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 5.3

Roadmap about Migration of Public Services into the Cloud

Work Package: WP5

Version: 1.0

Date: 31/03/2017

Status:

Nature: Other

Dissemination Level: PUBLIC

Editor: Kakderi Christina (AUTH-URENIO)

Authors: Kakderi Christina (AUTH-URENIO), Panagiotis Tsarchopoulos (AUTH-URENIO), Komninos Nicos (AUTH-URENIO)

Reviewed by: Agustin González-Quel (RTDI)

Version Control

Modified by	Date	Version	Comments
Kakderi Christina	11.03.2017	v0.2	
Panaiotis Tsarchopoulos & Nicos Komninos	31.03.2017	V1.0	Ready for submission

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.

WP5 of the STORM CLOUDS project aims 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.

Task 5.2 refers to the preparation of guidelines for Public Authorities and policy-makers. The aim this task is to refine all the available knowledge created in task T5.1 and create a number of guidelines for Public Authorities to help 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 guidelines will condense the knowledge emerging from different WPs, into a small number of practical steps towards to cloud service provisioning. The guidelines will help Public Authorities to address the technical and business challenges in the adoption of cloud computing.

This document presents a roadmap of five sequential steps (services and applications, cloud environment, migration of applications, cloud administration, data management) and two parallel procedures (security and validation/monitoring). The content of this roadmap is presented in an interactive, tree structured navigation tool, available through the STORM Clouds website (http://www.storm-clouds.eu/services/resources/roadmap/).

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

This document presents a roadmap of five sequential steps (services and applications, cloud environment, migration of applications, cloud administration, data management) and two parallel procedures (security and validation/monitoring). The content of this roadmap is presented in an interactive, tree structured navigation tool, available through the STORM Clouds website (http://www.storm-clouds.eu/services/resources/roadmap/).

It is based mainly on two deliverables: D5.1.2-Body of knowledge about migration of public services to the cloud and D3.4.2-Best practices for cloud-based public services deployment. However, it draws insight also from all other deliverables and activities undertaken throughout the project period.

2 A Roadmap about Migration of Public Services into the Cloud

STORM Clouds 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.

Drawing on the experience gained from this project we have created a simple methodology in the form of a roadmap that aims to help public authorities in their migration towards the cloud. An illustration of the roadmap can be found below (Figure 1).

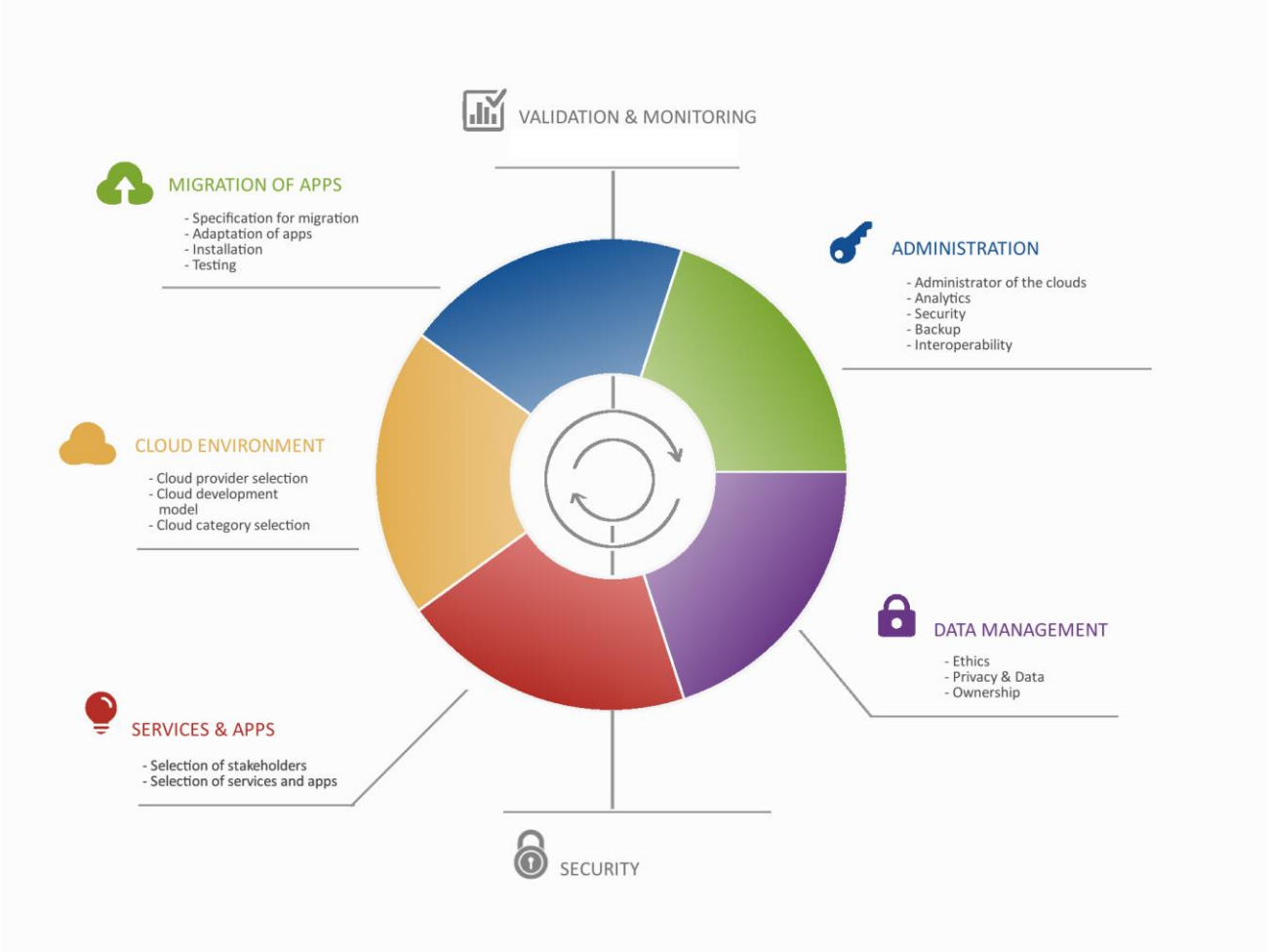

Figure 1: A roadmap for planning public services migration to cloud computing

The roadmap includes five sequential steps (services and applications, cloud environment, migration of applications, cloud administration, data management) and two parallel procedures (security and validation/monitoring). These steps represent the main roadblocks that public authorities have to face and for each one we provide guidance either by describing a case study solution or by providing a set of recommendations/guidelines. More analytically, the first step of the roadmap starts with the adoption of an open innovation methodology in the selection of the services to be cloudified and the identification of the stakeholders that will participate through a user driven process. The decision on the cloud environment which comes second, relates to the cloud service category selection (IaaS, PaaS, SaaS), the selection of the cloud development model (public, private, hybrid, community) and technologies and the selection of the cloud service provider. Third, it is the application migration, i.e the process redeploying an application, typically on newer platforms and infrastructure. Cloud computing imposes new concepts and challenges for the role of monitoring and management of the cloud environment and the smart city solutions, therefore, the fourth step is the administration of the cloud, while the fifth is about data management. Finally, two more horizontal issues are described: i) cloud security which refers to policies, technologies, and controls deployed to protect data, applications and the associated infrastructure and ii) monitoring and validation which targets the business aspect of the applictions' migration.

The Roadmap aims to be used in combination to the Best Practices and threrefore, in various cases it directs

users to it. In order to facilitate its usage by public authorities, the roadmap is being presented in an interactive, tree structured navigation tool, available through the STORM Clouds website (http://www.storm-clouds.eu/services/resources/roadmap/).

