agreed SLA). Whenever this occurs, the Gov Cloud owner/CSP will perform a set of remediation actions that might have different characteristics e.g. change the implementation of a control, negotiate a different SLA with the Cloud customer etc. In general, the actions taking place during the ACT phase can be grouped under two tasks:

1. "**Changes Management**": this task involves those actions that are related to changes in the operation of the service, such as for example changes affecting the actual Cloud service provision and requiring to renegotiate the agreed SLA (e.g. upgrading the encryption system), or events that may lead to the application of pro-active measures to avoid the actual violation of the SLA/contract.

Example: Extra requirements by the provider have to be considered by the CISO, then approved by the management board and then implemented (change in the terms of use, all customers accept etc.)

2. "**Exit Management**": this task involves the finalization of the Cloud service whether voluntarily or due to other reasons such as SLA violation or poor security performance in the Gov Cloud.

Example: There is a clause in the Collaboration Agreement related to finalization. Both parties can ask for termination with one month notice.

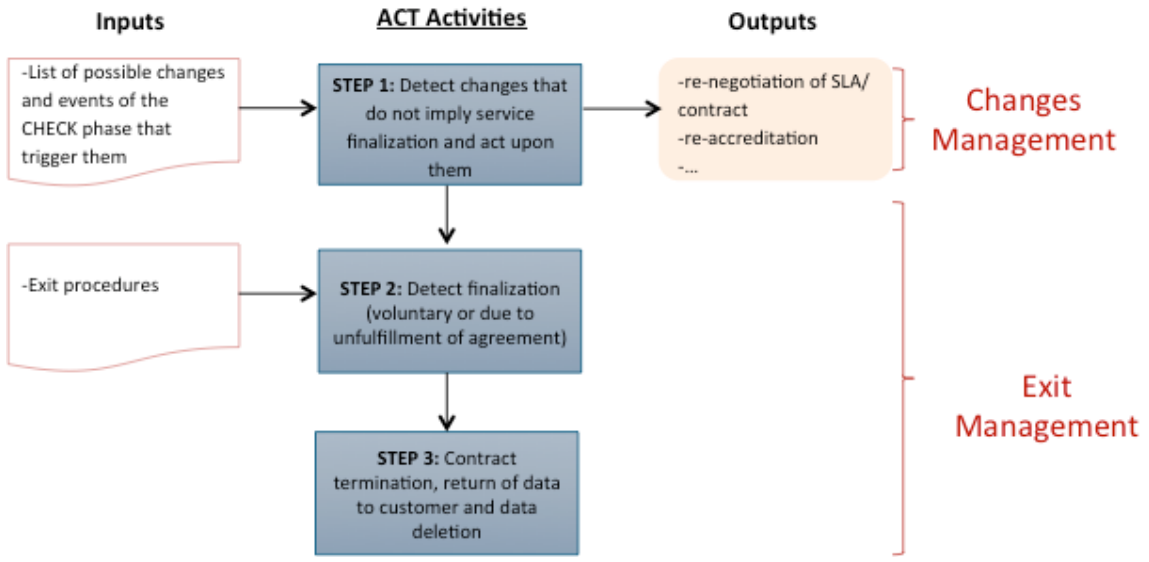


Figure 6. ACT Phase workflow: activities, inputs and outputs.

What do the different actors have to do in the ACT phase: a summary of the activities to be performed by each role during the ACT phase is presented below.

Gov Cloud Role	Activity
Cloud Customer	Mostly participates on Step 2 (e.g., requesting finalization), and Step 3 (e.g., upon termination receiving returned data).
Cloud Owner	Might participate on all three activities within the ACT stage (depending on how the responsibility is shared with the CSP's).
Cloud Service Provider	Participates during all three activities within the ACT stage.

Table 6. CHECK: roles and activities.

4 Framework through use cases

This section presents the examples of the developed Gov Cloud security framework, by applying it to the selected MS use cases of Estonia, Greece, Spain, and United Kingdom.

4.1 Selected use cases

Using the criteria discussed in Section 1.5, this report considered for its analysis four use cases based on Gov Clouds operating in MS[17]. This section provides general background information related to those use cases. The four countries use cases mapped against the framework questionnaire are in Annex A.

	Estonia	Greece	Spain	United Kingdom
Systems in cloud	Public administration services	Educational and academic community	Services of general and regional administration	Service of the public sector
Deployment model	Public/Private	Public cloud	Private	Public
Cloud Strategy	Yes	No	Yes	Yes
Service model	IaaS/ PaaS/ SaaS	IaaS	SaaS	IaaS/ PaaS/ SaaS
Status of deployment	In planning phase	Deployed	Deployed	Deployed

4.1.1 Estonia

In 2013, the Government of Estonia took the first steps to deploy a Gov Cloud by consolidating the networking and datacenter layers in order to develop high-quality and cost-effective services. An analysis carried out to this end, revealed a set of requirements that resulted on three main principles guiding the development of the Estonian Gov Cloud:

i. Using Cloud solutions located within Estonia's national borders,
ii. Using international private Cloud resources, and
iii. Using Data Embassies.

