



Good Practice Guide for securely deploying Governmental Clouds





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.

Authors

Thomas Haeberlen, Dimitra Liveri, Matina Lakka.

For contacting the authors please use Cloud.security@enisa.europa.eu

Acknowledgements

This study was conducted in cooperation with the Department of Civil Engineer and Computer Science, University of Rome Tor Vergata: Dr. Emiliano Casalicchio, Maria Cristina Brugnoli, Federico Morabito.

Many thanks to the experts of the ENISA Cloud Security and Resilience EG: Frank van Dam (Ministry of Economic Affairs, NL), Arjan de Jong (Ministry of the Interior and Kingdom Relations, NL), Tuija Kuusisto (Ministry of Finance, FI), Jesper Laursen (Agency for Digitisation, DK), Steve Agius (MCA, MT), Vangelis Floros (GRNET, GR), Aleida Alcaide (SEAP, ES), Veaceslav Puşcaşu (e-Government Center, MD), Tobias Höllwarth (EuroCloud), Roxana Banica (RO), Fritz Bollmann (BSI, DE), Ali Rezaki (Tubitak, TR), Marko Ambroz (MJPA, SI), Putigny Herve (ANSSI, FR), Boggio Andrea (HP Enterprise Security), Tjabbe Bos (DG CONNECT, EC), Daniele Catteddu (CSA), Peter Dickman (Google), Paul Costelloe (EuroCIO), Olivier Perrault (Orange, FR), Jan Neutze (Microsoft), Theo Dimitrakos (BT Research and Innovation), Antonio Ramos (Leet Security), Raj Samani (McAfee), Paul Davies (Verizon)

And also: Valentino Ditoma (ANCITEL, IT), Williams Harvey (Cabinet Office, UK), Guido Pagani (ICT, IT), Stefano Fabrizi & Sabina Di Giuliomaria (Bank of Italy, IT), Giuseppe Arrabito (Universita La Sapienza, IT), Simon Pascoe (BT Security Enterprise)

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2013

Reproduction is authorised provided the source is acknowledged.

Executive summary

Public and private sector organisations are switching to Cloud computing. While some years ago applications would be mainly run on servers on their own premises or dedicated data centres, now applications are outsourced to large Cloud service providers and run in a few large data centres. Public data on the uptake of Cloud computing shows that in a couple of years around 80% of organisations will be dependent on Cloud computing.

Public bodies could be a key player in Cloud computing area as it offers scalability, elasticity, high performance, resilience and security, together with cost efficiency while in the same time it could enable and simplify citizen interaction with government by reducing information processing time, lowering the cost of government services and enhancing citizen data security. Governmental Clouds offer to the public bodies, including ministries, governmental agencies and public administrations (PAs), the potential to manage security and resilience in traditional ICT environments and strengthen their national Cloud strategy.

ENISA has published in 2011 a guide for public bodies providing recommendations on the definition of their security and resilience requirements and how to evaluate and choose from the different Cloud computing service delivery models.

In this report, ENISA identifies the Member States with operational government Cloud infrastructures and underlines the diversity of Cloud adoption in the public sector in Europe. Moreover through this document, ENISA aims to assist Member States in elaborating a national Cloud strategy implementation, to understand current barriers and suggest solutions to overcome those barriers, and to share the best practices paving the way for a common set of requirements for all Member States (MS).

The study shows that, while there is no common agreement on a definition of Governmental Cloud, a common concept exists:

- 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)

After the examination of the wide and heterogeneous landscape of the EU countries a governmental Cloud classification is presented based on basic criteria:

- the existence of a legal background to support the implementation of Cloud computing in administrative systems, i.e. national Cloud strategy or digital agenda,
- and the phase of the governmental Cloud implementation (design, implementation, projects running etc).

The countries studies are categorised in the following groups:

- **Early adopters:** Countries that have a Cloud strategy and they have taken specific decisions on how to implement the governmental Cloud.
- **Well - Informed:** Countries that have a strategy but the implementation is still at design or prototype stage or they have only preliminary implementations of some governmental Cloud services.

- **Innovators** : Countries that do not have a high-level Cloud strategy with clear indications on governmental Cloud implementation, but they already have some Cloud-based services running.
- **Hesitants**: Countries that do not have a governmental Cloud strategy in place nor have the relevant Cloud initiatives or governmental Cloud experiences.

This study presents information from in total 23 European countries (20 EU countries): Austria, Belgium, Cyprus, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Malta, Republic of Moldova, Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Slovakia, Spain, Sweden, Turkey, UK.

Based on the study on the aforementioned Member States on their national Cloud strategy and applications a set of recommendations on how to securely deploy governmental Clouds is presented:

- EC and MS to support the development of an EU strategy to foster the adoption of governmental Cloud;
- EC and MS to develop a business model to guarantee the sustainability and economies of scale or governmental Cloud solutions;
- MS and Cloud providers to foster the development of a framework to mitigate the “loss of control” issue;
- EC and MS to promote the definition of a regulatory framework to address the “locality problem”;
- MS and Cloud providers to encourage the development of governmental Cloud solutions compliant with EU and country specific regulation;
- EC and MS to support the development of an SLA framework;
- EC and MS to foster the adoption of baseline security measures for both public and private Cloud deployment models;
- EC and MS to develop a certification framework;
- Academia and Cloud providers to foster research on governmental Cloud security;
- EC and MS to support privacy enhancement in the Cloud.

Table of Contents

Executive summary	iii
1 Introduction	1
2 Governmental Cloud Computing	4
2.1 Towards a definition of Governmental Cloud computing (Gov-Cloud)	4
2.2 Current core practices	6
3 Classification of governmental Clouds across the EU	9
3.1 The “Early adopters”	10
3.2 The “Well Informed”	12
3.3 The “Innovators”	18
3.4 The “Hesitants”	22
4 Best practice scenarios and analysis	24
4.1 A Governmental Cloud Catalogue	24
4.2 Consolidating Existing Clouds to Improve Efficiency	25
4.3 Building a National Cloud Infrastructure Based on Open Source	27
5 Recommendations	29
5.1 Recommendation 1: EU governmental Cloud strategy	31
5.2 Recommendation 2: a business model to guarantee sustainability	32
5.3 Recommendation 3: a framework to mitigate the “loss of control” issue	33
5.4 Recommendation 4: a regulatory framework to address the “locality problem”	33
5.5 Recommendation 5: governmental Cloud solutions compliant to EU and national law	34
5.6 Recommendation 6: a common framework for SLAs	35
5.7 Recommendation 7: Security measures for governmental Cloud	35
5.8 Recommendation 8: Certification framework	36
5.9 Recommendation 9: Foster research on governmental Cloud security.	36



5.10	Recommendation 10: Privacy enforcement	37
6	Conclusions and next steps	39

1 Introduction

Despite the considerable potential benefits offered by Cloud services, which were also recently highlighted in the European Cloud Strategy, few EU countries have so far developed a national Cloud computing strategy. The number of Member States (MS) with operational government Cloud infrastructures is even smaller. The diversity of Cloud adoption in the public sector in Europe is evident; in several countries local public administrators are developing Cloud strategies or launching test bed projects; in others, Cloud is not even considered an option.

Information on the lessons learnt and best practices of the “early adopters” is not readily available. Governmental bodies, national experts and policy makers from less advanced countries in the field of Cloud computing struggle to find case studies and, thus, cannot benefit from the valuable experience of other Member States.

In this study ENISA, aiming at “enabling and facilitating faster adoption of Cloud computing” collected information on Cloud services deployed (projects, initiatives, plans) in the public sector, collected the best practices and presents a list of recommendations, covering all aspects of Cloud computing. The goal is to help Member States in:

- the elaboration of a national Cloud strategy,
- the implementation of a national Cloud strategy and governmental Cloud infrastructure,
- understanding current barriers by suggesting solutions to overcome them,
- sharing the best practices and paving the way for a common set of requirements for all Member States.

Policy Context

The European Commission (EC), under the “[Digital Agend for Europe](#)” in the context of the Europe 2020, has set as one of the objectives to support the Information and Communication Technologies (ICT) in delivering sustainable economic and social welfare.

The [EU Cloud strategy](#) – subtitled “Unleashing the Potential of Cloud Computing in Europe” was launched by the European Commission in 2012. It describes the strategic plan of the European Commission aiming to enable and facilitate the adoption of Cloud services in the public and private Cloud computing sector across the EU. Before publishing the strategy, the Commission has conducted several desk research studies (Cloud uptake in the EU, standardization schemes for Cloud, Cloud contracts and SLAs), which led them to define the following key actions, closely related to information security and certification:

- Standardisation and certification: ETSI is asked to produce a map of existing standards relevant for Cloud computing. The Commission (COM) will work with ENISA to support development of EU-wide voluntary schemes and to make a list of such schemes by 2014.
- Cloud Contract Terms: The EC will develop model terms for Cloud SLAs as well as a set of safe and fair contract terms for consumers and SMEs. The EC will also work with experts to develop a code of conduct for Cloud providers regarding data protection, which will be submitted to the Article 29 Working Party for endorsement.
- European Cloud Partnership: The EC will set up a European Cloud Partnership, involving industry and public sector, which will develop common procurement requirements adapted to European needs.

As stated in the strategy “public authorities also stand to benefit from Cloud adoption both in terms of efficiency savings and in terms of services that are more flexible and turned to the needs of

citizens and business. [...] Cloud computing can help drive the transition to 21st century public services that are interoperable, scalable and in line with the needs of a mobile population and business that want to benefit from the European digital single market”. Cloud computing is the driveway towards the realization of the “Every European Digital” dream, where bureaucracy will be wiped out. In the strategy ENISA was asked to support the Commission in these activities.

Target audience

The target audiences of this report are:

- Public bodies in the EU (local and regional public administrations, agencies, local healthcare authorities, etc.) evaluating the costs and benefits for a public administration considering using Cloud services;
- European Union policymakers deciding on appropriate policy and economic incentives, legislative measures, awareness-raising initiatives, etc., vis-à-vis Cloud-computing technologies for governments and public administrations;
- Cloud providers and Cloud VAS (value-added services – including security) providers trying to achieve an early understanding of the needs and requirements of central governments, public administrations and citizens, to be able to develop Cloud services that are in line with these needs and requirements.

Methodology

This study and its outcome is based on desk research, an online survey and a set of interviews to subject matter experts: experts working in governmental agencies implementing Cloud services or being involved in the composition of the national Cloud strategy, experts from private sector who provide services to the public sector supporting private Clouds etc.

The interviews and the research activities focussed on the following topics:

- Governmental Cloud infrastructures that are currently operational, in the planning or in the implementation phase;
- Services (both “critical” and “non critical”¹) currently deployed by the governmental sector using Cloud technologies and/or services that will be migrated to the Cloud using Cloud technologies;
- National strategies across the EU that take into account the intent to foster Cloud computing for governmental services;
- Cloud computing projects and initiatives focusing on the dissemination and delivery of governmental Cloud services;
- Risk assessment and security frameworks for Cloud Computing and public services.

The interview templates and the questionnaire have been prepared according to the results from the survey on the state of the art and specifically designed for Cloud providers, governmental IT agencies, and public sector stakeholders. The questionnaires and the interviews covered quite a broad number of topics:

- Practices, orientations, expectations, initiatives, projects of the stakeholders in the deployment of public services with the adoption of Cloud technologies.