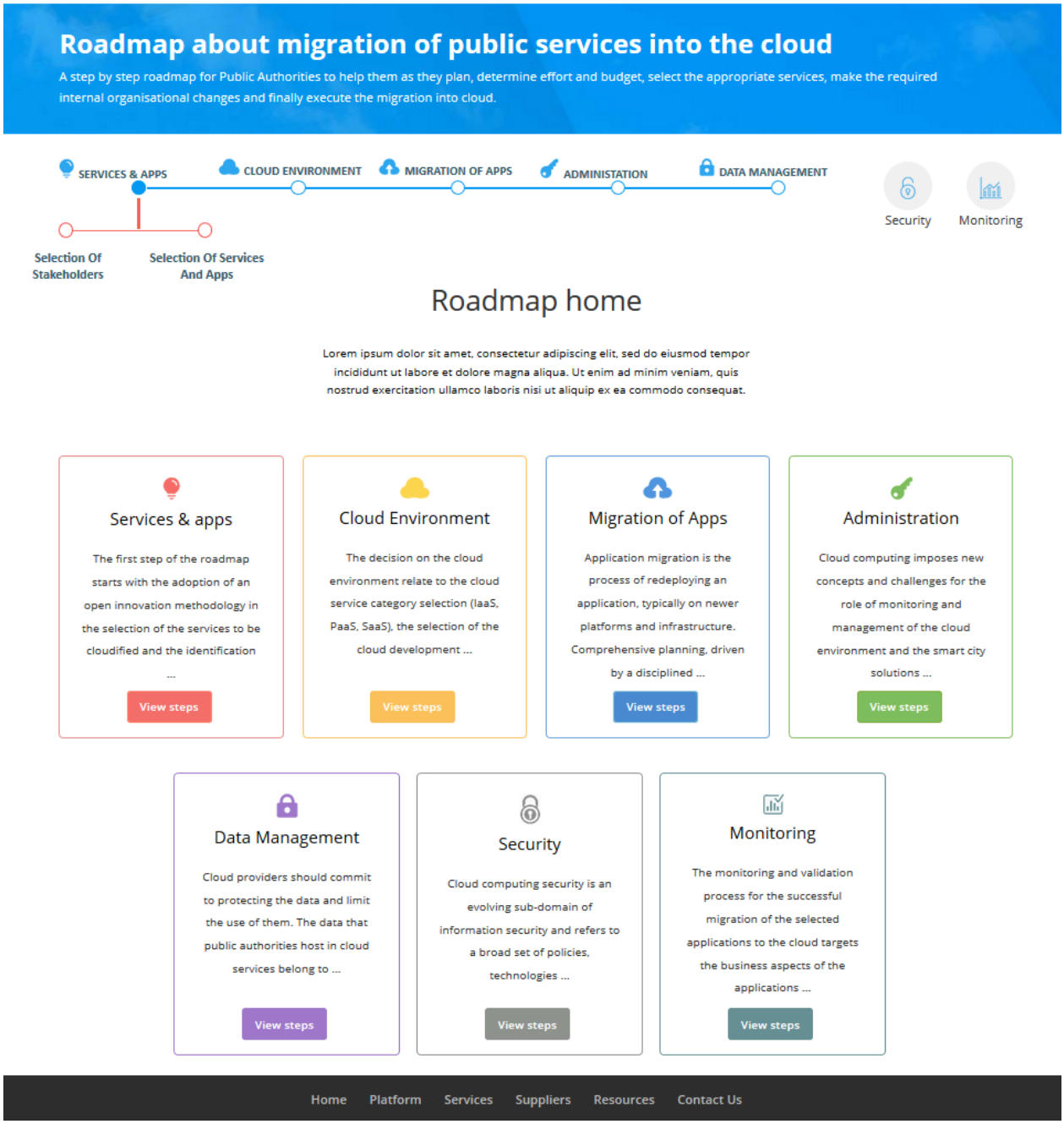

Figure 2: A screenshot of the home page of the roadmap

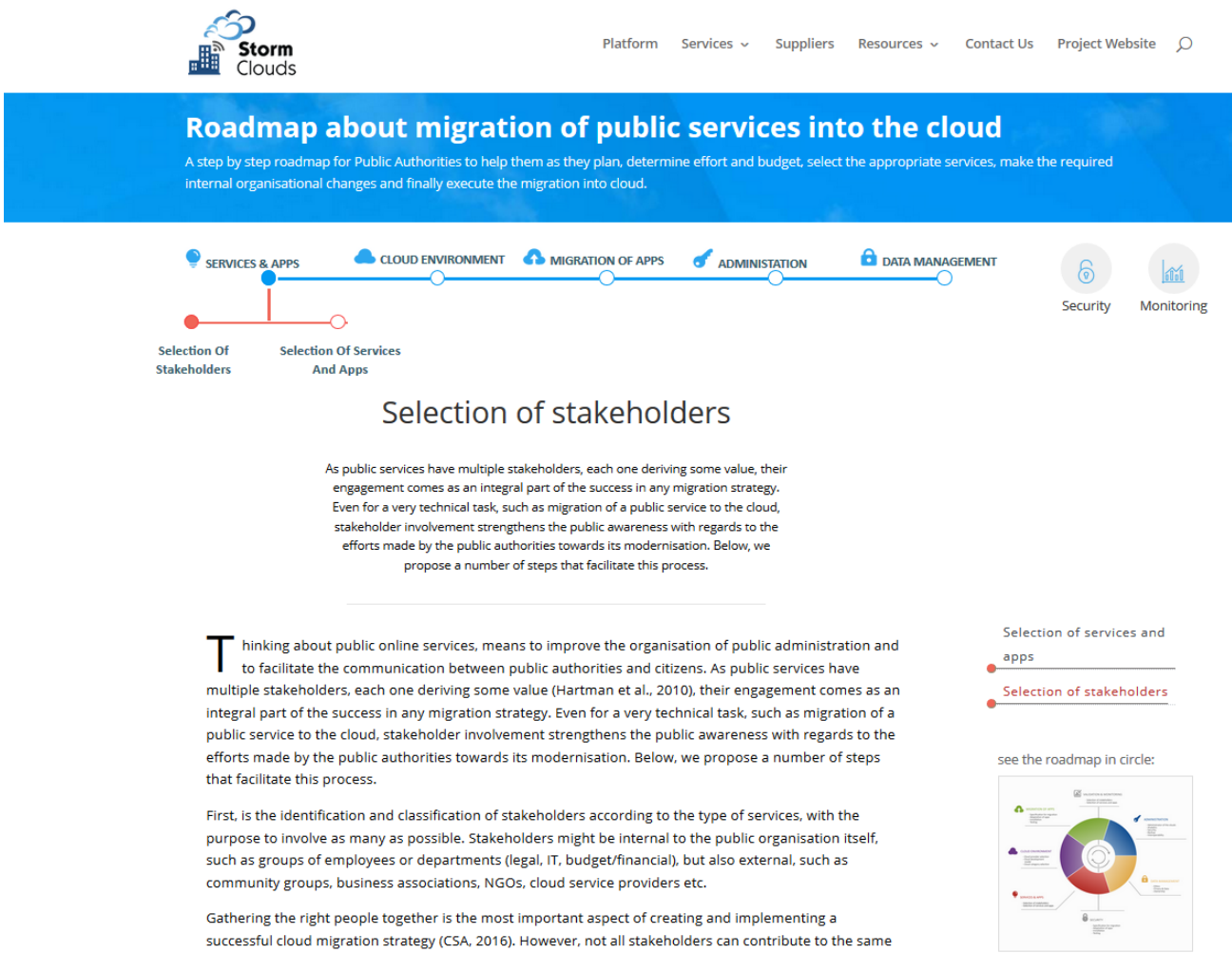

Figure 3: A screenshot of one of the steps

3 Selection of Services and Applications

3.1 Selection of stakeholders

Thinking about public online services, means to improve the organisation of public administration and to facilitate the communication between public authorities and citizens. As public services have multiple stakeholders, each one deriving some value (Hartman et al., 2010), their engagement comes as an integral part of the success in any migration strategy.

Stakeholder engagement might create many difficulties: increased complexity, need to achieve consensus among heterogeneous organisations with contradictory objectives, disclose information to third parties etc. However, even for a very technical task, such as migration of a public service to the cloud, stakeholder involvement strengthens the public awareness with regards to the efforts made by the public authorities towards its modernisation. Below, we propose a number of steps that facilitate this process.

First is the definition of objectives and associated indicators. Objectives should be in line with the expected benefits from the usage of cloud based systems. In order to monitor baseline and progress, public authorities should develop a number of Key Performance Indicators (KPIs).

Second is the identification and classification of stakeholders according to the type of services, with the purpose to involve as many as possible. Stakeholders might be internal to the public organisation itself, such as groups of employees or departments (legal, IT, budget/financial, procurement), but also external, such as community groups, business associations, NGOs, cloud service providers etc.

ADOPTING AN OPEN INNOVATION APPROACH

The Open Innovation Methodology focuses on the idea of gathering external and internal knowledge to accelerate the process of innovation. As over the last year the role of government has shifted from managing and administering to the orchestration of open innovation processes, stakeholders have become key players in deciding, contributing and delivering services (The World Bank, 2015). Such a development has not only removed all the burden from public authorities to a wider group of actors, but has also increased openness, transparency and inclusiveness.

The Open Innovation Methodology can be achieved through the following three dimensions:

- A user-driven innovation approach
- The treatment of innovation as an open system, allowing external actors to become key players in all parts of the innovation process
- The use of a series of iterative innovation cycles.

Element	Risk	Contingency Plan
Technical staff	Feel that their job is at risk and won't collaborate in the migration process	Training sessions to improve skills so they can work with the cloud Job redefinition
Management	Resources required are not provided	Apply a long temr reasoning to show that current investment will bring future savings.

Table 1: Methodology for risk mitigation

Gathering the right people together is the most important aspect of creating and implementing a successful cloud migration strategy. However, not all stakeholders can contribute to the same level. Therefore, public authorities should also identify the stakeholders which are expected to influence the service by acting as co-creators, as contributors or as users.

Criteria	Stakeholders' group
Cloudification depends on their decision	i.e. Policy makers, politicians

Their everyday work is affected by the cloudification	i.e. technical staff, accounting, procurement office personnel
The results of the cloudification may affect their everyday life	
Can influence the potential services by acting as co-creators, users etc.	

Table 2: Criteria for stakeholder segmentation

Third is the development of the engagement strategy. Stakeholder participation should not only refer to the identification and selection of potential services -for migration to the cloud or expansion due to improved IT functionalities such as storage, processing capacity etc.-, but to the whole process of services design and implementation through testing, validation and participation in dissemination. The activation can take place in five different phases: i) development of a communication strategy, ii) information disclosure about the services to be deployed and their benefits, iii) consultation, monitoring the stakeholders' response, iv) participation in the services' deployment, improvement and exploitation, and v) negotiation and partnerships aiming at future improvements and the sustainability of the deployed services.

Stakeholders should be informed and engaged, and therefore, public authorities should design and implement a plan for continuous collaboration and engagement. Such stakeholder engagement strategies might include:

- The *use of a series of iterative innovation cycles*. In which the services are being evaluated by users in order to lead to improved versions.
- *Definition of the roles and potential responsibilities* of the different stakeholders.

- *Educating stakeholders* on how cloud adoption can affect existing practices and/or changes the organisation's ability to meet its obligations. As transition to the cloud will primarily affect the IT departments, it is essential to make them understand the added-value of the cloud and provide solutions on potential risks.
- Mapping or creating and utilising tools and methods that will enable continuous collaboration with stakeholders. Different stakeholders might need to be contacted with different communication channels such as newsletters, social networks, personal meetings and working groups. Also, different tools might be used for different levels of engagement (information, consultation, training etc.). A mix of digital (i.e. online collaboration platforms and workspaces, social media) and traditional (face to face meetings) engagement tools can make sure to reap the benefits from any stakeholder.

Moving to the cloud public services means higher data storage and processing capacity, which allows –and may result to- the development of new functionalities and/or new and more improved services. Such services will require the collaboration of new stakeholders, i.e. other departments of the same municipality or external groups and organisations. It is important that stakeholder engagement will start before or at the first stages of the migration process in order to get an idea about the potential usability, type of data that will be treated etc.

STEPS FOR STAKEHOLDER ENGAGEMENT

Stakeholder engagement comes as an integral part of the success in any migration strategy. It should start from the first stages of the migration process in a series of iteration cycles that should include the following steps:

1. Definition of project objectives
2. Identification of as many potential stakeholders as possible
3. Segmentation of stakeholders based on their level of interest and influence
4. Development of a stakeholder engagement strategy:
   a. Communication plan and activities
   b. Definition of roles and responsibilities
   c. Mapping or development of tools that should be utilised for stakeholder participation
   d. Work with stakeholders (validate, co-create, co-disseminate)

3.2 Selection of Services and applications

As Public Authorities start migrating their applications to the Cloud, it is important to determine which applications fit better into this environment. Identifying and prioritising the best applications to be moved to the cloud means to consider and analyse different factors that have to do with the service/app itself (architecture, design, potential usage etc.), the experience and expectances of the responsible organisation, dependence on third party software etc. The selection of services should primarily be made based on the organisation's objectives and needs, and for this, internal reviews might provide important insight.

An application must meet certain requirements to be considered as a good candidate for migration to the cloud. The best ones are applications, which take advantage of the elasticity of Cloud Computing. Based on the Cloud Standards Customer Council (2013) the most and less suitable applications for migration to cloud computing are the ones described in the following table (Table 5).

FACTORS AFFECTING THE SELECTION OF SERVICES FOR MIGRATION

Identifying and prioritising the best applications to be moved to the cloud means to consider and analyse different factors, such as:

- **political priorities,**
- **user driven aspects**
- **technical and legal specifications/ restrictions** (including ownership, security, flexibility, level of maturity, language, documentation, target users etc.

Suitable Candidates for Cloud	Less Suitable Candidates for Cloud
• Applications that are used by a group of mobile workers to manage their time and activity, and that contribute only limited information to the company's broad management information databases. • Applications that are run infrequently but require significant computing resources when they run. • Applications that are run in a time zone different from that where your company's IT personnel are located. • Development, testing and prototyping of application changes, even if the final applications will be run on your own infrastructure. • Service Oriented Architecture (SOA) applications	• Applications that involve extremely sensitive data, particularly where there is a regulatory or legal risk involved in any disclosure. These will at minimum require special treatment if they are to be run in a cloud service. • Applications now being run on the company's private network and that are very performance-sensitive. • Applications that require frequent and/or voluminous transactions against an on premises database that cannot be migrated to cloud computing. • Applications that run on legacy platforms that are typically not supported (or may not be supported in the long run) by cloud providers.

