Project Acronym: STORM CLOUDS

Grant Agreement number: 621089

Project Title: STORM CLOUDS – Surfing Towards the Opportunity of Real Migration to CLOUD-based public Services

Deliverable 5.1.1

Body of Knowledge about the Migration of Public Services into the Cloud

Work Package: WP5
Version: 0.5
Date: 15/10/2015
Status: WP leader accepted
Nature: Other
Dissemination Level: PUBLIC

Editor: Kakderi Christina (AUTH-URENIO)

Authors: Kakderi Christina (AUTH-URENIO), Panagiotis Tsarchopoulos (AUTH-URENIO), Dimitris Simitopoulos (THESSALONIKI)

Reviewed by: Agustin Gonzales Quel (ASI)

Version Control

Modified by	Date	Version	Comments
Kakderi Christina	30/09/2015	0.1	1st version. First part on body of knowledge
Panagiotis Tsarchopoulos, Dimitris Simitopoulos	16/10/2015	0.2	Added second part
Kakderi Christina	20/10/2015	0.3	Ready for review
Kakderi Christina, Agustin Gonzales Quel	27/10/2015	0.4	Incorporate comments of the reviewer
Panagiotis Tsarchopoulos	20/12/2015	0.5	Include ethics and security section

Executive Summary

Surfing Towards the Opportunity of Real Migration to Cloud-based public Services (STORM CLOUDS) is a project partially funded by the European Commission within the 7th Framework Program in the context of the CIP project (Grant Agreement No. 621089).

The project aims to define useful guidelines on how to address the process of moving towards a cloud-based solution for Public Authorities and policy makers. These guidelines will be prepared based on direct experimentation in at least 4 European cities, creating a set of relevant use cases and best practices.

Work Package 5 (WP5) of the STORM CLOUDS project aims to create a reference guide for Public Authorities to facilitate them as they plan, determine effort and budget, select the appropriate services, make the required internal organisational changes and finally execute the migration into cloud.

The aim of this first iterative deliverable is to create a body of knowledge about migration of public services into the cloud. This body of knowledge will be built from the various sources:

- Knowledge gained from partners during the execution of previous WPs.
- Feedback from citizens and public servants related to use and operation of cloud-based public services.
- Input for web tools monitoring the cloud-based infrastructure.
- Literature review

As this is an iterative deliverable, it will be continuously updated until the end of the project, when an integrated deliverable will produced.

Table of Contents

List of Figures

List of Tables

Abbreviations

Acronym	Description
AaaS	Architecture as a Service
CaaS	Communications as a Service
CSR	Certificate Signing Request
DILA	Directorate of Legal and Administrative Information
EC	European Commission
ECP	European Cloud Partnership
ECPSB	European Cloud Partnership Steering Board
EU	European Union
FCCI	Federal Cloud Computing Initiative
GDP	Gross Domestic Product
GUI	Graphical User Interface
IaaS	Infrastructure as a Service
ICT	Information and Communication Technologies
IoT	Internet of Things
IT	Information Technologies
PaaS	Platform as a Service
RFID	Radio Frequency Identification
SaaS	Software as a Service
SCP	STORM CLOUDS Platform
SFTP	Secure File Transfer Protocol
SMEs	Small and Medium-sized Enterprises
SMTP	Simple Mail Transfer Protocol
SNI	Server Name Indication
SSH	Secure Shell
SSL	Secure Sockets Layer
VM	Virtual Machine

1 Introduction

Over the last years we notice an abundancy of publications on cloud computing; from government reports to corporate studies, all these show the significant benefits of cloud computing and the opportunities behind the migration of public services into the cloud. This deliverable aims to organise this abundancy of information and to provide an overall picture on cloud computing, giving emphasis on the new role and most importantly on the challenges that public authorities will have to face. More specifically, the main objectives of this deliverable include: the identification of solutions and best practices on how to address key challenges that relate to migration of public services into the cloud.

The report is structured in two main parts. The first part provides a review of the literature and the main reports on the adoption of cloud computing by the public sector. It starts with an introductory part which provides the background on cloud computing, gives some preliminary definitions and presents the main initiatives taken on the specific field. It continues with a section providing a review of the main deployment models and migration strategies of public administrations, followed by a section focusing on the identification of the main benefits and barriers for cloudification. The first part of the deliverable concludes with a summary of the main recommendations set by different organizations to public authorities regarding the migration of their services into the cloud.

The second part aims to reflect the experience gained from STORM Clouds project, especially with regards to the pilot activities in the four cities. It provides a list of problems that have been encountered during the migration of public services into the cloud along with the preferred solutions. Details on such problems have been collected from the list of deliverables prepared so far in the first half of project duration, but also from a short questionnaire distributed to the public servants (addressed both to technical and management staff) of the Municipalities in the three pilot cities regarding the use and operation of public services into the cloud.

2 Cloud Computing Fundamentals

2.1 State of play and background

An introduction to cloud computing

Cloud computing has received great attention during the last decade as an emerging paradigm beyond a simple computing system structure (Seo et al., 2014). In simplified terms, it can be understood as the possibility to store, process and use data on remotely located computers accessed over the internet (EC, 2012). It is an all-inclusive solution (Mahmood, 2015) based on the concepts of converged infrastructure, shared services/resources and dynamic reallocation based on demand. Cloud computing has the potential to bring significant benefits to its users (citizens, businesses, government) such as cost savings, increased efficiency, user-friendliness, accelerated innovation (ECPSB, 2014).

> **What is Cloud Computing?**
>
> "Cloud computing is a model for enabling ubiquitous, 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" (Mell and Grance, 2011).

Cloud computing as a technology, has now reached a certain level of maturity allowing for full commercial exploitation. It is estimated that, with the right policy framework, the cloud economy can generate nearly 1 trillion GDP and 4 million jobs by 2020 in Europe (IDC, 2012). A KPMG study for Australia, shows that the increase adoption of cloud computing in the country would lead to a growth of annual GDP by $3.3 till 2020. At the global level, IDC estimates that it can create $1.1 trillion of business revenues per year.

Cloud computing is a disruptive innovation that is expected to bring a new wave of benefits over the coming years. Apart from being a catalyst in terms of technology, enabling for flexible, responsive and customer centric IT services (KPMG, 2014), it is also expected to create new business models and ways of collaboration allowing SMEs, but also non IT companies and organizations to capitalize on the cloud (Hobson, 2014). Cloud computing divides the role of service providers into two: the infrastructure provider, who manages a cloud platform and leases resources according to a usage-based pricing model, and the service provider who rents such resources to serve the end-users (Zhang et al., 2010).

Why is this relevant to public authorities?

Cloud computing has nowadays gained significant attention, especially in the case of large organisations having IT departments with a high level of complexity which have to devote the

majority of time and budget to merely keep existing systems operating. The challenge brings at the centre of the interest public authorities, due to their size and scope of services. Most public sector organisations are very complex in nature with many entities (departments, agencies etc.) sharing large volumes of data, but also having rigid organizational structure and significant funding restrictions in terms of innovation. They also encompass services in diverse business and technological domains, which are often based on monolithic architecture models, disconnected from each other and difficult to be re-used (EC, 2014).

During the last few years, we notice a transformation of the dynamics between the public sector and the users of public services (Manzor, 2015). As now many public authorities are seeking new routes to improve their service quality and delivery, transparency, responsiveness as well as the effectiveness of their investments, there is an increasing interest on cloud computing. Cloud computing can be generally defined as a large-scale distributed computing paradigm in which a pool of computing resources is available to cloud consumers via the internet (Seo et al., 2014). In the case of public services the concept of cloud computing is not only relevant due to its significant benefits, such as coherence, flexibility and economies of scale; it is also linked to the idea of open, connected and re-usable public services (EC, 2014). According to Deloitte (2014) the more 'fundamental services'[1] available on the cloud, the higher the opportunity to reuse and combine them with existing services of other governmental departments or to develop new services in collaboration with third parties.