¹ Critical are those assets/services whose loss would lead to “severe economic or social consequences” i.e. water, energy, transport, communications according to CPNI, UK:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78902/section-a-natural-hazards-infrastructure.pdf

- Requirements, warranties, needs, expectations of the principal actors for enforcing security of the governmental Cloud services, the assets and the data of public institutions.
- Orientations, visions, views, positions on national Cloud computing strategies and on the guidelines for security of governmental Cloud services.

As a result, we collected information from a total of 23 European countries (20 EU countries), and specifically: Austria, Belgium, Cyprus, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Malta, Republic of Moldova, Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Slovakia, Spain, Sweden, Turkey, UK.

Structure

In [Chapter 2](#) of this document we present the characteristics of a governmental Cloud and its definition; in [Chapter 3](#) we give an overview of the Cloud uptake by the public sector in Europe classifying the respective countries according to specific criteria; in [Chapter 4](#) we provide best practice examples, based on the several cases of governmental Clouds in Europe; and in [Chapter 5](#) we present a set of recommendations and actions that can implement these recommendations on securely deploying Cloud services in the public sector. We conclude in [Chapter 6](#) with general remarks on the future of governmental Cloud in the EU.

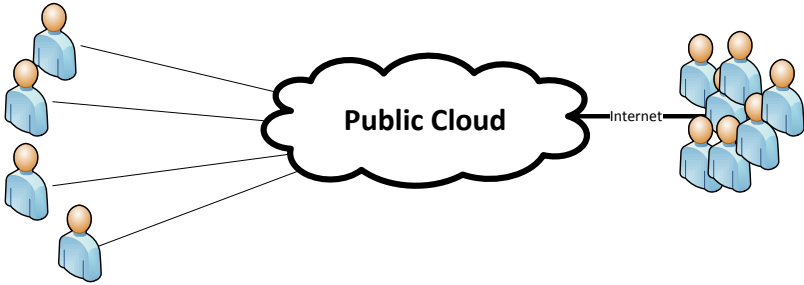
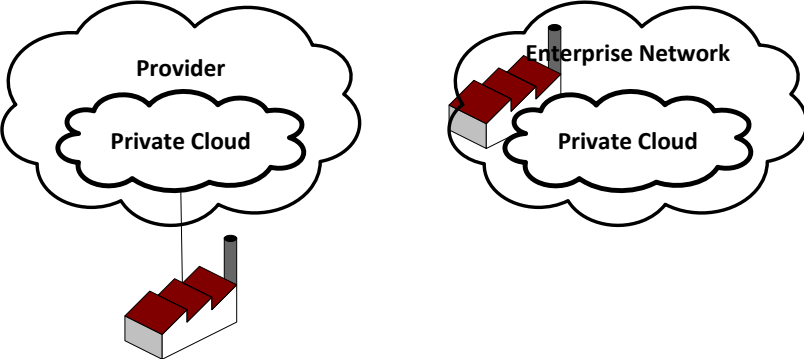
2 Governmental Cloud Computing

The goal of this chapter is to provide clarity on the definition and characteristics of governmental Cloud computing. We provide a definition of governmental Cloud computing based on experts' feedback and an outline of current core practices classified in a specific taxonomy that will be used throughout the complete document for a more in-depth analysis of best practices.

2.1 Towards a definition of Governmental Cloud computing (Gov-Cloud)

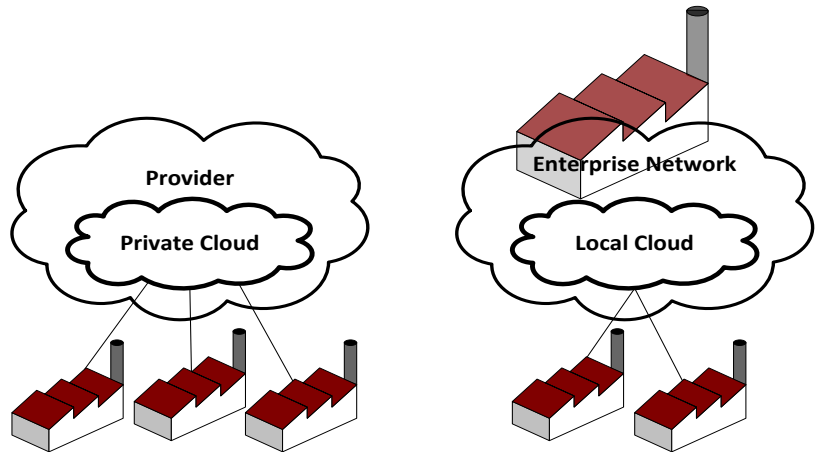
The definition of governmental Cloud should be based on the widely accepted definition of Cloud computing by the [National Institution of Standards and Technology \(NIST\)](#) : **Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.**²

Based on the NIST definition of Cloud Computing, below are the definitions of the different deployment models:

Deployment Model	Visualization
<p>Public Clouds: Cloud infrastructure and computational resources are made available to the general public over public network.</p>	
<p>Private Cloud (in house and out sourced) : one customer has the exclusive access and usage of the infrastructure and computational resources; hosted on the organisations premises (on-site) or provided by a provider (out-sourced).</p>	

² IaaS: Infrastructure as a Service, PaaS: Platform as a Service, SaaS: Software as a Service.

Community Cloud (on-site and outsourced): group of users sharing the same infrastructure and computational resources. Can be implemented in the enterprise premise (on-site) or deployed by a company (out-sourced).



For governmental Cloud services, a standard definition is not yet adopted, and while there is no common agreement on a definition for governmental Cloud, a common concept exists:

- 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)

Even though the above elements could help defining governmental Clouds, many implementations of eGovernment services do not meet these characteristics. All these implementations are based on virtualisation and web services technologies, and aim at consolidating resources to reduce the number of governmental datacentres, usually meeting none of the above mentioned attributes.

A governmental Cloud is more than a centralised platform based on virtualisation technologies, running eGovernment services and meeting the above-mentioned requirements. A gov-Cloud is usually based on a sustainable governmental business model allowing standardizing services and SLAs, to save cost, to help “smartening” the society. To achieve these goals, and more specifically to be efficient from an economic perspective, the governmental Cloud should be a deployment model providing basic services (e.g. authentication, storage, document management, workflow management) that would be used by governmental agencies and ministries to build eGovernment services for internal use, internal operation and management, and for services targeting at citizens and private companies (society).

In the same light, one of the biggest benefits (beyond cost) of leveraging public/community Clouds is the benefit of being much more agile and efficient, in terms of speed, processing power and elasticity. The adoption of a governmental Cloud should be also a driver / an opportunity to re-think the way ICT resources and eGovernment services are managed at government level, and to innovate eGovernment services. Cloud computing offers a method of driving common standardisation and then scale down commoditisation and hence costs. Tailored solutions to tailored requirements cost government departments significant overhead expenditure (and in many instances duplication – as one department specifies a solution which another department has already bought). Cloud computing uptake both depends and facilitates standardisation on features, technology and systems and classification against clearly documented relevant standards and best practices. Standardisation

and reuse should take place both at the level of the ICT / Cloud infrastructures and processes but also at the level of applications and services.

Cloud computing also introduces new risks. Generally for public organizations adopting Cloud computing, there is a risk of losing control over how the service is being delivered. This is of great interest when implementing Cloud in the public sector. Particularly for small organizations it may be hard to negotiate the right contracts and SLAs to get the proper guarantees about the delivery of the services; this can lead to lack of governance. There are also risks if (part of) the Cloud system is running across borders, in other jurisdictions. In these cases there may be risks for the confidentiality of data, privacy of personal data, but also, it may complicate auditing, fraud investigations, and services may become subject to foreign law enforcement or surveillance activities.

Characteristics of a governmental Cloud

Summarising, a **governmental Cloud** is a Cloud computing system (an infrastructure, a platform and a set of core services) which generally satisfies the following characteristics:

- A. The Cloud services are private (single tenancy), community (agreed set of tenants) or public (multi tenancy) Cloud to host processes and/or store data, to run eGovernment services and that can be controlled/monitored locally or in a centralised way by the public body;
- B. It provides a set of “building blocks” reusable services to create eGovernment services for public administration, citizens and private companies;
- C. It can be owned and managed by central government and/or external providers/ bodies. The central government or local bodies have the end responsibility (private or community deployment model);
- D. There is a business model that allows operating the infrastructure, the platform and the services and in a way guaranteeing efficiency and economy of scale;
- E. The infrastructure, the platform and the services are compliant with country governments and EU legislations on privacy, security and resiliency (location of the Gov-Cloud: on premises or off premises Cloud).

2.2 Current core practices

To understand the practices on governmental Cloud we investigated how governmental Cloud services are deployed (*deployment models*), what service models are adopted (*service models*), what type of services are provided (*type of gov-Cloud services*), how the governmental Cloud and services are managed (*management framework*), whether the adoption of Cloud computing will innovate eGovernment services and what are the benefits of adopting Cloud computing.

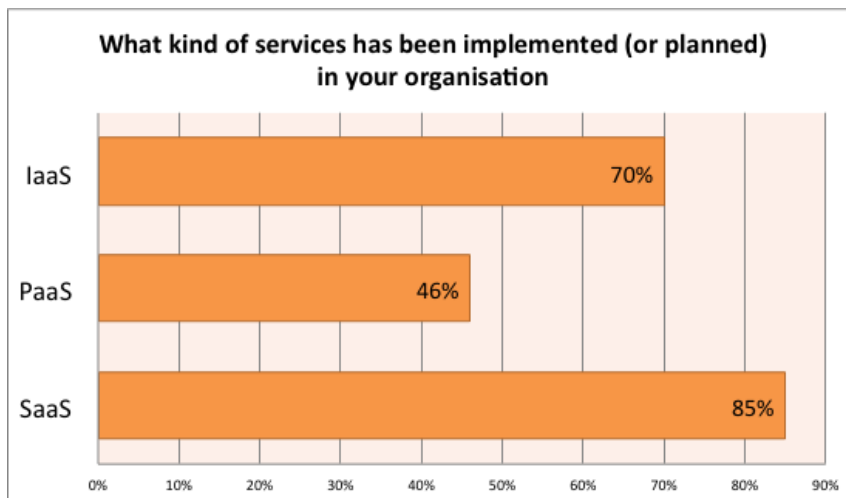


Figure 1 already implemented deployment models for governmental Cloud

The preferred **deployment models** (Public Cloud, Private Cloud or Community Cloud) implemented or planned to be implemented depicted in Figure 1. Figure 2 shows the most popular **services models**.