Table 3: Application Candidates for Migration to Cloud Computing. Source Cloud Standards Customer Council (2013, p. 7).

In particular, the following type of applications will benefit from Cloud's ability to automate the dynamic of resources to match the current demand:

- Applications that are designed to spread their workload across multiple servers.
- Applications that run occasionally but require significant computing resources when they run.
- Applications with unpredictable or cyclical usage patterns.
- Service Oriented Architecture (SOA) Applications.

For these type of applications, the rapid elasticity combined with the pay-by-usage characteristic of the cloud can lead to significant financial savings. For each of the services identified, the following table must be completed.

Type	Technologies
Operating Systems	
Programming Languages	
Databases	
Web/Application Services	
Frameworks	
Applications Lifecycle Tools	
Open Source Code Repository	

Table 4: Technical Information about candidate applications to migrate

Migration of services to the cloud means the possibility of other municipalities to access services and transfer them without the need to develop them from the scratch. Such a task includes the analysis of a different set of criteria such as i) documentation, ii) target users, iii) flexibility, iv) language, v) compliance with internal security regulations and vi) specifications.

4 Cloud environment

4.1 Cloud Service Category Selection

Public Authorities should consider, when they plan their Cloud strategy, the different service categories of Cloud Computing. The majority of documents that exist online provide a detailed description of the prevailing categories, which may altogether be referred to as the Cloud Computing Stack: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). A simplified description of what each one of these categories entails is that a) SaaS applications are designed for the end-users and are delivered over the web, b) PaaS is the set of tools and services designed to make coding and deploying these applications in a quick and efficient way and c) IaaS is the hardware and software (servers, storage, networks, operating systems) that powers all the above (Kepes, n.d.).

ADOPT OPEN TECHNOLOGIES

Systems composed of open technologies provide the freedom to change environments and deliver a robust and secure experience, extending existing IT to the cloud. The majority of existing cloud offerings are implemented in proprietary and highly standardized form. Embracing an open cloud means providers don't dictate technologies and that competition is embraced.
Examples of open technologies include Openstack, Cloud Foundry, Docker, LAMP, MySQL etc.
You can find more about the power of Open technologies here.

Each of the above services has its own specific implication for the public authority that is using it. The most popular and useful SaaS-based cloud opportunities for public authorities include collaboration, document management, content management and project management (Schwartz, 2011). SaaS describes the most abstract layer of the cloud stack and it is more suitable if the organisation wants ready-made online applications. However, SaaS cannot be applied in the case that theif Public Authorities want to deploy their existing applications to a Cloud Environment. Usually, most common choices among public authorities is a combination of SaaS and IaaS as public authorities first concentrate on the infrastructure (Bonneau et al., 2013). If Public Authorities want to migrate their own applications to the cloud, they have to select between IaaS and PaaS. Both IaaS and PaaS enable the extension of platforms so that public authorities' IT can respond proactively and reactively to increased demand for services at a lower cost (Vmware, 2011). To decide which of the two options (IaaS or PaaS) they will follow, the Public Authorities should evaluate the pros and cons of each solution.

On the one hand, the IaaS offers excellent flexibility, as it does not require architectural changes to the applications, and full control of the resources used for the deployment. However, it increases the deployment complexity, as the application owners must take care of installing and configuring all the components for high availability and scalability.

On the other hand, the PaaS "hides" the complexity of the underlying infrastructure and allows developers to deploy their web applications to the cloud without having to take care of the infrastructure. The PaaS provider usually offers the cloud infrastructure and manages levels of scalability, software upgrades and maintenance. However, the applications may require significant changes to comply with the PaaS principles and take full advantage of high availability and scalability features. In particular, as application instances are ephemeral and can be started, stopped or fail at any time, they must be stateless and share nothing. More about the selection of cloud service category can be found here.

4.2 Cloud deployment model and technologies

Cloud computing can be classified on the basis of the targeted service and its perspective use (Zhang et al., 2010; Seo et al., 2014) in four main types: public clouds, private clouds, hybrid clouds and community clouds (APPTIS, 2010; Mell and Grance, 2011). The different deployment models are: Public clouds, Private clouds, Hybrid clouds, Community Cloud. While identifying the right cloud development model, one has to examine multiple issues such as security, performance requirements, types of data handled, IT skills required, long-term costs etc.

When choosing a specific cloud deployment model, it comes down to a series of trade-offs related to cost, management and security. While public clouds may be the best option for small organisation from a cost

perspective, organizations that require more control and/or security may opt for a private or hybrid cloud — providing they have the manpower and budget to manage those deployments effectively.

4.3 Cloud selection provider

As public authorities transition to cloud computing, they have to choose a cloud provider to host their cloud-based virtual machines. The choice of a Cloud Service Provider (CSP) requires the evaluation of an extensive list of options, such as:

- **Service Levels:** This characteristic is essential as the Public Authorities in most cases have strict needs regarding availability, response time, capacity and support. Cloud Service Level Agreements (CSLA) are an essential element to choose the right provider and establish a clear contractual relationship between a cloud service customer and a cloud service provider of a cloud service. A prescriptive series of steps should be taken by Public Authorities to evaluate them when comparing multiple cloud providers (CSCC, 2015b): 1) understand roles and responsibilities, 2) evaluate business level policies, 3) understand service and deployment model differences, 4) identify critical performance objectives, 5) evaluate security and privacy requirements, 6) identify service management requirements, 7) prepare for service failure management, 8) understand the disaster recovery plan, 9) develop an effective governance process and 10) understand the exit process.
- **Support:** The support is a parameter to consider carefully. It could be offered online or through a call centre, and in some cases, it could be necessary to refer to a dedicated resource with precise timing constraints.
- **Security:** As already mentioned security is paramount. When a public entity enters the cloud, it is entrusting its information assets to a third-party provider. Although normally, the potential supplier should follow recognised security policies in line with industry best practice, Public Authorities have to formulate a number of relevant questions (i.e. what is the security level offered by the providers? which mechanisms are in place to preserve client's applications and data? etc.) to evaluate this essential feature for the overall architecture.
- **Privacy:** Particular attention has to be reserved to legal requirements for the protection of the personal data hosted in the cloud service. Public Authorities should understand the data privacy and retention policies too, as well as where the CSP's data will be located, including any transborder data transfer, if applicable.
- **Open Standards:** In order to avoid getting locked-in to cloud infrastructure that has restrictive contracts or proprietorial technologies (technologies that are unique to the particular supplier), Public Authorities should prefer solutions that are implemented with fully open source technologies and open cloud standards. These technologies have an elegant escape hatch built into them by their design. Public Authorities can take the entire stack and host it on another CSP or in their premises without losing productivity or data. This backup plan protects them against legislative changes, company restructuring, and much more.
- **Compatibility:** The requirement of the cloudified applications have to fit into the CSP's existing pre-configured templates and may increase the cost of configuration. Moreover, the CSP's architecture should meet scalability, availability, capacity and performance guarantees and should be sufficient for agency requirements.
- **Interoperability:** To maximise the value of the cloud services, the cloud provider should select a provider that enables workloads to span multiple environments. For greater interoperability value, it is best to look for a provider that offers a common infrastructure platform for public and private hosted clouds, as well as on-premises private cloud (Frost and Sullivan, 2011).
- **Pricing:** Although most cloud providers use the aforementioned "Pay per Use" model, each CSP has a different price system. As cloud providers disclose their pricing formulas in a complex way, it is very difficult to estimate the cost for each service in order to be able to make a meaningful comparison (Posey, 2015). Moreover, additional costs can still arise, for example through the use of extra features. Terms of the contract, payment methods and payment dates can be deciding factors as well. Public Authorities should validate the cost model against the CSP's pricing considering the following (Australian Government, 2012): 1) transparency of pricing system, e.g. subscription or pay-as-you-go pricing, upgrades, maintenance and exit costs, 2) examine potential costs for unexpected peaks in

demand, 3) require service price for upgrade and maintenance fees appropriate to the services being procured, some upgrades may be automatic and included in the service, 5) confirm the cost model is suitable and allows for scaling and changes to service, 6) look for commitment requirements, such as minimum use, 7) confirm setup, training and integration fees and 8) request references to clarify ongoing cost of service.

- **Redundancy:** The provision of duplicate or backup equipment that takes over the function of equipment that fails should be discussed at an early stage. The redundancy process and timeframe have to meet the agency's requirements and especially its obligations to the citizens Thus, adequate backup procedures and robust disaster recovery plans must be incorporated into the cloud offering.
- **Easy to use administration environment.** Make sure your potential provider has a user-friendly client portal. It should allow you to conduct admin tasks or add storage space or services quickly. Ask for a demonstration before you choose one CSP over another.

The majority of existing cloud offerings are implemented in proprietary and highly standardised form. What presents advantages for the provider – technological knowledge, economies of scale, etc. – creates troubles and frustration for the customer. Users complain of "vendor lock-in", where they are dependent on a given vendor with no freedom of choice. Embracing an open cloud means there is no technology lock-in, no contractual lock-in and no service lock-in. It means providers don't dictate technologies and that competition is embraced. New, emerging standards will increase the portability and interoperability of systems across cloud service providers, and will reduce or eliminate this current barrier to cloud adoption.

5 Migration of apps

5.1 Specifications for migration

Cloud migration is an application landscape redesign that changes not only the way IT administrators interact with the public organisation's systems but also the way applicatios interact with each other and are delivered to end users (Brophy, 2016). The decision on migrating an application to the cloud requires a deeper understanding of the application architecture, the operational requirements, the business requirements, and the security requirements in order to make the most well-informed decisions (EPA, 2017).

As already mentioned in the cloud migration strategy description, before starting the migration process it is essential to assess the already used hosting environment. The analysis covers both the network (e.g. configuration, connectivity requirements from the municipality premises to the cloud environment, and supplementary services such as SMTP, DNS and WWW) and architecture (e.g. use of resources, underlining technologies, licenses, and security mechanisms) of the service.

SPECIFICATIONS FOR CLOUD MIGRATION

Public authorities should define the functional and technical characteristics that will host the applications on the new Cloud Environment. Before the migration process public authorities should collect the following information per application:

Functional description: a brief description of the implemented functions and the users of the application

Availability: the current version of the application and a link to a deployment available on the Internet (if any)

Technical Information:

- The list of technologies used for implementing the application (e.g. operating system, programming languages, database engines, etc.)
- Resource information like amount of RAM required, disk space, number of vCPUs, etc.
- Deployment information like the number of servers for running the application, high availability solutions, load balancing solutions etc.

Together with the hosting environment it is crucial to analyse the applications' readiness for the cloud. Aspects, such as customization, regulatory compliance, complex service architectures and service maturity are carefully investigated, as they would negatively impact the cloudification process. A crucial aspect is the availability of both the application's source code and documentation (installation manual, code dependencies, required software packages, etc.). Finally, the commitment of the application's development and support team should be ensured.