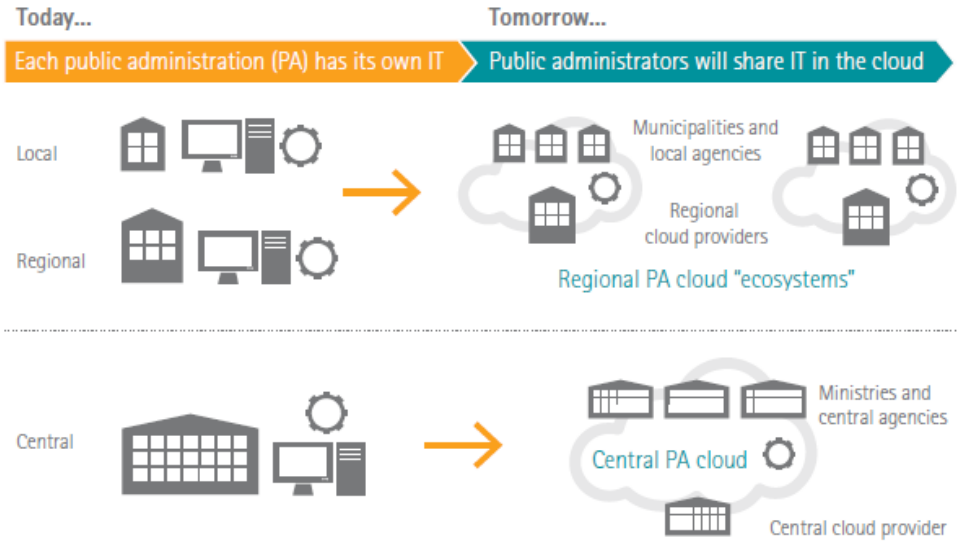


Figure 1: How IT governance looks at the moment and how it will look in the cloud.

[1] By 'Fundamental Service' the study means a basic public service that is autonomous and that is provided by a single responsible role, and receives as input only the output from Basic Data Services, documents or objects produced by citizens, businesses or public administrations (Deloitte, 2014).

Source: Accenture (2013)

It has been expressed that the impact of cloud computing will not reach its full potential unless it is adopted both by enterprises and by public authorities. Yet, governments, have to find ways to leverage these new advances in technology while meeting challenges related to the access, storage and use of data, adhering to standards of compliance and security. Due to these limitations, the degree of cloud adoption by the public sector varies significantly across the globe (Manzoor, 2015).

Why smart cities need cloud computing?

City governments and municipalities everywhere constitute for one thing complex public organisations which have more reasons to invest in cloud computing than any other public organisation. It is widely accepted that increasing urbanisation strains the limited resources of cities and affects its resilience, while at the same time, it highlights the significance of sustainable urban development, especially in terms of more efficient management of natural resources, such as energy and water, as well as of better planning and collaborative decision making (Khan et al., 2015). In this context, cloud computing can play a significant role facilitating cities in meeting the abovementioned tasks.

First of all, smart cities have to use a wide variety of ICT solutions to deal with urban problems and monitor their functions; they do not only require the use of new technologies and devices (sensors, RFID devices, smartphones, smart household appliances etc) to collect land use, transport, census, and environmental monitoring data which are generated every minute in the urban environment, but also the capacity to manage and process all this large scale data (Big data) in real time, in an interconnected and service/applications' specific way (Mitten et al., 2012). The emergence of cloud computing paradigm facilitates big data storage and big data integration, visualisation, processing and analysis in acceptable time frames. Cloud based big data mining and analytic tools can deal effectively with multi-disciplinary city data – coming from highly distributed, heterogenous, decentralised, real and virtual devices and data sources – and formulate a variety of smart city application scenarios (Khan et al., 2015; Suciu et al., 2013).

In terms of service provision, smart city services are typically delivered through domain-specific, tightly coupled systems, which entail limited scalability and extensibility. However, cities on limited budgets require a new methodology for service delivery; they should aim for open and scalable services, provided through cloud based and domain-independent service-delivery platforms (Dustdar et al., 2014). These constitute a type of Platform as a Service (PaaS) offering, which integrates and processes real time data from IoT and other data sources, and allows domain specific applications to employ both IoT and cloud resources on demand. Such platforms also benefit solution providers (including IT corporates, research institutions, cloud service providers etc.) which can forge alliances between real-time data sources and city applications and make profit by offering the same sophisticated services to other cities or organisations (Jander, 2014). This means that application developers do not need to worry on device maintenance or data acquisition; they can simply focus on the application logic and make on-demand use of the cloud

and the IoT resources. It also allows them to configure flexible usage models and billing schemes, giving the opportunity to other cities with relatively limited budgets make use of these services.

In the same line of reasoning, smart buildings which constitute the core of smart cities, also need to rely on enterprise scalable cloud architecture so that they can benefit from functions such as stream analytics, machine learning, Hadoop, Spark etc. (ADITI, 2015). Technologies in place today enable designers to integrate technical specification data about the materials, systems and equipment to yield greater efficiencies in terms of energy performance and better management throughout a buildings lifetime. Just as any other aspect of a city, in order to manage buildings efficiently one has to meter its sub-systems such as lighting, electrical, mechanical, security etc. in an instrumented and unifying way. Also, monitoring and management has to be on an aggregate level, for a group of buildings and across neighbourhoods. This requires the ability to access, collect and analyse a large volume of mostly private data, which can be done by cloud computing in a more efficient and cost-effective way than traditionally dedicated computing solutions (Microsoft, 2011).

Finally, cities with continuously rising population, feel significant pressures to become sustainable and energy efficient. Cloud computing opens up new possibilities for sustainable solutions; it is not only the cloud's economies of scale which contribute to economic and environmental sustainability, it is also the fact that sustainability of future cities is mainly based on their ability to manage increasingly large and complex data (on the environment, waste, water usage etc.), a task that can be performed more effectively though the cloud. According to a study from Accenture and WSP (2010), a shared cloud service can help in reducing energy use and carbon emissions by 30-90 percent (according to the size of each deployment) compared to on-premise services.

Examples for cloud based smart city solutions constantly emerge through alliances among IT companies, consultancy firms and municipalities, such as the following:

- The cloud-based smart city platform (SOFIA2) developed by Indra, Altia, Ilux and R and implemented in Coruna, Spain. It is a solution which facilitates the interoperability of multiple systems and devices, offering a semantic platform that enables making information about the real world available to intelligent applications (Internet of Things), with an open source and multi-language focus. The InCloud version of SOFIA2 will enable the 15 planned pilots connect to the infrastructure from the onset in order to integrate their solutions.
- The cloud-based smart city solutions offered by Cisco and Switzerland's AGT analytics combining on the one hand, intelligent networking, virtualised computing and video management software from Cisco, and on the other, a state-of the art smart city software platform, sensor gateway and analytics from AGT. The alliance aims to bring a holistic view of urban ecosystems and will enable cities to deal with current and future urban challenges (Cisco, 2014).

- A project called ClouT[2], for instance, a joint European-Japanese project, funded by the European Commission and the National Institute of Information and Communications Technology of Japan. The Project leverages Cloud Computing as an enabler to bridge the Internet of Things with Internet of People via Internet of Services, in order to establish an efficient communication and collaboration platform that will help make cities smarter and allow them face the emerging challenges such as efficient energy management, economic growth and development.