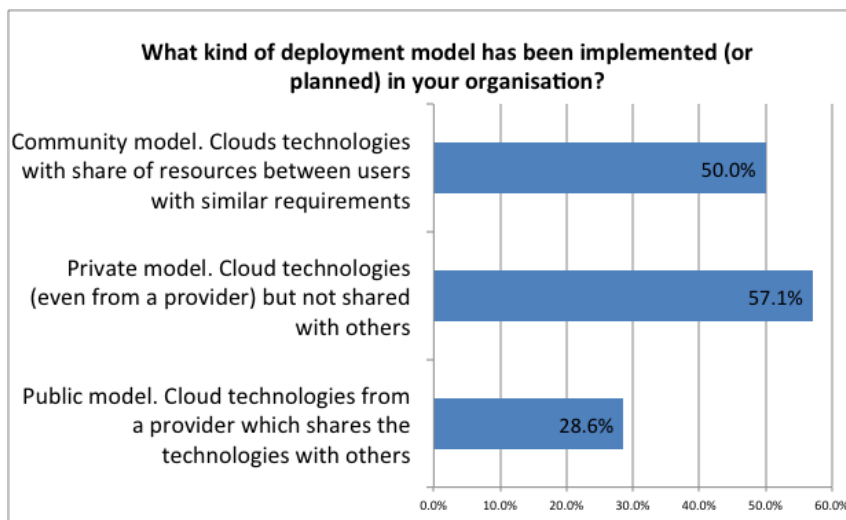


Figure 2 Service models for governmental Cloud

For the identification of the **type of government services**, the services have been classified as *“critical”* when they handle sensitive information or when the impact of a failure affects a number of citizens/ countries and as *“non critical”* when the services utilize low-sensitive information and the requirements in terms of security are quite loose.

The services are categorised as *“Government to Government”*, when a public institution provides Cloud services to others public institutions; *“Government to Citizen”*, when a public institution provides services to citizens (this option includes the *“Government to Private”*, where the end users are private companies) with a Cloud-based technology; *“Government internal”*, when the services are for the internal ICT services of the public organisation. Survey results are reported in Figure 3.

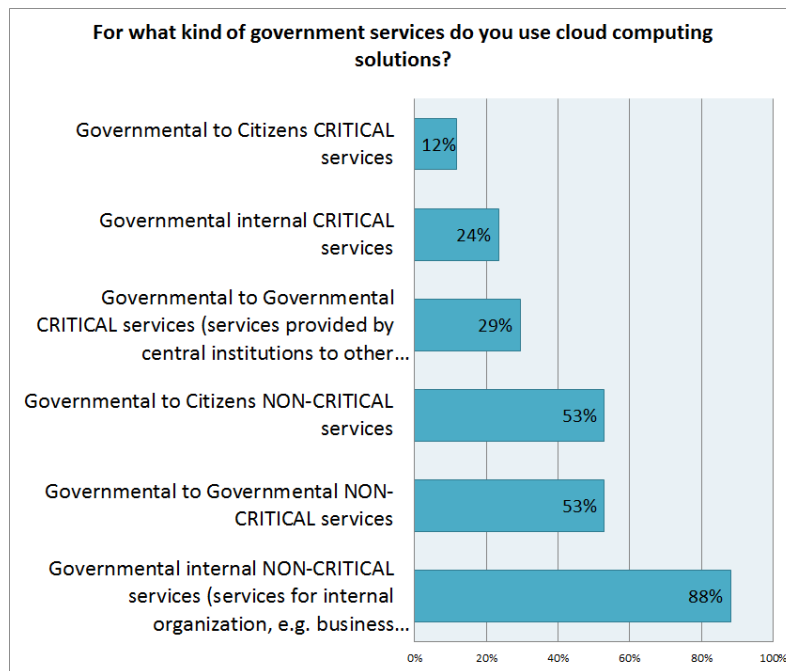


Figure 3 Categorization of government services by criticality and target users

Another aspect examined in this report is the management framework adopted by the public institutions for the governmental Cloud. The **management framework** options are “Government - Private”, when the public institutions buy the Cloud services from a private Cloud provider and/or the public institutions are assisted in the operations, in the set-up and in the management of the Cloud infrastructures with the help of private technology providers; “Government - Government”, when the public institutions buy the Cloud services from another public institutions which have the role of Cloud provider and/or the public institutions have in-house capabilities and know-how for the overall management of the technological Cloud infrastructures. Survey results are reported in Figure 4.

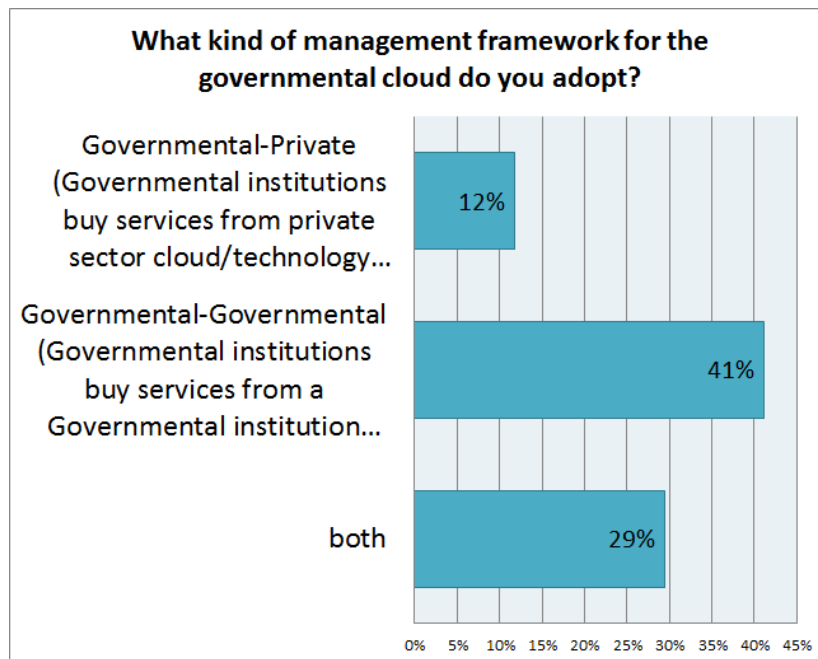


Figure 4 Management framework for governmental Cloud

3 Classification of governmental Clouds across the EU

To be able to present the wide and heterogeneous landscape of the EU countries concerning governmental Cloud a classification is needed. The basic criteria for this classification are as follows:

- the existence of a policy background to support the implementation of Cloud computing in administrative systems, i.e. national Cloud strategy or digital agenda,
- and the phase of the governmental Cloud implementation (design, implementation, projects running etc).

In the following we describe the main characteristics of each group we have identified.

- **Early adopters:** the countries in this group are: **The United Kingdom, Spain and France**. They have a Cloud strategy and they have taken specific decisions on how to implement the governmental Cloud. A number of initiatives is already running based on Cloud solutions.
- **Well - Informed:** the countries in this group are: **The Netherlands, Germany, Republic of Moldova, Norway, Ireland, Finland, Slovak republic, Belgium, Greece, Sweden and Denmark**. They have a strategy but the implementation is still at design or prototype stage or they have only preliminary implementations of some governmental Cloud services. In all cases, they are planning to massively adopt the governmental Cloud in the future, after an in-depth evaluation and investigation of the risks and the benefits of the Cloud solutions they have identified for the implementation and after the analysis of the first results of the implemented Cloud services.
- **Innovators :** the countries in this group are: **Italy, Austria, Slovenia, Portugal and Turkey**. The “Innovators” do not have a high-level Cloud strategy with clear indications on the solutions for the governmental Cloud, they could have a digital agenda that considers the adoption of Cloud computing, but they already have some Cloud-based services running, mainly based on bottom-up initiatives. Cloud implementation is forthcoming, but will need to be supported by a national or European high-level regulation.
- **Hesitants:** the countries in this group are: **Malta, Romania, Cyprus, and Poland**. This group is composed by countries that do not have a governmental Cloud strategy in place, they could have a digital agenda that considers the adoption of Cloud computing but do not have relevant Cloud initiatives or governmental Cloud experiences. They are planning to implement governmental Cloud in the future mainly to boost the country business and competitiveness and to attract investments.

These categories are not exhaustive, but are useful in describing the wide and heterogeneous landscape of the EU countries. Table 1 summarizes the categories by dimension of analysis.

	Early adopters	Well Informed	Innovators	Hesitants
Political and legal aspects (Cloud strategy)	Cloud strategy exists	On-going implementation of a Cloud strategy	Mainly limited to the Innovation and the digitalisation of the public administration	No Cloud strategy exists
Status (Governmental Cloud)	Mainly implemented governmental Cloud or supporting initiatives	The gov-Cloud is not fully developed (in most cases at design/prototype stage)	Gov-Cloud solutions exists, but very jeopardised and not integrated into a high level national vision	No gov-Cloud exists
Type of Cloud implementation	Private Cloud (except UK where is public Cloud)	Private Cloud (except Sweden where is community Cloud)	Public/Private Cloud	NA
Motivation for adopting Cloud	Innovation, Competitiveness, efficiency, job growth	Efficiency and cost saving, flexibility	Harmonisation of ICT, innovation in the public administration	Competitiveness and attraction of investments

Table 1 Categories outlined by dimensions

3.1 The “Early adopters”

The main countries composing the “Early adopters” group are: **United Kingdom, Spain and France**. The “early adopters” have published a Cloud strategy and its implementation actions. Usually, they have a number of Cloud initiatives running. In general, the ICT level of adoption in this case is very high and quite widespread. At national level there have been a number of investments on initiatives and activities in the area of Cloud computing funded by the government (for both private – e.g. SMEs – and public organisations). The overall design approach in defining and implementing public (multi-tenant) Cloud solutions is very pragmatic.

Policies, strategies and drivers

The key element of this group is the adoption of a Cloud implementation plan at national level, in some cases with a Cloud strategy (documents, frameworks, guidelines, regulations, implementation plans), or through a smooth migration of public services in Cloud solutions. We have encountered differences in the maturity of the solution and in the specific characteristics of the governmental Clouds; however, in all cases the adoption is quite widespread in administrative (various governmental bodies involved), geographically categorized (local, national, or regional bodies) and technical level (Cloud solutions have been adopted for a quite wide range of services - not only non-critical ones).

The most important dimension is the role played by the policy makers in preparing, developing and driving a high-level Cloud strategy for the country in all cases with a very pragmatic way. The definition of a Cloud strategy has been established inside a wider plan focused on a) innovation in

the public administration and efficiency in ICT, or as part of a strategy to b) support employment and growth.

Alongside the specific strategies and Cloud related initiatives, all these countries have invested time in supporting SMEs and research centres that have been funded with a number of projects and initiatives related to Cloud computing, building this way steady ground for the development of Cloud computing nationally.

Governmental Cloud practices

The governmental Cloud practices have been developed and launched by the central governmental authorities (in particular Ministries or other governmental bodies). The projects are often linked to other public activities or are specific initiative part of larger policies; for example, in Spain, e-invoice services using SaaS with the SARA infrastructure.

Below you will find more generic information on the status of the projects and details on the service models.