The Estonian government has built the foundation of a highly developed information society, and its ICT development has taken Estonia to a stage where many registries and services only exist in digital form. This development requires a flexible and secure Gov Cloud solution, the growth of which and future capacity requirements cannot be predicted today. Nevertheless, sufficient flexibility has to be planned in advance. The consolidation of domestic server rooms into standards-compliant datacenters, flexible involvement of private sector resources (both inside and outside the state's borders), and the deployment of the Data Embassy network will create a strong foundation for the Estonian Gov Cloud. Please note that the governmental cloud is still under development.

[17] The use cases were selected at the instance of ENISA for being representative of Gov Cloud adoption and also for their willingness to provide the needed documentation to conduct the validation.

The "State Infocommunication Foundation" leads the Gov-Cloud development, which is responsible for the consolidation of server resources and provision of high-quality server hosting services within Estonia's national borders.

4.1.2 Greece

The Greek Gov Cloud is comprised of *Okeanos*[18] and *ViMa,* which are Cloud services provided by the Greek Research and Technology Network S.A. (GRNET). The Greek Gov Cloud serves to the national academic and research community in order to promote academic, educational and research aims.

Okeanos is a Cloud service with customers in the academic and research community. Okeanos offers two main services: Cyclades (a virtual desktop), and Pithos+ (Cloud storage). The ViMa[19] (Virtual Machines) Cloud service provides Virtual Private Servers (VPS) to GRNET peers. ViMa aims to provide shared computing and network resources to the educational and academic community, with production-level quality.

In order to be able to ensure high availability, both Okeanos and ViMa are hosted on multiple computing clusters distributed in several data centres in Greece. The Gov Cloud network infrastructure ensures seamless connection to the telecommunications backbone (and Internet), at very high speeds. Okeanos and ViMa are based on open source software.

4.1.3 Spain

The Spanish public administration has taken important steps related to Gov Cloud, by using available infrastructure and resources. This is the case of SARA (Spanish Public Administrations Network) Network, which is connected to the TESTA (Trans European Services for Telematics between Administrations) network deployed by the European Commission. The initial strategy of Spain's Gov Cloud was to offer services to the Public Administration as a private CSP. The operation of the SARA network for delivering Cloud services started in 2010, but further upgrades and new deployments were made in 2011 and 2013. The SARA project connects and provides services to the General Administration, as well as to Regional and Local Governments. Currently, SARA offers Cloud services to the Spanish Public Administration, such as the @firma platform for e-certificate validation.

4.1.4 United Kingdom

The UK Gov Cloud (better known as "G-Cloud") consists of a framework for the provisioning of Cloud services to the UK public sector, and a marketplace called CloudStore[20]. The latter is an online catalogue of Gov Cloud services containing details about CSP's and their offered Cloud services. Currently, CloudStore comprises more than 1,200 providers, and approximately 13,000 Cloud services spread across four types of Cloud service models ("Lots"):

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)
4. Specialist Cloud Services (SCS)

CSP membership to G-Cloud is based on an accreditation process[21], which defines a minimum set of controls to be implemented by the (prospective) provider. At a glance, the CPS being accredited should provide information about the offered Cloud service's interoperability (including supporting

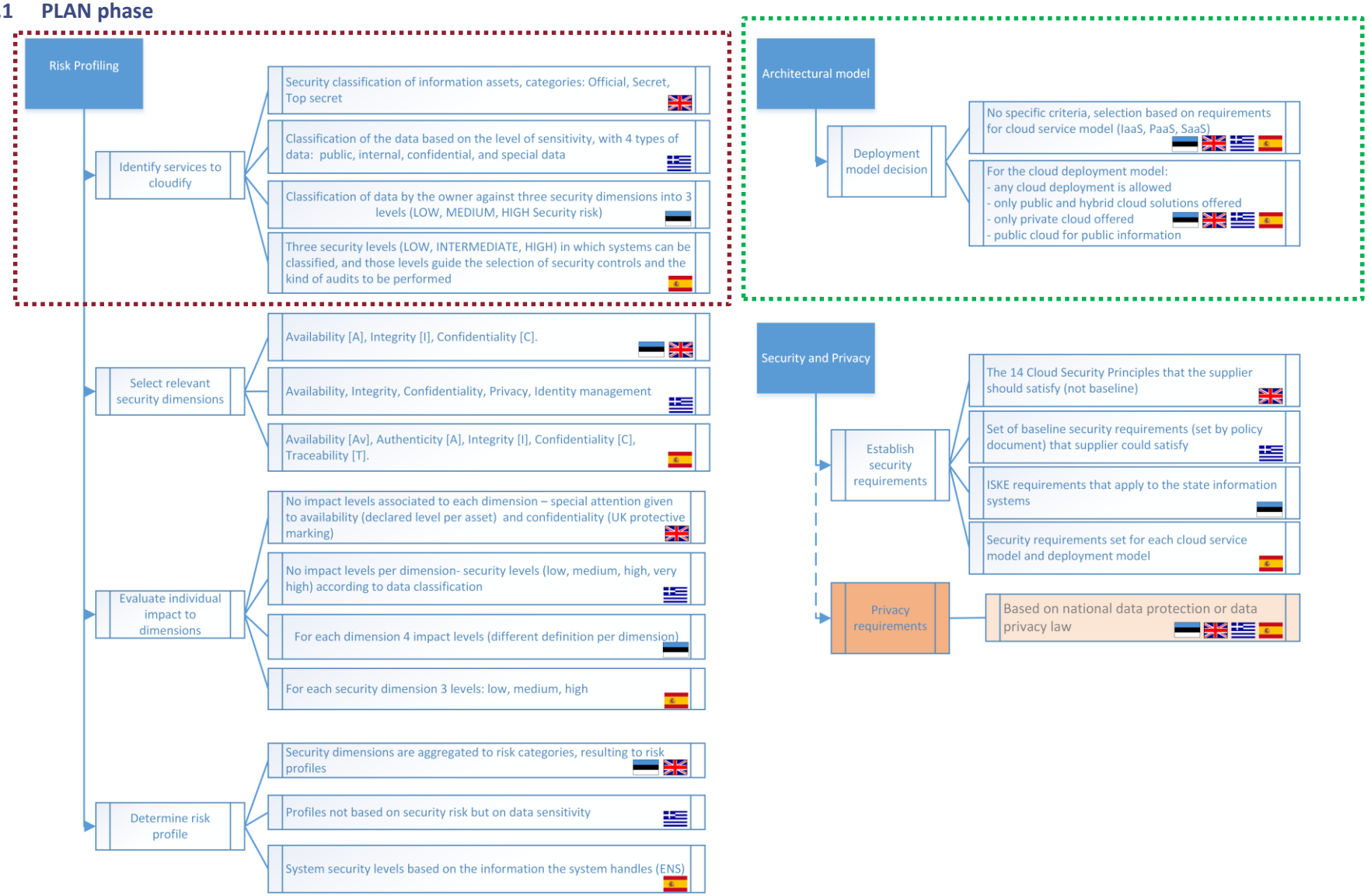
[18] Please refer to https://okeanos.grnet.gr/home/
[19] Please refer to https://vima.grnet.gr/about/info/en/
[20] Please refer to https://www.gov.uk/how-to-use-cloudstore
[21] Please refer to https://www.gov.uk/government/publications/g-Cloud-service-definitions