What are the current initiatives and emerging trends with regards to public sector cloud adoption in different countries?

As part of these technological developments and the expansion of the information society market, but also due to the need for an exit strategy in response to economic recession, multinational companies are investing in cloud computing on a large scale, while countries are politically encouraging cloud computing (Seo et al., 2014). Over the last years, the United States of America, the European Union, the United Kingdom, Australia, Japan, China and so on, quickly undertake actions with regards to policies and services on cloud computing, although most of them are driven by the need to reduce costs and move towards a digital environment (Accenture, 2015).

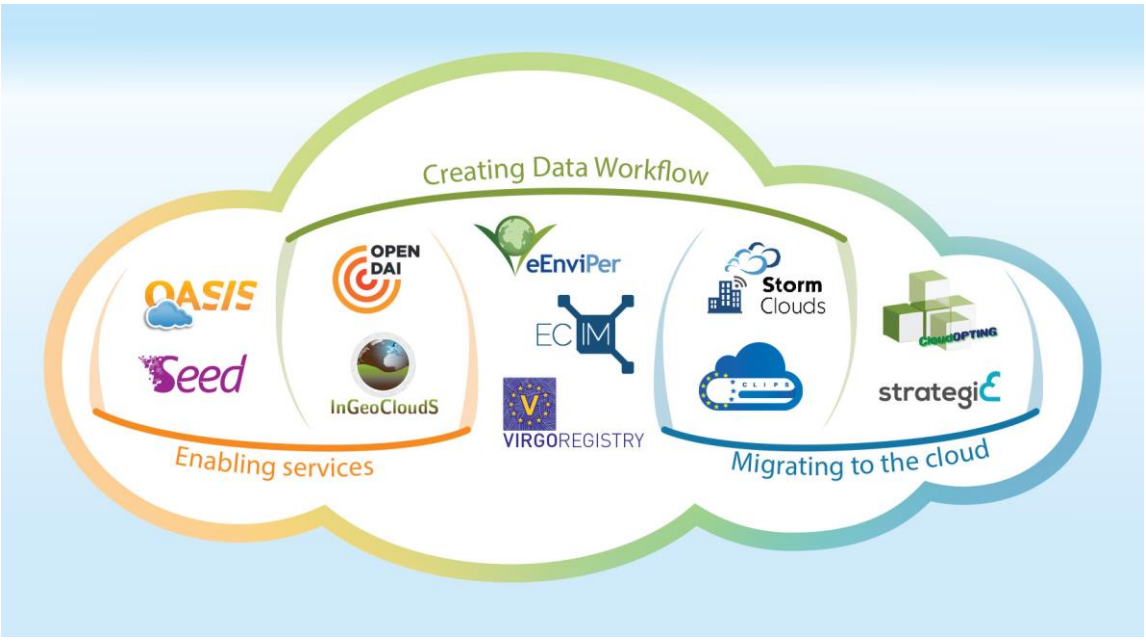
More specifically, the United States inaugurated in 2009 the Federal Cloud Computing Initiative (FCCI) as part of the IT-based integration of federal governments and public institutions, while a year later released a '25 point implementation plan to reform Federal Information Technology Management' which included a 'cloud first' policy shift of all federal agencies. The policy was intended to be implemented within the framework of the 'Federal Cloud Computing Strategy' which was published in 2011 (Kundra, 2011). Since the FCCI, a number of other supporting and complementary government initiatives and programmes appeared (e.g. TechStat, Apps.gov, PortfolioStat, Standards Acceleration to Jumpstart Adoption of Cloud Computing, CIO Council Executive Cloud Computing Steering Committee etc.) forming an integrated effort for cloud computing adoption by the US government (Figliola and Fischer, 2015).

In a 2014 report (GAO, 2014) on the process of this strategy, it was found that since 2012 federal agencies increased their IT budgets allocated to cloud services only by 1%, while they reported cost savings of about $96 million. A survey conducted by InformationWeek during the same period, reported that only 44% of 153 federal agencies have mature data governance practices in the cloud, only a third of them have complied with the Federal Risk and Authorisation Management Program, as well as that 56% of them are implementing data stewardship or a more formal data governance program for cloud computing (Figliola and Fischer, 2015).

[2] http://clout-project.eu/

The Australian Government following the release of the 'Cloud Computing Strategic Direction Paper' (Australian Government, 2011), announced that it would develop a National Cloud Computing Strategy, recognising the synergies between the National Broadband Network and cloud computing, but also the importance of cloud computing in achieving greater efficiency in government, greater value from ICT investments and better service delivery in a more agile public sector (Australian Government, 2013). Especially in the case of government agencies, the Australian Government in its report 'Government Cloud Computing Policy' (Australian Government, 2014) offers recommendations in procuring and using cloud services.

Japan is simultaneously promoting two strategies: the 'Kasumigaseki project' for the central government departments and the 'local government cloud' for local governments (Seo et al. 2014). Hong Kong's Government IT Strategy for 2011 focuses on cloud computing, while South Korea's Communication Commission allocated about $500 million for the development of Korean Cloud Computing facilities (Chandrasekaran and Kapoor, 2011).



Europe, on the other hand, despite the initiatives of various member states (such as G-Cloud in the UK, Trusted Cloud in Germany, and Andromede in France) is lagging behind in the take up of cloud computing (Bonneau et al., 2013a; ECPSB, 2014) mainly due to lack of regulatory consistency and to technologically conservative policies. The European Commission has recognized the need for rapid adoption of cloud computing in all sectors of the economy and has therefore set as a priority the development of a wide European single market for cloud services. In 2012, the Commission has released a strategy for 'Unleashing the Potential of Cloud Computing in Europe' (EC, 2012) which is based on three key actions:

- *Cutting through the jungle of standards*, referring to the need for certification of cloud services and the endorsement of such certificates by independent regulatory authorities. Standardisation is crucial for the potential of lock-in, especially in the case of SMEs and non IT companies which are rarely able to evaluate a product's/service's characteristics as to the level of interoperability, data portability and reversibility.
- *Safe and fair contract terms and conditions*, tackling the complex and uncertain legal framework for cloud service providers. The Commission thinks that the development of

model contract terms for cloud computing (both between cloud providers and professional cloud users and with regards to consumers and small firms) will increase trust, while improving existing legislation (such as the proposed Regulation on personal Data Protection and the Common European Sales law) will accelerate the take up of cloud computing in Europe

- *Promoting common Public Sector Leadership through a European Cloud Partnership* (ECP) as an umbrella for comparable initiatives at Member State level building common procurement requirements for cloud computing in an open and fully transparent way.

According to the Steering Board of the European Cloud Partnership the adoption of cloud in Europe is being currently impeded by different legal, technical, operational and economic barriers which arise depending on the case. In order to address these problems it proposes a) the creation of a common framework of best practices (legal and operational guidelines, technical standards etc.) which can be voluntarily adopted by cloud service providers and b) building of a wider consensus among public authorities, citizens, stakeholders and the cloud industry on the needs of specific case studies and on appropriate solutions (privacy and security requirements, legislative reform, enforcement methods etc.) (ECPSB, 2014).