	Status	Application and Services
France	Cloud strategy running	Creation of a Cloud infrastructure company to deploy services for IT players, companies and administrations Computing, storage and bandwidth capacity on demand for private companies and public administrations , as well as for the IT sector (software and application publishers, SSII, etc.).
Spain	The operation of SARA (Spanish Public Administrations Network) platform for delivering Cloud services for the Public Sector started in 2010 . Upgrades and full implementations have been made in 2011 and later in 2013.	e-invoice services, delivery system, validation of electronic signature
United Kingdom	Cloud strategy running (announced in April 2012)	- Email , storage, website, data authentication, collaboration applications -National saving investments -Identity assurance service - PKI as Cloud service

Table 2 Status and implemented services from the “Early adopters” governmental Cloud practices

	Service model	Deployment model	Type of governmental Service	Management framework
France	IaaS	Private Cloud	Government to Government Government to Citizen Government to Business	Government - Business Government - Government
Spain	The current services are SaaS. Future plans include IaaS (but a more flexible architecture of server/storage/network will be needed)	Private Cloud	Government to Government Government to Citizen	Government - Government
United Kingdom	IaaS, PaaS, SaaS	Public Cloud	Government to Government Government to Citizen	Government - Business

Table 3 Service model, deployment model, type of gov services and management framework from the “Early adopters” governmental Cloud practices

3.2 The “Well Informed”

The main countries composing the “Well Informed” group are: **The Netherlands, Germany, Republic of Moldova, Norway, Ireland, Finland, Sweden, Slovakia, Denmark, Belgium and Greece.** These countries have a “live-document” for Cloud strategy or digital agenda, but the implementation is mostly still at the design or prototype stage, or they have partially implemented governmental Cloud services. Cloud computing is considered as a technical solution suitable for governmental IT services, but mainly in the form of “private Cloud” for reasons related to privacy concerns and/or due to the lack of compliance of the solutions of the providers to the governmental security requirements. Currently these countries are assessing how to implement Cloud in the best way and according to their specific needs; or have already started implementing Cloud services as a pilot, and need to evaluate the results before fully extending Cloud services. They might have Cloud-based services not fully running but in a development/implementation phase, Cloud based solutions only for limited services, or only for the use of single body (e.g. public agencies in the Netherlands using SaaS solutions, in Germany, “the technology program [Trusted Cloud](#) is the central contribution of the BMWi (Federal Ministry of Economics and Technology) for Cloud computing program, which was launched in cooperation with partners from industry and academia in October 2010. It is part of the ICT strategy “Digital Germany 2015” and the “High-Tech Strategy” of the federal government). In other cases “Cloud-like” solutions might be already in place (e.g. virtualisations of public datacentres storage solutions in the Netherlands). The implementation is designed carefully; a number of studies (market research, exchange with other countries, R&D preparatory work, etc.) are realised or

planned to support Cloud deployment and to ensure the adoption of the best possible Cloud solution. Other European countries could provide guidelines - based on previous experience.

Policies, strategies and drivers

In these countries the adoption of Cloud computing by governmental organisations is quite limited or (in some cases) almost absent. However there is a very strong political willingness to promote and widen the adoption of Cloud in public bodies. Within this group, the policy makers and governmental bodies (e.g. Ministries) are indeed confident about the benefits and opportunities that Cloud solutions can offer, specifically for the public bodies. However, all the potential constraints and defaults are carefully considered and currently under investigation and – as a result - for most of these countries, the political will is to go for the adoption of a “private Cloud” solution.

These countries have realised (or are willing to realise) an in-depth and extensive preparatory phase before deciding what kind of Cloud solutions will be more suitable for the governmental bodies organisations. Within this preparatory work, a number of market studies, evaluation of technological solutions, definition of the specific requirements for governmental Cloud, have been realised in order to sensibly assess all the aspects related to the adoption and migration towards the Cloud.

Governmental Cloud practices

In the “Well Informed” group, governmental Cloud computing experiences are quite limited or very recent. However, it has been possible to outline the main characteristics of the current solutions as well as the ones of the future solutions that these countries are willing to implement.

More general information on the status of the projects and details on the service models are presented below.

	Status	Application and Services
Finland	No adoption of actual “governmental Cloud”. Small initiatives have been realised by single governmental bodies.	Providing public vacancy information through web-base access interface (realised for the Ministry of Employment and the Economy by a private Finnish company)
Moldova³	In 2011 the Government of Republic of Moldova approved The Strategic Program for Governance Technological Modernization (E-Transformation) which specify the use of shared government technology platform based on Cloud Computing as mean to achieve the Program objectives. In 2012 “First Cloud Policy” (Prime Minister decision 21-d) was issued by the decision of Prime Minister which states that all government ministers and agencies will use primary MCloud platform to deliver e-Service	Mainly provides IaaS service to central public authorities (ministers and agencies). A number of PaaS service, like government electronic payment service and government authentication service, was developed and are provided to public and private sector. By the end of 2013 first SaaS service (document management)will

³ Interview with the e-Government Centre

	<p>to citizen, business and other government agencies.</p> <p>The first phase of the Government Cloud Platform (MCloud) was officially launched in February 2013.</p>	<p>start to be provided to central government authorities. . Currently the government uses the services for free (economic model models are under discussion).</p>
Germany	<p>goBerlin project from 2012 to 2014; Trust Cloud and Cloud Action Programme started in 2010.</p>	<ul style="list-style-type: none"> - “goBerlin” (platform to develop innovative applications for citizens, industry and administration) - online marketplace for information and analysis based on the data of the German Web. So use common analysis tools, e.g. to improve their market research and better customize products (MIA).
The Netherlands ⁴	<p>In 2011 Dutch government presented its Cloud Strategy. The Central Government identifies two main problems inhibiting the implementation of Cloud computing: the relative immaturity of the Cloud computing market, and the government’s highly stringent requirements with respect to data protection and privacy.</p> <p>Initially, therefore, Cloud computing will only be implemented internally, within the Central Government itself. That is to say, no use will be made of ‘open’ Cloud computing, but rather a ‘closed’ Cloud will be set up under Central Government’s management and control. The Cloud will exist within Central Government’s own secure network and be managed by its Central Government’s own IT staff.</p> <p>As of June 2013, the Goal Architecture of the Closed Governmental Cloud has been approved.</p>	<p>Small projects have been realised at local level, by the municipalities by creating an autonomous and independent datacentres.</p> <p>SaaS solutions are used by agencies responsible for different type of policies, often for storing open data in the Cloud</p> <p>The Dutch agency responsible for providing license plates for cars is using the Cloud platform for its open data.</p>
Norway	<p>In the “Digital Agenda for Norway” published in 2012-2013, the Norwegian State included the Cloud Computing as one of the main key topics.</p>	<p>For assisting the public and private institutions, the Ministry of Government Administration, Reform and Church Affairs will produce guidelines on the use Cloud services, comprehending relevant regulations and developing specifications and standard agreements for use in procuring</p>

⁴ Interview with the Operational Management Department, Ministry of Economic Affairs, the Netherlands

		such services, as an alternative to the standard agreements currently used by Cloud service providers.
Ireland	In 2012, the Irish Government developed the Government Cloud Computing Strategy for the public service, which places Cloud computing in the heart of future government ICT strategy: providing an approach for the public service deploy Cloud Computing and to undertake a comprehensive program of Datacentre Consolidation.	Examples of Cloud initiatives: Cloud services for research application is the EduStorage , a new network Cloud data storage service deployed by HEAnet (Ireland’s National Education and Research Network) providing advanced Internet and associated ICT and e-Infrastructure services to Educational and Research organizations.
Slovakia	The Slovak Republic has already prepared the Strategic Document for Digital Growth and Next Generation Access Infrastructure for the 2014-2020 periods. One of the strategic objectives and priorities, to be accomplished by 2020, proposed under the strategic document is for the Slovak Republic to introduce a common Cloud platform to share public administration services and information.	A project entitled “Datacentre for Towns and Municipalities” is now at its implementation stage, with its target outcome being Cloud platform based electronic services for local government authorities.
Denmark	There are few experiences of governmental Cloud. At high level, an e-governmental strategy has been produced for the 2011-2015 period. The strategy specifically report about an initiative for Updated rules on Cloud computing	Small deployments across the public sector i.e. emails etc.
Sweden	There are several solutions at the moment. Also there have been some discussion about a “unique” Cloud solution (the GOV-NET), but this is not in place at the moment.	e-Health solutions
Greece	There is no centralized Cloud strategy in Greece but a governmental Cloud implementation plan is signed under the e-gov National Strategy	GRNET (responsible for providing a multitude of e-infrastructure services to the Greek Research and Academic community) is developing an IaaS solution which will be provided free of charge to the Greek Academia. It was decided to build this using open source software. Three “pilot” organizations have been selected for Cloud services, and the

		expectation is that they will be able to provide backup services. GRNET is developing its own Cloud solution named Okeanos . Okeanos is one of the two platforms that provide resources to EC- funded projects.
Belgium	Federal e-government strategy	Fedict is in charge of implementing the e-government strategy in Belgium. They launched in May 2013 a public procurement process for IaaS Cloud services (including a datacentre) to be implemented in Fedict.

Table 4 Type of governmental Cloud and applications from the “Well Informed” governmental Cloud practices

	Service model	Deployment model	Type of governmental Service	Management framework
Finland	N.A.	Planning to adopt a private Cloud	Government to Government Public to Citizen	Government - Government
Moldova	IaaS, PaaS, SaaS	Private Cloud (“Government private Cloud – GCloud”)	Government to Government Government to Citizen	Government - Government
Germany	IaaS, PaaS, SaaS	Community/ Private (already existing Cloud- infrastructures of the public IT- contractor ITDZ Berlin)	Government to Private (TrustCloud) Government to Government and Government to Business (goBerlin)	Government - Business
The Netherlands	Planning IaaS, PaaS, SaaS Some running services are SaaS	Planning to adopt Private Cloud (“Closed governmental Cloud”), however, some services are from Public Cloud providers (Public Cloud)	Government to Government	Government - Government

Norway	SaaS	community (in municipality lev	Government to Government Government to citizen	Government - Government
Ireland	SaaS	Private/ Community Cloud	Government to Government Government to citizen	Government - Business
Slovakia	PaaS, SaaS	Private Cloud	Government to Government	Government - Government
Denmark	IaaS, PaaS, SaaS	Public Cloud	Government to Government Government to citizen Government to Business	Government – Business
Sweden	IaaS, SaaS	Public and private Cloud	Government to Government	Government - Business
Greece	IaaS	Public Cloud	Government to Government Government to Citizen	Government – Business
Belgium	IaaS	Community Cloud	Government to Government Government to Citizen Government to Business	Government - Government

Table 5 Status, service model, deployment model and management framework from the “Well Informed” governmental Cloud practices

Regulation and security practices

In this group, national regulation on ICT security is quite tight. However, it is not an obstacle that halts the adoption of Cloud computing by the government; handling of security and privacy issues could be simpler than expected, once a trustworthy relation is established with the Cloud providers. The on-going activity focusses on how to concretely manage the relationship with the Cloud provider, and which are the clauses the Cloud providers could fulfil. Specification of needed certifications, SLAs, audits, security and privacy requirements are currently under investigation as well. The fact that security requirements are not fully met by the provider is also a drawback.

Due diligence is also another drawback in this case. In particular, the issue of sharing responsibilities among the private providers, the agencies or a public third party (if there), and the government is very critical.

3.3 The “Innovators”

The main countries composing the “Innovators” group are: **Italy, Austria, Slovenia, Turkey and Portugal**. The “Innovators” do not have a high-level Cloud strategy (they could have a digital agenda that considers the adoption of Cloud computing) but they already have some initiatives/services running at local level or in specific sectors (e.g. e-Health); these existing initiatives are covering mainly (but not only) non-critical services. For most countries there is a willingness to design and implement a public Cloud in short term (1-2 years). The adoption of Cloud is mainly due to a bottom-up approach in the building and stimulating Cloud uptake. The industry, service providers, local agencies, SMEs play a very active role by promoting their Cloud solutions or pushing for the adoption of innovative IT service in the public.