standards), data portability, extraction and removal. Despite the components of the G-Cloud are expected to be delivered by multiple CSP's/organisations, they must be interconnected and available to all customers, thus creating a single private Cloud.

4.2 Use Cases Validation

During our study, the case studies were used as examples to the security framework introduced in Section 3. Based on the suggested framework, we mapped these four use cases to indicate the different approaches each country has followed according to their needs and the national security requirements. We decided to depict this in a visual way, so that it would be evident how follow the proposed workflows. For each visual we give an example follow a specific path (indicated in red).

4.2.1 PLAN phase



Exemplar uses of the logic model:

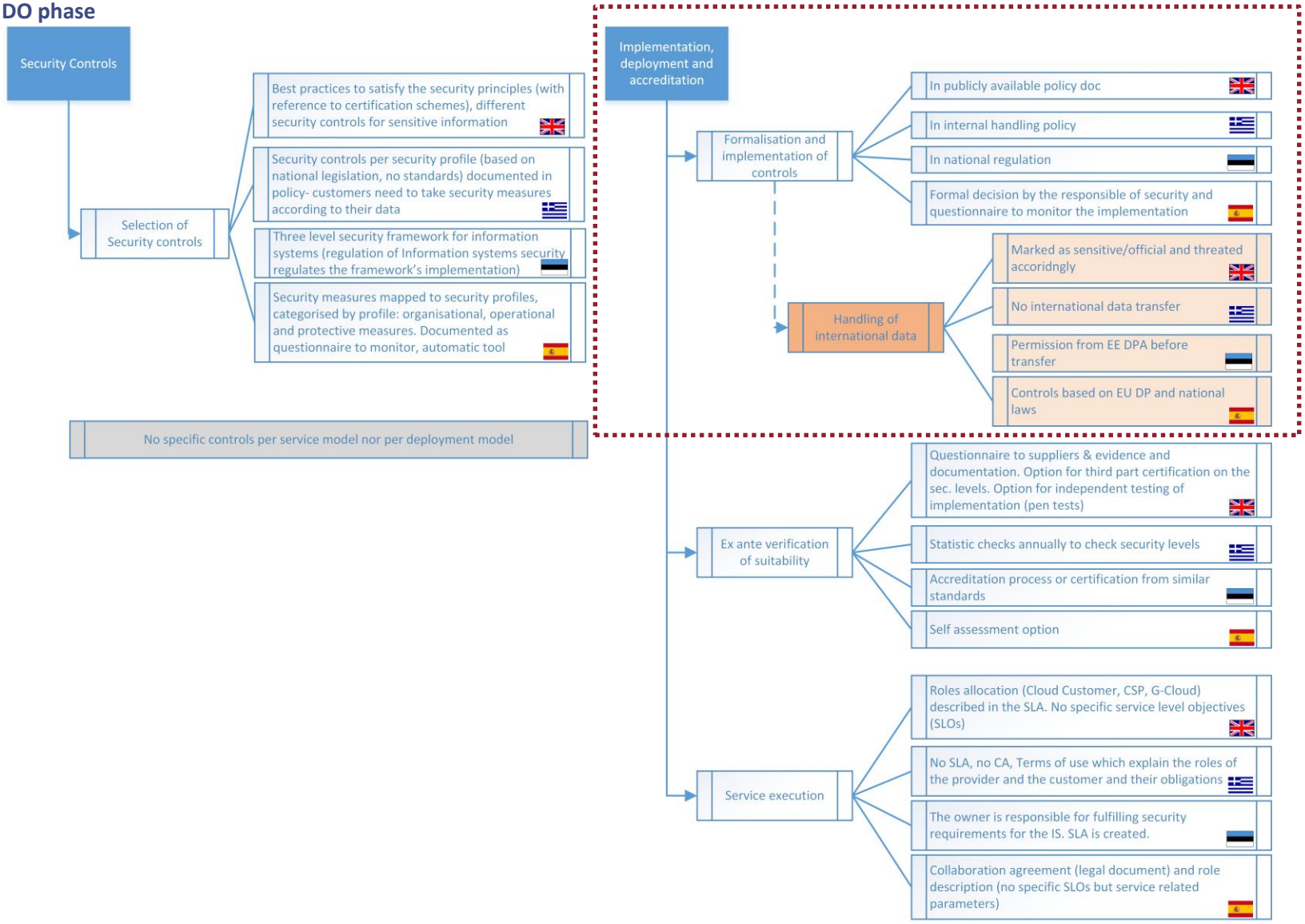
On the first activity of the PLAN phase, Risk Profiling, the first step the cloud owner would have to take is to identify the services they would like to deploy on cloud. For this step we see four different approaches (one per country use case):