Next, public authorities should define the functional and technical characteristics of the Virtual Machines that will host the applications on the new Cloud Environment. The analysis of the functional requirements covers technical details (e.g. Operating System, Scripting Language, Database, Web/Application Server, Data Formats, Frameworks/Libraries and External Services used), interoperability issues, and static characteristics such as hard-coded IP address and directory paths. Furthermore, the analysis of the non-functional requirements addresses issues related to the proper functioning of the application such as security, regulatory compliance, performance, availability, backup; privacy, reusability, and interoperability. An estimation of the use of resources regarding RAM, Disk Space, CPUs, Bandwidth, Hits/Month, Registered Users, Max On-line Users, and Average On-line Users contributes to the calculation of the expected workload per application. An important characteristic that should be examined in this step is if the application's design supports its deployment in multiple servers. In that case the application will take full advantage of the performance benefits that cloud offers. An example of the information that should be collected per application is given in the Tables below.

This analysis of the functional and technical requirements also highlights potential obstacles to the transformation or the porting of the applications to the cloud due to technical or functional reasons. For example, applications implemented with legacy technologies might require licenses for using commercial software products. When porting an application to the cloud, one should make sure that is does not constitute an infringement of the licensing rights that the application proponent(s) have in place with the software vendor. From a functional point of view, a potential problem might be the use of sensitive information, such as personal data that could raise privacy and security issues. Besides the implementation of extensive security

controls like unauthorised access prevention, data encryption and ad hoc firewall policy, there still remain questions about where data is being located.

Type	Technologies
Operating Systems	Ubuntu
Programming Languages	Javascript, PHP, Java
Databases	PostgreSQL, PostGIS
Web/Application Servers	Tomcat, Apache, Geoserver
Frameworks	ExtJS, NodeJS
Application Lifecycle Tools	IDE: Eclipse Version Contro l: git Build Management: -
Open Source Code Repository	N/A

Type	Value
RAM [GB]	12
Disk Storage [GB]	60
vCPUs	8
Network usage [GB]	N/A
Hits/Month	250
Registered Users	691
Maximum On-line Users	N/A
Average On-line Users	N/A

All the abovementioned reqirements also define the tools for managing the applications (e.g. administering, monitoring, automating etc.) and the components of the solution itself. More details about such tools can be found in the installation and cloud administration sections.

5.2 Adaptation of apps

The applications that have been selected to be migrated to the Cloud may require significant changes to take full advantage of Cloud' characteristics such as high availability and scalability. In particular, as application instances are ephemeral and can be started, stopped or fail at any time, they must be stateless and share nothing. All persistent data must go to external services (e.g. databases, file storage, message queues, caches). Applications should be re-architected in order to take full advantage of the Cloud's features, especially when: (Headspring, 2014)

- **Hardware cost is substantial.** Re-architecting an application for the cloud means access to world-class hardware without needing a world-class budget. Companies are able to pay as they go and avoid the investment required for more hardware.
- **IT staffing levels are low.** Moving to the cloud automates a lot of the server and application management, as well as maintenance tasks that would otherwise be performed by in-house IT staff.
- **Geolocation is a requirement.** The cost to do geolocation on the cloud is miniscule since many data centres are located in central regions.
- **The application needs to scale for predicted, but infrequent, uptime.** The cloud allows systems that have occasional spikes, such as an e-commerce application that sees a lot of activity on Black Friday, to quickly and easily scale servers on demand without an expensive hardware investment or footprint.

Determining the right migration strategy for an application depends on its level of cloud alignment, cloud readiness, potential benefits achieved from migrating, and risks. More about the adaptation of apps can be found here.

5.3 Installation

The next step in the migration process is the deployment in the new environment. Depending on the type of workload being considered and the type of target cloud environment chosen, migration might be moving from the non-cloud environment to the cloud environment, cross-platform migration or application only migration (Writer, 2013). During the migration process considerations arise with regards to privacy, interoperability, data integrity, data application portability and security which may cause a high level of complexity. Over the last years a large numer of online tools and services help to simplify this process.

Automated tools can help design the cloud environment and plan the migration. Such tools may be of general purpose or application specific. Most common are automated tools that help setting up the replication of Virtual Machines from on-premises installations to the cloud. For example, automatic deployment can be implemented using OpenStack Heat, the "orchestration engine to launch multiple composite cloud applications based on templates in the form of text files that can be treated like code". The aim of orchestration is to create a human -and machine- accessible service for managing the entire lifecycle of infrastructure and applications within the SCP Cloud environment.

Case Study

Within STORM Clouds project a set of tools and procedures have been designed and implemented. This allows interested cities to automatically deploy selected services from the cloud-based services portfolio and municipalities to re-deploy their services in another CSP. The deployment process took place in four steps:

a) setup of the cloud environment that will host the selected services;

b) perform all the necessary modifications/customisations to services in order to be transferred into the private cloud infrastructure

c) launch the VM instances that will host the applications and their data (e.g. database and file sharing modules).

d) migrated both the applications and their data to the Cloud environment

In STORM Clouds, general purpose tools were used for implementing functions common to all applications running on the cloud platform and promote standard practices in the deployment of the applications as well as on the use of the resources available in the cloud platform (e.g. all the applications use the Object Store for saving backup-data, the name of the backup data set follow the same naming conventions, all the virtual machines hosting applications are named according the same naming conventions, etc.). The STORM Clouds Platform included a library of artefacts used for facilitating the deployment of cloud based applications. These included:

a) a list of prefabricated virtual machines images obtained manually installing the software packages. The images are used as the 'starting point' for manually deploying the application services.

b) Tools for automating the creation of the prefab VM images

c) Tools for automatically deploying the applications.

MAIN STEPS FOR AUTOMATING THE DEPLOYMENT OF SERVICES TO THE CLOUD USING HEAT

The main steps needed for automating the deployment of services to the cloud are presented below.

Step 1: Automate software installation and configuration. Before the automation process bash shell scripts should be implemented to a) configure the VM hosting the application and b) install and configure the application and its dependencies. This is a necessary step as it will ensure that the bash scripts are working properly before moving into creating the Heat template. This way we reduce the complexity of having to identify what went wrong in case the deployment was unsuccessful.

Step 2: Integrate with Heat and execute the template. Create Heat scripts, using the Heat template format that describe the infrastructure (servers, floating IPs, security groups, ports) of the cloud applications, integrating the software installation and configuration scripts made at the previous step.

Step 3: Validation. Validation of the automation process includes functional tests in order to ensure that the deployed application performs as designed.

The automatic deployment is obtained using OpenStack Heat. OpenStack Heat permits the IaaS cloud user to describe all the IaaS objects she needs for an application in a script – called stack – and to "control the entire lifecycle of infrastructure and applications within OpenStack clouds". In this perspective, the activation and deactivation of the IaaS objects can be simply obtained by 'submitting a stack' to Heat that takes care of automatically creating/destroying the listed IaaS objects (e.g VMs, Virtual Disks, etc.).

- The 1st step in the automation process is to prepare the bash shell scripts that will configure the VM hosting the application, and install and configure the application and its dependencies.
- The 2nd step is to create the Heat scripts (Heat Templates) that describe the infrastructure (servers, floating IPs, security groups, ports) of the cloud applications and to integrate with them the application's installation and configuration scripts made at the previous step.

The available Heat Templates allow interested cities to automatically deploy the selected applications from the cloud-based service portfolio, as well as the municipalities to re-deploy their services in another instance of STORM CLOUDS Platform. It does not require any architectural change of the applications, while the application owner has full control of the resources used for deployment.

5.4 Testing

Cloud scalability does not always eliminate application performance problems, and even after migrating to the cloud, applications might not scale up correctly (Pelerin, 2015). Performance testing aims to ensure that the deployed applications are fully functional and that they meet the initial set of requirements regarding cloudification. It also helps to solve issues such as database errors or application and website crashes. Testing should be done periodically and include general performance and compatibility tests, stress and load tests and security/vulnerability tests.

Validation of the automation process and functionality tests: Tests to ensure that the automation process is working well and the application performs as designed (e.g. the users can log in, capha works, google maps can be shown etc). For this test stakeholders should be involved as much as possible. More about monitoring and validation methodologies can be found here.

Stress and load tests: These tests evaluate the maximum load that the application can support, highlight potential weaknesses and size the cloud machines on which applications are deployed. There is a plethora of open source load test tools that can be used in the cloudification process, such as JMeter, the Grinder, Garling, lsung etc.

Security tests: security testing is a multilevel exercise that includes software performance and vulnerability assessment and it should be applied in different phases of the migration process. An entire section dedicated on security can be found here.

DISASTER PREVENTION AND RESTORING USING HA

In information technology, High Availability (HA) refers to the availability of systems and/or components in the aftermath of a failure. Availability is measured relative to "100% operational" or "never failing". HA can be implemented using clustering, in order to increase the systems uptime. Generally speaking high availability is implemented using a group of machines, collectively called a **high availability cluster**, where the workload of a failed machine is automatically and quickly taken over by a different machine in the cluster. The main steps to perform such a task is to update the database related configuration files and then to perform the validation, using the same tools with the automation process described before.

6 Administration of the cloud

6.1 Administration

Cloud Computing imposes new concepts and challenges for the role of monitoring and management of the Cloud environment and the smart city applications. The System Administrator no longer needs to provide servers, install software and wire up network devices since all this work is replaced by few clicks and command line calls. Nowadays, most of the daily tasks performed by system administrators are related with the applications.

The Cloud environment should offer both to system administrators and application owners the necessary tools required to manage and maintain the platform and the deployed applications. Using these tools, they can focus on how to optimize the cloud-based application in order to increase cost savings. The "pay for what you use" approach of the Cloud, leads application owners to strive to optimize the system whatever possible. Even a small optimization might result in thousands of euros of savings.

Case Study

The STORM CLOUDS Platform includes features that both the platform administrator and the application owners can use for managing, monitoring and administering the platform's components as well as the applications running in the cloud. The actions that a user can perform, depend on his/her role: the platform administrator has full control on all the components deployed in the cloud while application owners have full control of their applications and can perform only some actions on the platform components. For instance, application owners have full control over databases and shared volumes used by their applications but they do not have any control on databases and shared volumes used by other application owners. The following management and monitoring tools are available:

- **The Platform Administrator's Console**, which allows the SCP administrator to have full control of the layers of the platform. Through the console, (s)he can manage the databases, the filesystem, the IaaS layer, and the PaaS layers.
- **The Database Administration Console**, which allows administrators and applications' owners to administer the supported databases. The module includes phpMyAdmin for MySQL administration and phpPgAdmin for PostgreSQL. Both tools implement very similar functions for the corresponding database engines like creating, modifying and deleting database users, databases and database objects (e.g. tables, indexes, etc.), submitting queries, importing/exporting data, managing database accounts, etc. The platform's administrator has full control of all databases and configures database accounts for the application owners, giving them the rights of managing only the database objects created for their applications.