Several private organisations are responsible for implementing and maintaining the public Cloud services and infrastructures, with the effect of having a number of not well harmonised services, applications and general IT solutions that have very limited level of interoperability.

In fact there is also a fragmented and not heterogeneous environment with regards to the applications, services, contracts and SLAs with multiple Cloud providers. However, a number of outstanding initiatives exists (mainly started by public administrators at middle management level or regional levels) showing a very good level of novelty and value in the adoption of governmental Cloud services. Nonetheless, these initiatives still remain isolated, and are not integrated into a strategic vision or at political or high-level public administration.

The issues of security and privacy in relation to the Cloud computing for the governmental bodies have not been well addressed; in some cases such regulation is perceived either as too tight, or is not focused on the specific needs and issues of Cloud computing for governmental institutions, or is completely lacking. These countries look at Europe as the main actor that should start up a “European Cloud legal framework” and drive the harmonisation of the different regulations across the EU; specifically (and at least) Europe should push for making the governmental Cloud as a main topic to be covered by each national ICT strategy.

Policies, strategies and drivers

The “Innovators” do not have an official governmental Cloud strategy in place, but do have policies, frameworks, programmes, and initiatives that mainly deal with the digitalisation and innovation in the governmental bodies and public administration. In general these countries have a variety of public administration bodies, agencies and third parties (both at local and central level) operating as/with/and-on-behalf of the governmental body; in some cases they also deal with the deployment and provisioning of IT services.

In comparison to the “well informed” that are willing to adopt the Cloud but with a more long-term schedule (3-4 years) and that already are in the phase of studying and investigating of governmental Cloud solutions, the “Innovators” are less “long-suffering” and would like to move to the governmental Cloud quite quickly and effectively. Assessment studies and research should be done by a single high-level public central entity but realised in a concrete manner by each body that is willing to move to the Cloud. From this point of view, this cluster group is very keen on having high-level guidelines in the form of regulations and legal frameworks: “practical” suggestions on how to select, move, implement, and maintain the governmental Clouds are not perceived as relevant. It

seems that the practical implementation should be done on-the-field and to be realised by each body itself, but of course under a Cloud strategy.

So far, there is no specific plan on the deployment type of service the governmental body should have. In some specific cases (e.g. Austria⁵) the adoption of a governmental Cloud is perceived as unfeasible at the moment due to the lack of Cloud quality criteria and certifications schemes that would increase transparency concerning the security of public Cloud services.

Governmental Cloud practices

Despite the lack of an overall Cloud strategy and high-level vision, governmental Cloud projects are taking place, with some peaks of excellence. The adoption of Cloud is mainly due to a bottom-up approach (realised mainly by the middle management and the operational personnel of the public administration or in regional cases) and is building and stimulating the Cloud uptake. In most cases drivers of these initiatives are mainly the push for competitiveness and innovations rather than the cost-saving benefits that Cloud claims to provide. As well as for the IT adoption, also for the Cloud most cases are running in specific sectors (e.g. e-Health) or in specific organisations (e.g. local bodies).

To by-pass the “no-Cloud-vision” approach, some large governmental institutions have started themselves a process toward the implementation of Cloud infrastructure owned by them, to deploy Cloud services for internal purposes as well as for other public bodies. In this scenario, the governmental body is not only the final user, but also becomes a Cloud provider for other public/no public users.

As an example of good Cloud practices, large governmental institutions have started a process of evaluation of the technological infrastructures providing Cloud services to the local municipalities under their administration and jurisdiction. This implementation model has been perceived in a positive way, as municipalities are reassured from the issue of controlling and managing data, which are actually managed by a public institution.

The “innovators” look at Europe as the main actor that should start up a “European Cloud legal/policy framework” and drive the harmonisation of the different regulations across the EU; specifically Europe should push for making the “governmental Cloud” a main topic to be covered by each national regulation. This framework could suggest guidelines on how to setup a Cloud strategy, guidelines on public procurement with solutions on the locality of data and governance issues.

	Status	Application and Services
Austria	EMD Project started 2011 (the project was also winner of the EuroCloud award in 2012 for the “Best Case in the Public Sector”).	EDM Environment Data Management realised by the Ministry of Life and Environment. It has about 45 registered organisations and about 800 users every month. It combines local and central governmental organisations, including specialist from organisation that are managing waste.
Italy	First projects and pilots started from 2009	National Registry (example of governmental Cloud established under the Italian authority) Federa Project (Emilia Romagna) that provides an

⁵ Interview with EuroCloud Austria chapter.

		<p>integrated authentication systems to access all public online services of the region.</p> <p>The Department of Treasury of the Minister of Economy and Finance has a Cloud platform providing services that can be used internally and by other public administrations.</p> <p>The Ministry of Foreign Affairs has developed a private Cloud to ensure service continuity for Italians residing abroad by strengthening active and passive security as well as ICT safety of diplomatic-consular offices located in areas of high conflict.</p> <p>The Region of Tuscany has inaugurated the new Cloud datacenter for providing services to the local municipalities. At the beginning IaaS and PaaS, in the next SaaS.</p>
<p>Turkey</p>	<p>There is no national Cloud strategy in Turkey, but there is a datacentre consolidation strategy encompassing Cloud.</p>	<p>E-government services are provided by communications provider Turksat. In the education sector there are plans to replace all books by tablets, and to provide all schools with smart boards. The budget for this has been allocated and the hardware is being rolled out. Some of the hardware would have to be manufactured in Turkey. Academia Cloud is the biggest Cloud project in the country.</p>
<p>Slovenia</p>	<p>No official Cloud strategy defined, however is under study the modernization of eGovernment services using Cloud computing, in the specific a solution customized for the government requirements in term of legislation on security and privacy</p>	<ul style="list-style-type: none"> -Portal for e-procurement (in development phase), infrastructure registry, portal for citizens services -the Slovenian Ministry for Higher Education has partnered with the European Commission and industry to develop the KC Class-Cloud Assisted Services project. KC Class goal is to develop services and products in the area of Cloud computing for local adoption
<p>Portugal</p>	<p>GPTIC - Strategic plan by 2016. Not officially Cloud strategy but Cloud initiative is one out of the 25 measures of the Portuguese global strategy.</p>	<ul style="list-style-type: none"> - AMA (Agency for the Modernization of the Public Administration) coordinates the operational and technical level the development of ICT tools and structures for e-government and has also considered the implementation of the GO-Cloud (Governmental Open Cloud), a platform with shared Cloud services - Portal services - IaaS, email, file sharing, storage, identity management, financial and human resources management, patrimony management and others.

		- Critical applications are involved
--	--	--------------------------------------

Table 6 Status and applications from the "Innovators" governmental Cloud practices

	Service model	Deployment model	Type of governmental Service	Management framework
Austria	PaaS	Private	Government to Government	N.A.
Italy	IaaS, PaaS, SaaS	Public /private Cloud	Government to Government Government to Citizen Government internal	Government - Business Government - Government
Turkey	IaaS, PaaS	Public Cloud	Government to Citizen	Government - Government
Slovenia	IaaS	Private and customised public solutions	Government to Government Government to Citizen	N.A.
Portugal	IaaS, PaaS, SaaS	Public Cloud	Government to Government Government to Citizen	Government - Government

Table 7 Service model, deployment model, type of gov-Cloud services and management framework from the "Innovators" governmental Cloud practices

Regulation and security practices

Regulation is not only perceived as too tight but also - in some cases - lacking in clarity. Moreover, the high-level legal framework is absent that should be the reference point when adopting Cloud for governmental bodies. The need for specific regulation designed to support, promote, and fund activities aiming at widespread of the governmental Cloud adoption is evident.

In this case, the need for national regulation (or at least guidelines), as a starting point, is considered a catalyst to create efficiency and innovation in the governmental services and the public administration itself, therefore spreading the innovation to all the country. In particular the adoption of governmental Cloud, if realised under a high-level policy design, could harmonise the “plethora of public administration IT services”, centralise and optimise resources (both tangible and non-tangible ones), and offer an engine for competitiveness of national Cloud providers. Policy level guidelines

should be given in order to have a specific regulation for the adoption of Cloud for the governmental bodies.

With regards to the **security and privacy issues**, it is perceived that addressing these requirements will greatly increase the cost of the Cloud-based service and will also make SLAs quite complex from the point of view of the governmental bodies (considering both the preparation of the contracts and the actual verification during deployment). The current security and privacy regulations are perceived to be in some cases obsolete and do not take into account the specific characteristics (such as locality of data, governance models, offering no flexibility to the Cloud user) of Cloud computing for governmental bodies. Therefore, the full adoption of Cloud technologies will need to be supported by the development of an overall legal framework specifically designed for the IT for the governmental services. The new legal framework should take into account not only technical and commercial issues but mainly organisational ones, including the interrelation of the services between different governmental organisations (small/large, local/central) as well as the security governance issues. Risks such as lack of governance or cross border compliance should be dealt with in the framework, to avoid confusion when carrying out law enforcement and to prevent unauthorised state surveillance activities.

3.4 The “Hesitants”

The main countries composing the “Hesitants” group are: **Malta, Romania, Cyprus and Poland**. They neither have a high level strategy, nor specific planning for future implementation. In most cases this is more due to the limited resources available rather than to the lack of IT innovation. Despite the fact that no specific policies or strategies are in place, the absence of a Cloud strategy does not indicate that Cloud computing is perceived as an unsuitable technology for governmental IT services; in fact in these countries there is a widespread positive attitude towards the adoption of Cloud computing in the future.

The intention of adopting Cloud in the long term (3-4 years) exists. In parallel there is a quite diffuse awareness (in particular from the operators providing support, R&D, and consultancy IT services to the public administration) on the benefits of adopting Cloud, as well as the potential risks and costs for the deployment of Cloud services. The will to implement Cloud is mainly linked to the benefits that it could provide to the country's business activities and for attracting investments (rather than being a benefit mainly for the governmental body itself and for the citizens). In most cases these countries also claim that the start-up of Cloud adoption is delayed due to the lack of a European regulation on the topic of governmental Cloud, as well as the exchange of best practices and lesson learnt from other European countries. National legislation or agreements between government and vendors does not suffice due to lack of trust, transparency and new investment costs.