- Classification of information assets (nature of assets)
- Classification based on data sensitivity (nature and criticality of data)
- Classification based on risk– three risk classes- against the three security dimensions (Confidentiality, Integrity, Availability) – multi criteria classification
- Classification based on predefined security levels (clearly defined security levels in the strategy)

Following the path of the PLAN phase on the Architectural Model, the specific activity is called deployment model decision. On this topic the steps on decision making can be split in two different topics: the cloud service model (IaaS, PaaS, SaaS) and the cloud deployment model (public, private, hybrid etc).

As depicted, none of the four use case countries specifications are in place to make an informative decision on the cloud model based on the security requirements. The same applied for the deployment model. In the latter case, the offerings are different in each country and this is defined in the national cloud strategy (if any).

4.2.2 DO phase


Security Controls
Selection of Security controls
Best practices to satisfy the security principles (with reference to certification schemes), different security controls for sensitive information
Security controls per security profile (based on national legislation, no standards) documented in policy- customers need to take security measures according to their data
Three level security framework for information systems (regulation of Information systems security regulates the framework's implementation)
Security measures mapped to security profiles, categorised by profile: organisational, operational and protective measures. Documented as questionnaire to monitor, automatic tool
No specific controls per service model nor per deployment model
Implementation, deployment and accreditation
Formalisation and implementation of controls
In publicly available policy doc
In internal handling policy
In national regulation
Formal decision by the responsible of security and questionnaire to monitor the implementation
Handling of international data
Marked as sensitive/official and threated accoridngly
No international data transfer
Permission from EE DPA before transfer
Controls based on EU DP and national laws
Ex ante verification of suitability
Questionnaire to suppliers & evidence and documentation. Option for third part certification on the sec. levels. Option for independent testing of implementation (pen tests)
Statistic checks annually to check security levels
Accreditation process or certification from similar standards
Self assessment option
Service execution
Roles allocation (Cloud Customer, CSP, G-Cloud) described in the SLA. No specific service level objectives (SLOs)
No SLA, no CA, Terms of use which explain the roles of the provider and the customer and their obligations
The owner is responsible for fulfilling security requirements for the IS. SLA is created.
Collaboration agreement (legal document) and role description (no specific SLOs but service related parameters)

Exemplar uses of the logic model:

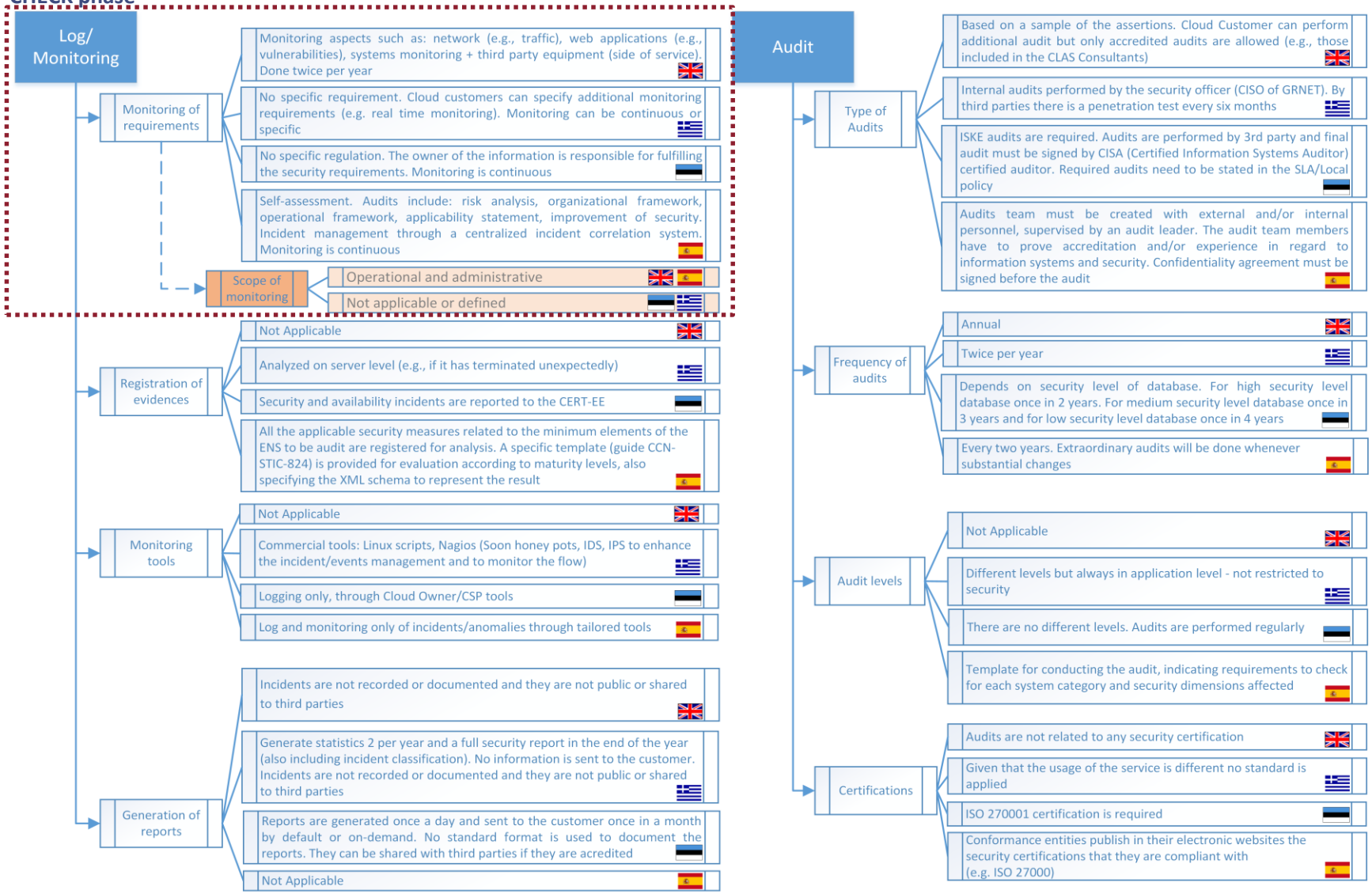
In the second activity of the DO phase, the implementation, deployment and accreditation, one step is the formalisation and implementation of the security controls. For this step we present four different approaches based on the country use cases. The formalisation can be included in:

- Publicly available policy document
- In internal handling policy
- In national regulation
- In formal decision by the national security body

In this case there is a sub-step that should be taken into account in this process, namely the handling of international data. Again here we present four different cases:

- The data is marked as sensitive or official and treated accordingly (different procedure for sensitive data)
- International data transferred is not provisioned thus it is not taking place
- Specific controls based on the national data protection framework are implemented and a specific procedure is followed
- Data protection authority has to give confirmation before the transfer takes place.

4.2.3 CHECK phase



Exemplar uses of the logic model:

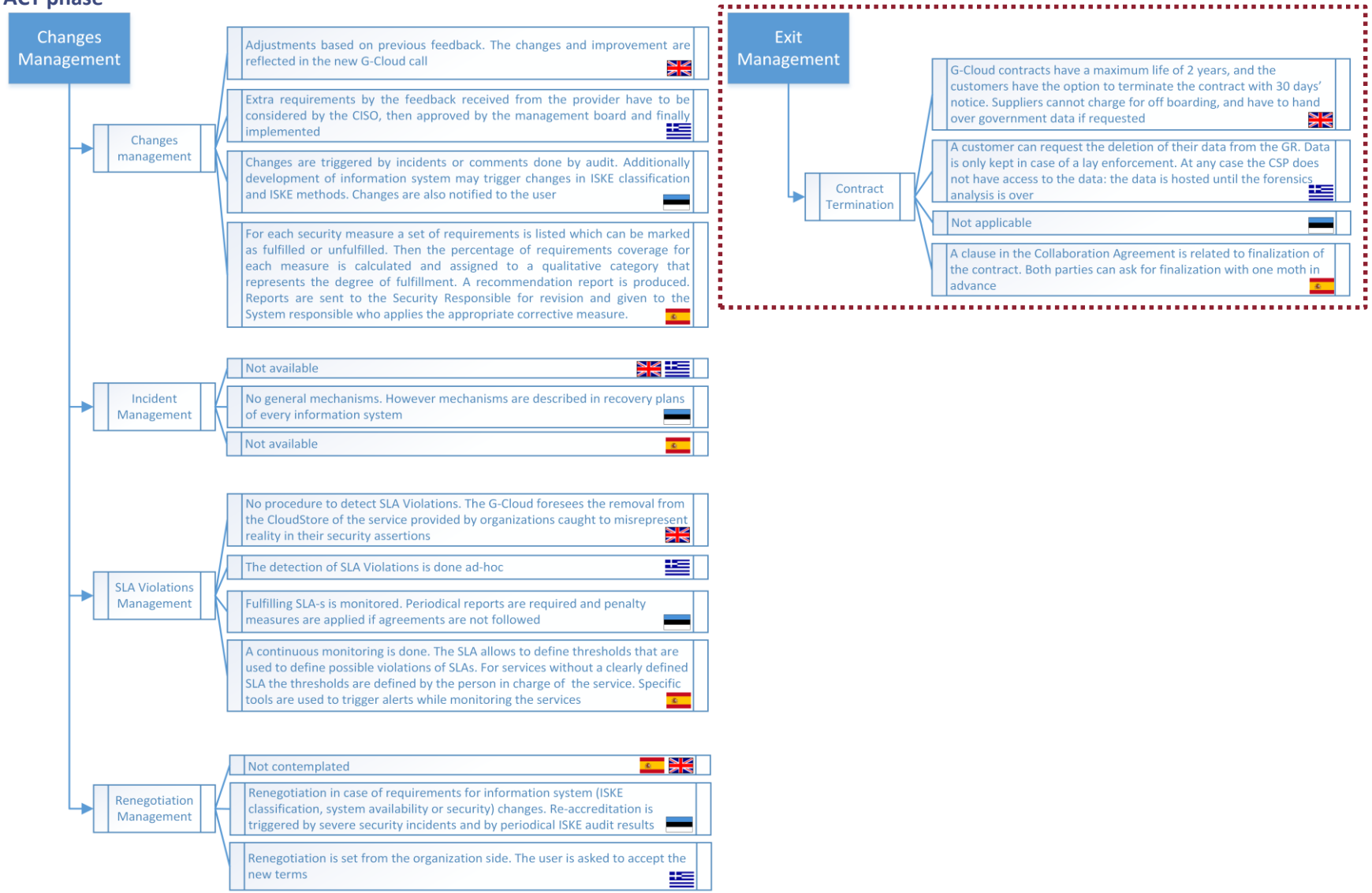
In the third phase of the logic model, the DO phase, one of the two activities to be followed is logging/ monitoring. More specifically a step to be taken towards that approach is monitoring of requirements, again here we present four different approaches:

- Monitoring aspects such as network (traffic) web applications and systems;
- No specific requirements for monitoring open to the customers to decide (non obligatory)
- The customer is responsible to decide the approach (obligatory)
- Monitoring is continuous

Part of monitoring is the specification of the scope, in this sub-step we define two different approaches (and countries are divided):

- Operational and administrative scope for monitoring
- No specified scope

4.2.4 ACT phase



Exemplar uses of the logic model:

In the last phase of the logic model, the ACT phase, in one of the two activities, namely exit management, under the step of contract termination, the approaches noticed are four:

- Contracts can have a predefined maximum duration, leaving the customers free to end the contract whenever they want prior to a 30 days' notice (as states in the guidelines).
- The customer can request termination of contract and ask the data to be removed (following a specific data migration plan including logs, metadata etc) .
- Finalisation has to be agreed by both parties of the collaboration agreement
- No specific provision is applicable.

5 Conclusions

This report proposed a security framework for Gov Clouds, structured through the widely used Plan-Do-Check-Act security cycle. The presented framework was developed based on comprehensive research that included coverage of relevant state of the art/practice, and was also iteratively validated thanks to the valuable feedback from Gov Cloud experts in the four selected use cases (Estonia, Greece, Spain, and United Kingdom).

The main conclusions drawn from the report are:

- Despite considerable efforts from the EC, ENISA and other international organisations and market actors (e.g. CSP's) the level of adoption of Gov Clouds is still low. Some EU MS have already defined a Cloud strategy, some others show a tactical or opportunistic adoption of Cloud services, but very few (actually only UK and Spain) have defined and implemented a national wide Cloud strategy. This security framework will be one more reason to support the systematic adoption of Cloud security strategies and actual governmental cloud deployment.
- The report's analysis made evident that "common security denominators" exist across the MS deployed Gov Clouds, in particular related to aspects like defined roles, use of standards, and adopted security controls. It is our expectation that the discovered commonalities will be the basis to develop homogeneous security best practices, SLA's and contracts for Gov Clouds in the short term.
- The analysis of the input collected from Estonia, Greece, Spain and UK also shows that these Gov Clouds apply different practices in the registration of evidences, selection of monitoring tools, SLA violation management, types and frequency of performed audits, and accreditation procedures.
- From the consideration of change-management practices, all the use cases portend mechanisms for the continuous improvement of the implemented security frameworks (policies, mechanisms).
- The analysed Gov Clouds have established policies for incident management. However, the adopted approaches do not directly appear under the ACT phase, but are scattered among the other stages of the framework. This means that incident management is not only one step in the lifecycle but is a horizontal activity that has to be considered in all different stages.
- The security framework proposed in this report (a) encompasses the analysed Gov Clouds, and (b) is projected to be flexible for extension and adaptation to new security needs and requirements from other Gov Clouds in the EU. This was demonstrated by its empirical validation through four selected use cases. This framework is also meant to be used during the design phase of new Gov Clouds, as it contains specific guidance related to different security features/best-practices that should be taken into account by practitioners and Cloud security architects. On the other hand, the framework can be also used by existing Gov Clouds as a baseline for analysing side-by-side different deployments from MS.