Details about additional tools, i.e. a monitoring console, a back up tool and an automation tool can be found in the respective links.

6.2 Analytics

Administration platforms are usually accompanied by monitoring tools that facilitate data analysis in order to find meaningful insights and empower administrators with knowledge that lets them optimize their cloud systems. Monitoring tools are used for cloud monitoring, performance management, automation, cost management etc. Over the last years, a number of cloud monitoring tools have been developed including Nagios, Prometheus and Zabbix (open source), CloudMonix, New Relic, AppDynamics, etc. These provide the ability to collect and visualise information using table and graphs, analyse historical trends, create alerts and conduct a variety of functions from a single web-based console.

Case Study

In STORM Cloud Project a **Monitoring Console** was developed, which monitors the resources (CPU load, disk

space occupation, network traffic, number of processes, etc.) used by the platform's services or by the applications. The module, implemented using Zabbix[1], continuously gathers information from the servers under control and, in case one or more parameters reach a threshold value, it notifies the operator by e-mail, Instant Message or SMS. Zabbix offers several monitoring options ranging from simple checks for verifying the availability/responsiveness of a server, to sophisticated measurements of parameters like CPU load, disk volume occupation, network traffic, number of processes, etc. Zabbix provides several ways for representing monitoring data in both graphical and textual/tabular format.

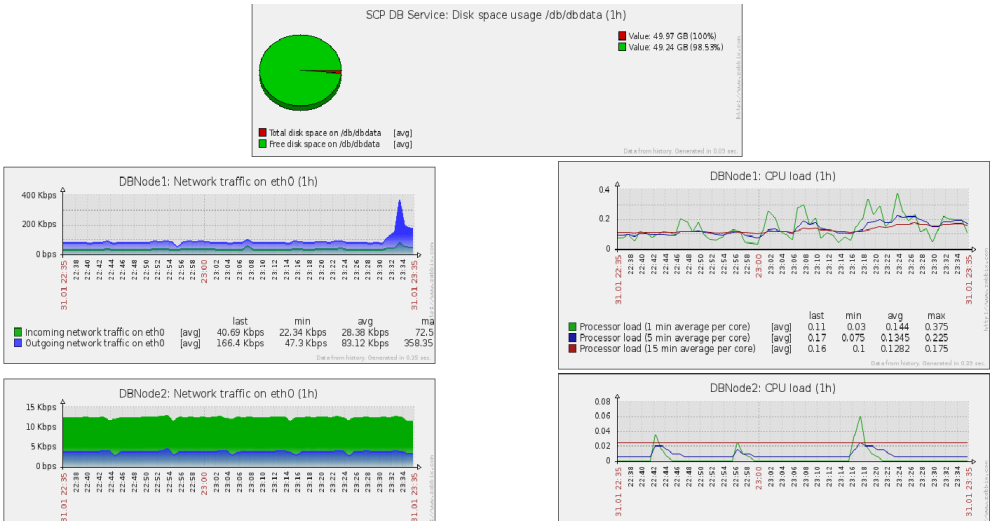

Figure 4: Zabbix Monitoring Pages

6.3 Backup

Backup is the process of making a secondary copy of data that can be restored to use if the primary copy (the production copy which is the official working copy of the data) becomes lost or unusable. Backups usually comprise a point-in-time copy of primary data taken on a repeated cycle – daily, monthly or weekly.

It is the most important means to keep the data from being lost due to intentional or unintentional access. It is also important to encrypt the up-to-date backups. Backup is easiest and the most familiar process for most situations. A backup copy is used to recover data needed to restart an application correctly.

Backup may be required in the following scenarios:

- **Logical corruption**. That can happen due to application software bugs, storage software bugs or hardware failure, such as a server crash.
- **User error**. Where an end user may accidentally or intentionally delete a file or directory, a set of emails or even records from an application.
- **Hardware failure**. In the form of hard disk drive (HDD) or flash drive failure, server failure or storage array failure.
- **Hardware loss.** Possibly the worst case scenario where an event such as a fire results in hardware being inoperable and permanently unrecoverable.

The following backup service levels exist:

1. Recovery Point Objective (RPO).
2. Recovery Time Objective (RTO)

[1] *Zabbix – Main Page*, viewed November 10, 2015 <http://www.zabbix.com>

6.4 Interoperability

Interoperability is "*the ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged*" (ITU-T, 2002). In the context of Cloud Computing, interoperability can be further described as the "*capability of public clouds, private clouds, and any other systems in the enterprise to understand each other's application and service interfaces, configuration, forms of authentication and authorization, data formats etc. in order to cooperate and interoperate with each other*"(ISO/EC, 1994). In our case, interoperability could be understood as how well a public administration service interacts with external entities in order to organise the efficient provisioning of its public services to other public administrations, businesses and or citizens.

The European Commission's ISA (Interoperability Solutions for *European* Public Administrations) programme (EC, 2016) developed an Interoperability Maturity Model (IMM)[2] to provide public administrations insight into two key aspects of their interoperability performance:

- **The current interoperability maturity level of a Public Service;**
- **Improvement priorities to reach the next level of interoperability maturity.**

The IMM helps owners of a Public Service to enhance the quality of the service delivery, reduce costs and overcome integration issues by reusing available services and orchestrate services in an effective manner to maximise service outcome and benefits for citizens and public administrations (EC, 2013).

In the context of interoperability maturity, the IMM measures how well a public service is able to interact with other organisations to realise mutually beneficial and agreed common goals through the exchange of information and reuse of services. Three different domains of interoperability are distinguished:

- **Service Delivery** – Providing end-users accessibility to the public service
- **Service Consumption** – Consumption of reusable services from other public administrations and businesses. This can include the consumption of functionalities, base registry information and security services
- **Service Management** – Controlling and monitoring the process flow related to external service interactions from trigger to outcome

RECCOMENDATIONS FOR INTEROPERABILITY

- Principle 1: Each interoperability attribute differentiates between at least two maturity levels;
- Principle 2: The improvement tables provide recommendations how to improve maturity step-by-step for a specific interoperability attribute;
- Principle 3: When a public service does not have the maximum level yet for a specific interoperability attribute, a recommendation is given to make the step towards the next interoperability level;
- Principle 4: When a public service does have the maximum level for an interoperability attribute, no recommendation is given;
- Principle 5: When the foreseen maturity improvement is a sliding scale (e.g. from less to more), a generic recommendation (not maturity level specific) is given to improve the maturity further along the sliding scale.

[2] https://joinup.ec.europa.eu/elibrary/document/interoperability-maturity-model

7 Data Management

7.1 Ethics

The popularity of the "smart city" is growing as a route to city management. A key issue is that city municipalities operate in a legal context – they are data controllers for a good deal of citizen focused data, much of which is sensitive, personal and highly regulated. Minicipalities are also are trusted bodies, and citizens expect that their approach to data collection, retention, storage and sharing is in line with these responsibilities.

New technologies, particularly where they are being created by private sector businesses, look to build on the advantages of innovation, often ahead of the ethical framework. Cloud computing for example is a technical and social reality, and also an emerging technology which is rapidly expanding. When moving from traditional servers to a cloud paradigm, the technological foundations change as well as the implication regarding Ethical issues. For this, early recognition of ethical and related issues is essential. Timmermans, J et al, (2010) three areas of ethical concern are raised:

- The shifting of control from technology users to the third parties
- The storage of data in multiple physical locations
- The interconnection of multiple services

Through the identification of ethical issues arising from these new functionalities, it is possible to inform and raise awareness to vendors, users or system designers of ethical questions, in order for them to be proactive in assessing their role in specific implementations and uses. The main challenges from an ethical point of view are:

Control: Cloud computing entails the outsourcing of Information Communication Technologies (ICT) tasks to third party service providers (Haeberlen, 2010; Kandukuri and Rakshit, 2009). As such, information that once used to be stored in local premises is now stored in the cloud. Users therefore place data on machines that are not directly controllable and therefore renounce control these resources and data. As mentioned by Paquette (2010) risks associated with this change of control in cloud computing mainly rely in data corruption, infrastructure or system architecture failure or unavailability/outing and unauthorized access by third-parties. Ethical problems arise in times of disaster or simply if something goes wrong. In fact, it is hard to distinguish the entity that has originated the problem, to the point that, as mentioned by Haeberlen

A THREE STEPS ETHICS STRATEGY

A recommended ethical issues strategy is based on the following three tasks:

1. **Proactivity:** It is urgent that all parties involved in cloud computing are proactive, in order to anticipate unforeseeable consequences. Players shoul never use uncertainty to refrain from designing and providing services that invite moral sound use and inhibit undesirable or controversial actions. It is thus recommended as ethical for Cloud providers to have a **Terms and Conditions** available and for users to know Terms and Conditions of providers.
2. **Regulations and policies:** All technology should be subject to regulation arrangements at least just enough to have innovation leading towards the benefit of society and not enough to have it limit innovation. In any case, regulations can have ethics integrated into technological development and use. It is vital that governance arrangements are more conducive to the inclusion of ethics, including regulations for private companies, which are usually much less subject to ethics-related oversight and more towards profit generation. Such regulations will adapt as cloud computing evolves, similar to what happened with labour law year ago. In the latter case, it is important to remember the core definition of corporate responsibility and follow policies defined by the European Union, such as the ISO26000.
3. **Responsible Research and Innovation:** Responsible Research and Innovation (RRI) has a particular importance since it can be defined as an inclusive approach to Research & Innovation (R&I), aiming at better aligning both the process and outcomes of R&I with the values, needs, and expectations of the society, notably through reinforcing public engagement, open access, gender dimension, ethical issues, and (formal and informal science) education.

(2010), it is almost impossible to hold someone accountable and responsible for a problem in a dispute, when lacking strong supporting evidence. In addition, the de-parameterisation1 shadows the border of organizations IT infrastructure and consequently disguises their accountability.

Responsibility: Since responsibilities are divided between customer and provider of the service, neither is in position to address emerging problems (Haeberlen, 2010). In cloud computing a service delivered to a user depends on another system that also depends on other systems. A cloud service to the end-users may use service-oriented architecture (SOA) where functionalities aggregate services into larger applications. Once again, ethical problems arise in times of disaster or simply if something goes wrong. By having a highly multifaceted structure of cloud services, it is most certainly difficult to determine who is responsible in case of an undesirable event. This lead to a severe ethical problem called the "Problems of many hands", that dictates that in a complex chain of systems where people a share in an action that leads to undesirable consequences, many people have also had the opportunity to prevent these consequences, and therefore no-one can be held responsible (Pieters and van Cleeff, 2009).

Accountability: Accountability is a concept with many different dimensions, but in its core meaning, accountability refers to the existence of a relationship whereby one entity has the ability to call upon another entity and demand an explanation and/or justification for its conduct (Alhadeff et al, 2012). In a de-parameterised world the border of an organization accountability blurs and becomes less evident. Personal data stored in the cloud should be managed accordingly, as not doing so would not be ethical by all persons involved in that process. Users of cloud should be empowered by being able to check whether the cloud is performing the agreed the provision of accountability transparency and clear allocation of responsibility, as when recorded, these elements can be used to decide who is responsible whenever a problem occurs or dispute arises. In 2010, the Article 29 Data Protection Working Party issued an Opinion on the principle of accountability in which it elaborated upon the possibility of including a general provision on accountability in the revised Data Protection Directive.