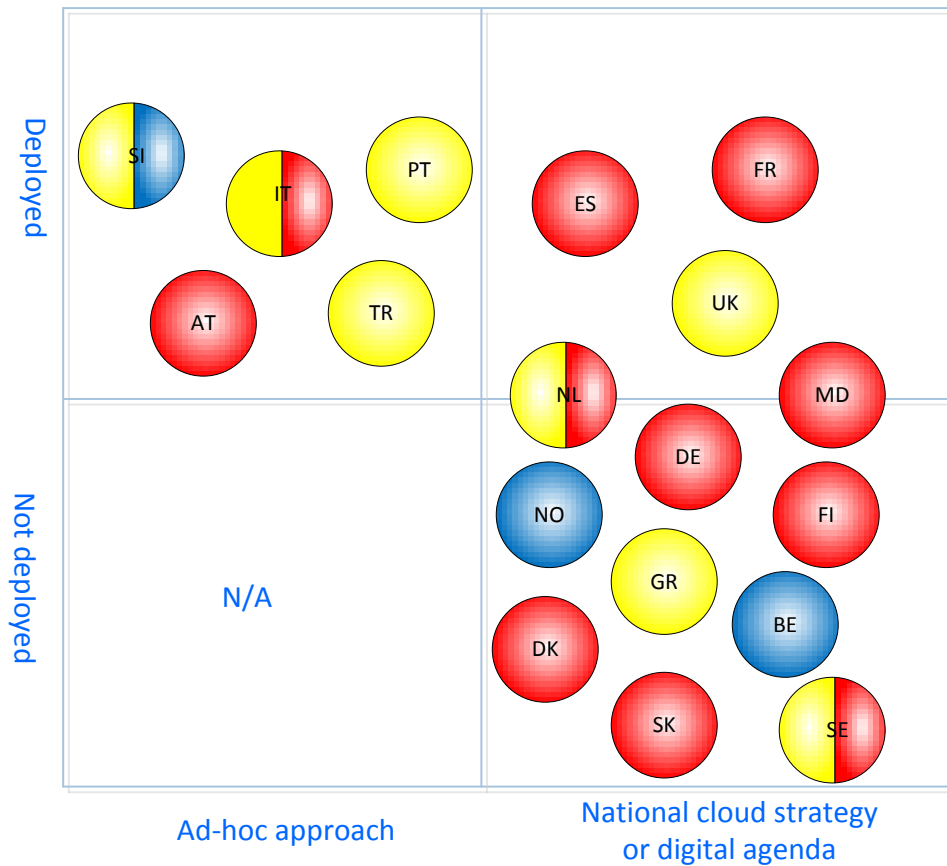


Figure 5 Visualization of the deployment models of gov Clouds

In the image above we depict the categorization of the EU governmental Clouds according to the information described above: red circles refer to private Cloud services, yellow to public and blue to community Clouds. In some countries, two implementation types could exist.

4 Best practice scenarios and analysis

In this chapter we present three scenarios, based on the three first categories described above. A SWOT analysis per scenario is conducted at the end of each scenario. The scenarios are based on the actual situation in Europe, as presented in chapter 2 and 3, with some additional elements.

4.1 A Governmental Cloud Catalogue

Having adopted a national Cloud strategy, a European country “Greenshore” seeking to support governmental bodies in the smooth adoption of Cloud solutions, sets up a governmental Cloud catalogue to be used by governmental bodies. In the catalogue, each provider (big providers or SMEs) can offer their product: the types of Cloud services provided are IaaS, PaaS and SaaS with a large range of categories of services i.e. email, storage, website, CRMs, collaboration applications etc. The implementation model is public Cloud, meaning that the Cloud resources of the providers are shared and used by multiple customers. Each provider listed in the catalogue has its own infrastructure to support the services offered. The idea behind this national project is that government will eliminate all the drawbacks that were keeping the governmental bodies from going into the Cloud.

In essence, what this catalogue (implemented by public sector) offers is an intermediary solution for contract enforcement and security accreditation, held by a governmental organization. Before procuring a service, a risk assessment by public agencies is taking place; they analyse the Cloud-based solutions and verify if the candidate services meet the specific requirements (including security and privacy issues). The providers joining this catalogue should be compliant to a baseline set of security requirements; the requirements will include measures categorized in different risk-impact maturity levels. A specific procedure is in place for this task and when it is complete the service is accredited and can be used by governmental agencies.

This catalogue is open for providers based in Greenshore, reassuring that the datacentres are in Greenshore and falling no other jurisdiction but Greenshore’s. If a foreign provider would like to offer services, additional security requirements must be met and adopt the contractual clauses on data protection. To allow more SMEs to participate in this project, the accreditation process is free of charge and obligatory to all potential providers. In the offered services list, it is signified if the service is accredited or not. This way the buyers know which service is suitable or not for handling sensitive or personal data. The pre-assurance is not only helping SMEs but everybody in streamlining the process, cutting costs, standardising and re-using without the need to engage in re-assurance. All providers of services or applications in the catalogue need to be pre-assured as do the service assembly workloads and the deployment and life-cycle management processes of the government catalogue.

Below we conduct a SWOT analysis for the scenario described above.

Strength

Security guarantees. The security accreditation is guaranteed (by the governmental authority that will perform this task) with an efficient cost effective process, which permits both to offer secure Cloud services and simple Cloud services for low-level of criticality type of ICT services.

Weakness

Slow diffusion of Cloud. The public institutions are not obliged to select Cloud-based solutions for the ICT services. The real uptake of the Cloud in the public sector could be uncertain

Change in the ICT culture and approach

<p>Central consolidation of know-how on security for Cloud based services which is enriched and updated continuously with the advances in the regulations and the progress in the security frameworks</p>	<p>from the public sector. A cultural change is required for the adoption of Cloud services</p> <p>Dissemination of Cloud services used by governmental institutions: Diversification of services could lead to interoperability and portability issues</p>
<p>Opportunities</p> <p>ICT innovation in the public sector and potential increase of competitiveness in the private sectors (SMEs and big companies)</p> <p>Efficiency by eliminating the duplication of effort for cost-effective procurement and security verification of information systems/services</p> <p>Ensure the adequate level of security for gov-Cloud services</p>	<p>Threats</p> <p>Scalability. The centrally managed security and procurement requires an appropriate department/structure that will not create “bottle-neck” for the services accreditations</p> <p>Complexity of the start-up. The set-up of processes, integration, and governance needs a strong initial effort</p>

Table 8 SWOT analysis of the “Early adopters” use case scenario

4.2 Consolidating Existing Clouds to Improve Efficiency

In the country of “Fairlyn”, it can be said that the use of Cloud computing dates back to before the term Cloud computing was even coined. Municipalities, counties and regions have been using shared computing resources and infrastructure already for a long time, to run applications and databases supporting processes such as population registers, issuance of identity documents, registration of vehicles, or budget planning and management.

The cornerstone of this structure is based on the fact that the corresponding administrative bodies founded ICT service providers, wholly owned by them (ICT service provider is part of administrative bodies). These service providers were tasked with setting up and running datacentres in the corresponding administrative regions, hosting the applications used to support most of the administrative processes of the participants, and in many cases also managing the networks connecting the users to the datacentres. The owners of the ICT services are the different governmental institutions.

Recently, many of these IT service providers have been introducing new services explicitly branded as “Cloud” services.

This model has allowed the participating administrative bodies to benefit from significant economies of scale. It can be seen as a good example of the “community Cloud” model (used by a closed group of independent entities).

The approach predates the development of the Cloud computing concept itself and also Fairlyn’s Digital Agenda, and therefore didn’t follow a defined strategy initially. However, exchange of

information about good practices and lessons learned both among the participating administrations (i.e. the customer side) and the different regional service providers (i.e. the provider side) has led to a surprisingly homogeneous picture.

In its recently finalised Digital Agenda, the government of Fairlyn recognises the potential offered by this successful model, and aims to build on the experience gathered in the past. Fairlyn’s Digital Agenda calls for increased standardisation of IT environments across several levels of public administration, and for increased cooperation between the different regional datacentres, to further improve the economies of scale, and to enable new operation modes increasing the resilience of the services.

Strength

Strategic vision for the development of a government-wide “i-infrastructure”. The strategy will aim at realizing a “closed” Cloud infrastructure under the Central Government’s management and ownership, as unique ICT infrastructure for the public sector

Clear “step-by-step” plan for introduction of secure Cloud services. The Cloud strategy is particularly focused on implementing a gradual introduction of Cloud technologies in the public sector, with intermediate steps for the analysis of the results and decision for the further progress of diffusion of Cloud services

Accurate preliminary analysis of the Cloud computing risks and benefits. A set of research studies for the deep understanding of the Cloud computing risks and benefits has been conducted, covering the aspects about security and data privacy issues and the compliance of the Cloud technologies.

Weakness

Unclear definition of the governance. The unclear definition of the governance model for the initiative could be revealed as a problem that will occur during the working phase and that could be an obstacle

Governmental public Cloud services requirements are not addressed. Even if the offers from the Cloud providers evaluated are still immature, the strategy does not include any specific positions on the type of governmental Cloud services implementations.

Cost effectiveness issues. The development of own datacentres will be cost prohibitive for most countries.

Opportunities

ICT modernization of the IT infrastructures for the public sector

Efficiency by preventing the redundant and similar applications and services within the public agencies and institutions

Consolidation of the multiple Fairlyn’s governmental datacentres into a single “i-infrastructure”

Threats

Not effective achievement of the final objective of the Cloud strategy. The public institutions are not obliged to select Cloud-based solutions for the ICT services. The development of own datacentres in parallel with the closed Cloud infrastructure could be go on with the effects of the slowing the diffusion of closed Cloud and to not achieve the overall objectives of the Cloud strategy

	<p>Concerns about security and privacy issues for high-sensitive information. Feedback from some public agencies not to use Cloud infrastructure for high sensitivity data could become problematic.</p>
--	---

Table 9 SWOT analysis of the “Well Informed” scenario

4.3 Building a National Cloud Infrastructure Based on Open Source

In this country, “Atlandia”, there is no Cloud strategy; the government doesn’t consider Cloud adoption as a priority. However the external commercial providers’ community is very active in this domain; a national initiative was launched to support universities, research centres and other public academic institutions in building the “Academic Cloud”. A local network provider (networks and public infrastructures, not telecommunications), contracted by the government, with the assistance of other small providers (SMEs consortium) built a Cloud platform where students can enrol for free, create a virtual machine, connect to virtual networks and the Internet and gain process to all the academic books shared in the country. The vision behind this is to offer scalability, a service open to everyone, no customer lock-in (by the vendor) and low admin costs making it accessible to small admin teams.

The provider offers a public IaaS solution, with datacentres located in Atlandia (and under the data protection law of Atlandia, compliant with the EU data protection law) offering storage solutions, with all stacks being built using open source software. Other members of the consortium offer back up services to the main datacentre. According to the requirements of the customer the service can be updated to provide flexibility. Data storage and processing procedures are compliant with national data law.

In IaaS security is a non-trivial matter; it is considered a feature covered by the provider via security measures i.e. firewall services. When building the virtual machine, use of encryption methods is suggested. It is very important that security is integrated at the lowest level; one can have very secure platforms and software, but the “construction” will collapse if the underlying infrastructure is compromised. Plans for the future are mainly for SaaS: email, document management, office automation service used by the government and public bodies will be moved to Cloud.

Below we conduct a SWOT analysis for the scenario described above.

<p>Strength</p> <p>Strategic relevance of Cloud computing for the public sector. Cloud computing is considered strategic for the public sector because this service can be used by governmental bodies. This example can be a model for when considering implementation in the administrative systems.</p> <p>Security is considered as an important aspect of the IaaS. Often, local laws and regulations prevent the use</p>	<p>Weakness</p> <p>Needs of high-level guidelines. The lack of high-level guidelines covering technical, legal and organisational issues is a major concern i.e. procurement guidelines for securely procure services for the citizens, contractual recommendations for public sector.</p>
---	--

<p>of IaaS providers that will store data outside the country borders because of stringent security requirements of Government. So security is very important for IaaS providers. Projects and initiatives of governmental Cloud infrastructures have started with a bottom-up approach and security is part of all layers.</p>	<p>Lack of open source software support. Service level for supporting open source software may not correspond to expectations (maintenance, patching, updating etc).</p>
<p>Opportunities</p> <p>The governmental agencies will adopt a Cloud-based paradigm in IaaS. The project can make more simple and faster the process of integration on the governmental Cloud for the public institutions.</p>	<p>Threats</p> <p>Cloud services from private Cloud providers are not addressed at all. The high-level guidelines should include recommendations for services of private Cloud providers.</p> <p>Security and privacy aspects to be addressed in case of extending to PaaS/SaaS. Before making the services available to governmental bodies, all security aspects should be addressed. The provider should find a way to guarantee baseline security measures compliance.</p>

Table 10 SWOT analysis of the “Innovators” scenario

5 Recommendations

Based on the current situation in Europe concerning the adoption of Cloud computing and the derived scenarios, we present a set of recommendations on how to securely deploy governmental Clouds. A description of the recommendations follows as well as the actions that need to be taken to fulfil them:

- EC and MS to support the development of an EU strategy to foster the adoption of governmental Cloud;
- EC and MS to develop a business model to guarantee the sustainability and economies of scale of governmental Cloud solutions;
- MS and Cloud providers to foster the development of a framework to mitigate the “loss of control” issue;
- EC and MS to promote the definition of a regulatory framework to address the “locality problem”;
- MS and Cloud providers to encourage the development of governmental Cloud solutions compliant with EU and country specific regulation;
- EC and MS to support the development of an SLA framework;
- EC and MS to foster the adoption of baseline security measures for both public and private Cloud deployment models;
- EC and MS to develop a certification framework;
- Academia and Cloud providers to foster research on governmental Cloud security;
- EC and MS to support privacy enhancement in the Cloud.

In the matrices below the benefits and beneficiaries per recommendation are presented:

Recommendations	Benefits (direct)		
	Economic)	Security	Take-up
R1: Support the development of an EU strategy to foster the adoption of gov-Cloud	x		x
R2: Develop a business model to guarantee sustainability	x		x
R3: Foster the development of a framework to mitigate the “loss of control” issue		x	x
R4: Promote the definition of regulatory framework to address the “locality problem”		x	x
R5: Encourage the development of gov-Cloud solutions compliant with EU and countries specific regulation		x	x
R6: Support the development of an SLA framework gov-Cloud		x	x
R7: Foster the adoption of stringent security measures for gov-Cloud services		x	x

R8: Develop a framework to incentivise provider's certification		x	x
R9: Foster research on gov-Cloud security leveraging existing research programmes		x	x
R10: Provision of privacy enhancement		x	

Recommendations	Beneficiaries (for WHO)			
	Central government regulators (EC and MS)	Local government regulator (MS)	Cloud providers	R&D Sector, Academia
R1: Support the development of an EU strategy to foster the adoption of gov-Cloud	x	x	x	
R2: Develop a business model to guarantee sustainability	x	x		
R3: Foster the development of a framework to mitigate the "loss of control" issue	x	x	x	
R4: Promote the definition of regulatory framework to address the "locality problem"	x	x		
R5: Encourage the development of gov-Cloud solutions compliant with EU and countries specific regulation	x	x	x	
R6: Support the development of an SLA framework gov-Cloud	x	x	x	
R7: Foster the adoption of stringent security measures for gov-Cloud services	x	x	x	x
R8: Develop a framework to incentivise provider's certification	x			
R9: Foster research on gov-Cloud security leveraging existing research programmes			x	x
R10: Provision of privacy enhancement	x	x		

5.1 Recommendation 1: EU governmental Cloud strategy

The adoption of Cloud computing in the government sector is very heterogeneous in Europe. This slow take-up is due to many issues described above related to security, loss of control, data protection and awareness. Although existing or proposed security legislative pieces cover some of the security aspects, the use of Cloud computing has a significant impact in differentiating how IT and services operate and their adoption will have to lead to a revision of such security measures

Our study reveals that the adoption of gov-Cloud in a systemic way is more advanced in countries that already have a national strategy addressing the Cloud computing adoption. Moreover, many experts are convinced that the development of an EU strategy focussing only on public sector and national strategies for governmental Cloud computing will foster the adoption of gov-Cloud in the EU countries.

Actions

Some recommendations based on our findings:

1. To elaborate and design a strategy with high-level guidelines, covering technical, legal and organisational issues. The clear definition of the governance model for the Cloud initiative should be defined before the implementation phase. A coherent plan presenting the objectives and the vision of the governmental bodies, the agile dissemination of Cloud services within several public institutions, and if a centrally designed strategy is defined, is needed. The lack of strategy and the deficiency on technical, legal and procedural aspects are critical obstacles for the start-up of governmental Cloud services.
2. To consider a program that can envisage the incremental introduction of secure Cloud services, with a step-by-step execution plan and with meaningful deliverables and milestones. A "step-by-step" plan would be an option for gradually introducing the Cloud in the public sectors, by taking more confidence to the technologies during a soft transition period, and thus permitting the public institutions to assimilate the new way of managing and deploying IT services and core processes for IT operations.
3. To promote well-informed, risk-based policies that will encourage and stimulate the start-up of Cloud in the public sectors and encourage use of external public Cloud solutions for the "open data". The policies should facilitate the ability of governmental bodies to choose Cloud computing for their services. "Cloud first policy" that is currently adopted in UK, Netherlands, the Republic of Moldova and the US FedRAMP program could support growth in Cloud computing. The "Cloud first policy" recommends the public sector organisations to consider and evaluate potential Cloud solutions first – before making any new investments for new services.
4. To relate the national Cloud strategy with projects and initiatives for increasing the government ICT efficiency and datacentre simplification. Initiatives for datacentre consolidation and/or ICT portfolio assessment can become important drivers to boosting the Cloud computing strategy; at the same time, Cloud computing can accelerate datacentre consolidation efforts and ICT portfolio simplification by reducing the number of applications hosted within government datacentre.
5. To evaluate the option of the public Cloud deployment model. Public Cloud is a more viable option for the public sector for leveraging some of the main benefits of Cloud computing paradigm, if security issues and concerns are addressed. In a strategy for the Cloud computing with step-by-step execution planning, the public Clouds could be deployed for non-critical services or in a second phase of the implementation of the strategy.
6. The MSs need to ensure the strategy's compliance with laws, regulations, and national agency requirements for the security and data protection. The MS should also make sure

that the national strategy is be compliant to national and EU laws and regulations on security and protection of information, assets, and infrastructures and taking into account the privacy of data. We encourage that the EC adopts one European set of rules and regulations concerning security and privacy, to support MS in this action.

7. To evaluate options for developing government service catalogues encompassing pre-assured Cloud products / applications and services catalogues, which are further classified against targeted government Cloud platforms, usage profiles and best-practices

5.2 Recommendation 2: a business model to guarantee sustainability

Today, the private Cloud model (governance and use in the governmental institution) is the most widely used in EU governmental Clouds (as indicated by the 57% of the experts interviewed). The slow take-up of the public Cloud model found roots in regulatory weaknesses and immaturity of public Cloud solutions. The relative immaturity of the Cloud computing market creates three significant difficulties:

1. Although there are plenty of providers of Cloud computing services, most are start-ups, and therefore cannot guarantee the level of stability that a company partnering with the government would need to have.
2. Most solutions have so far been designed for the business context. As a result, few open Cloud solutions on the market can meet the specific requirements of government.
3. Few solutions on the market today take account of the government's special responsibility for data protection. As a result, there are still relatively few open Cloud computing solutions on the market that would be suitable for use by the Central Government.

However, to build and operate a private Cloud, migrating existing services could be really expensive and the development of cost model capable to evaluate the real cost saving is actually a difficult task. To really boost the adoption of governmental Cloud, EC and MS competent authorities, in cooperation with Cloud providers, should develop a business model that will guarantee the efficiency and the economy of scale of the governmental Cloud solutions. The solution is to move towards the use of an appropriate public/community Cloud business model. This model will reduce costs to improve data and service availability, service reliability and security.

Actions

A pan European regulatory framework is needed to enable the adoption of multi-tenancy infrastructures and service sharing among governments. This framework should address the problem of data and service locality. The framework should also address issues that come with changing Cloud vendor or terminating a Cloud contact. It should be focusing on the terms and conditions that should be in a SLA, and the enforceability of those terms and conditions to do so. Second, an independent third party assurance can contribute to building trust whereby European SME's and other organizations will use Cloud computing services more. The idea is to establish a maturity level based framework, where governmental institutions will accredit the Cloud vendor, and offers a kind of active and proactive escrow service by a third party, in such a way that this party can assure a seamless takeover of the Cloud operations that provider A executes for a user to Cloud provider B. This should therefore include the (functionality of the) software, the users' data and the current state of transactions. Third, the public Cloud providers should improve their reputation and trustworthiness.

More specifically a public/ community Cloud business model should be supported by:

- An EU regulation on the use of multi-tenant infrastructures for eGovernment services;

- A framework to evaluate/certify the public Cloud provider qualification (e.g. introducing light auditing procedures, voluntary certification scheme)-(more details in recommendation 5.8);
- A public procurement framework for all governmental bodies that need to procure Cloud services;
- Creating a legal framework to deal with cross border procurement;
- The definition of standard procedures for application and data migration;
- A framework to monitor/control data locality and data handling in general.

5.3 Recommendation 3: a framework to mitigate the “loss of control” issue

Loss of control of data and resources is one of the main barriers to gov-Cloud take-up, as indicated by the 58% of the experts interviewed. The “loss of control” issue is not only a matter of technologies but also of awareness, transparency, regulation, contractual agreements between providers and governmental customers.

For example, from a theoretical point of view, when a governmental institution puts data and applications in the Cloud it still remains the owner but, the lack of transparency of the Cloud provider procedures (e.g. standard procedures for data disruption), the lack of common contractual clauses and of an EU regulation, still leaves doubts on the Cloud provider potential to access and ability to manipulate customers data. Another aspect of “loss of control” is the vendor lock-in problem i.e. what is the mitigation action for bankruptcy of the Cloud provider cases. Concerning vendor lock-in, from a technical point of view, without cost and time constraints, it should always be possible to migrate data and applications from one Cloud provider to another. All these provisions need to be agreed and declared in the services contract.

Actions

EC and MS competent authorities in cooperation with Cloud providers and government customers should closely work to mitigate “loss of control” addressing the issues of governance, monitoring and auditing, vendor lock-in and data handling. Required steps are:

- **Definition of a monitoring framework for Gov-Cloud public service layers.** This monitoring framework should allow central and local government to oversee the Gov-Cloud platform (operated by the CSP) running their eGovernment services. The monitoring framework, provided itself as a Cloud service, should allow the proper view of the system, depending on the service level used to implement the eGovernment services, i.e. IaaS, PaaS or SaaS. This monitoring framework could become, in some cases, an alternative to auditing practices that are discouraged by providers.
- **Definition of standard procedures for data handling.** The standard procedures for data handling should clearly define what are the access policies on data and applications for the different service levels, how data are physically (or virtually) handled during the contract and after a contract resolution.
- **Definition of standard procedures for data and service migration.** The standard procedures should clearly define the process behind the migration of services and data and the role of the provider and of the customer in this process.

5.4 Recommendation 4: a regulatory framework to address the “locality problem”

Cloud providers usually store data in their datacentres which can be located in many different countries. The possibility to locate data and resources outside the country is often perceived as a

barrier for gov-Cloud adoption rather than an advantage for data privacy issues. The definition of regulatory framework for data location can reduce the risks of objections from the governmental users, but the most critical concern for data protection is to ensure the security of data more than location of data. To achieve this, technical solutions (as for example, the use of encryption) are also indicated as appropriate (see Recommendation 6). However, it is not only about taking technical measures. Often local jurisdiction simply forbids that data owned by Government is located abroad. Second, it is not only about location, but also about under which legal framework the Cloud provider falls.

However it is important to note that it will be difficult and cost prohibitive for smaller countries to be able to establish their own datacentres, we well as back-up centres. The regulatory framework should take this into account and offer solutions to overcome it.

Actions

The definition of a new framework requires that EC and MS competent authorities in cooperation with Cloud providers and government customers to work closely on the following topics:

- Definition of measures to improve the awareness of government agencies and Cloud service providers on existing EU legislation on the subject;
- Foster the development of technological solutions compliant with the existing legislation;
- Categorization of specific governmental institution requirements on data ownership and data privacy judged by the type of data handled;
- Enhancement of the existing EU legislation on data and resource ownership with a focus outsourcing;
- Enhancement of the existing EU legislation on data privacy with a focus on outsourcing.

5.5 Recommendation 5: governmental Cloud solutions compliant to EU and national law

To soften the scepticism of governmental institutions of the technological solution proposed by service providers, measures should be promoted to encourage the development of systems and services that are compliant with EU regulation and specific country legislation.

Actions

EC and MS competent authorities in cooperation with Cloud providers, governmental bodies, standardisation bodies and R&D sector should closely work to promote the development of technological solutions compliant to EU and national regulation.

Needed steps could be to:

- Setup of an accreditation(certification) framework to certify or guarantee that each Cloud solution is compliant with the relevant legislation (national and/or EU law) – specific recommendation 8;
- Promote the definition of standard contracts including regulatory compliance;
- Promote the awareness of EU and country regulation;
- Promote Cloud trainings and education on Cloud topics for EU governments.

5.6 Recommendation 6: a common framework for SLAs

The development of a common framework for standard service level agreements is largely debated in the community. Survey results suggest (from a governmental customer's point of view) additional clauses: allowing penetration tests (about 60% of respondents to our survey), obligatory incident reporting (about 65% of respondents to our survey) and the right to conduct auditing to the Cloud provider (about 75% of respondents to our survey).

A common framework for SLAs should be a measure to boost the take-up of gov-Clouds. Having a SLA framework will overthrow the difficulties government agencies could find in the definition of contracts and the scepticism to public Cloud solutions. This work has been initiated in the EU Cloud Strategy and ENISA has a supportive role.

Actions

- Assurances and guarantees linked to the public organizations by the Cloud providers to support security and privacy claims should be verified and assessed through the specific penetration tests and with the introduction of auditing activities possibly through independent third parties. Customers can leverage the attestations/reviews by 3rd party auditors to avoid duplication.
- The incident response and reporting obligation should be enforced in the contract with the aims to push the providers to respond promptly to incidents, to report the ones that deem critical and affect the availability of the services to the appropriate authorities and/or the public users and to recover rapidly from the faults or the attacks.
- The incident response and reporting is especially needed in the context of public services of some level of criticality for the type of services or the sensitivity of the data. For those cases, it should be helpful to differentiate the SLAs in terms of timelines of the response and the reporting.
- Penalties in case of service level constraints violation should be included in the contract. It might be worth considering the creation of a reputation system (if not an entirely voluntary accreditation scheme) that is used to inform of past violations to contracts of a similar service or against similar standardised classifications.

5.7 Recommendation 7: Security measures for governmental Cloud

To define standard approach and procedures for the security certification of the services and/or the providers. To ensure security for the public institutions, a maturity model must be developed; consisting of sophistication levels that Cloud providers have to adapt via a certification scheme and by defining clearly the requirements of each level of security. The accreditation model of the Cloud services can be done by a dedicated central actor. The public users and providers should be free to choose the level of security provided and requested for the public services, with positive effects on the competition between providers and leaving the departments the possibility for implement the most effective and the best value for money solutions. A set of security measures is the next step after a risk assessment that should take place before deploying Cloud services. A specific set of security measures focussed on governmental Cloud deployment would be the way to improve trustworthiness in the Cloud supply chain.

Actions

Suggested actions to enhance the security and protection of information for the governmental Cloud services are:

- Support pre-assessment process before procuring services;
- Create a set of baseline security measures focussed on governmental Clouds; for this reason the measures should include domains like security management, identity management, data redundancy, services availability etc;
- Include risk impact levels in each domain in order to offer a sophistication/maturity model;
- Enable voluntary auditing (and/or certification) framework of information security measures
- Foster security labelling systems.

5.8 Recommendation 8: Certification framework

While considering a public-private management framework, 87% of respondents declared they require the certification of the providers participating in public tender for governmental Cloud services. The problem is when considering the public-public management framework because certifications within the public institutions are not widely diffused. The governmental institutions prefer to be compliant to standards without the need to be certified by an external auditor. Currently the European Commission, under the EU Cloud Strategy, has launched the activities supporting certification in the Cloud and more specifically creating one metaframework for all providers to be accredited against. ENISA, is part of the selected industry group in charge of this action, and fully supports the EC. This work has been initiated in the EU Cloud Strategy and ENISA has a supportive role.

Actions

- Moving towards the certification of gov-Cloud platform and services is a debated and difficult process. The main driver to accomplish the goal can be to include this obligation in an EU regulatory framework or a pan European voluntary certification scheme.
- Consider leveraging global, industry led standards, as well as exploring government requirements in other countries.
- Support the creation of national “pre-assured Cloud products/applications and service catalogues”. This approach reduces the cost of the service to be assured many times introducing the “assure once- deploy many times” model.
- This action can be combined with the previous recommendation on the security measures, creating a pan European accreditation system for all providers that would like to offer Cloud services to the public sector. A metaframework on information security domains, including security controls per domain, classified in sophistication levels is a good starting point.

5.9 Recommendation 9: Foster research on governmental Cloud security.

To support the evolution of Cloud technologies compliant with government requirements it is important to foster research on gov-Cloud computing leveraging existing research programmes. Research should be oriented improve the risk-impact level of Cloud solution for governmental services.

EC and the MSs R&D competent authorities in cooperation with academia, Cloud providers should assure that existing and future national and European research programmes, such as Horizon 2020, will incorporate into their work programmes research lines on gov-Cloud computing security aspects. Some of these research lines (non-exhaustive list) are:

- Cloud service life cycle management;

- Cloud supply chain control;
- Incident management;
- Cyber risk analysis;
- Cyber threat modeling;
- Encryption;
- Data protection;
- Cloud privacy and security metric;
- Privacy level agreement;
- Data protection accountability and transparency;
- Information assurance in Cloud systems.

Actions

EC and MS competent authorities in cooperation with Cloud providers, government customers, R&D sector and academia should undertake the following actions:

- Establish priorities for the different research objectives;
- Make contact with existing security programmes at EU and National levels, such as Horizon 2020;
- Work together with appropriate organisations and bodies (e.g. Framework Programme Committee and Advisory Groups, Technology Platforms, etc.) to define an appropriate Work Programme.

5.10 Recommendation 10: Privacy enforcement

Data protection is a vital aspect when we talk about governmental Clouds due to the sensitivity of the information processed. The EC and MS should ensure Cloud services compliance with the EU data protection laws. To guarantee privacy in the Cloud services encryption by the Cloud provider and authenticated access by the users seems to be a straightforward solution. However the implementation of cryptographic solutions in Cloud services still remains in low maturity level.

Actions

Data protection enforcement techniques have become a core issue; access control and cryptographic techniques may provide part of the solution:

- A clearly expressed and up-to-date policy about the management of personal information by the agency, including information about likely disclosures to overseas recipients should be considered;
- In public Clouds usage of cryptographic solutions should be considered;
- In IaaS and PaaS, as well as in private Clouds, cryptography doesn't promote privacy guarantees. In the private Cloud data security should be assured by other means like access control, than cryptographic techniques;
- In SaaS provisioning, the provider should include cryptographic solutions to the contractual agreement with the customer by default and not upon request;
- When privacy is explicitly required in IaaS and PaaS, alternative solutions to the IaaS or PaaS provider offering cryptographic functions need to be considered. These may include the government service encrypting data prior to their storage in the Cloud or the use of cryptographic services (such as key management servers, access policy for the servers) that are hosted and managed by a 3rd party (preferably a government department or a trusted



security service provider) that enable controlling and attesting the enforcement of cryptographic operations on the IaaS and PaaS environment.

6 Conclusions and next steps

This study has presented the Cloud computing status of a majority of European countries, giving the initial impressions on how the European landscape is currently on the matter. The first conclusions are evident: the Cloud uptake in Europe is not accelerated as expected in the European countries; in this project, by investigating on the governmental Cloud uptake in the European countries, we identified several issues that still need to be solved to give a boost to the public sector to adopt:

- Lack of a concrete and unanimous definition of governmental Clouds;
- The Cloud uptake in national level is slow due to lack of national Cloud strategies, privacy and security constraints, lack of legal and contractual frameworks and relative immaturity of the Cloud market;
- Research needs to be promoted since many areas are still “undiscovered”.

Due to great diversity of Cloud solutions and the different approaches, it is difficult to reach a consensus on fundamental aspects of Cloud security such as: common Cloud contract clauses, common Cloud services model etc. In a relatively new environment with great deal of competitiveness, getting all the big players together in a room and decide upon a baseline of common requirements and models is a “mission impossible”.

This study is addressed to both the EC and the Member States. On the one hand the Member States now are aware of the status of Cloud services implementation across the EU; knowledge can work as an accelerator to the elaboration and implementation of a national Cloud strategy. The use cases presented, demonstrate best practices on how to implement the provisions (or not) of a national Cloud strategy according to the target outcome. The goal is to foster an information sharing mentality between the respective parties across the EU, share the good practices and lesson learnt and pave the way for a common set of security requirements for all Member States.

On the other hand, as indicated by the recommendations made in this study, the EC can play a very important role in leading this kind of initiatives, bringing all the related parties (in collaboration with the public and private sector) together to decide upon a common Cloud roadmap for Europe.

Taking into account the recommendations of this report, ENISA will continue to support all these actions, by providing advice and recommendations to the Member States and competent authorities. We will continue working on the topic of governmental Clouds deployment, scanning Europe to investigate the Cloud uptake by the public sector, working on public procurement requirements and issuing recommendations on how to design and implement a national Cloud strategy. ENISA will also support the development of a pan European security certification metaframework, working closely with the EC.



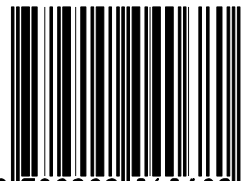
ENISA

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

ISBN 978-92-9204-068-0



9 789292 040680

doi: 10.2824/25181



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