At the member states level, governments are taking steps to facilitate implementation and reduce potential barriers. In the United Kingdom, the G-Cloud, as part of the Digital Britain Strategy, G-Cloud consists of 10 detailed strategies focusing on cost reduction, through the migration of common tasks into SaaS, integrated purchasing over infrastructure, integration of information resources of public data centers and the establishment of cloud computing markets offering services to governmental agencies (Seo et al., 2014). The Netherlands have adopted a Cloud Strategy for the Central Government, giving emphasis on infrastructures and rules for the implementation (Bonneau et al., 2013a). In France, the Directorate of Legal and Administrative Information (DILA) adopted a private cloud approach for the delivery of services to citizens and the public sector.

Finally, apart from the efforts made at the national and EU level in terms of legislation and standardisation, the last years we see a growing number of programmes, initiatives and joint efforts towards the adoption of cloud computing, such as the following:

- **Eurocloud** (www.eurocloud.org), an independent non-profit organisation acting as a pan-European hub, working towards the maintenance of a constant open dialogue and the sharing of knowledge between cloud computing customers and providers, start-ups and research centers.
- **Cloud28+** (https://cloud28plus.eu) a European-based community aimed at increasing the visibility and revenue of its members and accelerating adoption of cloud technologies through the creation of a cloud service catalogue, with a strong focus on compliance with the European rules on data privacy and security

Despite the abovementioned initiatives, the public sector has been slightly wary of cloud adoption compared to the growth of cloud computing in enterprises. Strategic actions and policies taken at the individual country level, have not proven to be adequate to address security, privacy and regulatory issues.

2.2 Benefits and barriers towards cloudification

Benefits of cloud computing in the public sector

Cloud computing characteristics (Apptis, 2010; Zhang et al., 2010; Accenture, 2013; Mell and Grance, 2011) bring significant benefits to all types of organisations such as higher efficiency and effectiveness, as well as the ability for innovation. The main impact of cloud computing in service delivery is that it reduces the need for resources (cost, time), enables the provision of more integrated and user centric services and facilitates the development of innovative services (Deloitte, 2011).

Cloud Computing Characteristics

- **On demand self-service/High scalability**: Cloud Computing enables the access of computer services on a pay-as-you-go basis, with the flexibility to scale up or down quickly and for little marginal cost.
- **Resource pooling:** The resources provided from a cloud provider may be pooled to serve multiple organisations using a multi-tenant model. Dynamically assigned and reassigned physical and virtual resources according to an organisations' self-service demand, can provide significant economies of scale which help reduce costs and accelerate innovation.
- **Rapid elasticity:** The service provider's capabilities (e.g. memory space, calculation power etc.) can be elastically provisioned and released, based on demand. A change of configuration is also possible with a short reaction time by the provider.
- **Device agnostic**: Users can access cloud services over a network through a broad range of devices.
- **Broad network access:** The service provider's capabilities are available over the network and can be accessed through standard mechanisms which promote use by heterogeneous client platforms and other services.
- **Metering**: Cloud usage is monitored, controlled and reported so that users can measure their consumption quickly and easily and adjust accordingly.

Just as in the case of a private organisation, cloud computing can also offer attractive advantages to the public sector. Mahmood (2015, xvii) has summarised the benefits of cloud computing adoption in the public sector by grouping them in two categories: the ones that address to public organisations and the ones that address to citizens. More specifically, governments can have 'better business process management; cost and time savings; more accurate and timely information; automation and process improvement; easy maintenance and upgrading of services; and seamless collaboration, vertically and horizontally, with other governmental departments'. Citizens, on the other hand, have easy-to-use and on demand access to government e-services;

online transactions e.g. payment of bills and filing tax returns; information reliability and ready availability of services around the clock; more accurate and timely information; opportunities for e-participation including e-voting; and citizen oriented decision making by the political leadership'.

According to a study from Accenture (2013), governments may move into the cloud each one trying to leverage different advantages. The study, identified three main approaches: a) cutters, such as UK, France, Italy and Ireland, trying to reduce expenditures, b) builders, such as Russia and other Central EU countries, trying to build their infrastructures and c) enhancers, such as Belgium and the Nordic countries, trying to use digital technologies to encourage citizens to engage with government.

Cloud computing can help in many ways public administrations shift from responsive entities towards value driven service providers. The value proposition of cloud computing in the public sector, involves cost reduction, agility, high transparency and much more, which are described analytically below (Chandrasekaran and Kapoor, 2011):

- **Cost reduction of IT spending:** With cloud computing, public organisations can create a central pool of shared resources, securing at the same time, increased efficiency of infrastructure. The primary savings are created from datacentre consolidation, aggregation of demand and multi tenancy.
- **Higher agility:** It refers to the ability of an organisation to adapt rapidly and cost efficiently to changes in its environment. Public authorities usually operate in a strictly hierarchical manner, in which any type of service provision is a time consuming activity. Cloud computing can help public administrations accelerate operational execution of projects with limited cost as well as to adapt quickly to new policies or operating requirements.

Figure 2: Business agility for the public sector

Source: vmware (2011)

- **Elimination of Procurement and IT infrastructure maintenance:** The characteristics of high scalability, elasticity and resource pooling eliminates the need to procure, monitor and

maintain IT resources. This has a significant effect in reducing the workload and the need for IT staff, allowing public agencies to focus on their core responsibilities.

- **Access to new technologies:** Cloud computing provides the opportunity to public organisations to access at all times the most updated software and hardware at a very low cost.
- **Universal resource access:** Cloud computing enables universal access to resources while it helps in establishing common platforms for service provision, which are also accessible by the citizens.
- **Flexibility:** Cloud computing allows different governmental departments and organisations to change service providers without lengthy procurement processes avoiding 'lock-in' contracts (Bonneau et al., 2013b).

Challenges for public administrations

Despite the significant benefits described above, there are a number of reasons cloud adoption is not occurring more rapidly in the public sector. Many challenges relate to its newness and the relative underdevelopment of the marketplace for cloud services (Craig et al., 2009). The most common concerns are related to security and data protection; these challenges are also raised by the private sector, with different though weight.

Challenges related to cloud computing

- **Data security:** It refers to the protection of cloud-stored data from unauthorized access, modification, disclosure or destruction (Mustonen, 2011). Typically, service providers do not have access to the physical security system of data centers or can only specify the security settings remotely, they must rely on the infrastructure provider. Due to the sensitive nature of public sector information, storing of data on the internet or by a third party is generally being avoided, especially when there are differences in the regulatory requirements among countries.
- **Privacy:** It refers to the access and use of private information without the user's awareness. Still there are significant variations in the privacy laws among countries which creates a problems especially with cross border data localisation.
- **Portability and interoperability**: it refers to the ability to move data and/or services from one provider to another, or bring it entirely back in house avoiding vendor or technology lock-in.
- **Performance and bandwidth costs**: It refers to the potential high cost for data intensive applications.

Apart from the above, there are also some organisational challenges that public authorities have to consider before moving their services to the cloud. The fist is related to **lack of flexibility in public procurement**. Public authorities can use their procurement weight in order to promote the development and uptake of cloud computing based on open technologies and secure platforms (EC, 2012). However, IT budgets in the public sector are usually planned in advance, allowing little flexibility for last minute changes. The second refers to the **lack of uniformity in standards** across nations. Contrasting rules on privacy, security, storage and accessibility creates difficulties for cloud providers to deliver on the full promise of the information technology (West, 2010). Finally, there are some **cultural problems** which emerge from the fact that different organisations – or departments within the same organisation – are not used to collaborate or share solutions with each other.

A GAO report on cloud adoption by US federal agencies (GAO, 2014) identified five main challenges towards the transition to cloud computing: 1) vendors have difficulties in meeting federal security requirements as these are continuously updated to address new threats and vulnerabilities, 2) overcoming cultural barriers within agencies while shifting to new business models, 3) meeting new network infrastructure requirements since existing networks are often inadequate to meet new needs, 4) having appropriate expertise for acquisition processes and 5) lack of funding for initial implementation.