In summary, this novel framework for Gov Clouds should become part of the public administrations' toolbox when planning their migration to the Cloud, and when assessing the effectiveness of the deployed security controls and procedures.

References

[1] Dimitra Liveri, Thomas Haeberlen, Matina Lakka. (2013). "*Good Practices for Securely Deploying Governmental Clouds*", ENISA. Available online at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds/at_download/fullReport, last accessed August 2014.

[2] Catteddu, D. (2011). "*Security and resilience in governmental clouds*". European Network and Information Security Agency (ENISA). Available online at http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds , last accessed August 2014.

[3] Brunette, G., & Mogull, R. (2009). Security guidance for critical areas of focus in Cloud computing. Cloud Security Alliance (CSA). Available online at https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, last accessed August 2014.

[4] Erl, T., Mahmood, Z., and Puttini, R. "*Cloud Computing. Concepts, Technology & Architecture.*" Prentice Hall/PearsonPTR, 2013.

[5] GRNET. (2014). "*About the Service*". Available: https://vima.grnet.gr/about/info/en/, last accessed August 2014

[6] ADAE. (2013). "*Κανονισμός για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών*". Available online at: http://www.adae.gr/fileadmin/docs/enimerosi/sxedio_kanonismou_adae_asfaleia_akeraiotita.pdf, last accessed August 2014

[7] Cabinet Office (2014). "*Government Security Classifications*". Available online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf, last accessed August 2014.

[8] Cabinet Office (2013). Available online at "*Government Security Classifications FAQ Sheet 1: Working with OFFICIAL Information v1.2- April 2013*". Available online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251475/FAQ1-Working-with-Official-Information-v1.2-Apr-2013.pdf, last accessed August 2014.

[9] Gobierno de España. Ministerio de la Presidencia. Secretaría General Técnica. "Spanish National Security Framework, Royal Decree 3/2010, of January 8th, which regulates the National Security Framework within the e-government scope". January 2010. http://www.seap.minhap.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/Monografias0/parrafo/011111113/text_es_files/Span-nac-secur-fram.pdf, last accessed August 2014.

[10] Centro Criptológico Nacional, Ministerio de Defensa de España. "*Guía de Seguridad (CCN-STIC-803). Esquema Nacional de Seguridad, Valoración de los sistemas*". Enero 2001. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/803-Valoracion_en_el_ENS/803_ENS-valoracion_ene-11.pdf, last accessed August 2014.

[11] Centro Criptológico Nacional, "Guía de Seguridad (CCN-STIC-804). Esquema nacional de seguridad, guía de implantación". October, 2011. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/804-Medidas_de_implantacion_del_ENS/804-Medidas_de_implantacion_del_ENS-20111026.pdf

[12] Centro Criptológico Nacional, "Guía de Seguridad (CCN-STIC-811).Interconexión en el ENS".September, 2011. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/811-Interconexion_en_el_Esquema_Nacional_de_Seguridad/811-Interconexion_en_el_ENS.pdf

[13] Centro Criptológico Nacional, Ministerio de Defensa de España. "*Guía/Norma de Seguridad de las TIC (CCN-STIC-823), Seguridad en Entornos Cloud (Borrador).*" Abril, 2014. Available online at https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/823-Seguridad-en-entornos-Cloud/823-Cloud_Computing_ENS.pdf0020, last accessed August 2014.

[14] CESG, Cabinet Office. (2009). "*Extract from HMG IA Standard No.1 Business Impact Level Tables*". Available online at https://www.cesg.gov.uk/publications/Documents/business_impact_tables.pdf, last accessed August 2014.

[15] Ministerio de Administraciones Públicas (2006). "*Magerit-versión 2, Methodology for Information Systems Risks Analysis and Management*". Available online at http://rm-inv.enisa.europa.eu/methods/m_magerit.html, last accessed August 2014.

[16] NIST (2010). "*Federal Information Processing Standards Publications*". Available online at http://www.nist.gov/itl/fips.cfm, last accessed August 2014.

[17] Cabinet Office (2014). "*Government Security Classifications FAQ Sheet 2: Managing Information Risk at OFFICIAL v2.0.*" Available online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/286667/FAQ2_-_Managing_Information_Risk_at_OFFICIAL_v2_-_March_2014.pdf , last accessed August 2014.

[18] Centro Criptológico Nacional, Ministerio de Defensa de España. Available online at "*Guía/Norma de Seguridad (CCN-STIC-825), ESQUEMA NACIONAL DE SEGURIDAD CERTIFICACIONES 27001*." Noviembre, 2013. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/825/825-27001_ENS.pdf, last accessed August 2014.

[19] CESG, Cabinet Office (2014). "*Cloud Security Principles*". Available online at https://www.gov.uk/government/publications/Cloud-service-security-principles, last accessed August 2014.

[20] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Available online at https://www.boe.es/diario_boe/txt.php?id=BOE-A-1999-23750, last accessed August 2014.

[21] European Comission (2012), "*Reglamento General de Protección de Datos*". Available online at http://lopd-agpd.com/documentos/NuevaLopd.pdf last accessed August 2014, last accessed August 2014.

[22] CESG (2014). "*Implementing the Cloud Security Principles*" Available online at https://www.gov.uk/government/publications/implementing-the-Cloud-security-principles, last accessed August 2014.