Ownership: The storing of data in different location premises also raises the question of who owns the data a user stores in the cloud. By doing so, the IT admins, engineers, and troubleshooting agents of a provider of cloud services all have access to this information (Murley, 2009). Moreover, the cloud also generates data itself for different purposes, such as providing accountability, improving services provided, or security performance or security. Digital interactions and tracks are thus being gathered together through unique identifiers and algorithms, which leaves a trail of personal information. There is an ethical duty to not access this information with harmful intent or reckless behaviour, either by providers or third-parties such as hackers (fraudulent use), or it may be accessed and used in ways that individuals did not envisioned.

Also, information stored with a third party can be of easy access to Government agencies and private litigants more easily than from the original owner or creator of the content. This causes a severe ethical issue has to whether it righteous or not to do so, even by Public Authorities figures.

Ownership problems also incur in situations related with infringements on copyrights, since access to massive computing storage, cloud services might facilitate sharing copyrighted material (Nelson, 2009).

Lock-in: According to Nelson (2009), if only a limited number of companies are able to achieve a dominant position in the market for cloud services due to economies of scale, this might lead to abuse user needs. Users would become dependent on certain cloud service providers, be it infrastructural or intermediaries. Several ethical risks might exist from these unwanted dependencies on cloud service providers and vendor lock-ins. With little emphasis on interfaces that guarantee data and service portability users may face difficulties migrating from one provider to another or to migrate their data and services back to an in-house IT environment. Similarly, if a service provider ends its operation in the market, not along the data privacy that will be mentioned at a later stage, the possibility to migrate data must be possible. Ethically, such concerns are of vital importance and must be tackled in order to introduce independence from a particular cloud providers and vice versa.

Legal: Providers also need to take into account the laws a specific country follows in terms of data privacy. It is ethically correct to respect customers' laws and companies should might store data in jurisdictions that may not respect the rights of their users and customers. Favourable privacy laws represent important challenges that need to be faced ethically.

Privacy: As stated above, many companies providing cloud services collect data, much of it consists of sensitive personal information, which is then stored in data centres in countries around the world. Whenever ethical issues arise concerning information about persons they are typically cast in terms of privacy (Stahl, et al, 2010). Privacy aims to constrain access to certain types of personal data and prevent persons to acquire and use information about other persons. Consumers need to trust their cloud provider that certain personal information will not be exposed, as according to their terms that have been previously accepted by the users.

7.2 Privacy & Data

Privacy is understood as the right of a person to have his/her personal data properly secured. Moreover, it is related with the ability of a person to control, edit, manage and delete information about them and to decide how and to what extent such information is communicated to others (Ico, 2014). Data protection is the process of safeguarding important information from corruption and/or loss (Microsoft, 2014).

Cloud services make it easier for Public Authorities to take advantage of opportunities to share information. For example, sharing personal information with another public Authority or Agency may be achieved by simply creating user accounts with the appropriate permissions within a SaaS solution rather than having to implement a system-to-system interface to exchange information. Although cloud services have the potential to lower the technical barriers to information sharing Public Authorities must ensure that they appropriately manage access to personal information and comply with the requirements of the European and National Privacy Legislation.

Cloud providers should commit to protecting the data and limit the use of them. The data that Public Authorities host in cloud services belongs to them—and should not be used by a cloud provider for purposes other than to provide the customer's service. Moreover, cloud providers should not use customer data for purposes unrelated to providing the service, such as advertising. Additionally, each service has established a set of standards for storing and backing up data, and securely deleting data upon request from the customer.

The best-designed and implemented service cannot protect customer data and privacy if it is deployed to an environment that is not secure. Customers expect that their data will not be exposed to other cloud customers. They also assume that the processes used at the datacentre, and the people who work there, all contribute to keeping their data private and secure.

The main threats to privacy in a cloud computing environment are:

- Lack of User Control
- Lack of Training and Expertise
- Unauthorized Secondary Usage and Loss of Trust
- Complexity of Regulatory Compliance
- Transborder Data Flow
- Litigation
- Legal Uncertainty

In 2014, the International Organization for Standardization (ISO) adopted ISO/IEC 27018:2014, an addendum to ISO/IEC 27001, the first international code of practice for cloud privacy. Based on EU data-protection laws, it gives specific guidance to cloud service providers (CSPs) acting as processors of personally identifiable information (PII) on assessing risks and implementing state-of-the-art controls for protecting PII (ISO, 2014).

The new standard sets out best practices for public cloud service providers. It establishes security guidelines to protect personal data and provides a privacy compliance framework that addresses the fundamental obligations of a data processor under EU data protection laws. Any organisation that processes PII through a cloud computing service under a contractual arrangement can be certified under ISO 27018 – this means all types and sizes of organisations, including public and private companies, government entities and not-for-profit organisations, are eligible. To qualify for certification under ISO 27018, the applicant provider must agree to be audited by an accredited certification body and must also submit to periodic third party reviews.

Public Authorities can use this standard as an independent measure when evaluating and comparing privacy controls of potential public cloud service providers. An essential step is the signature of the service level agreement with the cloud provider. The agreement defines, among other things, a privacy policy prescribing where and how the organization's data is stored, processed and used (i.e. accepted and prohibited uses) by the cloud service provider. It should also define some privacy related measures and technical controls to be applied on the cloud side, such as the vetting of employees, breach notification, isolation of tenant applications, and the use of products certified to meet national or international standards.

Although the agreement covers a lot of privacy issues, the lack of physical control by cloud users over data storage, and the absence of standardised and mature techniques for monitoring how data is accessed, processed and used inside the cloud, it is harder to verify a cloud's compliance with such privacy policies.

In addition to the evaluation of cloud provider, Public Authorities should also assess their Smart City services to identify issues that may lead to infringing users' privacy. This applies mainly to applications that keep personal information or handle payments. In the first case the application must comply local laws about storing personal data, including any rules about the location of data centres, such as the EU Directive on data Protection [1] while in the second with any rules about safe payments, such as the Payment Card Industry's Data Security Standard (PCI DSS)[3].

BACK UP STRATEGY PLAN

4. Analyse the type of data and usage
5. Set up a limit for the back up volume
6. Identify software tools for back up
7. Select the more appropriate back up policy
8. Choose where to store back ups

However, there are many Smart City infrastructure management applications, such as applications related to public transport, street lighting or road traffic management that do not fall into any of the above categories, and for these data privacy is not such an issue. Agencies planning to place personal information on a cloud service should perform a Privacy Impact Assessment (PIA) to verify that privacy requirements are adequately addressed.

The STORM CLOUDS approach

The STORM CLOUDS Smart City services have been evaluated regarding privacy issues. The involved Public Authorities in collaboration with the applications' developers perform a Privacy Impact Assessment (PIA) to ensure that they identify any privacy risks associated with the use of the services together with the controls required to manage them effectively.

The privacy impact assessment questionnaire, about the type of information collected and its usage.In order to drive consistent privacy practices during the development of new Smart City Applications, the Public Authorities should define a privacy framework, which will define standard privacy features and practices. Because security is critical to privacy, the alignment of complementary privacy and security processes helps minimise vulnerabilities in software code, guard against data breaches, and helps to ensure that developers factor privacy considerations into Smart City Services. More about privacy issues can be found here.

In STORM Clouds a detailed back up strategy was developed and implemented based on the data requirements of the services and the architecture of the SCP. The backup process aims to best exploit the features implemented by the IaaS cloud where the VMs are hosted and more specifically Swift, the Object Storage Service implemented by OpenStack. The main steps needed for backing up application's data are presented below.

1st Step: Design a Backup Strategy. During this step, several aspects related to the data and/or the application(s) managing the data were analysed in order to put together a list of what needs to be backed up, when to backup, how long to keep the backup data and how long it takes to restore. It includes the following tasks:

- **Analysis of current data usage** that reveals:
  - Types of data used.
  - Data locations, including folders and/or databases.

[3] PCI Security Standards Council, viewed June 2, 2016, https://www.pcisecuritystandards.org

- Approximate amount of data.
- How often data changes, as this affects our decision on how often the data should be backed up.
- Data sensitivity. For critical data, such as a database, we should have redundant backup sets that extend back for several backup periods. For sensitive data, we should ensure that backup data is encrypted, using public/private key-pair technology.
- How quickly we need to recover the data.
- What's the best time to schedule backups (scheduling backups when system use is as low as possible will speed up the backup process).

- **Set an up limit for the backup volume** as the amount of data we need to backup is only going to increase as time goes by.
- **Identify the software tools that will be used**
- **Select the appropriate backup type/policy** (Full or Incremental). Typically, one of the following approaches is used: (a) Full daily, (b) Full weekly + Incremental daily. The process of taking incremental backups following an initial full backup is known as data deduplication. The final choice depends on the required performance levels and data protection levels, the total amount of data retained and the cost associated with it, since cloud storage space comes at a cost that depends on the service provider.
- **Choose where to store the backups**. Using the cloud environment to store the backup data is arguably more resilient to disaster than other technology solutions because it is not physically located at the same place as the organisation. Moreover, since the applications are hosted in the Cloud we also save bandwidth and time taken to transfer the files needed to restore the application correctly. However, the cost associated with storing the backup data in the cloud is a significant factor in our decision.

2nd Step: Generate a Key-Pair on the Client Machine

Although we can create the key pair directly on the VM, it is good practice to keep a copy of the keys outside the VMs using them. The reason is that VMs are "ephemeral", meaning that once a VM is deleted, we are not anymore able to decrypt our backup data when restored. Moreover, creating key-pairs requires some level of "entropy" for ensuring randomness in the generation.

3rd Step: Prepare the VMs for Backup

Install and configure

4th Step: Implement the Backup Strategy

The backup scripts that address all the aspects of backup strategy are created and executed using the Duplicity tool.

5th Step: Validation tests.

Validation includes tests on the restore mechanism. More specifically both incremental and full backups were used to bring the applications to a previous operational state successfully. The backup solution should be tested many times after it has been implemented in order to ensure that it is working as intended. Moreover, the applications should be re-tested periodically to ensure they're functional, and data is being backed up appropriately. Validation not only will help us to identify problems in the backup process but will also train the Municipalities' IT personnel to recover quickly and efficiently the files if this becomes necessary.

After the initial setup the backup process is scheduled according to the backup strategy.

7.3 Ownership

The storing of data in different location premises also raises the question of who owns the data a user stores in the cloud. By doing so, the IT admins, engineers, and troubleshooting agents of a provider of cloud services all have access to this information (Murley, 2009). Moreover, the cloud also generates data itself for different purposes, such as providing accountability, improving services provided, or security performance or security. Digital interactions and tracks are thus being gathered together through unique identifiers and algorithms, which leaves a trail of personal information. There is an ethical duty to not access this information with harmful

intent or reckless behaviour, either by providers or third-parties such as hackers (fraudulent use), or it may be accessed and used in ways that individuals did not envisioned.
Also, information stored with a third party can be of easy access to Government agencies and private litigants more easily than from the original owner or creator of the content. This causes a severe ethical issue has to whether it righteous or not to do so, even by Public Authorities figures.

Ownership problems also incur in situations related with infringements on copyrights, since access to massive computing storage, cloud services might facilitate sharing copyrighted material (Nelson, 2009).

8 Validation and Monitoring

The monitoring and validation process, for the successful migration of the selected applications to the Cloud, targets the business aspects of the applications rather than the technological ones. This approach is more holistic as the successful migration in business terms implies the success of the technical one. Validation can be done in different perspectives, such as:

- Validation of the services deployed. This includes the service itself utilizing feedback both from the stakeholders and from the technical staff.
- Validation of the migration process of existing applications on the cloud that public authorities want to utilise.

Cloud migration of public services is not a process visible to the citizens, therefore, their validation of the migration process might be limited. However, the leadership of the top management of the organisation is essential. Technical people in charge of migration will have to consider political cycles and be prepared for changes in the management structure. There may be internal personal in the Municipalities that is reluctant to change. Therefore change management policies must be foressen and put in practice from the very begining. These actions may require training activities on personal to adapt their copetencies to a new IT environment.

In order to monitor from a technical point of view, one has to consider the following aspects:

- Before going into a migration process, it must be checked that all the documentation for the applications is available. If this is not the case, the impact must be evaluated.
    - It is particularly important to have a detailed technical plan to safeguard that all the required elements will be available prior to the migration. This refers to aspects such as source code, documentation, availability of technical support either internal or external, similarities/diferences between the existing IT environment and the cloud environment and how to cope with these differences (e.g. O.S. versions) etc.
- The availability of trained personnel for the new environment is to be ensured. Either by training the existing technical people or by hiring new personnel.
- The ownership of applications to be migrated must be ensured before the process is to start. Existing applications may be locked in by legal agreements with vendors.
- Security and Data privacy are a serious concern. The technical staff must ensure them and communicate effectively to the management.

The STORM CLOUDS approach

The process consists of three different steps: i) identifying the aspects to monitor and the specific indicators or criteria (depending on the task), ii) information gathering throughout the entire process of cloudification, and iii) analysis of the usage and acceptance of the new applications and/or variations on the usage patterns. The main indicators that usually apply to this process are the following: indicators monitoring the supply side of the service, indicators monitoring the demand side of the service, indicators related to dissemination, indicators related to validation of the service and, finally, indicators showing the financial benefits of migrating an application to the cloud.

As an example, the following two figures present the indicators for “Virtual City Market” and “CloudFunding” applications, which have been cloudified for the Municipality of Thessaloniki. Some of the indicators are common between the two applications, mainly those that are related to the dissemination and validation aspects. On the contrary, the indicators for the supply and demand sides are mainly different as they are tailored to the context of the applications.

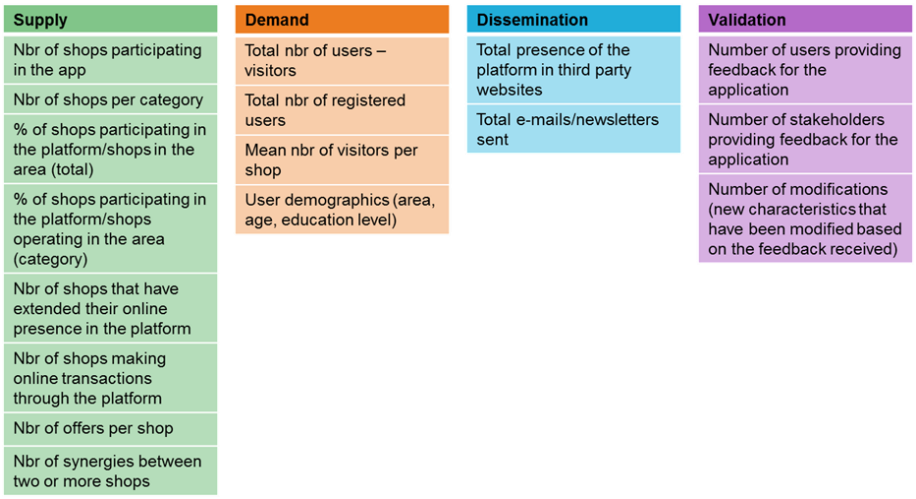

Figure 5 – Monitoring and validation indicators for the Virtual City Market application

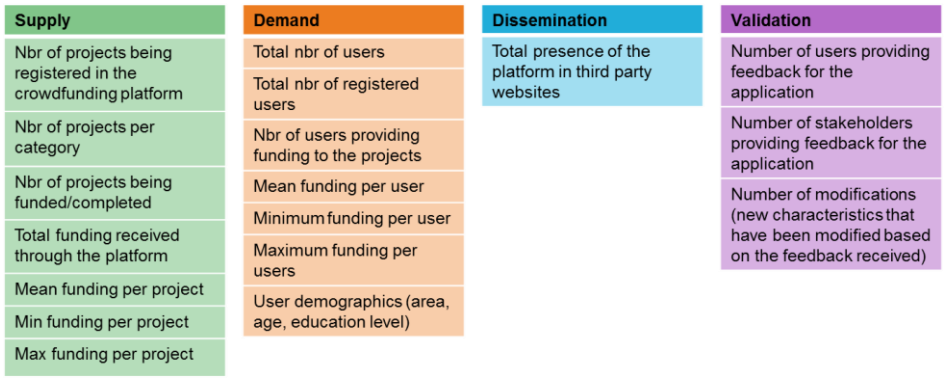

Figure 6 – Monitoring and validation indicators for the CloudFunding application

9 Security

Cloud computing security is an evolving sub-domain of information security and refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure[4]. There are a number of security concerns associated with cloud computing, which can be broadly classified in two categories: (a) issues faced by Cloud Service Providers (CSPs) and (b) issues faced by their customers. Providers must ensure that their infrastructure is secure and clients' data and applications are protected; customers, on the other hand, must ensure that their provider has taken appropriate security measures to protect their information. The security expectations and obligations of both supplier and user are described in Service Level Agreements (SLAs) (Gianakoulias, 2016).

Organisations need to understand the specific security requirements, regarding data protection, audits, etc., and any regulations that are applicable to a particular application that they are looking to move to the cloud. To achieve this, they should map every application that is a candidate for migration to cloud computing to a set of security, governance, and compliance issues that are specific to that application. Thus, they have the ability to understand the application requirements, and how the migration and re-development effort to the cloud should impact application operations.

The UK's National Technical Authority for Information Assurance, which provides advice on Information Assurance Architecture and cyber-security to UK government and the wider public sector and suppliers to UK government, published 14 security principles to consider when evaluating cloud services, and why these may be important to an organisation[5].

Cloud Security Principle	Description
1. Data in transit protection	Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.
2. Asset protection and resilience	Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.
3. Separation between consumers	Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.
4. Governance framework	The service provider should have a security governance framework that coordinates and directs their overall approach to the management of the service and information within it.
5. Operational security	The service provider should have processes and procedures in place to ensure the operational security of the service.
6. Personnel security	Service provider staff should be subject to personnel security screening and security education for their role.
7. Secure development	Services should be designed and developed to identify and mitigate threats to their security.
8. Supply chain security	The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.

[4] *What does the Commission mean by secure Cloud computing services in Europe?,* 2013, European Commission, viewed November 10, 2015 <http://goo.gl/M0Rqia>

[5] Cloud Security Guidance: Summary of Cloud Security Principles, viewed June 24, 2016 <http://goo.gl/mUf5c2>

9. Secure consumer management	Consumers should be provided with the tools required to help them securely manage their service.
10. Identity and authentication	Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.
11. External interface protection	All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.
12. Secure service administration	The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.
13. Audit information provision to consumers	Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.
14. Secure use of the service by the consumer	Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.

Table 5 - Cloud Security Principles (Source http://goo.gl/mUf5c2)

Consumers of cloud services should decide which of the principles are important, and how much assurance they require in the implementation of these principles, while providers of cloud services should consider these principles when presenting their offerings to public sector consumers. This will allow consumers to make informed choices about which services are appropriate for their needs.

The STORM CLOUDS approach

In order to achieve a clear understanding of the security requirements of both the SCP and the Smart City applications, the following vulnerability scanning tools were used to scan web applications to look for known security vulnerabilities, such as ZAP, OpenVAS, SQL Inject Me, Qualys SSL Server Test, Vega etc.

The security testing identified a number of critical security issues resulting in applications' modifications in order to address them. In particular, the following issues were fixed:

- "Cross Site Scripting" (XSS) security risk, being the most prevalent web application security flaw, whereby an attacker's malicious content is supplied to our application as a result of that content not being properly validated or escaped. To address it we used the OWASP ESAPI reference implementation for HTML entity escaping and unescaping as well as JavaScript escaping and unescaping.
- "Directory listing" security risk, whereby an attacker can simply list directories to find files. To address it we have updated the Apache configuration file by removing the *Indexes* from the file.
- "Insufficient Transport Layer Protection" security risk, caused by not requiring SSL (at least for all sensitive pages) allowing an attacker that monitors our network traffic to obtain an authenticated victim's session cookie, itself then replayed to take over the user's session. To address it we have included an HTTPS certificate and requested that all traffic is forwarded to the secure connection (HTTPS). However, new vulnerabilities introduced by the HTTPS certificate, such as the RC4 cipher and the POODLE attack vulnerability, resulted in the disabling of:
    - TLS 1.0 compression and weak ciphers
    - SSL 3 in our browser and our servers
- "Clickjacking" security risk, caused by an attacker that is "hijacking" our clicks meant for the application page and routing them to another malicious page. To address it we send proper X-Frame-Options HTTP response headers that instruct the browser to not allow framing from other domains. This is done at the Apache configuration file.

Regarding the use of the above-mentioned tools, one should always check the terms of service of the selected CSP to determine whether running security tests on the CSP infrastructure is allowed, even if own machines are the target. If this is not so, either a CSP that allows penetration tests on own VMs must be chosen, or have tests run on a development or testing environment before deployment to the production environment.

In order to enhance the authentication process, applications have been updated to support session expiration, thus minimizing the time available to an attacker who uses a valid session identifier. In order to balance between security and usability, applications have properly selected the timeout values, allowing users to complete their operations without frequent session expirations.

The acquisition of SSL certificates is necessary for protecting *data in* motion. The Apache server was configured to forward all traffic to the secure connection. However, as applications don't deal with sensitive data no encryption is applied for data at rest, apart from the OpenStack object storage that is protected using LUKS (Linux Unified Key Setup or LUKS is the standard for Linux hard disk encryption).

Virtualization technologies have their own vulnerabilities such as those coming from the virtual switch, those coming from reallocation of resources from one VM to another and vulnerabilities coming from the remote administration port that is turned on by default on all VMs. To respectively address these attack vectors:

- We've used layered security mechanisms to increase the security of the system as a whole. This was achieved using OpenStack security groups in order to define a number of IP firewalling rules that describe what kind of network traffic is allowed to go to or come from the VMs. With this solution even if a VM is compromised the security group rules continue providing the required level of security because they are implemented in the host operating system.
- We've used OpenStack functionality for zeroing all data used by a virtual resource once the resource is released.
- We associated each VM with a valid SSH Keypair. This was then forwarded to the application owners in order to allow them to access the VM instances given the public IP address the VM is configured to use.

Finally, securing our cloud infrastructure means not only implementing controls for the layers we are able to do so, but also auditing our CSP regarding actions taken to lock-down the tenant instances. We must conduct our own analysis of our needs, and assess, select, engage and oversee the cloud services that can best fulfil those needs.

USEFUL TOOLS FOR SECURITY TESTING PURPOSES

The tools needed in order to facilitate the process are identical to the automation procedure.

The penetration testing tools needed to facilitate the security testing procedure are:

1. An **OpenVPN client**[2] installed on the client machine used for the security testing procedure, in order to access the cloud environment;
2. **Zed Attack Proxy** (ZAP)[3], installed on the client machine used for the security testing procedure;
3. **OpenVAS**[4], installed on the client machine used for the security testing procedure;
4. **SQL Inject Me**[5], installed on the client machine used for the security testing procedure;
5. **Qualys SSL Server Test**[6], installed on the client machine used for the security testing procedure;
6. **Vega**[7], installed on the client machine used for the security testing procedure.

10 Conclusions

The report presents a roadmap of five sequential steps (services and applications, cloud environment, migration of applications, cloud administration, data management) and two parallel procedures (security and validation/monitoring). The content of this roadmap is presented in an interactive, tree structured navigation tool, available through the STORM Clouds website (http://www.storm-clouds.eu/services/resources/roadmap/).

It is based mainly on two deliverables: D5.1.2-Body of knowledge about migration of public services to the cloud and D3.4.2-Best practices for cloud-based public services deployment. However, it draws insight also from all other deliverables and activities undertaken throughout the project period.

The report is part of WP5 of the STORM CLOUDS project aims 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.

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).

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] Alhadeff, J., van Alsenoy, B., and Dumortier, J. (2012) The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions, Managing Privacy through Accountability, pp. 49-82, doi: 10.1057/9781137032225_4

[5] Amazon Web Services (2017) *10 Considerations for a Cloud Procurement*, Available online at: http://bit.ly/2oRo4sl [Accessed March 23, 2017].

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

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

[8] Australian Government (2012) *A Guide to Implementing Cloud Services*, Available online at: http://bit.ly/1BVy181 [Accessed June 5, 2016].

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

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

[11] Battarra, M., Consonni, M., De Domenico, S., & Milani, A. (2016). Storm Clouds Platform: A Cloud Computing Platform for Smart City Applications. *Journal of Smart Cities*, *2*(1).

[12] Barnaby, P. (2010) *Cloud Computing: A Guide for Business Managers*, ICAEW, Available online at: http://bit.ly/2otrIWM [Accessed March 22, 2017].

[13] 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

[14] 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

[15] Brophy, T. (2016) 7 Cloud Migration Considerations, Network Computing http://www.networkcomputing.com/cloud-infrastructure/7-cloud-migration-considerations/1926792235 [Accessed March 31, 2017]

[16] 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

[17] 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

[18] Cloud Security Alliance (CSA) (2016) *A Repeatable Cloud-first Deployment Process Model*, Available online at: http://bit.ly/2ox9nHz [Accessed March 22, 2017].

[19] 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

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

[21] Cloud Standards Customer Council (CSCC) (2015b) *Practical Guide to Cloud Service Agreements (Version 2.0)*, Available online at: http://bit.ly/2j7XFCn [Accessed June 5, 2016].

[22] 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

[23] Crisp Research AG (2014) *Open Cloud Alliance: Opennes as an Imperative*, Available online at: http://goo.gl/db8fZr [Accessed November 9, 2015].

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

[25] 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

[26] Environmental Protection Agency (EPA) (2017) EPA Hosting Readiness Assessment Process, https://developer.epa.gov/guide/wp-content/uploads/sites/3/2016/04/conops_epa_cloud_readiness_508_092116.pdf [Accessed, 31 March 2017]

[27] Eskelinen, J., García Robles, A., Lindy, I., Marsh, J. & Muente-Kunigami, A. (2015) *Citizen-Driven Innovation – A Guidebook for City Mayors and Public Administrators*. World Bank and ENoLL. Available online at: http://bit.ly/1IF6WaS [Accessed March 18, 2017].

[28] 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

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

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

[31] European Commission (EC) (2016), Interoperability Solutions for European Public Administrations Programme, viewed June 2, 2016 <http://ec.europa.eu/isa/>

[32] 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

[33] Frost and Sullivan (2011) *Tips for Choosing a Cloud Service Provider*, Available online at: https://ibm.co/2plUvkr [Accessed March 23, 2017].

[34] Giannakoulias, A. (2016) Cloud computing Security: protecting cloud-based smart city applications, Journal of Smart Cities, Vol.2, No. 1, pp. 66-77

[35] Glover, J. (2014) *How to create an effective stakeholder engagement strategy*, kahootz, Available online at: http://bit.ly/1IF6WaS [Accessed April 18,2017].

[36] 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

[37] Greve, G. C. F. (2013) *Do cloud right: Four critical steps to selecting the provider for you*, Available online at: https://goo.gl/bwVJdY [Accessed June 5, 2016].

[38] Haeberlen, A. (2010). case for the accountable cloud. SIGOPS Oper. Syst.

[39] Hartman, A., Jain, A., Ramanathan, J., Ramfos, A., Van der Heuvel, W., & Zirpins, C. et al. (2010). Participatory Design of Public Sector Services. *Electronic Government and The Information Systems Perspective*, pp. 219-233.

[40] Headspring, 2014, Migrating to the Cloud: Re-Platforming Legacy Enterprise Applications, Best Practices Guide, viewed June 15, 2016< https://goo.gl/shTHBi >

[41] 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

[42] Ico (2014) Conducting privacy impact assessment code of practice, DataProtection Act, Information Commissioner's Office, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

[43] 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

[44] IT Lab (2013) *Cloud Migration Guide*, Available online at: https://goo.gl/u8YRjW [Accessed June 5, 2016].

[45] ITU-T, 2002, Global Information Infrastructure terminology: Terms and definitions

[46] ISO, ISO/IEC 19941 standard: "Information Technology -- Cloud Computing -- Interoperability and Portability"

[47] 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

[48] Kakderi C, Komninos N and Tsarchopoulos P, 2016, Smart cities and cloud computing: lessons from the STORM CLOUDS experiment. Journal of Smart Cities, vol.2(1): 4–13. http://dx.doi.org/10.18063/JSC.2016.01.002.

[49] Kandukuri, B. R., & Rakshit, A. (2009). Cloud Security Issues. IEEE international Conference on Services Computing (pp. 517-520). Washington: IEEE Computer Society

[50] Kepes, B. (n. d.) *Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS*, Available online at: http://bit.ly/1SLp35B [Accessed June 5, 2016].

[51] 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

[52] Komninos, N., Kakderi, C., and Tsarchopoulos, P. (2014) "New services design for smart cities: a planning roadmap for user-driven innovation", *Proceedings of 2014 ACM Conference, International Workshop on Wireless and Mobile Technologies for Smart Cities (WiMobCity)*, pp. 29-39.

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

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

[55] 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

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

[57] 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

[58] 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

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

[60] Microsoft (2014) Protecting Data and Privacy in the Cloud, Microsoft Corporation https://download.microsoft.com/download/2/0/a/20a1529e-65cb-4266-8651-1b57b0e42daa/protecting-data-and-privacy-in-the-cloud.pdf

[61] 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

[62] Murley, D. (2009). Law Libraries in the Cloud. Law Library Journal

[63] Nelson, M. R. (2009). The Cloud, the Crowd, and Public Policy. Issues in Science and Technology

[64] Oracle (2015) *Finding Your Right Cloud Solution: Private & Public Clouds*, Available online at: http://goo.gl/KRolV6 [Accessed November 9, 2015].

[65] Paganini, P. (2014) *Best practices for moving workloads to the cloud*, Available online at: https://goo.gl/D21nMS (Accessed June 5, 2016).

[66] Panori A, González-Quel A, Tavares M, et al. (2016) Migration of applications to the Cloud: a user-driven approach. *Journal of Smart Cities*, *2*(1), pp. 41–52.

[67] Pelerin, R. (2015) Testing Key to Successful Cloud Migration, DataCentreKnowledge, http://www.datacenterknowledge.com/archives/2015/04/29/testing-key-successful-cloud-migration/ [Accessed March 4, 2017].

[68] Posey, B. (2015) *Criteria for choosing a public cloud provider*, Available online at: http://bit.ly/1QeOlHm [Accessed March 4, 2017].

[69] Rangwala, Y. (2011) *Application migration to the cloud: Selecting the right apps*, ComputerWeekly.com, Available online at: http://bit.ly/2pISXH5 [Accessed April 18, 2017].

[70] Schwartz, K. D. (2011) *3 flavors of cloud computing give agencies options for getting started*, Available online at: http://bit.ly/2pL0QTB [Accessed March 21, 2017].

[71] 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

[72] 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

[73] Stahl, B.C., Heersmink, R., Flick, C., van den Hoven, J., Wakunuma, K.J. et al (2010) Identifying the ethics of emerging information and communications technologies: an essay on issues, concepts and method. International Journal of Technoethics, 1 (4), pp. 20-38

[74] 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

[75] Tastogi. I.; Adesh, C/, Kumar, G.V., and Abhishek, V. (2013) Privacy Issues and Measurement in Cloud Computing: A Review, International Journal of Advanced Research in Computer Science . Mar/Apr2013, Vol. 4 Issue 2, p81-86. 6p

[76] Timmermans, J., Stahl, B.C., Ikkonen, V., and Bozdag, E. (2010) The Ethics of Cloud Computing A Conceptual Review, Conference: Cloud Computing, Second International Conference, CloudCom 2010, 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

[77] Varia, J. (2010) Migrating your Existing Applications to the AWS Cloud: a Phase-driven Approach to Cloud Migration, Amazon Web Services, https://d0.awsstatic.com/whitepapers/cloud-migration-main.pdf [Accessed 31.03.2017]

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

[79] Walden, S. (2015) *The pros and cons of public, private and hybrid clouds*, Available at: http://goo.gl/D6jBYX [Accessed November 9, 2015].

[80] Wiggins, A. (2012) *The twelve-factor app – A methodology for building software-as-a-service apps*, Available online at: http://12factor.net/ [Accessed April 14, 2017].

[81] Williams, M. I. (2012) *Making the move to Cloud Computing*, ICAEW Information Technology Faculty, Available online at: http://bit.ly/2pKUcwC [Accessed March 27, 2017].

[82] Writer, S. (2013) A reference model for moving your applications to cloud, https://www.ibm.com/blogs/cloud-computing/2013/08/a-reference-model-for-moving-your-applications-to-cloud/ [Accessed 31.03.2017]

[83] 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