2.3 Transition to the cloud: computing services, deployment models and implementation strategies

The fundamental issue public authorities face for moving into the cloud is the identification and implementation of the appropriate strategy which meets the aims of their organisation whilst uptakes the cloud's significant benefits. Migrating to the cloud raises many questions and poses and number of risks for organisations if not handled correctly. Although published reports review the multiple advantages of cloud computing as well as the most significant challenges that public authorities have to address, the exact way of doing such a task is still an unknown process. In fact, there is not a single strategy: a public service organisation can choose to be one of three things; a user, a provider or both. The complexity also derives from the fact that all key players can get involved, such as regional governments, citizens and service providers (Accenture, 2013).

Before describing proposed guidelines and strategies towards cloud migration, we should first list the most common service and deployment models. More specifically, cloud computing service models can be defined based on the targeted services, such as Architecture as a Service (AaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Communications as a Service (CaaS) etc. (Seo et al., 2014).

Service models

- **Infrastructure as a Service (IaaS)**: on-demand provisioning of infrastructural resources without management or control over it, but only over operating systems, storage, deployed applications and possibly over networking components.
- **Platform as a Service (PaaS)**: provision of platform layer resources, including operating system support and software development frameworks, for the deployment of consumer created or acquired applications. Management or control is only over the deployed applications and, possibly, over the configuration settings for the application-hosting environments.
- **Software as a Service (SaaS)**: on-demand provision of applications over the internet, without management or control over the cloud infrastructure or even the individual application capabilities with the exception of a limited number of user-specific application configuration settings.

Also, cloud computing can be classified on the basis of the targeted service and its perspective use (Zhang et al., 2010; Seo et al., 2015) in four main types: public clouds, private clouds, hybrid clouds and community clouds (APPTIS, 2010; Mell and Grance, 2011).

Types of clouds

- **Public clouds**: a cloud in which service providers offer resources as services to the general public.
- **Private clouds**: a cloud platform designed for exclusive use by a single organisation. In a private cloud-based service, data and processes are managed within the organisation without the restrictions that a public cloud entails (e.g. security exposure, legal requirements etc). This does not mean though that it is necessarily managed and hosted by the organisation that uses it.
- **Hybrid clouds**: a combination of a public-private cloud model, offering more flexibility, tighter control and security over application data. In this case, users typically outsource non-business-critical information and processing to the public cloud, while keeping business-critical services and data in their control.
- **Community Cloud**: a platform provisioned for exclusive use by a specific community with share concerns or mission.

The migration of public services and applications to the cloud should be done in a strategic and methodological manner, after considering key aspects such as the cost of migration, application redesign, application performance and availability, security and privacy requirements, regulatory requirements etc. (CSCC, 2013).

But firstly, we need to clarify that when we talk about public services we mean the services which are produced and supplied by the government and public institutions to satisfy the benefits of social communities and the public needs. Deloitte (2011) propose a taxonomy of public services based on the concepts of granularity and orchestration; these imply a certain hierarchy of services with services at higher and lower levels, where different services can be combined to create a new service. According to the proposed taxonomy, public services can be categorised in a) process public services, which represent actual workflows or business processes, combining other (basic and/or composed public) services through service orchestration, b) composed public services, which are based on other services, combined into a new composed service and c) basic public services which implement a basic functionality. The implementation of this service decomposition in three case study countries led to the identification of three key elements in a cloud of public services (Figure 3):

- End-user (client or web) applications which allow the end-user to use the service and interact with the service provider;
- The collection of public services serving as building blocks, which can be offered in an open and interoperable way and reused
- The different categories of public services – Process, Composed, or Basic (data and Logic) Services – as defined by the service taxonomy

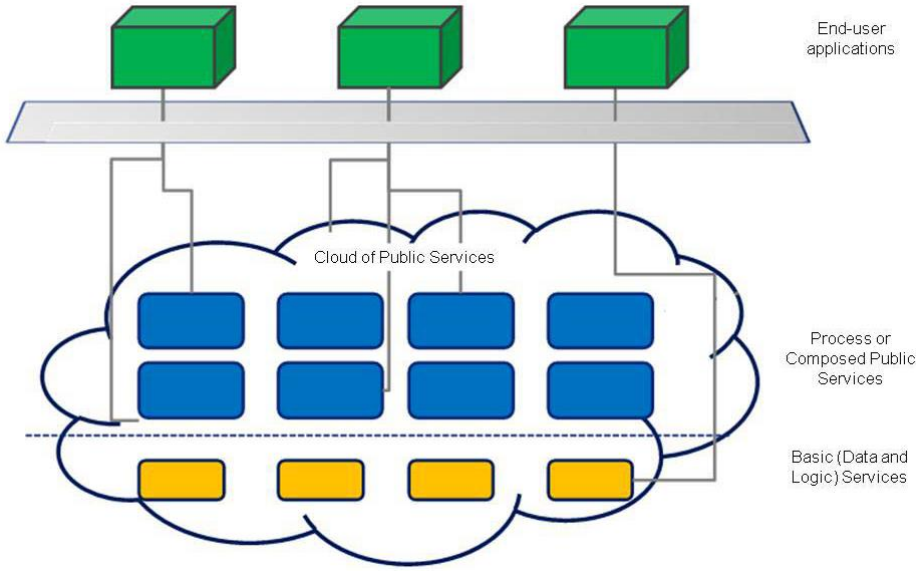


Figure 3: Conceptual model for the design of a cloud of public services. Source: Deloitte (2014)

Bonneau et al. (2013a) group cloud-based application and services of the public sector in three similar categories (Table 1): i) Horizontal/Citizen engagement and service delivery, i.e. applications that allow interaction between citizens and governments and support dematerialisation processes ii) Horizontal/ Productivity applications, i.e. applications used by internal employees for overall management and administrative processes, and iii) Vertical applications, i.e. applications addressing specific needs around some vertical expertise.

Horizontal/Citizen engagement and service delivery	**Horizontal/ Productivity applications**	**Vertical applications**
Applications for citizen – government interaction	Applications for the internal management of administrative processes	Applications addressing specific needs
Accounts of different services • Taxes • Transactional (Payment) • Online voting • Website hosting • Social applications (wiki, billboards, blogs) • Access to public sector information	• Email and communication tools • Office automation • Procurement • HR management • Virtual Desktop • Records Management	• E-Health • E-Education • Energy management/ smart grid • Smart transport/ intelligent transportation systems • Urban planning • Utility Management (waste, water etc.)

		• Smart Logistics

Table 1: Taxonomy of public sector application fields. Source: Bonneau et al. (2013a, 9)

Many public organisations find the process of migrating to the cloud as a complex process that requires careful planning and deliberation. For this, it is essential that they should primarily consider all risks and challenges and make sure that migration is right for their organisation and their services. Although there is not a single path, planning for cloud migration should entail careful preparation and a defined strategy in a form of a roadmap that will act as a guide, as well as a checklist with technical, managerial, financial and other considerations.

According to Deloitte (2011), strategies for migrating public services to the cloud will be more effective when they adopt a gradual, phased or incremental approach. This means that i) they should focus on different subdomains (and specific services per sub-domain and subsequently expand by developing new services) and ii) reuse existing public services by adding a service layer and exposing this to a cloud of public services. It should also be added, that migrating existing services to the cloud mostly involves an evaluation exercise that examines the readiness of applications and their business models.

Seo et al. (2014) propose a strategy for the implementation of a public service based on cloud computing. The strategy includes three steps and a list of 15 guidelines in six different domains (Table 2). According to the authors, the process should start with the establishment of cloud-based common infrastructure and platform, continue with the design of the services according to a list of predetermined guidelines in order to confirm that these are appropriate for the cloud foundation, and conclude with the actual implementation of the services.

Division	Guideline
Governance	- Determination of the system, organization, and function of government-wide governance for service implementation
Platform and common technology	- Government-wide CC architecture reference model - Standard model for the construction of cloud data centers - Connection standard for mutual management between PSBCC - Guideline for the use of open software that can be commonly used
Security	- Security guidelines for each factor such as the data (information), system, and network
Implementation	- Technology guideline to confirm possibility of implementation in the case of new CC establishment - Guideline on the implementation of the cloud work environment in the public sector - Evaluation and authorization standards of cloud-related solutions
Migration	- Standards for selection of convertible services

	– Technology guideline on the conversion of the legacy system into the cloud system – Guideline for economic feasibility analysis
Management	– Guideline of standard service level agreements (SLA) for services – Standard for service quality evaluation – Metering system on the service use

Table 2: List of guidelines required for the implementation of cloud-based public services.

Source: Seo et al. (2014)

KPMG (2012) has identified six steps that government organisations have to take in order to gain better understanding on how the cloud will impact their operations. These are i) taking a comprehensive approach, ii) identifying the right leadership, iii) balancing risk and reward, iv) creating centers of excellence, v) collaborating with vendors and the private sector. Finally, a recent study analyzing the current national initiatives of ten EU countries for the deployment of cloud computing in the public sector, recognized three emerging models which differentiate in the type of services addressed, the nature of cloud infrastructure and level of centralization (Bonneau et al., 2013a). These models are:

i) **Procurement and Marketplace**: this model, adopted mainly by UK, Portugal and partly by the Netherlands, is a very centralized and top-down approach, only for procurement aspects and involves bottom up approaches regarding application development and adoption. It relies mainly on external providers which develop applications that can be used by pubic authorities.

ii) **Resource Pooling:** it is also a top-down model, in which resources are pooled to provide a common infrastructure that can be leveraged for IaaS services and for more specific applications

iii) **Standalone Applications**: it is a pure bottom up model in which public authorities deploy standalone applications, without being coordinated even if there is a form of central strategy/policy on this. The focus in this model is on SaaS, therefore, most of the applications rely on public cloud solutions.

3 The STORM Clouds experience

During the cloudification process the Municipalities and the technical partners encountered and overcame a lot of issues/problems. The following table present these problems grouped in categories, along with the proposed solutions.

Category	Issue/Problem
Ethical Issues and Security	A lot of ethical and data protection issues arise when City Authorities consider transitioning to cloud computing. City municipalities, which operate in a legal context that considers the individual's right to privacy as a fundamental issue, should protect citizens from the misuse of their personal information. As they are trusted bodies, citizens expect that their approach to data collection, retention, storage and sharing is in line with these responsibilities. Therefore, the ethical dimension is a key part of the cloud migration process. The following three issues are essential (Timmermans et al., 2010): • The shifting of control from technology users to the third parties • The storage of data in multiple physical locations • The interconnection of multiple services essential The rapid growth in data volume, complexity of usage, and business information in the urban environment, criticality requires that new approaches, risk-based and business-focused need to be developed for protecting information. They also need to be flexible while providing consistent protection. Today's regulatory compliance and daily reliance upon critical data makes data protection more important than ever. But data protection has become far more complex and sophisticated to deploy and manage because of Virtual Machine sprawl and the increased transformation of environments from physical, on-premises infrastructure to virtualized and cloud-based architectures. Municipalities should focus on good practices for how to guard against frequent data protection issues common in online platforms, under the condition that they should be simple to implement. Data protection issues include software updates, SQL injection, unnecessary services, password storage, configuration of SSL and TLS, inappropriate locations for processing data and default credentials. Moreover, the Municipalities should create a breach management plan in order to address an event of a security breach. This will assist municipalities in deciding on an appropriate course of action if a breach occurs. In general, regarding data protection the following key

	recommendations should be taken into account: • Cloud computing must not lead to a lowering of data protection standards as compared with conventional data processing; • Cloud service providers should offer greater transparency, security, accountability and trust in CC solutions in particular regarding information on potential data breaches and more balanced contractual clauses to promote data portability and data control by cloud users; • Further efforts be put into third party certification, standardisation, privacy by design technologies and other related schemes in order to achieve a desired level of trust in CC; and • Privacy and Data Protection Authorities continue to provide information to data controllers, cloud service providers and legislators on questions relating to privacy and data protection issues. Municipalities must have a clear understanding of potential security benefits and risks associated with cloud computing, and set realistic expectations from our CSPs. Attention must be given to the different service models (IaaS, PaaS or SaaS) as each model brings different security requirements and responsibilities. The Cloud Standards Customer Council (CSCC) has released a guide namely "Security for Cloud Computing: Ten Steps to Ensure Success" (Cloud Standards Customer Council, 2015) that can be used by municipalities to analyze and consider the security implications of cloud computing on their environments. These 10 steps can be used as a basis for evaluation of cloud provider security while the associated standards provide detailed guidance to help municipalities evaluate their CSP: 1. Ensure effective governance, risk and compliance processes exist. 2. Audit operational and business processes 3. Manage people, roles and identities 4. Ensure proper protection of data and information 5. Enforce privacy policies. 6. Assess the security provisions for cloud applications 7. Ensure cloud networks and connections are secure.

	8. Evaluate security controls on physical infrastructure and facilities 9. Manage security terms in the cloud SLA 10. Understand the security requirements of the exit process. Cloud computing services certification is an important aspect since it provides assurance that our critical security requirements are being met. Therefore, we should identify which security certifications are important to us and insist from our CSP to demonstrate their conformance.
Security	• **Acquiring SSL certificates for organizations**: The acquisition of an SSL certificate with Organization Validation requires extra validation steps that make the procedure very time consuming and involves IT and administration personnel step by step cooperation. • **SSL certificate CSR formation**: In order to create the Certificate Signing Request (CSR) and submit it to an SSL certificate provider, the *openssl* software has to be used. The required process generates first the Private-Key file for the decryption of the SSL Certificate and then the certificate signing request (CSR) file. • **SSL certificate installation and HTTPS setup**: After receiving the .crt and .ca-bundle files from the SSL certificate provider, these files have to be copied to the application VM. Then various changes in the web server configuration files have to be performed in order to enable SSL access to the web server, specify a specific port for HTTPS access and instruct the VM to allow traffic through this port, (possibly) restrict access to the server using HTTPS only, and instruct the web server to use the .crt and .ca-bundle files of the Municipality. • **Same SSL certificate for different domain names (SAN certificates) using Apache SNI**: There are cases that the https enabled website for an application has to be offered through two or more distinct domain names. In this case a SAN/UCC SSL certificate for the required number of aliases or a number of different certificates has to be acquired. The former solution can be used when the same owner is managing all domains. Otherwise, the latter solution can be applied by exploiting the fact that an apache server can

	handle two or more different certificates for two different domain addresses that correspond to the same web server/website/ip address through the *Server Name Indication* (*SNI*) protocol. • **Extensive security testing:** After the successful cloudification the applications were assessed against various security requirements. These tests revealed some issues which leaded to updated, more secured applications.
Remote Access of SCP	• **SSH access setup (using private key) to a Virtual Machine hosted in IaaS:** Instead of using a password, the SSH access to a Linux Virtual Machine is accomplished using a private key. Using the Openstack interface a private key is created and then associated to the Virtual Machine that is going to be instantiated. After the Virtual Machine instantiation this key is used in order to connect to the server by any SSH client.
File Transfer	• **SFTP write access for uploading new application version:** The VM hosting the applications of each Municipality in the cloud doesn't allow non-root user SFTP access with write permissions. That means that in case any binary data has to be uploaded to the VM for the application, which resides in an area of the VM file system where only root user access is possible, a two-step process is required. Specifically, the file(s) first have to be uploaded in the user data space using SFTP. Then an SSL connection to the VM is required in order to copy the files to the proper location while having root user access.
Installation/operation	• **Detailed documentation and collaboration with applications' developers during the installation process:** The installation manuals of the applications, which were candidates for cloudification, were updated and the applications' developers collaborated with the technical partners. In some cases there were delays in the collaboration process that delayed the cloudfication process. • **Collaboration with developers during the operation of the applications:** The collaboration between applications' developers and technical partners solved issues (bugs) that revealed during applications' operation. The non-availability of some developers when it was required, caused delays in the debugging process.
DNS Management	• **DNS A record for application subdomain:** The domain name provider of each Municipality was asked to create an A record that

	points the subdomain name of the application to the IP address of the VM hosting the application in the SCP, in order to make the application of the Municipality accessible through Internet.
Application Server	• **Critical updates installation in Municipality VM in IaaS**: By default, Ubuntu server installations supplied by the SCP provider don't automatically install critical updates. The required changes in the Ubuntu configuration files need to be applied in order to activate automatic critical updates installation.
Web server	• **Changes in Configuration to support security requirements**: In the configuration file of the Apache web server a number of changes was made in order to address the new security requirements.
Database Management	• **SCP MySQL remote access**: Easy MySQL management using a Graphical User Interface (GUI) can be accomplished in two ways. In the first case the MySQL server is accessed using a suitable GUI that is executed in the connecting host. This requires "opening" a special port in the application VM which is not considered very secure, since access to a database is supposed to occur only from the database hosting VM itself or from within the server farm. The best way to access MySQL using a GUI is to additionally run a web based database management tool in the VM where the MySQL server is executed (or in another VM in the server farm), like *PhPMyAdmin*.
SMTP Server	• **Configure external SMTP Server to allow connections from SCP in order to send email from the applications hosted in SCP**: The setup of the mail server that is used in order to allow an application hosted in SCP to send email messages may have security restrictions that don't allow it. In such a case changes in the Municipality's mail server are needed in order to mark the IP address(es) used by the application server as trusted. The problem can also be solved using an external mail server as a service or by imposing only secure connections to the email server and trusting all connecting hosts.
Backup	• **Backup in other physical locations, different from the SCP**: Backing up of each application data in more than one physical location is strongly advised. For this reason an Object Storage Solution (provided by the cloud provider) that automatically replicates the backup data in more than one physical location is required.

	Additionally a remote backup procedure that backs up the application data in a storage server located in the Municipality is considered necessary. • **Automation/scripting for backup purposes**: Automating the backup process is vital for ensuring timely executions of the backup procedure. In the Virtual Machine hosted in the cloud this is accomplished by creating scheduled jobs which call shell scripts that prepare the database and other files to backup and use the *Duplicity software* in order to create the final backup files. In a remote host located in the Municipality scheduled execution of similar scripts is required. Connecting to the remote Virtual Machine should also be automated. *WinSCP software* is a good option for this process. • **Review of the database backup settings in order to perform the backup while mysql service is on**: The DB backup can be performed by shutting down the DB service or by locking the DB tables in different ways. The best procedure for the DB backup is selected based on the uptime requirements of each application and the specific DB engine that is used by application. **Automating** backup using Duplicity: The *Duplicity* software for Ubuntu is a very powerful backup system. After an analysis of the data that each application stores involving the location of the data, the frequency that it changes, the importance of the data, the time required to maintain the backed up data and other factors, a backup plan is customized for the application. Then the appropriate duplicity commands are scheduled for execution.
High Availability and Load Balancing	• **Experimenting with high availability and load balancing of the cloudified applications:** The Municipalities and technical partners were evaluated the way that high availability and load balancing could be implemented.
Migration strategy	• **Selection of potential applications to migrate to the cloud**: The Municipalities had to select the best possible applications to migrate to the cloud considering the strategical plans for the city, cost savings, the benefits that the services would bring to the city/citizens, the ease of moving to the cloud, the benefits of migrating the app/service to the cloud etc. From the STORM experience it was not clear wether the initial selection of applications should involve a more publicly available process. • **Selection of stakeholders and users to actively participate in the**

	process of cloudification. These groups include council staff (technical and administrative), citizens, businessmen, entrepreneurs, .. representation of all the collectives that may be interested in the application and in the Storm Clouds platform. It was revealed from the STORM experience that a deeper implication of the personnel of the Municipalities is required in the migration process. Also an extensive involvement of final users (citizens, local entrepreneurs etc) is very positive, though this process should include initial explanation of the cloud migration benefits for non technical peopel, a communication camplaign as well as the implementation of on-line participation mechanisms. • **Internal organisation and need for restructuring**: The process of cloudification makes services and municipal units less dependent on the internal IT unit, which was responsible for procurement and decisions of all applications. This change had a positive effect on the functionality of the service, as previously there were a lot of delays due to organisational procedures or for the sake of security.
Monitoring and evaluation	• **Selection of a set of indicators**: Once the applications are deployed in the cloud, municipalities had to define and deploy a monitoring and tracking process of their use and overall success.

4 Conclusions and next steps

The report intends to offer a basic background with regards to the migration of public services into the cloud, with the purpose to make this information comprehensive to public servants and stakeholders with non IT experience. Therefore, it provides the reader with some introductory information on cloud computing and how this is relevant to public authorities. What is more, based on the STORM experience, it reveals a number of issues that municipalities could face during the migration process and makes recommendations on how these could be addressed.

As a next step, we intend to enrich the list of issues/problems connected to the migration process, improve and supplement the recommendations for potential solutions and, finally, organise this information in an easy to read way, formulating a usefull roadmap for managers and public servants. Of course, the literature on best practices will also be updated.

References

[1] Accenture (2015) A new era for European public services: Cloud computing changes the game.

[2] Accenture and WSP (2010) 'Cloud Computing and Sustainability: The Environmental Benefits of Moving to the Cloud'.

[3] Aditi Technologies (2015) Building "Smart" Cities on the Cloud, Available online at: https://blog.aditi.com/cloud/building-smart-cities-cloud/

[4] Apptis (2010) An Introduction to Cloud Computing in the Federal Public Sector, White Paper

[5] Australian Government (2011) Cloud Computing Strategic Direction Paper: Opportunities and applicability for use by the Australian Government, Department of Finance and Deregulation, April 2011

[6] Australian Government (2013) The National Cloud Computing Strategy, Department of Broadband, Communications and the Digital Economy, May 2013

[7] Australian Government (2014) Australian Government Cloud Computing Policy: Smarter ICT Investment, Department of Finance, October 2014

[8] Bonneau, V., Mahieu, B., Dudenbostel, T., Gaudemer, J., Giarracca, F., Good, B., Poel, M., Ramahandry, T. and Van Til, J. (2013a) Analysis of cloud best practices and pilots for the public sector, Final Report, A study prepared for the European Commission, DG Communications Networks, Content & Technology by Digiworld by IDATE and Technopolis group

[9] Bonneau, V., Mahieu, B., Dudenbostel, T., Gaudemer, J., Giarracca, F., Good, B., Poel, M., Ramahandry, T. and Van Til, J. (2013b) Analysis of cloud best practices and pilots for the public sector, Annex to the Final Report: Country profiles, A study prepared for the European Commission, DG Communications Networks, Content & Technology by Digiworld by IDATE and Technopolis group

[10] Chandrasekaran, A. and Kapoor, M. (2011) State of Cloud Computing in the Public Sector – A Strategic Analysis of the business case and overview of initiatives across Asia Pacific, Frost & Sullivan

[11] Cisco (2014) Cisco and AGT form a Smart City Global Strategic Alliance to Transform the Way Cities are Managed and Secured, Cisco Press Release, Available online at: http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1342178

[12] Cloud Standards Customer Council (CSCC) (2013) Migrating Applications to Public Cloud Services: Roadmap for Success, Available online at: http://www.cloud-council.org/Migrating-Apps-to-the-Cloud-Final.pdf

[13] Cloud Standards Customer Council (CSCC) (2015) Security for Cloud Computing – 10 Steps to Ensure Success, Available online at: http://www.cloud-council.org/Security_for_Cloud_Computing-Final_080912.pdf

[14] Craig, R., Frazier, J., Jacknis, N., Murphy, S., Purcell, C., Spencer, P., and Stanley, JD. (2009) Cloud Computing in the Public Sector: Public Manager's Guide to Evaluation and Adopting Cloud Computing, White Paper, Cisco Internet Business Solutions Group

[15] Deloitte (2011) Study on cloud and service oriented architectures for e-government' Final report summary, Commissioned by the European Union

[16] Dustar, S., Vögler, M., Sehic, S., Qanbari, S., Nastic, S. and Truong, H.L. (2014) The Internet of Things Meets Cloud Computing in Smart Cities, Bridges Vol. 41, OpEds & Commentaries, Available online at: http://ostaustria.org/bridges-magazine/item/8280-the-internet-of-things-meets-cloud-computing-in-smart-cities

[17] European Cloud Partnership Steering Board (ECPSB) (2014) Establishing a Trusted Cloud Europe: A policy vision document by the Steering Board of the European Cloud Partnership, Final Report prepared for the European Commission, DG Communication Networks, Content & Technology

[18] European Commission (EC) (2012) 'Unleashing the Potential of Cloud Computing in Europe', Brussels, 27.9.2012, COM(2012) 529 final

[19] European Commission (EC) (2014) 'Towards a Cloud of Public Services', Digital Agenda for Europe

[20] Figliola, R.M. and Fischer, E.A. (2015) Overview of Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management, Congressional Research Service, Report prepared for Members and Committees of Congress

[21] Government Accountability Office (GAO) (2014) Cloud Computing: Additional Opportunities and Savings Need to Be Pursued, September 2014, Available online at http://www.gao.gov/assets/670/666133.pdf

[22] Hobson, L. (2014) Major Disruption – Cloud computing is disrupting more than our technological norms, Available online at https://www.linkedin.com/pulse/20141006134234-1064759-major-disruption-cloud-computing-is-disrupting-more-than-our-technological-norms

[23] IDC (2012) Quantitative estimates on the demand for cloud computing in Europe and the likely barriers to take up, Smart 2011/0045, D2 Interim Report

[24] Jander, M. (2014) Why Smart Cities Need Cloud Services, UBM's future cities, http://www.ubmfuturecities.com/author.asp?section_id=234&doc_id=526607

[25] Khan, Z., Anjum, A., Soomro, K., Atif Tahir, M. (2015) Towards cloud based big data analytics for smart future cities, Journal of Cloud Computing: Advances, Systems and Applications, Vol. 4, No. 2, pp. 1-11

[26] KPMG (2012) Exploring the Cloud: A Global Study of Governments' Adoption of Cloud' KPMG International Cooperative

[27] Kundra, V. (2011) Federal Cloud Computing Strategy, U.S. Chief Information Officer, The White House

[28] Macias, F. and Thomas, G. (2011) Cloud Computing Concerns in the Public Sector: How Government, Education, and Healthcare Organisations are Assessing and Overcoming Barriers to Cloud Deployments, White Paper, Cisco

[29] Mahmood, Z. (2015) (eds.) Cloud Computing Technologies for Connected Government (Advances in Electronic Government, Digital Divide, and Regional Development), IGI Global, p. 417

[30] Manzoor, A. (2015) Cloud Computing Applications in the Public Sector, In Mahmood, Z. (2015) (eds.) Cloud Computing Technologies for Connected Government (Advances in Electronic Government, Digital Divide, and Regional Development), IGI Global

[31] Mell, P. and Grance, T. (2011) The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology (NIST), U.S. Department of Commerce

[32] Microsoft (2011) 'The Central Role of Cloud Computing in Making Cities Energy-Smart', Microsoft Corporation

[33] Mitton, N., Papavassiliou, S., Puliafito, A. and Trivedi, K.S. (2012) 'Combining cloud and sensors in a smart city environment', EURASIP Journal on Wireless Communications and Networking 2012:247

[34] Seo, J., Min, J. and Lee, H. (2014) Implementation Strategy for a Public Service Based on Cloud Computing at the Government, International Journal of Software Engineering and its Applications, Vol. 8, No. 9, pp. 207-220

[35] Shin, D.H. (2013) User centric cloud service model in public sectors: Policy implications of cloud services, Government Information Quarterly, Vol. 30, Issue 2, pp. 194-203

[36] Suciu, G., Vulpe, A., Halunga, S., Fratu, O., Todoran, G. and Suciu, V. (2013) "Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things," in Control Systems and Computer Science (CSCS), 19th International Conference, pp.513-518, 29-31 May 2013

[37] Timmermans, J., Ikonen, V., Stahl, B.C., Bozdag, E. (2010) The Ethics of Cloud Computing: A Conceptual Review, Proceedings of the IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), pp. 614-620

[38] vmware (2011) Your Cloud in the Public Sector, Industry Brief White Paper

[39] Zhang, Q., Cheng, L. and Boutaba, R. (2010) Cloud computing: state-of-the-art and research challenges, Journal of Internet Services and applications, Vol. 1, Issue 1, pp. 7-18High Availability (HA) definition, Margaret Rouse, September 2005, http://searchdatacenter.techtarget.com/definition/high-availability

Annex A Questionnaire

Questionnaire distributed to public authorities in order to acquire feedback from public servants related to the use and operation of public services into the cloud

1) During the process of migrating public services into the cloud did you face any procedural changes or **changes related to the internal organization of the public authority**?

   [Organization streamlining, changes in the responsibilities of municipal departments, changes in the need of specialized IT department – less or new skills required, organizational restructuring etc.]

2) In your opinion, what were the **most visible benefits** from migrating public services into the cloud?

   [Qualitative assessment based on your everyday activities and workload/time management comparing the situation before and after the cloudification, such as requirements in the maintenance and administration, improved characteristics and/or overall efficiency/performance of the cloudified services, overall added value to the organisation etc.]

3) Did you face any **technical issues during cloudification** of public services into the cloud?

   [Issues related to integration with existing systems, network re-configuration, application code improvement or alteration, application reconfiguration in order to execute over different infrastructure, application data backup, security risks, file and CLI access, etc.]

4) During the process of migrating public services into the cloud did you make any **changes due to the feedback received from end users** (other employees of the municipality or citizens)?

   [Application re-design or improvement of specific components/features and cause of change e.g. regulatory compliance, application performance, user engagement and satisfaction]