[23] Centro Criptológico Nacional, Ministerio de Defensa de España. "*Guía de Seguridad (CCN-STIC-824), Esquema Nacional de Seguridad , Informe del Estado de Seguridad*", Septiembre 2012, https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/824-Informe_del_Estado_de_Seguridad/824-Informe_del_estado_de_seguridad-sep12.pdf, last accessed August 2014.

[24] Mañas, J. A. (2006). EAR / Pilar Tool. Available online at http://rm-inv.enisa.europa.eu/tools/t_EAR_Pilar.html, last accessed August 2014.

[25] Boletín Oficial del Estado (2013), OTRAS DISPOSICIONES, 8074 Resolución, Available online at http://www.boe.es/boe/dias/2013/07/24/pdfs/BOE-A-2013-8074.pdf, last accessed August 2014.

[26] Veriscommunity.net, Available online at "Vocabulary for Event Recording and Incident Sharing (VERIS)", http://veriscommunity.net/, last accessed August 2014.

[27] Centro Criptológico Nacional, Ministerio de Defensa de España. "*Guía de Seguridad (CCN-STIC-802), Esquema Nacional de Seguridad, Guía de Auditoría*". Junio, 2010. Available online at https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/802-Auditoria_ENS/802-Auditoria_ENS-jun10.pdf, last accessed August 2014.

[28] Centro Criptológico Nacional, Ministerio de Defensa de España. "*Guía de Seguridad (CCN-STIC-808), Verificación del Cumplimiento de las medidas en el ENS"*, Octubre 2010, Available online at https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/808/808-Verificacion_del_cumplimiento_medidas_ENS-2010-10-16.pdf, last accessed August 2014.

[29] Zwattendorfer, B., Stranacher, K., Tauber, A., & Reichstädter, P. (2013). *"Cloud Computing in E-Government across Europe".* In Technology-Enabled Innovation for Democracy, Government and Governance (pp. 181-195). Springer Berlin Heidelberg. Available online at http://link.springer.com/chapter/10.1007/978-3-642-40160-2_15, last accessed August 2014.

[30] Twobirds.com, Bird&bird &Cloud computing & your legal questions answered, http://www.twobirds.com/~/media/PDFs/Expertise/IT/Cloud%20computing%20law%20interactive.pdf

[31] Gongolidis, E., Kalloniatis, C., & Kavakli, E. (2014). "*Requirements Identification for Migrating eGovernment Applications to the Cloud*". In Information and Communication Technology (pp. 150-158). Springer Berlin Heidelberg. http://link.springer.com/chapter/10.1007/978-3-642-55032-4_15 , last accessed August 2014.

[32] Department of Economic and Social Affairs (UN DESA). E-Government Survey, United Nations, New York (2012). Available online at http://www.un.org/en/development/desa/publications/connecting-governments-to-citizens.html, last accessed August 2014.

[33] European commission. "*European eParticipation, Summary Report*", November 2009, prepared by the Danish Technological Institute, Leeds University and University of Macedonia. Available online at http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1499, last accessed August 2014.

[34] Information Society (2008). Greek Interoperability Framework. Available online at http://www.e-gif.gov.gr/portal/page/portal/egif, last accessed August 2014.

[35] Wyld, D. C. (2010). "*The cloudy future of government IT: Cloud computing and the public sector around the world*". International Journal of Web & Semantic Technology, 1(1), 1-20. Available online at http://airccse.org/journal/ijwest/papers/0101w1 , last accessed August 2014.

[36] Wyld, D. C. (2009). "*Moving to the Cloud: An introduction to Cloud computing in government*". IBM Center for the Business of Government. Available online at http://www.ukeig.org.uk/sites/default/files/WyldCloudReport_0.pdf, last accessed August 2014.

[37] Tripathi, A., & Parihar, B. (2011, June). "*E-Governance challenges and Cloud benefits*". In Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on (Vol. 1, pp. 351-354). IEEE. Available online at http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5953237 , last accessed August 2014.

[38] Smitha, K. K., Thomas, T., & Chitharanjan, K. (2012). "*Cloud based e-governance system: A survey*". Procedia Engineering, 38, 3816-3823. Available online at http://www.sciencedirect.com/science/article/pii/S1877705812023508, last accessed August 2014.

[39] Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). "*Identifying the security risks associated with governmental use of Cloud computing*". Government Information Quarterly, 27(3),245-253. Available online at http://www.sciencedirect.com/science/article/pii/S0740624X10000225, last accessed August 2014.

[40] Kurdi, R., Taleb-Bendiab, A., Randles, M., & Taylor, M. (2011, December). "*E-Government Information Systems and Cloud Computing (Readiness and Analysis)*". In Developments in E-systems Engineering (DeSE), 2011 (pp. 404-409). IEEE. Available online at http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6150014 , last accessed August 2014.

[41] European Comission, Digital Agenda for Europe (2013). "*Analysis of Cloud best practices and pilots for the public sector*", Available online at http://ec.europa.eu/digital-agenda/en/news/analysis-Cloud-best-practices-and-pilots-public-sector) , last accessed August 2014.

TP-07-14-063-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

doi: 10.2824/57349

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu