



Project Acronym: STORM CLOUDS

Grant Agreement number: 621089

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

Deliverable 5.1.2

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

Work Package: WP5

Version: 0.3

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), Dimitris Simitopoulos (THESSALONIKI)

Reviewed by:

Legal Notice and Disclaimer

This work was partially funded by the European Commission within the 7th Framework Program in the context of the CIP project STORM CLOUDS (Grant Agreement No. 621089). The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the STORM CLOUDS project or the European Commission. The European Commission is not liable for any use that may be made of the information contained therein.

The Members of the STORMS CLOUDS Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the STORMS CLOUDS Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

© STORMS CLOUDS Consortium 2015

Version Control

Modified by	Date	Version	Comments
<i>Kakderi Christina</i>			

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 5.1 refers to the compilation of knowledge, feedback and input from previous WPs, along with citizens and public authorities' feedback during the innovation cycles. The aim of this task is to create a body of knowledge about migration of public services into the cloud and formulate a comprehensive guide for Public Authorities about cloud service provisioning.

This is an updated version of the documentation that was delivered in M18 about migration process of public services into the cloud. The report proposes a navigation route and presents some of the most common roadblocks which public authorities may encounter.

The content of the report is mainly based on recent scientific papers in addition to about 100 relevant reports. A catalogue of these reports can be found in the Annexes (Annex I) and the project website (<http://www.storm-clouds.eu/services/resources/body-of-knowledge/>). In this catalogue reports are organized according to their content category (e.g. privacy, security, cloud environment etc.) while users may read a short summary of each report and/or download the report.

Table of Contents

Version Control	2
Executive Summary	3
Table of Contents.....	4
List of Figures	5
List of Tables	6
Abbreviations.....	7
1 Introduction.....	8
2 Cloud Computing Fundamentals	9
2.1 State of play and background: basic concept and relevance to public authorities.....	9
2.2 Benefits and barriers towards cloudification.....	10
2.3 Smart cities and cloud computing.....	13
2.4 Current initiatives and emerging trends with regards to public sector cloud adoption in different countries	15
2.5 Conclusions from the literature: research trends and future challenges	16
3 Transition to the cloud	18
3.1 Migration strategies and guidelines found in the literature	18
3.2 The STORM Clouds Migration Process	21
4 Selection of Services and Applications	25
4.1 Selection of stakeholders.....	25
4.2 Selection of Services and applications	27
5 Cloud environment.....	31
5.1 Cloud Service Category Selection.....	31
5.2 Cloud deployment model and technologies.....	32
5.3 Cloud selection provider	34
6 Migration of apps	36
6.1 Specifications for migration	36
6.2 Adaptation of apps	37
6.3 Installation.....	41
6.4 Testing.....	42
7 Administrator of the clouds.....	44
7.1 Administration.....	44
7.2 Analytics	44
7.3 Backup	45
7.4 Interoperability	46
8 Data Management	49
8.1 Ethics.....	49
8.2 Privacy & Data	51
8.3 Ownership.....	54
9 Validation and Monitoring.....	55
10 Security	56
11 Conclusions	59
References	60
Annex A Body of knowledge about migration of public services to the cloud	65

List of Figures

Figure 1: How IT governance looks at the moment and how it will look in the cloud. Source: Accenture (2013)	10
Figure 2: Business agility for the public sector. Source: vmware (2011)	12
Figure 3: The 6 most common application migration strategies. Source: Amazon Web Services	20
Figure 4: A phase driven approach to cloud migration. Source: Varia (2010, p.4)	21
Figure 5: STORM CLOUDS migration process	22
Figure 6: A roadmap for planning public services migration to cloud computing	24
Figure 7: Conceptual model for the design of a cloud of public services. Source: Deloitte (2014)	28
Figure 8: Traditional vs Cloud Aligned Application Architectures (Source: New Relic)	38
Figure 9: Application Migration Common Methods and Approaches (Source: New Relic)	39
Figure 10: SCP “Scale-up” Architecture for traditional applications	40
Figure 11: SCP “Scale-out” Architecture for Cloud-ready applications	40
Figure 12: Zabbix Monitoring Pages	45
Figure 13: The three different domains of interoperability in IMM (Source: European Commission)	47
Figure 14 – Monitoring and validation indicators for the Virtual City Market application	55
Figure 15 – Monitoring and validation indicators for the CloudFunding application	55

List of Tables

Table 1: List of guidelines required for the implementation of cloud-based public services. Source: Seo et al. (2014).....	19
Table 2: Methodology for risk mitigation.....	25
Table 3: Criteria for stakeholder segmentation.....	26
Table 4: Taxonomy of public sector application fields. Source: Bonneau et al. (2013a, 9).....	28
Table 5: Application Candidates for Migration to Cloud Computing. Source Cloud Standards Customer Council (2013, p. 7).	29
Table 6: Technical Information about candidate applications to migrate	30
Table 7: Different application migration options supported by STORM CLOUDS Platform.	32
Table 8: Pros and cons of private, public and hybrid deployment Cloud models.....	33
Table 9: Cloud Application Maturity (Source: New Relic).....	39
Table 10: Five maturity stages of IMM (Source: European Commission).....	47
Table 11 - Cloud Security Principles (Source http://goo.gl/mUf5c2).....	57

Abbreviations

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

1 Introduction

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

The report is structured in three main parts. The first part provides a review of the literature and the main reports on the adoption of cloud computing by the public sector. It starts with an introductory which provides the background on cloud computing, It continues with a section dedicated on the relation of the concepts of smart cities and cloud computing and ends with the main initiatives taken on the specific field.

The second part continues with a literature review on the main deployment models and migration strategies of public administrations. The section ends with the experience of STORM Cloud project by defining a migration process with sequential steps.

The third part of the report aims to reflect the experience gained from STORM Clouds project, especially with regards to specific issues that public authorities face during the cloudification process. It starts with the definition of stakeholders and applications, the selection of the cloud environment, the process of migrating applications to the cloud, the administration of the cloud, and the management of data. The part ends with two more sections, one related to monitoring and validation and one related to security.

The report ends with a catalogue of publications related to cloud computing which comprises the body of knowledge on migrating public services to the cloud.

2 Cloud Computing Fundamentals

2.1 State of play and background: basic concept and relevance to public authorities

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

WHAT IS CLOUD COMPUTING?

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (Mell and Grance, 2011).

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

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

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

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

‘fundamental services’¹ available on the cloud, the higher the opportunity to reuse and combine them with existing services of other governmental departments or to develop new services in collaboration with third parties.

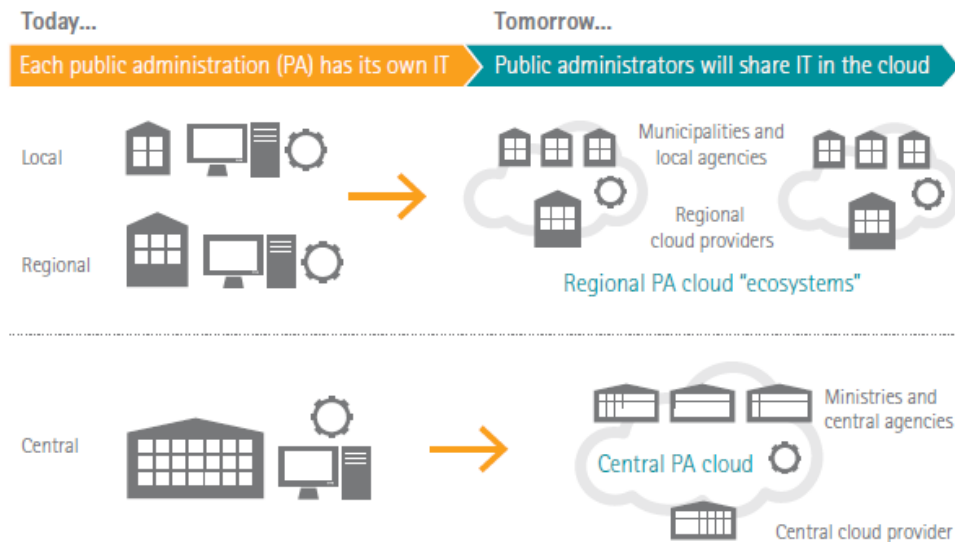


Figure 1: How IT governance looks at the moment and how it will look in the cloud. Source: Accenture (2013)

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

2.2 Benefits and barriers towards cloudification

Benefits of cloud computing in the public sector

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

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

Just as in the case of a private organisation, cloud computing can also offer attractive advantages to the public sector. Mahmood (2015, xvii) has summarised the benefits of cloud computing adoption in the public sector by grouping them in two categories: the ones that address to public organisations and the ones that address to citizens. More specifically, governments can have ‘better business process management; cost and time savings; more accurate and timely information; automation and process improvement; easy maintenance and upgrading of services; and seamless collaboration, vertically and horizontally, with other governmental departments’. Citizens, on the other hand, have easy-to-use and on demand access to government e-services; online transactions e.g. payment of bills and filing tax returns; information reliability and ready availability of services around the clock; more accurate and timely information; opportunities for e-participation including e-voting; and citizen oriented decision making by the political leadership’.

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

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

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

CLOUD COMPUTING CHARACTERISTICS

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



Figure 2: Business agility for the public sector. Source: vmware (2011)

- **Elimination of Procurement and IT infrastructure maintenance:** The characteristics of high scalability, elasticity and resource pooling eliminates the need to procure, monitor and maintain IT resources. This has a significant effect in reducing the workload and the need for IT staff, allowing public agencies to focus on their core responsibilities.
- **Access to new technologies:** Cloud computing provides the opportunity to public organisations to access at all times the most updated software and hardware at a very low cost.
- **Universal resource access:** Cloud computing enables universal access to resources while it helps in establishing common platforms for service provision, which are also accessible by the citizens.
- **Flexibility:** Cloud computing allows different governmental departments and organisations to change service providers without lengthy procurement processes avoiding 'lock-in' contracts (Bonneau et al., 2013b).

Challenges for public administrations

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

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

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

CHALLENGES RELATED TO CLOUD COMPUTING

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

2.3 Smart cities and cloud computing

City governments and municipalities everywhere constitute for one thing complex public organisations which have more reasons to invest in cloud computing than any other public organisation. . Despite their limited resources they have to provide a wide number of municipal services (ranging from sanitation, water, schools, health, transportation etc.) and serve the needs of their citizens in their everyday life. At the same time, they face a variety of challenges including job creation, economic growth and environmental pollution. It is widely accepted that increasing urbanisation strains the limited resources of cities and affects its resilience, while, it also highlights the significance of sustainable urban development, especially in terms of more efficient management of natural resources, such as energy and water, as well as of better planning and collaborative decision making (Khan et al., 2015). In this context, cloud computing can play a significant role facilitating cities in meeting the abovementioned tasks.

Over the past years, the term 'smart cities' has evolved to denote the cognitive processes combined with the deployment of ICTs, institutional settings for innovation and physical infrastructure, which taken altogether increase the problem solving capability of a city or a community (Kominos, 2013). The main features of a smart city include applications that connect, manage and optimize data from a complex set of devices, sensors, people and software, creating real-time, context-specific information intelligence and analytics, which aim to transform the urban environment and address its specific needs (Mitchel et al. 2013). Managing such enormous amount of heterogeneous data requires, among others, high storage capacity and performance computing power (Fu et al., 2015). For this, the latest developments in Cloud Computing and the Internet of Things are widely deployed in smart cities (Schaffers et al., 2011).

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

distributed, heterogenous, decentralised, real and virtual devices and data sources - and formulate a variety of smart city application scenarios (Khan et al., 2015; Suciu et al., 2013).

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

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

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

Real time processing of big data and the deployment of multiple applications is possible due to one of the main enabling technologies of cloud computing, which is virtualisation. Virtualisation is software that abstracts the physical infrastructures as virtual machines (VMs) and makes servers, workstations, storage and other systems independent of the hardware layer creating various dedicated resources according to the needs of the users. It increases infrastructure utilization, enables more efficient use of the hardware and allows for true scalability and increased uptime (Jarvis, 2014).

Smart city solutions are applicable to all three service models of cloud computing (IaaS, PaaS, SaaS). Firstly, as already mentioned, cloud solution providers integrate IoT infrastructure (devices, networks) through virtualisation, offering computer resources as a utility (IaaS).

Secondly, cloud computing can shift domain specific tightly coupled systems (i.e. systems focusing on energy, transportation etc., orchestrated by domain specific service providers) to open domain-independent and scalable smart city services, provided through cloud based and domain-independent service-delivery platforms (Dustdar et al., 2014). These constitute a type of Platform as a Service (PaaS) offering, which integrates and processes real time data from IoT and other data sources, and allows domain specific applications to employ both IoT and cloud resources on demand.

Thirdly, cloud computing can enable standardisation of smart city applications and turnkey solutions for software as a service (SaaS), providing on-demand self-services and decreasing significantly the associated development costs (Schaffers et al., 2011; Komninos, 2014). The provision of smart city services through flexible usage models and billing schemes, gives the opportunity to other cities with relatively limited budgets make use of them. Standardisation of core city services, platforms and applications is extremely important as it accelerates technology diffusion and the uptake of proven smart city solutions, while at the same time

enhances the emergence of collaborative innovation systems in these areas (Komninos, 2014).

Much like open innovation, cloud-based smart city solutions require the collaboration among different actors of the urban ecosystem, meaning citizens, enterprises and the public sector. Besides, the existence of technologies being able to manage the cloud of things within cities does not automatically guarantee the development of smart city services (Clohessy and Acton, 2013). According to Clohessy et al. (2014) cloud computing smart city initiatives could harness the capabilities of open innovation paradigms such as living laboratories and crowdsourcing, taking full potential of the emerging collective intelligence. To this end, the use of open data is imperative for the development of innovative solutions and the opening up of new business opportunities.

2.4 Current initiatives and emerging trends with regards to public sector cloud adoption in different countries

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

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

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

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

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

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

2012) which is based on three key actions:

- *Cutting through the jungle of standards*, referring to the need for certification of cloud services and the endorsement of such certificates by independent regulatory authorities. Standardisation is crucial for the potential of lock-in, especially in the case of SMEs and non IT companies which are rarely able to evaluate a product's/service's characteristics as to the level of interoperability, data portability and reversibility.
- *Safe and fair contract terms and conditions*, tackling the complex and uncertain legal framework for cloud service providers. The Commission thinks that the development of model contract terms for cloud computing (both between cloud providers and professional cloud users and with regards to consumers and small firms) will increase trust, while improving existing legislation (such as the proposed Regulation on personal Data Protection and the Common European Sales law) will accelerate the take up of cloud computing in Europe
- *Promoting common Public Sector Leadership through a European Cloud Partnership* (ECP) as an umbrella for comparable initiatives at Member State level building common procurement requirements for cloud computing in an open and fully transparent way.

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

Governments across the EU have initiated Government Cloud (G-Cloud) programmes to deliver computing, storage and software capabilities to central and local governments using cloud computing. Government G Clouds are considered as promising models for smart cities, which can create urban clouds that reduce IT costs, offering platforms for business applications and e-services (Schaffers et al., 2012). Contrary to the abundance of G-cloud initiatives, Clohessy et al. (2014) propose the development of a single G-Cloud, with the collaboration of government, citizens, businesses, and researchers, which will implement a number of cloud technologies on a hosted platform to create and deliver an integrated pool of smart city services and solutions. Examples of smart city cloud based platforms include SCOPE, implemented in Boston, USA as well as SOFIA2, implemented in Coruna, Spain. Finally, in line with the above, we also see the emergence of a number of joint initiatives aiming to battle the fragmentation of efforts towards smart cities and cloud computing:

- Cloud28+ (<https://cloud28plus.eu>) a European-based community aimed at increasing the visibility and revenue of its members and accelerating adoption of cloud technologies through the creation of a cloud service catalogue, with a strong focus on compliance with the European rules on data privacy and security
- EU's MoU on Smart Cities Open and Interoperable Urban Platforms, which aims to integrate data flows within and across city systems with the use of modern technologies (cloud services, analytics, social media) enabling cities to shift from fragmented applications and to create confidence on the demand side. The initiative is part of the European Innovation Partnership on Smart Cities and Communities (<https://eu-smartcities.eu/>).

Eurocloud (www.eurocloud.org), an independent non-profit organisation acting as a pan-European hub, working towards the maintenance of a constant open dialogue and the sharing of knowledge between cloud computing customers and providers, start-ups and research centers.

2.5 Conclusions from the literature: research trends and future challenges

Based on the advances made so far, this section aims to highlight new scientific directions and future challenges with regards to smart cities and cloud computing. Although the trends that define the future of cloud computing can be numerous, ranging from technological aspects to new business models/opportunities, we identify four areas that are about to play a significant role with regards to cloud computing adoption

from municipalities and city governments.

As Petrolo et al. (2014) mention, “in Smart City context, Cloud of Things (CoT) is expected to play a significant role making a better use of distributed resources, achieving higher throughput and tackling large scale computational problems, to enable the horizontal integration of various (vertical IoT platforms and the Smart City vision”. This means that over the next years the focus will be on cloud platforms dedicated for IoT and on technologies for real time processing of big data and linked data. Advanced analytics over millions of data streams coming from highly distributed, heterogeneous, decentralised, real and virtual devices and data sources (Khan et al, Suci, 2013) bring a new vision on the notion of cloud scalability. Here, issues of interoperability, privacy and security should be carefully considered.

Although SaaS applications can offer higher flexibility and lower cost, integration between SaaS and on-premises legacy applications has been identified as a significant obstacle to adopt and deploy SaaS and other web-based applications. However, cloud integration does not only refer to cloud and on-premises integration, but also to integration among different clouds. Services convergence and multi cloud integration (Li et al., 2013) is a promising paradigm which creates new system design possibilities but also presents technological and management challenges, such as portability, compliance, elasticity and high availability (Paraiso et al., 2014). These issues will be the focus of interest over the following years.

Despite the significant benefits of cloud computing in public administrations (cost savings related to scalability, increased efficiency, accelerated innovation etc.), there is still a lot of effort associated to the development and running of composite applications on the cloud. Based on principles similar to component based software development (CBD) and service oriented architecture (SOA), cloudification of core application components and component portability can create repositories of the essential building blocks of smart city applications, reducing the cost of development and enhancing the emergence of new business models. The development of online libraries with re-usable software components providing different services for processing requests (e.g. database connection for the performance of database queries, user authentication, mail composing and sending etc.) has already a significant background (Heineman and Council, 2001), however, delivery as a service over different cloud providers requires specific considerations including issues of interoperability, reusability, open standards etc.

Finally, we see the growth of cloud-based platforms and/or marketplaces being able to offer standardised core smart city services with on-demand infrastructure aiming to make smart city application deployment a simple process to follow. Marketplaces have emerged over the last few years as a way to provide a unified channel of distributing high quality cloud services, bringing together cloud service providers, data center operators and technology partners (Fugate and Tang, 2015). The idea of having third party cloud-based applications integrated into one application suite has started gaining momentum as most municipalities do not have the resources, e.g. funds, expertise and available technology, which will enable them to move towards the vision of becoming a smart city. Cloud marketplaces and cloud-based application suites can help in speeding up the implementation process of smart city turn-key solutions in different domains of cities including transportation, sanitation, urban planning, policy making and so on. Research on this topic will have to focus also on issues such as Service Licence Agreements (SLAs), open standards etc.

3 Transition to the cloud

3.1 Migration strategies and guidelines found in the literature

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

SERVICE MODELS

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

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

TYPES OF CLOUD

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

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

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

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

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

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

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

Table 1: List of guidelines required for the implementation of cloud-based public services. Source: Seo et al. (2014)

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

- i) **Procurement and Marketplace:** this model, adopted mainly by UK, Portugal and partly by the Netherlands, is a very centralized and top-down approach, only for procurement aspects and involves bottom up approaches regarding application development and adoption. It relies mainly on external providers which develop applications that can be used by public authorities.
- ii) **Resource Pooling:** it is also a top-down model, in which resources are pooled to provide a common infrastructure that can be leveraged for IaaS services and for more specific applications
- iii) **Standalone Applications:** it is a pure bottom up model in which public authorities deploy standalone applications, without being coordinated even if there is a form of central strategy/policy on this. The focus in this model is on SaaS, therefore, most of the applications rely on public cloud solutions.

Six of the most common application migration strategies include: 1) rehosting, 2) replatforming, 3) repurchasing (i.e. moving to a different product), 4) refactoring/re-architecting (i.e. re-imagining how the application is architected and developed, typically using cloud-native features), 5) retire (turn off) and 6) retain (revisit later/do nothing for the time being) (Orban, 2016).

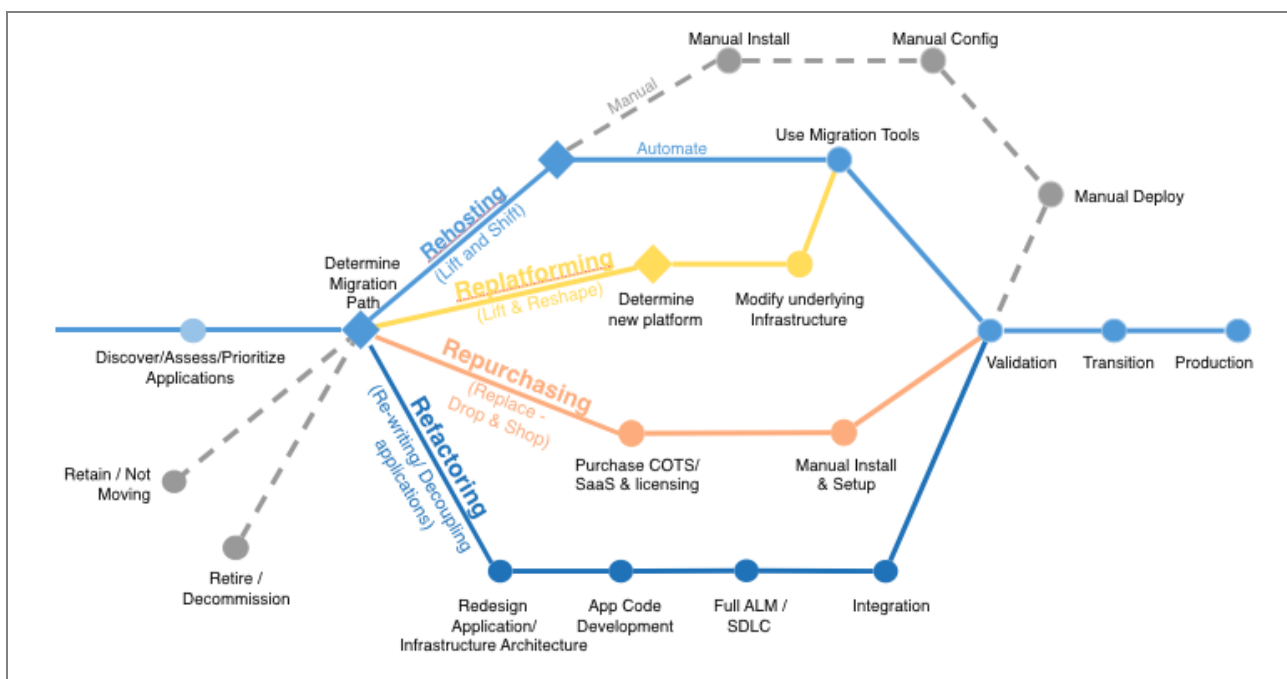


Figure 3: The 6 most common application migration strategies. Source: Amazon Web Services²

Comprehensive planning, driven by a disciplined migration process will contribute greatly to a successful redeployment of the applications to a new cloud environment. Successful initiatives have developed sophisticated, multi-phased migration methodologies to reduce implementation risk and speed-up the

² <https://medium.com/aws-enterprise-collection/6-strategies-for-migrating-applications-to-the-cloud-eb4e85c412b4>

migration process.

Varia (2010) in a document describing a migration methodology of existing applications to the AWS Cloud proposed a six phase approach: 1) the cloud management assessment phase, 2) the proof of concept phase, 3) the data migration phase, 4) the application migration phase, 5) the leverage the cloud phase and 6) the optimisation phase (Figure X).

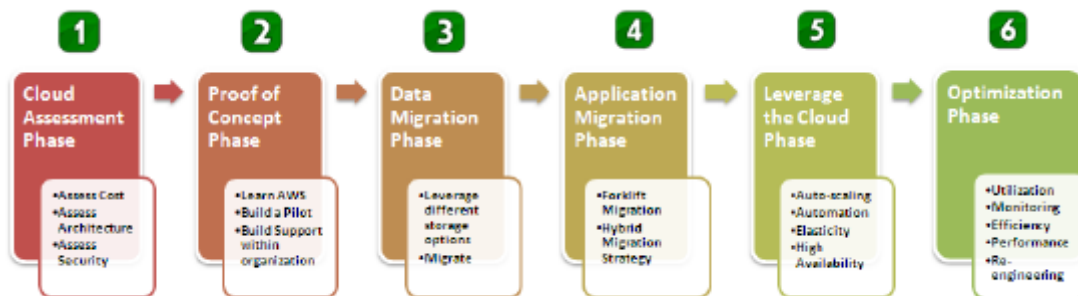


Figure 4: A phase driven approach to cloud migration. Source: Varia (2010, p.4)

During the migration process the following technical considerations must be taken into account^{3,4}:

- The creation of a detailed inventory of the current application portfolio really helps in terms of understanding the scope of the migration effort. This includes capturing information regarding the number of software modules, scripts, and external interfaces involved. It also includes hardware and software configuration information, including operating system versions, database versions, features/functionalities in use, and similar information.
- A security audit of the application and its data is vital. The cloud service's security features may be very different from those of the in-house environment, and the security risks and the measures applied to counter them must be assessed carefully.
- Temporary subsystems can be established to facilitate migrations.
- Standardization and automation can help reduce the risk of migration errors. Virtual machine templates can be rapidly deployed and bring an environment online in a day. Automated data integrity and validation methods can be used to verify and validate data, databases and files during the initial synchronization.
- The creation of migration tools, which ensure a high level of automation along with accuracy in migration can result in less time spent in migration and testing.

3.2 The STORM Clouds Migration Process

Application migration is the process of redeploying an application, typically on newer platforms and infrastructure. Comprehensive planning, driven by a disciplined migration process will contribute greatly to a successful redeployment of the applications to a new cloud environment. STORM CLOUDS followed a multi-phase migration process, which included all the necessary steps that ensured the smooth deployment of the selected Smart City applications to the SCP. The process started with the assessment of each application

³ *Best Practices for Federal Agency Adoption of Commercial Cloud Solutions*, 2015, Professional Services Council, viewed November 6, 2015 <<https://goo.gl/j5Nbff>>

⁴ *Migrating Applications to Public Cloud Services: Roadmap for Success*, 2013, Cloud Standards Customer Council, viewed November 5, 2015 <<http://goo.gl/EGHN8l>>

regarding its readiness for the new Cloud environment, its architecture and its functional and non-functional requirements. This analysis led to some necessary improvements in order the application to be optimised for the SCP. Afterwards, the code and data deployed in the platform's Application and Data Service Layers, respectively. The process was completed with the validation that the application was fully operational in the new Cloud environment.

The following diagram presents the STORM CLOUDS migration process.

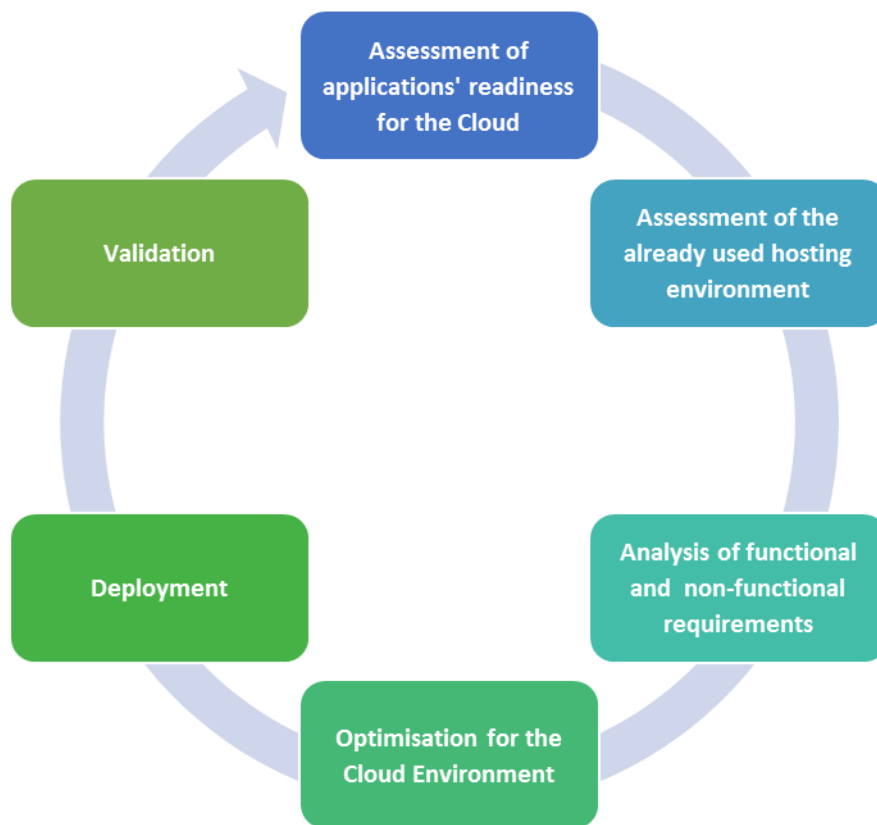


Figure 5: STORM CLOUDS migration process

The STORM CLOUDS migration process includes the following six steps:

Step 1 - Assessment of applications' readiness for the Cloud

The 1st step aims to evaluate if the services are ready for the cloud environment. 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.

Step 2 - Assessment of the already used hosting environment

The 2nd step aims to analyse the environment used to host the services. 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.

Step 3 - Analysis of functional and non-functional requirements

The 3rd step aims to define the 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.

Step 4 - Optimisation for the Cloud Environment

The 4th step aims to solve the problems identified in the previous step, so the application to be ready for deployment in the new environment. Moreover, it includes modifications that enable the application to support natively the most prominent Cloud characteristics (e.g. high-availability and scalability). The latter is closely related to the available budget or the internal IT capabilities.

Step 5 – Deployment

The 5th step aims to transfer the ready to be cloudified applications to the new Cloud environment. The deployment process includes the following actions:

- a) setup of the cloud environment that will host the selected services;
- b) launch the VM instances that will host the applications and their data (e.g. database and file sharing modules).
- c) migrated both the applications and their data to the Cloud environment

Step 6 – Validation

The final step aims not only to ensure that the deployed applications are operational but especially that they meet the initial set of requirements regarding cloudification. The validation is made in collaboration with the municipalities and includes functional tests ensuring that the deployed application performs as designed.

In the following sections we describe a number of issues that should be taken into account throughout the process of migrating public sector applications to the cloud. These issues have a sequential character in the form of a methodological roadmap: i) services and applications, ii) cloud environment, iii) migration of applications, iv) cloud administration, v) data management. Two other subjects are also examined which penetrate the whole process, that is security and validation-monitoring.

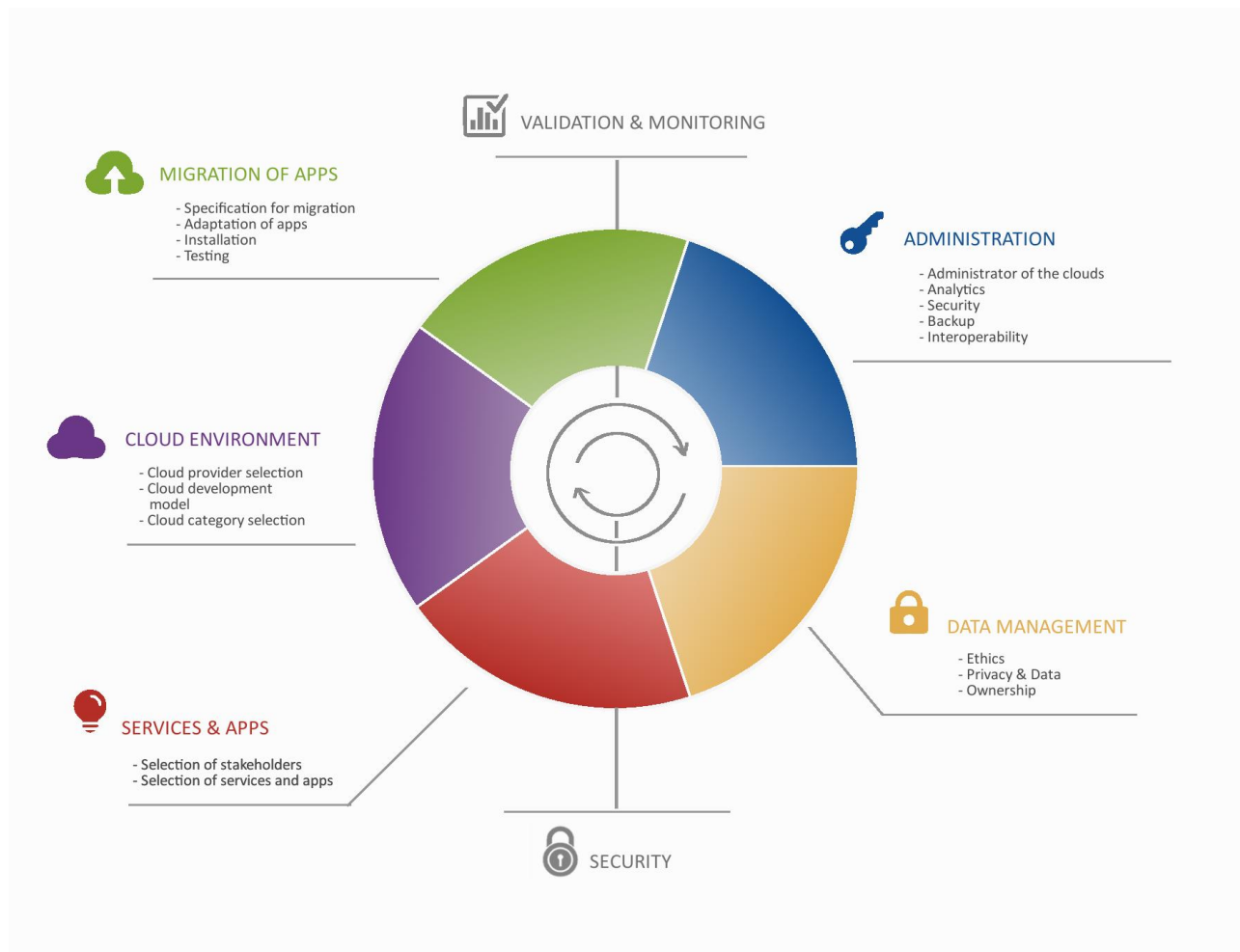


Figure 6: A roadmap for planning public services migration to cloud computing

Based on the Figure above, 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 applications' migration.

4 Selection of Services and Applications

4.1 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). During this process, context elements should be analysed along with a contingency plan to mitigate potential risks. The table below, provides an example of such an exercise (Table 2).

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 term reasoning to show that current investment will bring future savings.

Table 2: Methodology for risk mitigation

Gathering the right people together is the most important aspect of creating and implementing a successful cloud migration strategy (CSA, 2016). 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. Glover (2014) proposes a way to map stakeholders

based to their level of interest and influence, and engage them in a different level accordingly (inform, involve and consult, engage, collaborate). Below is a table that facilitates this exercise (Table 3):

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 3: Criteria for stakeholder segmentation

Each one of the stakeholders identified should be related to the objectives set in the initial phase. Also, the profile of the stakeholders should be carefully selected in order to have the richest input to the process. It is necessary to select adequate stakeholders and keep them engaged to the project.

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 (Komninos et al., 2014). 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. These can be articulated using for example a responsibility assignment matrix, also known as a RACI (Responsible, Accountable, Consulted, Informed) chart. People internal to the organisation which have a better view of the needs and expected requirements, should have a more significant role and perhaps a more valid opinion. This also avoids bypassing established information governance practices and expose the organisation to undue risk (Williams, 2012).

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)

- Educating stakeholders on how cloud adoption can affect existing practices and/or changes the organisation's ability to meet its obligations. This provides the opportunity to reset expectations with regards to budgeting, security and performance (Amazon, 2017) or highlight tasks that might need to be outsourced (CSA, 2016). As with any other new system, migration to Cloud Computing might encounter strong resistance by an organisation's employees (Barnaby, 2010). This can be avoided with training. Also, upraising stakeholders' digital skills increases their ability to contribute (Eskelinen et al., 2015). 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. The use of web based tools is a cost and time efficient way of bringing different persons together and reach their boundless reservoir of ideas and creativity.

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.

CASE STUDY

The Municipality of Thessaloniki, Greece, identified the cloud as an opportunity to expand its services beyond the barriers of traditional municipal service provision. The municipality was particularly keen to select applications related to entrepreneurship and quality of life in the city. Therefore, during the process of migration to cloud computing it developed a set of new services, among which is a virtual marketplace. This virtual marketplace enables every commercial enterprise located in the city center to create its own virtual shop. For this endeavour, the business community had to be engaged in order to provide content to the service (information about their store and products) but also to validate the service, provide suggestions for improvement and test potential new functionalities (online shops through this marketplace).

The municipality of Thessaloniki identified from the very beginning groups and individuals with an interest in public available services operated from the cloud. It organised from the very beginning general meetings with stakeholders and municipal services and after the creation of a first version of the service, training sessions and validation sessions with end users (shop owners and citizens as potential customers) as well as dissemination activities. During these meetings, the business owners had access to informative material such as leaflets, service manuals and telephone support.

4.2 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. But firstly, we need to clarify that when we talk about public services we mean the services which are produced and supplied by the government and public institutions to satisfy the benefits of social communities and the public needs. Deloitte (2011) propose a taxonomy of public services based on the concepts of granularity and orchestration; these imply a certain hierarchy of services with services at higher and lower levels, where different services can be combined to create a new service. According to the proposed taxonomy, public services can be categorised in a) process public services, which represent actual workflows or business processes, combining other (basic and/or composed public) services through service orchestration, b) composed public services, which are based on other services, combined into a new composed service and c) basic public services which implement a basic functionality. The implementation of this service decomposition in three case study countries led to the identification of three key elements in a cloud of public services (Figure 47)

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

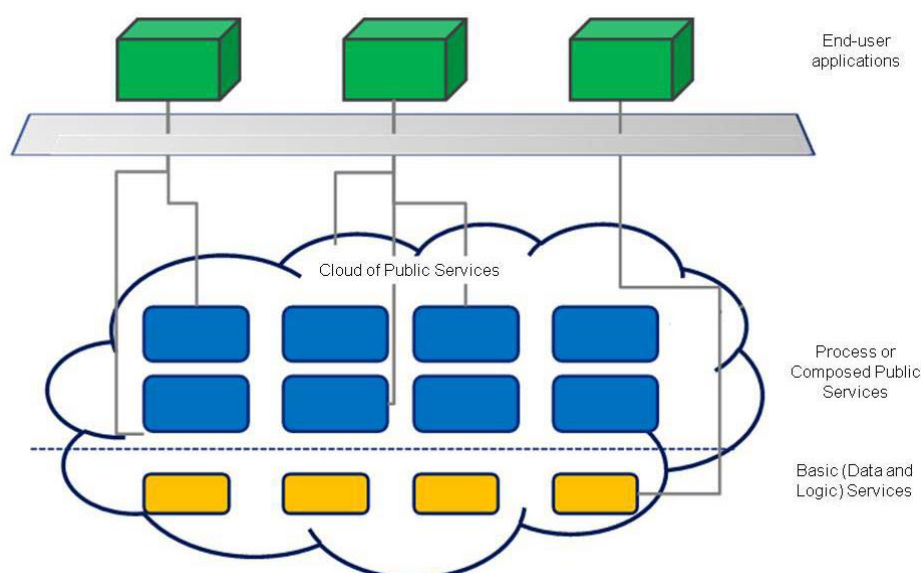


Figure 7: Conceptual model for the design of a cloud of public services. Source: Deloitte (2014)

Bonneau et al. (2013a) group cloud-based application and services of the public sector in three similar categories (Table 4): i) Horizontal/Citizen engagement and service delivery, i.e. applications that allow interaction between citizens and governments and support dematerialisation processes ii) Horizontal/Productivity applications, i.e. applications used by internal employees for overall management and administrative processes, and iii) Vertical applications, i.e. applications addressing specific needs around some vertical expertise.

Horizontal/Citizen engagement and service delivery	Horizontal/Productivity applications	Vertical applications
Applications for citizen – government interaction	Applications for the internal management of administrative processes	Applications addressing specific needs
Accounts of different services <ul style="list-style-type: none"> • Taxes • Transactional (Payment) • Online voting • Website hosting • Social applications (wiki, billboards, blogs) • Access to public sector information 	<ul style="list-style-type: none"> • Email and communication tools • Office automation • Procurement • HR management • Virtual Desktop • Records Management 	<ul style="list-style-type: none"> • E-Health • E-Education • Energy management/ smart grid • Smart transport/ intelligent transportation systems • Urban planning • Utility Management (waste, water etc.) • Smart Logistics

Table 4: Taxonomy of public sector application fields. Source: Bonneau et al. (2013a, 9)

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 expectancies of the responsible organisation, dependence on third party software etc. (Rangwala, 2011). 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. Williams (2012) provides the following checklist for the selection of services to be migrated to the cloud that includes the following:

- Reviewing current information governance policies and processes with cloud computing in mind
- Take stock of current IT costs and capabilities
- Engage open with employees and customers
- Perform all necessary legal checks
- Find genuine problems/opportunities with a clear business case for solving through cloud computing
- Select an urgent problem
- Create requirements documentation with key stakeholders

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
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 5: 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.

In STORM Project, services selection was based on three main criteria: political priorities, technical specifications/restrictions and user driven aspects (Panori et al., 2016). The whole process started with the compilation of available services and applications susceptible to being cloudified. A list of services was created based on the following conditions: services offered by public authorities, services that do not involve developing additional infrastructure in the city, services that are simple and easy to change and services that cover a necessity in the city. To the point that was possible, services were also interoperable to each other. For each one of the services in list, the following information was recorded (Table 6.)

The list of services was presented to stakeholders for evaluation. After some consultation rounds involving meetings, forum groups and crowdsourcing activities, a first round of applications was selected to migrate to the cloud.

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

Table 6: 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.

5 Cloud environment

5.1 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.).

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 their 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 (Battara et al., 2016). All persistent data must go to external services (e.g. databases, file storage, message queues and caches) (Wiggins, 2012).

Case Study

Within STORM Clouds project, the STORM Clouds Platform was developed. The platform enhances the IaaS solution with two modules that provide the high-availability and scalability features in a way that is transparent to the application owners. By accompanying the IaaS layer with the Data Service layer and Access layer, the data and the HTTP traffic management are delegated to the platform while the application's business logic is still contained on the VM(s). This approach offers great flexibility as it does not require architectural changes to the applications but also keeps the deployment complexity low because the application owner “leverages” the high-availability and scalability features of the platform. The only

TIPS FOR SELECTING THE RIGHT CLOUD SERVICE CATEGORY

Before selecting a cloud service category, public authorities have to examine the following issues:

- Ownership of the applications
- Level of infrastructure management
- Interaction with external digital services
- Technical assessment of the services to be migrated (operating system, language, database)
- Management of sensitive data

drawback of this solution comparing with the SaaS is that the application owners are not entirely independent from platform administrators as the later should configure the high-availability and scalability features per application.

The following table summarises the different application migration options supported by SCP (Battara et al., 2016).

Option	Description	Pros	Cons
Full IaaS	All the application components are deployed on VM(s) explicitly managed by the application owner	+ No architectural change of the application + Full control on the resources used for the deployment	- High deployment complexity because the application owner must take care of installing and configuring all the components for high availability and scalability
IaaS + Data Service Layer + Access Layer	Data and HTTP traffic management are handled by the platform, while the application business logic is still deployed on VM(s)	+ No architectural change of the application + Less deployment complexity because the application owner 'leverages' the high-available and scalable features of the platform layers	- Because of the centralized administration of the shared functions (e.g. data service layer), application owners cannot deploy their applications in full autonomy
PaaS + Data Service Layer	Applications are hosted on the PaaS Layer and use the Data Service Layer for storing data	+ No infrastructure management required by the user (the platform does it for her)	- Applications may require significant changes to comply with PaaS principles

Table 7: Different application migration options supported by STORM CLOUDS Platform.

5.2 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. The following table summarises the pros and cons of the different deployment models (Oracle, 2015; Walden, 2015).

Option	Pros	Cons
Private Cloud	+ More control and reliability: IT can control the security of data, set compliance requirements, and optimize networks more effectively with cloud. + Customizable: IT can customize storage and networking components so that the cloud is a perfect fit for the specific organization and its needs.	- Requires IT expertise: A high-level of IT expertise is required to ensure maximum effectiveness and optimal configuration of the deployment. - Costlier: The long-term costs may be higher due to increased management responsibilities and smaller economies of scale.

Public Cloud	<ul style="list-style-type: none"> + Ease of management: Organisations IT departments do not manage their public cloud; they rely on Cloud provider to administer the cloud. + Ease of deployment: With the public cloud, there is low barrier to entry, so you can quickly configure and stand up a cloud. + Flexible: Users can add or drop capacity easily. Moreover, the environment is typically accessible from any Internet-connected device, so users don't need to jump through many hurdles to access. 	<ul style="list-style-type: none"> - Can be unreliable: Public cloud outages are quite common, leading to headaches for users. - Less secure: The public cloud often has a lower level of security and may be more susceptible to hacks. In some cases, cloud providers may not be able to meet the strict constraints mandated by government institutions.
Hybrid Cloud	<ul style="list-style-type: none"> + Flexible and scalable: Organisations are able to combine and match for the ideal balance of cost and security. + Cost effective: Organisations can take advantage of the cost-effectiveness of public cloud computing, while also enjoying the security of a private cloud. 	<ul style="list-style-type: none"> - Complexity of management: Moving parts between public and private clouds can be a challenge. - Requires IT expertise: A high-level technical staff is required to guarantee security vulnerability on all aspects is decreased.

Table 8: Pros and cons of private, public and hybrid deployment Cloud models

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.

Case Study

The STORM Clouds Platform has been developed to support Public, Private, as well as Hybrid Cloud deployment models. In case of the Private Cloud, the cities can install the SCP in their IT infrastructure and use it as the Cloud environment for their Smart City applications. Alternatively, cities can use an instance of the platform that is offered by an external provider and deploy their applications in the Public Cloud. A hybrid approach is also supported, as they can combine a Private Cloud, which will host the high-risk applications—those with high privacy and security requirements (i.e. applications that contain customer data and other sensitive information)— with a Public Cloud for the rest of them. SCP can also be the foundation for the creation of a Community Cloud that will support not only a Municipality but also other Public Organisations, which operate in a city and offer services to citizens and local business.

In terms of the technologies used, the Storm Clouds Platform was developed using the following open source solutions:

- ✓ **OpenStack** for the implementation of the IaaS Layer. OpenStack is the most popular and most adopted open source IaaS solution [1].
- ✓ **Cloud Foundry** for the implementation of the PaaS Layer. Cloud Foundry was chosen because had

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.

the best combination of usability, open-source community, developer experience, and relation to SCP's needs. It is supported by the Cloud Foundry Foundation where EMC, HP, IBM, Intel, Pivotal, SAP and VMware are platinum members.

- ✓ **LAMP** (Linux, Apache, MySQL and PHP) for the implementation of applications' VMs.
- ✓ **MySQL/MariaDB** and **PostgreSQL** database engines for the implementation of Database Services Module.
- ✓ **Gluster**⁵ for the implementation of file Sharing Service Module.
- ✓ **HAProxy**⁶ for the implementation of Load Balancer Module.
- ✓ **Zabbix**⁷ for the implementation of the Monitoring Module
- ✓ **phpMyAdmin**⁸ for the implementation of the MySQL Database Administration Module
- ✓ **phpPgAdmin**⁹ for the implementation of the PostgreSQL Database Administration Module
- ✓ **Duplicity**¹⁰ for creating the backups

5.3 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. The principal elements to consider for almost every organisation are (Paganini, 2014; Greve, 2013; IT Lab, 2013):

- **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.

⁵ Gluster – Main Page, viewed November 2, 2015 <<https://www.gluster.org>>

⁶ HAProxy – Main Page, viewed November 10, 2015 <<http://www.haproxy.org>>

⁷ Zabbix – Main Page, viewed November 10, 2015 <<http://www.zabbix.com>>

⁸ phpMyAdmin – Main Page, viewed November 10, 2015 <<https://www.phpmyadmin.net>>

⁹ phpPgAdmin – Main Page, viewed November 10, 2015 <<http://phpPgAdmin.sourceforge.net/doku.php>>

¹⁰ Duplicity – Main Page, viewed November 10, 2015 <<http://duplicity.nongnu.org/>>

- **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 (Crisp Research AG, 2014). 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.

6 Migration of apps

6.1 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 applications 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.

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 it does not constitute

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.

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	Type	Value
Operating Systems	Ubuntu	RAM [GB]	12
Programming Languages	Javascript, PHP, Java	Disk Storage [GB]	60
Databases	PostgreSQL, PostGIS	vCPUs	8
Web/Application Servers	Tomcat, Apache, Geoserver	Network usage [GB]	N/A
Frameworks	ExtJS, NodeJS	Hits/Month	250
Application Lifecycle Tools	IDE: Eclipse Version Control: git Build Management: -	Registered Users	691
Open Source Code Repository	N/A	Maximum On-line Users	N/A
		Average On-line Users	N/A

All the abovementioned requirements 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.

6.2 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 (**Error! Reference source not found.**) (New Relic, 2015).

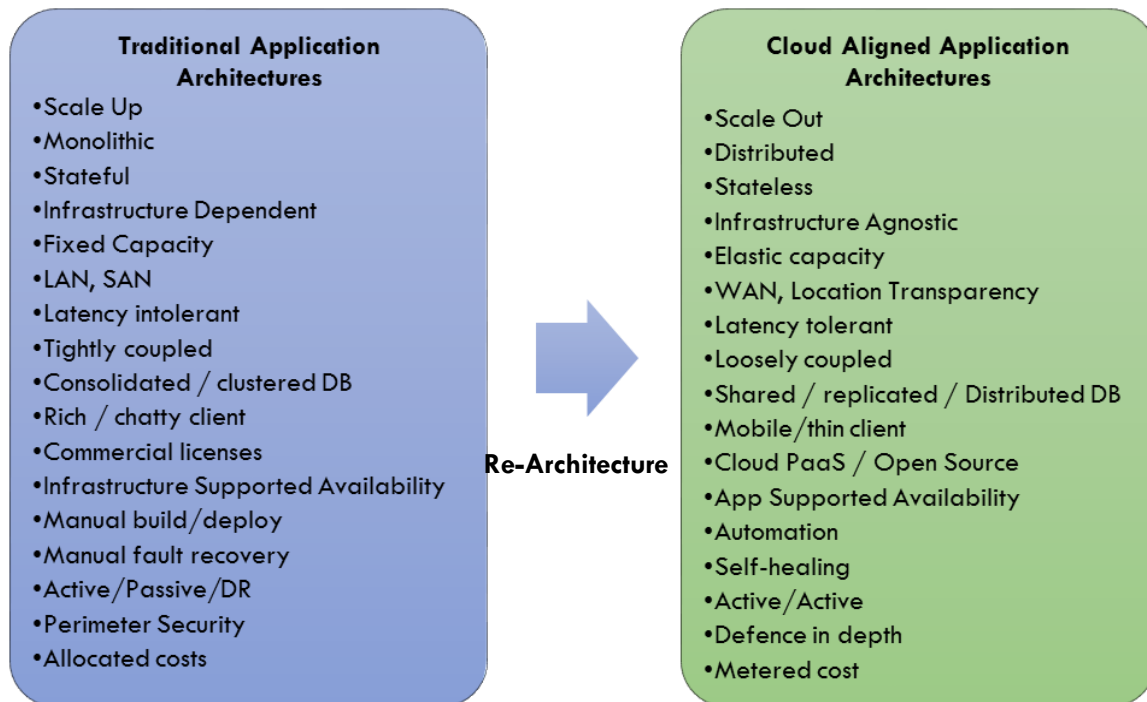


Figure 8: Traditional vs Cloud Aligned Application Architectures (Source: New Relic)

Moving an application to the cloud will require some work under the hood. However, choosing to re-architect an application is ideal 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. There is several application migration common methods and approaches, which should consider the Public Authorities for their existing applications (**Error! Reference source not found.**) (New Relic, 2014):

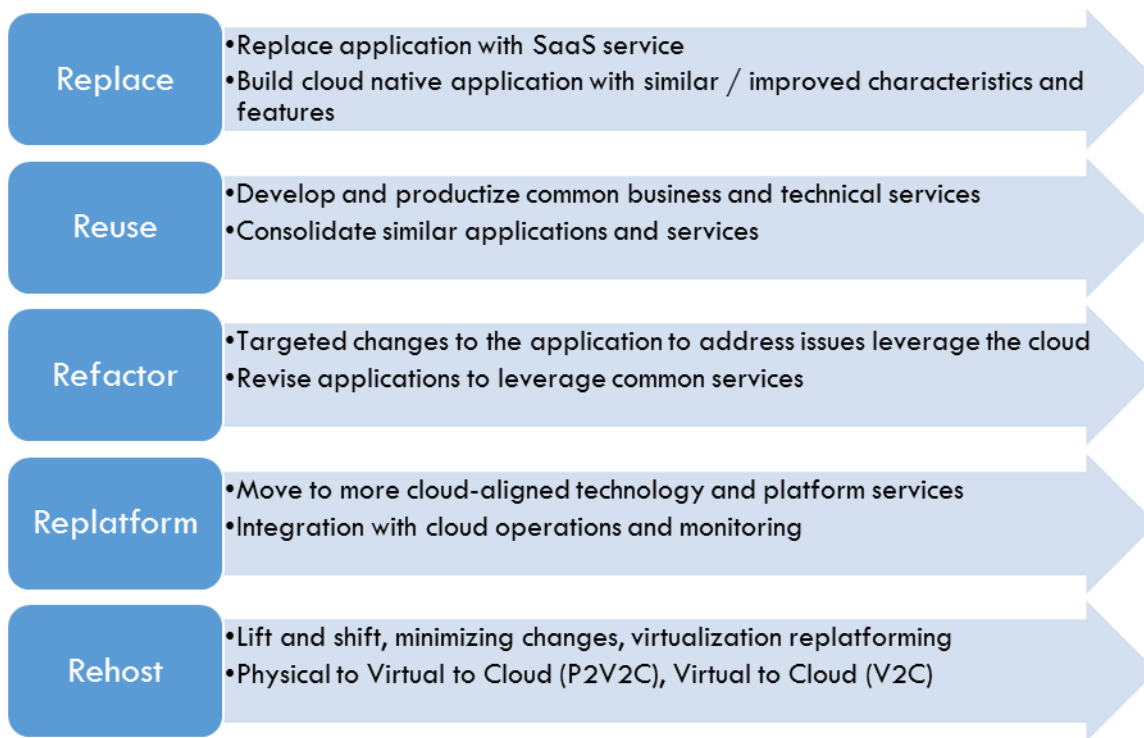


Figure 9: Application Migration Common Methods and Approaches (Source: New Relic)

Depending on the changes the candidate applications reach different Cloud maturity levels. The characteristics of each level are presented in the following table (New Relic, 2014):

Maturity Level	Characteristics
Cloud Washed	<ul style="list-style-type: none"> - Force fit to run in cloud environment - Resources not optimize – no horizontal scaling - Minimal modification done to be cloud compliant
Cloud Adopted	<ul style="list-style-type: none"> - Resources not optimize – no automatic elasticity-instance manually started - Some modification done to be cloud compliant
Cloud Optimized	<ul style="list-style-type: none"> - Resources being optimized – horizontal scaling possible - Elastic on instance level – cloud management layer determines when to start/stop additional instances - Major modification done to be cloud compliant
Cloud Native	<ul style="list-style-type: none"> - Fully cloud aware - can communicate with the cloud management layer to start-up or shutdown instances of itself - Designed for failure and self-healing - Elastic and resource efficient

Table 9: Cloud Application Maturity (Source: New Relic)

Case Study

The STORM CLOUDS platform supports two different architectures; a “scale-up” architecture for applications with traditional architectures (**Error! Reference source not found.10**) and a “scale-out” architecture for applications with Cloud-aligned architectures (**Error! Reference source not found.11**).

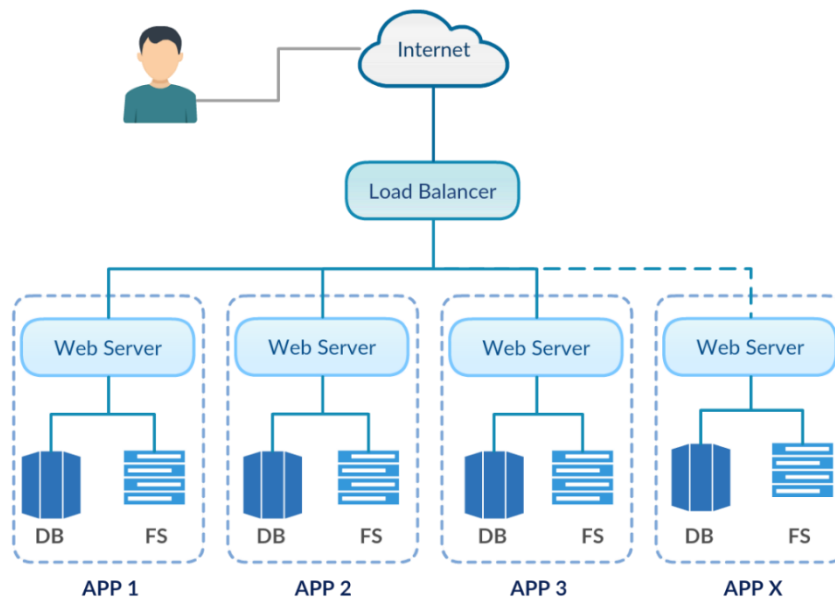


Figure 10: SCP “Scale-up” Architecture for traditional applications

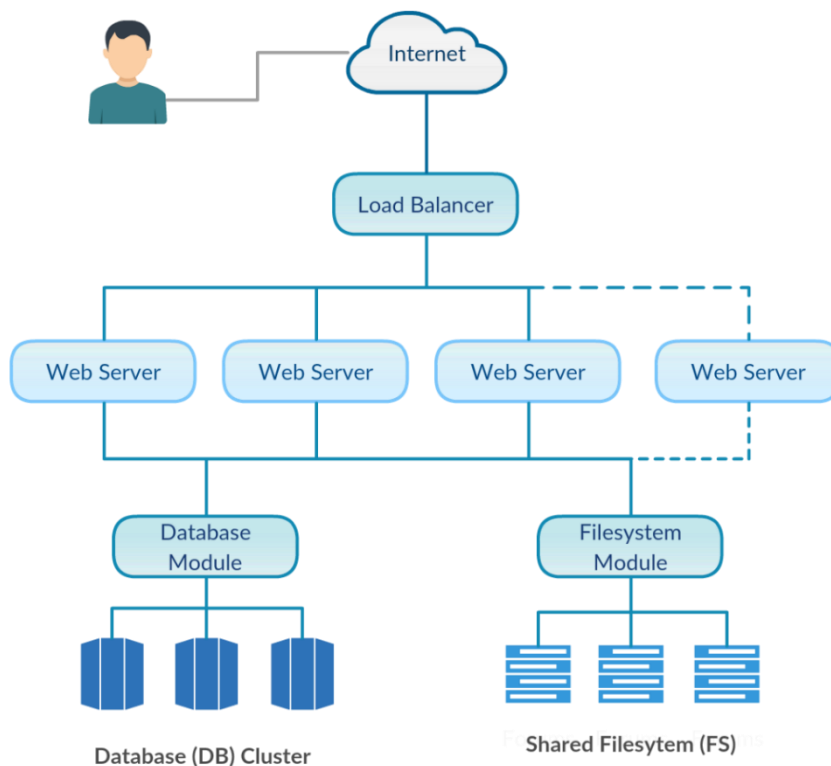


Figure 11: SCP “Scale-out” Architecture for Cloud-ready applications

The “scale-up” architecture is the one where the application can benefit from more resources, such as CPU and memory, being added to a single server or node. In contrast, the “scale-out” architecture is the one where an application scales by additional nodes being made available for the workload; that is, it scales horizontally.

Scale-out applications can take advantage of the pay-by-usage cost model of the cloud. When there are increased requests for an application, more nodes can be deployed to handle the increased load. When the requests slow down, the additional nodes can be powered off to reduce costs.

Although virtualisation technologies have started to support the dynamic scale-up and scale-down of a single VM’s resources (memory, CPU and disc space), this action requires, at the moment, the use of custom scripts. On the contrary, the systems that support the scale-out architectures provide native support to the dynamic

increase of resources.

6.3 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 number 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:

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.

- 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.

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.

6.4 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, captcha 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, Isung 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.

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.

Case Study

Disaster prevention and restoring using High Availability: 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.

7 Administrator of the clouds

7.1 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. One of the characteristics of the Cloud, which facilitates the agile deployment of the applications, is the fact that administrators don't have to master the art of capacity planning because they can create an automated elastic environment (Varia, 2011). If they can understand, monitor, examine and observe the applications' load and traffic patterns, they will be able to manage this elastic environment more effectively. Moreover, by measuring and monitoring the performance of the cloud applications, the application developers will have the opportunity to identify proactively any performance issues and to diagnose the root causes, so they take appropriate actions.

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.

The STORM CLOUDS approach

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 pages.

7.2 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 Zabbix¹¹, 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.

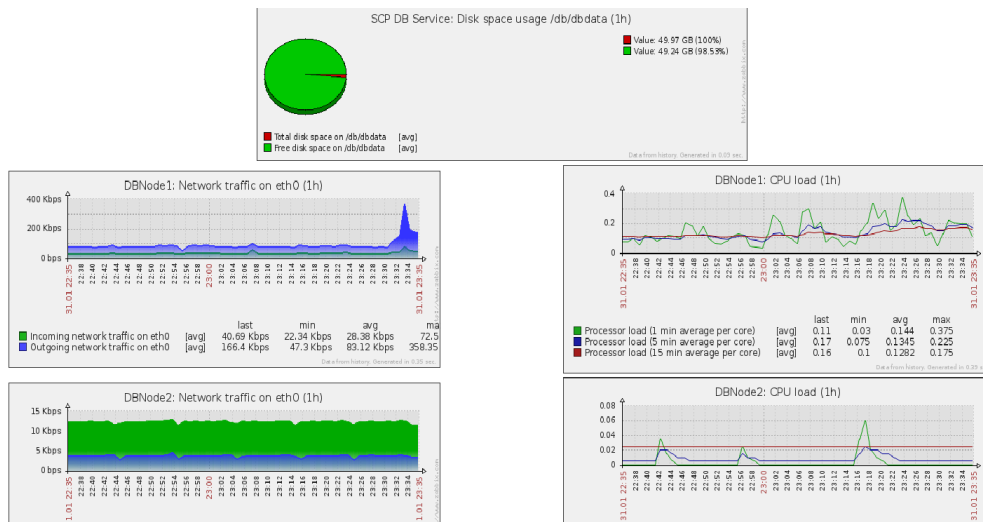


Figure 12: Zabbix Monitoring Pages

7.3 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:

¹¹ Zabbix – Main Page, viewed November 10, 2015 <<http://www.zabbix.com>>

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

Case Study

In STORM Clouds project a Backup Tool was developed as part of the administration platform, which takes backups from databases and file systems. This module is implemented using Duplicity, an application that creates encrypted bandwidth-efficient backups using the rsync algorithm.

7.4 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)¹² 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

¹² <https://joinup.ec.europa.eu/elibrary/document/interoperability-maturity-model>

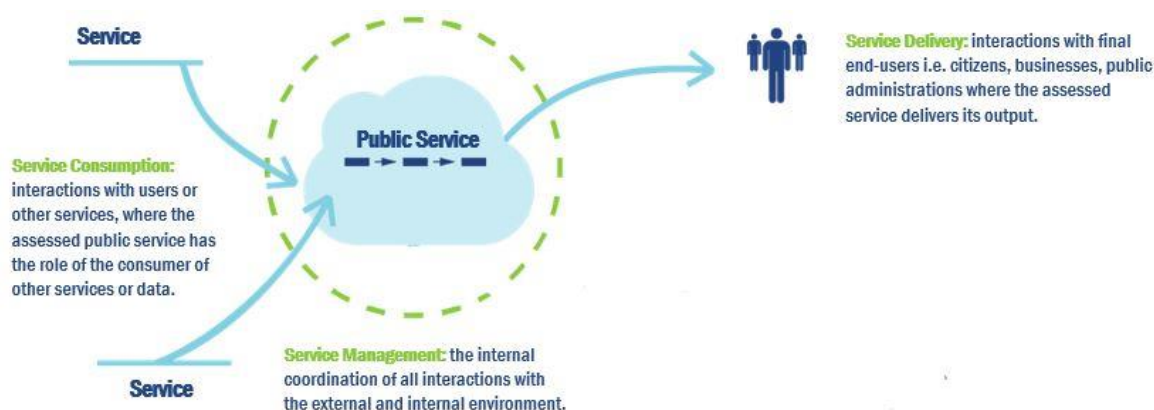


Figure 13: The three different domains of interoperability in IMM (Source: European Commission)

The IMM uses a five-stage model to indicate the interoperability maturity of the public service. The reason for the usage of these various maturity levels is two-fold:

- To measure the interoperability maturity of the public service as a whole and of the underlying aspects;
- To indicate which capabilities and next steps are required to improve interoperability maturity.

The five maturity levels for the IMM are summarised in the table below:

Maturity level	Maturity stage	Interpretation
1	Ad Hoc	Poor interoperability – the service has almost no interoperability in place
2	Opportunistic	Fair interoperability – the service implements some elements of interoperability best practices
3	Essential	Essential interoperability – the service implements the essential best practices for interoperability
4	Sustainable	Good interoperability – all relevant interoperability best practices are implemented by the public service
5	Seamless	Interoperability leading practice – the service is a leading example for others

Table 10: Five maturity stages of IMM (Source: European Commission)

The desired interoperability level for a public service is at minimum level 4: 'Sustainable'. At this level, the public service is considered to have implemented all relevant best practices.

The STORM CLOUDS approach

The STORM CLOUDS Smart City Applications were evaluated using the Interoperability Maturity Model Questionnaire. Based on the assessment a tailor-made set of recommendations was provided towards the service owner. The following five principles are applied to generate recommendations:

- 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.

For each improvement step the provided recommendation tables show the next maturity level to be achieved through improvement and the general recommendation as to how to achieve the next maturity level (EC, 2016).

8 Data Management

8.1 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. Municipalities are also 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

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 should 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.

hard to distinguish the entity that has originated the problem, to the point that, as mentioned by Haeberlen (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.

8.2 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). [Any data that could uniquely identify a person or, which is not supposed to be known to any person other than its owner and/or her immediate family, without her consent is called Private Data (Rastogi, 2013).

Data protection is the process of safeguarding important information from corruption and/or loss (Microsoft, 2014). We define customer data as *“all the data, including all text, sound, software or image files that a user provides, or are provided on the users’ behalf, to the cloud provider through use of the online services.”*¹³The term data protection is also used to describe operational backup of data that usually comes in the form of incremental backups. The aim of the backup procedure is to keep data from being lost due to intentional or unintentional access.

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-

¹³ Data protection, viewed November 10, 2015 <<http://goo.gl/MipM9c>>

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 [7] while in the second with any rules about safe payments, such as the Payment Card Industry's Data Security Standard (PCI DSS)¹⁴.

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.

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

¹⁴ PCI Security Standards Council, viewed June 2, 2016, <https://www.pcisecuritystandards.org>

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.
 - 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.

8.3 Ownership

The primary difference between encryption key management in an enterprise's data centre versus key management in the cloud is ownership and management of the keys. In a traditional data centre, all key management functions and tools can be configured and maintained by an IT operations team. In cloud environments, the cloud providers and public authorities should make encryption key management a shared responsibility between the cloud provider and the cloud user (citizens and/or public servants). The goal is to reduce costs and improve efficiency as part of a formal key management strategy.

The type of cloud service in use dictates the types of key management available.

It must be noted upfront that in all architectural solutions where cryptographic keys are stored in the cloud, there is a limit to the degree of security assurance that the cloud Consumer can expect to get, due to the fact that the logical and physical organisation of the storage resources are entirely under the control of the cloud Provider.

Error! Reference source not found.

The Key Management Interoperability Protocol (KMIP) is a standard that is designed to be a comprehensive protocol for secure exchange of keys between key management systems and encryption devices or applications. By using a standardised protocol, public authorities are able to simplify key management and deploy key management systems that span multiple use cases and equipment vendors.

According to Ponemon, 54 percent of respondents said that KMIP is most important for cloud based applications and storage.

9 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.

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.

Supply	Demand	Dissemination	Validation
Nbr of shops participating in the app	Total nbr of users – visitors	Total presence of the platform in third party websites	Number of users providing feedback for the application
Nbr of shops per category	Total nbr of registered users	Total e-mails/newsletters sent	Number of stakeholders providing feedback for the application
% of shops participating in the platform/shops in the area (total)	Mean nbr of visitors per shop		Number of modifications (new characteristics that have been modified based on the feedback received)
% of shops participating in the platform/shops operating in the area (category)	User demographics (area, age, education level)		
Nbr of shops that have extended their online presence in the platform			
Nbr of shops making online transactions through the platform			
Nbr of offers per shop			
Nbr of synergies between two or more shops			

Figure 14 – Monitoring and validation indicators for the Virtual City Market application

Supply	Demand	Dissemination	Validation
Nbr of projects being registered in the crowdfunding platform	Total nbr of users	Total presence of the platform in third party websites	Number of users providing feedback for the application
Nbr of projects per category	Total nbr of registered users		Number of stakeholders providing feedback for the application
Nbr of projects being funded/completed	Nbr of users providing funding to the projects		Number of modifications (new characteristics that have been modified based on the feedback received)
Total funding received through the platform	Mean funding per user		
Mean funding per project	Minimum funding per user		
Min funding per project	Maximum funding per users		
Max funding per project	User demographics (area, age, education level)		

Figure 15 – Monitoring and validation indicators for the CloudFunding application

10 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 infrastructure¹⁵. 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) (Gianakoulis, 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 organisation¹⁶.

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.

¹⁵ What does the Commission mean by secure Cloud computing services in Europe?, 2013, European Commission, viewed November 10, 2015 <<http://goo.gl/MORqia>>

¹⁶ Cloud Security Guidance: Summary of Cloud Security Principles, viewed June 24, 2016 <<http://goo.gl/mUf5c2>>

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.
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 11 - 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:

- **Zed Attack Proxy (ZAP)**, an easy to use integrated web applications vulnerability scanning tool;
- **OpenVAS**, a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution;
- **SQL Inject Me**, a Firefox Extension used to test for SQL Injection vulnerabilities
- **Qualys SSL Server Test**, an online service performing deep analysis of the configuration of any SSL web server on the public Internet;
- **Vega**, an open source scanner and testing platform to test the security of web applications.

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.

11 Conclusions

The report included a bibliographic review on cloudcomputing and proposed a navigation route facilitating the migration process of public services. This is an updated version of the documentation that was delivered in M18 about migration process of public services into the cloud. The content of the report is mainly based on recent scientific papers in addition to about 100 relevant reports.

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/2otrlWM> [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](http://www.cloud-council.org/Security%20for%20Cloud%20Computing-Final%20080912.pdf)
- [21] Cloud Standards Customer Council (CSCC) (2015b) *Practical Guide to Cloud Service Agreements (Version 2.0)*, Available online at: <http://bit.ly/2i7XFCn> [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: Openness 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. & Munte-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/2pIUvkr> [Accessed March 23, 2017].
- [34] Giannakoulis, 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/KRoIV6> [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/1QeOIHm> [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] Suci, G., Vulpe, A., Halunga, S., Fratu, O., Todoran, G. and Suci, 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 Bozdog, E. (2010) The Ethics of Cloud Computing A Conceptual Review, Conference: Cloud Computing, Second International Conference, CloudCom 2010, Timmermans, J., Ikkonen, V., Stahl, B.C., Bozdog, 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. 7-18 High Availability (HA) definition, Margaret Rouse, September 2005, <http://searchdatacenter.techtarget.com/definition/high-availability>

Annex A Body of knowledge about migration of public services to the cloud

1 A Cloud for Global Good: A policy roadmap for a trusted, responsible and inclusive cloud



The roadmap, published by Microsoft, is a list of policy considerations and recommendations that lead to a trusted, responsible and inclusive cloud. The trusted cloud includes recommendations on privacy, national sovereignty, and public safety. The policy recommendations in the responsible cloud section, focus on environmental sustainability, human rights, protecting people from the dangers of online exploitation and fraud and artificial intelligence. Policy recommendations in the in the inclusive cloud section include education and skills training, accessibility, affordability and support for small businesses. These recommendations can offer a framework for implementing a new generation of laws designed specifically to capture the benefits of cloud computing while managing the challenges..

Microsoft (2016) A Cloud for Global Good: A policy roadmap for a trusted, responsible and inclusive cloud.

<https://news.microsoft.com/cloudforgood/ media/downloads/a-cloud-for-global-good-english.pdf>

2 Making the move to Cloud Computing



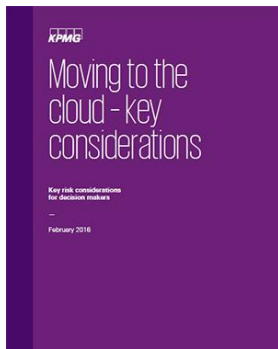
The report aims to cover the uncertainty and confusion that prevents many businesses from adopting cloud computing. It is a guide, developed as a follow up of the 2010 study “Cloud Computing: A guide for business managers”, which presents the journey to the clouds in four key stages:

1. understanding the options, i.e. the service and deployment models of cloud computing,
2. identifying opportunities through the conduction of internal IT/business/legal reviews (these opportunities might be requirements for operational expenditure or a problem that needs to be assessed or an opportunity for a positive choice) before the selection of a cloud provider,
3. cloudsourcing, i.e. begin ruling out some potential providers, armed with the knowledge of what risks and costs are acceptable to your organisation and
4. implementation, i.e. test selected clouds and implement a project plan with an exit strategy. The study concludes with a six-step iterative process for cloud computing adoption based in the above.

Williams, M. I. (2012) Making the move to Cloud Computing, ICAEW Information Technology Faculty.

<https://www.icaew.com/-/media/corporate/archive/files/technical/information-technology/technology/making-the-move-to-cloud-computing.ashx?la=en>

3 Moving to the cloud – key considerations



This report is a short guide for decision makers who are accountable for information risk and other senior individuals who need to make appropriate, proportionate and risk-aware choices when considering the purchase of cloud computing services for enterprise use. It outlines key features and risks of the various forms of cloud computing and provides decision makers with a set of key issues to address when considering the adoption of cloud services. The report analyses commercial, contractual, privacy and security considerations and concludes with a set of recommendations in response to these considerations.

KPMG (2016) Moving to the cloud – key considerations.

<https://assets.kpmg.com/content/dam/kpmg/pdf/2016/04/moving-to-the-cloud-key-risk-considerations.pdf>

4 Cloud Computing: A Guide for Business Managers



This is an introductory guide to cloud computing targeting at managers in both IT and other disciplines. It includes a definition of the cloud along with its pros and cons. The report continues with recommendations on how to select a cloud provider, after having defined a number of requirements such as compatibility, availability and performance, as well as security and compliance. The report concludes with a number of internal issues that should be addressed (e.g. staff involvement or resistance) and the myths around cloud computing.

Barnaby, P. (2010) Cloud Computing: A Guide for Business Managers, ICAEW.

<http://www.icaew.com/-/media/corporate/archive/files/technical/information-technology/it-management/cloud-computing-a-guide-for-business-managers.ashx>

5 Cloud Computing: Benefits, risks and recommendations for information security



The report focuses on the benefits and the risks that arise from a security point of view from cloud computing. The key conclusion of the report is that the cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defences can be more robust, scalable and cost-effective. The report allows an informed assessment of the security risks and benefits of using cloud computing – providing security guidance for potential and existing users of cloud computing.

The security assessment is based on three use-case scenarios: 1) SME migration to cloud computing services, 2) the impact of cloud computing on service resilience, 3) cloud computing in e-Government (e.g., eHealth). These scenarios are used to explain what cloud computing means for network and information security, data protection and privacy, covering technical, policy and legal implications. The report concludes with concrete recommendations on how to address the risks and maximise the benefits of cloud computing.

ENISA (2009) 'Cloud Computing: Benefits, risks and recommendations for information security', European Network and Information Security Agency.

https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport

6 Steps to improve Cloud Computing in the Public Sector

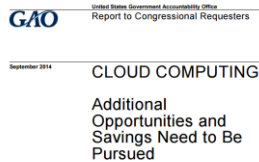


The paper addresses a number of Federal Computing Policy problems and provides a list of recommendations to improve the efficiency and effectiveness of cloud computing adoption by the US government. The public sector makes relatively little use of cloud computing even though the private sector has achieved excellent cost savings and studies have suggested substantial government savings from a migration to the cloud. To deal with the existing problems, a number of policy changes should be adopted, such as to improve transparency, promote cloud-based services, modernise laws and seek international agreements on cloud computing etc.

West D., M. (2010) Steps to improve Cloud Computing in the Public Sector, Issues in Technology Innovation, Number 1, pp. 1-13.

https://www.brookings.edu/wp-content/uploads/2016/06/0721_cloud_computing_west.pdf

7 Cloud Computing: Additional Opportunities and Savings Need to Be Pursued



The report is an assessment of seven selected US government agencies' progress in implementing cloud services. More specifically, the report aims to (1) assess these selected agencies' progress in using cloud computing services, (2) determine the extent to which the selected agencies have experienced cost savings when such services have been deployed, and (3) identify any challenges the selected agencies are facing as they use cloud computing. This performance audit was conducted from December 2013 through August 2014 and it is a very useful example on how to assess the impact of cloud computing on public sector organisations.

The agencies' relatively small increase in cloud spending as a percent of their overall IT budgets, is attributed in part, to the fact that these agencies collectively had not considered cloud computing services for about 67 percent of their investments.

The agencies collectively reported cost savings of about \$96 million from the implementation of 22 of the 101 cloud services. These savings included both one-time and multiyear savings. For example, the General Services Administration saved \$2.6 million by migrating to a cloud customer service solution, and Homeland Security saved \$1.2 million from fiscal years 2011 through 2013 by implementing a cloud-based collaboration service. Agency officials cited two major reasons for why the other services they had implemented did not save money. First, a motivation for changing to some of the cloud-based services was not to reduce spending, but to improve service. Second, in selected cases, the cloud computing service opened up a new service or provided a higher quality of service; while this provided useful benefits to the agency, the associated costs negated any savings.

United States Government Accountability Office (2014) Cloud Computing: Additional Opportunities and Savings Need to Be Pursued' Report to Congressional Requesters, GAO-14-753.

<http://www.gao.gov/assets/670/666133.pdf>

8 A new era for European public services



Across Europe, people's lives are becoming increasingly digitized. In addition to interacting with organizations like banks, airlines and retail outlets on the web, European citizens now expect that transactions with their public services should take place online too.

Digital government is on the way—and cloud computing is the next logical step towards it. Before adopting cloud in earnest, however, Europe's governments will have to overcome a number of barriers, some of which are structural issues at the national level while others are more global in nature.

As European governments actively seek ways to leverage modern technology to serve citizens better, two conflicting demands arise. Governments have to make sure they invest enough to maintain and improve standards, but must work to ever-tighter budgets, finding cost-effective ways to tailor services. It's the classic dilemma of introducing efficiency while also driving economic growth.

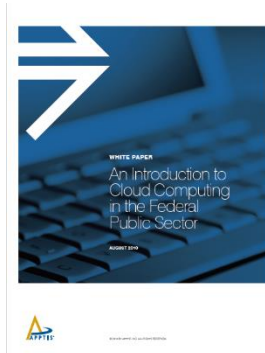
To meet these demands, governments need to start providing services in a new and innovative way. The introduction of cloud computing represents a cost-effective and scalable approach, while also being agile, flexible and secure.

In this major new piece of thought leadership, Accenture examines the issues, implications, benefits and opportunities facing Europe's governments as they grapple with integrating cloud computing across the full range of public services they provide.

Accenture (2013) A new era for European public services: Cloud computing changes the game.

https://www.accenture.com/t20150527T211057_w_/fr-fr/acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/fr-fr/PDF_4/Accenture-New-Era-European-Public-Services-Cloud-Computing-Changes-Game.pdf

9 An Introduction to Cloud Computing in the Federal Public Sector



The Cloud Computing industry represents a large ecosystem of many models, vendors, and market niches each with their own approaches to exploiting the gains that cloud promises. In May 2010, a simple Web search of the term “Cloud Computing” returned over 14 million hits, creating an intractable task for any leader, team, or agency trying to define the cloud and adapt it to further their mission. This vendor-neutral white paper presents the concepts and application of Cloud Computing in the U.S. public sector and can be used as a starting point for formulating an agency’s cloud strategy.

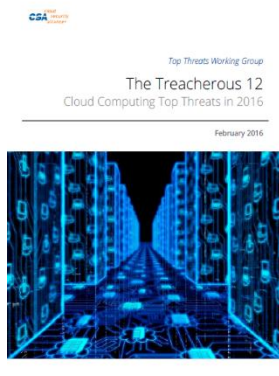
The economic gains of Cloud Computing are so compelling that Office of Management and Budget (OMB) budget and guidance contains cloud requirements as follows:

- In FY10, OMB requires agencies to launch a series of Cloud Computing pilots across the government using the E-Government Fund.
- In FY11, the OMB will require agencies to develop an alternative analysis discussing how they could use Cloud Computing for all major technology projects in FY12.
- In FY12, OMB will require agencies to provide complete alternatives analysis for IT programs that are new development or are steady state, explaining how they could incorporate Cloud Computing in their environment.

APPTIS (2010) White Paper: An Introduction to Cloud Computing in the Federal Public Sector.

http://cloud.report/Resources/Whitepapers/22303cd5-813c-42f7-a1b9-2a33969e13fa_Apptis%20-%200826-2_IntroToCloudComputing_Whitepaper.pdf

10 The Treacherous 12: Cloud Computing Top Threats in 2016



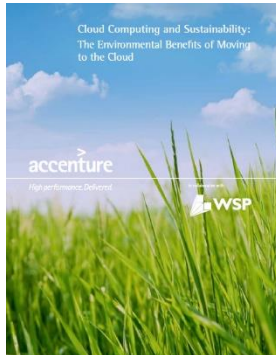
The 2016 Top Threats release mirrors the shifting ramifications of poor cloud computing decisions up through the managerial ranks, instead of being an IT issue it is now a boardroom issue. The reasons may lie with the maturation of cloud, but more importantly, higher strategic decisions by executives in cloud adoption. The 2013 edition highlighted developers and IT departments rolling out their own self-service Shadow IT projects, and the bypassing of organizational security requirements. In 2016, cloud adoption may be effectively aligned with the executive strategies to maximize shareholder value. The always-on nature of Cloud Computing impacts factors that may skew external perceptions and in turn company valuations. Wider reaching architecture/design factors of Identity, Credential and Access Management, Insecure APIs and System & Application Vulnerabilities rise in the survey, while data loss and individual account hijacking fell in comparison.

With descriptions and analysis of the Treacherous 12, this report serves as an up-to-date guide that will help cloud users and providers make informed decisions about risk mitigation within a cloud strategy. This threat research document should be utilized in conjunction with the best practices guides, “Security Guidance for Critical Areas in Cloud Computing V.3” and “Security as a Service Implementation Guidance”. A threat analysis was also conducted with the STRIDE Threat Model[1] and the working group recommends the NIST Risk Management Framework[2] on guidance for how to manage information technology risk. Together, these documents will offer valuable guidance during the formation of comprehensive, appropriate cloud security strategies.

CSA (2016) The Treacherous 12: Cloud Computing Top Threats in 2016, Top Threats Working Group, Cloud Security Alliance.

<https://cloudsecurityalliance.org/group/top-threats/>

11 Cloud Computing and Sustainability



To assess the environmental impact of cloud computing, Microsoft engaged with Accenture—a leading technology, consulting and outsourcing company— and WSP Environment & Energy—a global consultancy dedicated to environmental and sustainability issues—to compare the energy use and carbon footprint of Microsoft cloud offerings for businesses with corresponding Microsoft on-premise deployments.

The analysis focused on three of Microsoft’s mainstream business applications—Microsoft Exchange®, Microsoft SharePoint® and Microsoft Dynamics® CRM. Each application is available both as an on-premise version and as a cloud-based equivalent.² The team compared the environmental impact of cloud based vs. on-premise IT delivery on a per-user basis and considered three different deployment sizes—small (100 users), medium (1,000 users) and large (10,000 users).

The study found that, for large deployments, Microsoft’s cloud solutions can reduce energy use and carbon emissions by more than 30 percent when compared to their corresponding Microsoft business applications installed on-premise. The benefits are even more impressive for small deployments: Energy use and emissions can be reduced by more than 90 percent with a shared cloud service.

Several key factors enable cloud computing to lower energy use and carbon emissions from IT:

- **Dynamic Provisioning:** Reducing wasted computing resources through better matching of server capacity with actual demand.
- **Multi-Tenancy:** Flattening relative peak loads by serving large numbers of organizations and users on shared infrastructure.
- **Server Utilization:** Operating servers at higher utilization rates.
- **Data Center Efficiency:** Utilizing advanced data center infrastructure designs that reduce power loss through improved cooling, power conditioning, etc.

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

<http://gesi.org/files/Reports/Cloud%20Computing%20and%20Sustainability%20-The%20Environmental%20Benefits.pdf>

12 Australian Government Cloud Computing Policy



The Australian Government recognises that the community expects government services to be responsive to their needs and available where and when they want them. Key to realising this vision is the effective use of ICT by government, including the adoption of cloud services.

To do this, government agencies need to think and act smarter when it comes to investing in ICT. The availability of cloud services offers an opportunity for government to deliver services more efficiently, as well as providing services that are more responsive to business and community needs.

This policy aims to drive a greater take up of cloud services by federal government agencies by adopting a 'cloud first' approach. Under the Government's Cloud Policy agencies now must adopt cloud where it is fit for purpose, provides adequate protection of data and delivers value for money.

The Australian Government procures approximately \$6 billion of ICT services annually and combined with state and territory governments, public sector expenditure on ICT accounts for approximately 30 per cent of the domestic market.

Australian Government, Department of Finance (2014) Australian Government Cloud Computing Policy: Smarter ICT Investment, Version 3.0.

<http://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf>

13 Cloud Computing in the Public Sector



Cloud computing—delivering infrastructure, services, and software on demand via the network—offers attractive advantages to the public sector. For example, it has the potential to reduce information and communications technology (ICT) costs by virtualizing capital assets like disk storage and processing cycles into a readily available, affordable operating expense.

Some public sector organizations have made early moves into cloud computing. For example, in Washington, D.C., all 38,000 city government employees have unlimited access to Google documents and services such as Gmail. The U.S. General Services Administration recently announced moving the government-wide portal usa.gov to the cloud and issued an RFI for cloud infrastructure services. In Japan, the Ministry of Internal Affairs and Communications has announced plans to shift all government agencies into a private cloud environment by 2015.

One of the most significant cloud computing opportunities for the public sector is the ability to share ICT resources among multiple agencies. While governments have tried hard to create frameworks geared toward shared services, these have not always been successful. Cloud computing offers an easier and less burdensome route to more efficient and effective public sector information management. This may be especially true for developing countries that do not have the technology, skilled personnel, or resources to create world-class ICT infrastructures.

Cloud computing is a natural evolution of the Internet, requiring careful consideration and planning.

Cisco (2009) White Paper. Cloud Computing in the Public Sector: Public Manager's Guide to Evaluate and Adopting Cloud Computing, Cisco Internet Business Solutions Group (BSG).

http://www.cisco.com/c/dam/en_us/about/ac79/docs/sp/Cloud_Computing.pdf

14 Analysis of cloud best practices and pilots for the public sector



Analysis of cloud best practices and pilots for the public sector



The objective of this study was to analyse the current national initiatives for the deployment of clouds in the public sector in ten Member States, to identify and describe best practice use cases and to propose pilots for those application areas where current cloud take-up is absent or however limited.

So far, in the 10 Member States covered by the study (Austria, Belgium, Denmark, France, Germany, Italy, the Netherlands, Portugal, Spain, the United Kingdom), the deployment of cloud in the public sector (at the national level) is at a very early stage.

The Member States have taken very different approaches regarding cloud in terms of applications covered (citizen-type, employee-type, vertical, critical, sensitive), type of infrastructure (public cloud versus private cloud), relationships with e-government applications (development from scratch or just migration of existing applications), or global policy.

These approaches can be clustered into 3 main emerging models (with their own best practices) that are presented below. They differentiate mainly in the nature of the infrastructure and the level of centralisation, implying the search for a trade-off between level of control (to ensure better technical performances or security, especially when sharing data) and short-term savings.

- First model: Procurement and Marketplace
- Second model: Resource Pooling
- Third model: Standalone applications

Bonneau, V., Mahieu, B., Dudenbostel, T., Gaudemer, J., Giarracca, F., Good, B., Poel, M., Ramahandry, T., Van Til, J. (2013) Analysis of cloud best practices and pilots for the public sector, Study prepared for the European Commission DG Communications Networks, Content and Technology, Digiworld by IDATE and Technopolis [group] DOI: 10.2759/35653.

<https://ec.europa.eu/digital-single-market/en/news/analysis-cloud-best-practices-and-pilots-public-sector>

15 Cloud Computing: An overview of economic and policy issues



Cloud computing providers can take advantage of variable demand cycles of different clients and economies of scale to supply computing services at lower cost than would be possible in individual, in-house data centres. More importantly, because cloud customers can ramp up services quickly, they can innovate with new products at low cost or rapidly scale up successful prototype services. Cloud computing is also considered to be more energy efficient than traditional in-house centres, potentially reducing negative effects on the environment. Individual consumers of cloud-based email, file- or media-sharing services get access to their information anywhere, often at little or no cost.

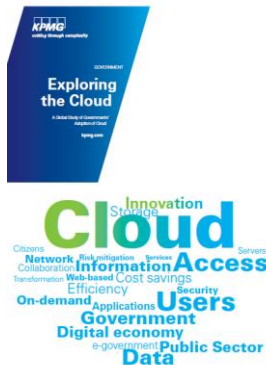
However, because cloud computing uses shared computing environments and relies on the public internet for transmitting information, it raises concerns about security and personal data protection. Also, the lack of interoperability between cloud service products and the absence of standards that would facilitate data portability may make it difficult for customers to switch vendors. Fixed or obscure contract terms that limit liability or service guarantees may also restrict customers' rights.

The European Commission considers cloud computing central to the EU's competitiveness and a key to economic growth and innovation. As part of its Digital Single Market Strategy, the Commission has a European Cloud initiative that will propose certification of cloud services, reduce the risks of vendor lock-in, and provide a research cloud for researchers to share access to research data. The Commission has also promised to propose in 2016 a 'free flow of data initiative' that will tackle restrictions on where data is located.

EPRS (2016) Cloud Computing: An overview of economic and policy issues, European Parliamentary Research Service doi: 10.2861/705354.

[http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA\(2016\)583786_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA(2016)583786_EN.pdf)

16 A Global Study of Governments' Adoption of Cloud



How are governments planning for and adopting cloud? What are the challenges of cloud-enablement? How will the integration of cloud technologies disrupt the status quo of governance? More importantly, what are governments doing to ensure they get the most from their cloud investments?

These are just some of the questions that KPMG International hopes to answer with this report. Working in conjunction with Forbes Insights, close to 430 public-sector government executives from 10 countries were surveyed to learn more about their cloud strategies and expectations.

Key findings are as follows:

- Government adoption of cloud is happening slowly, but is poised to accelerate:
- The public sector has modest expectations of cloud:
- Security remains the biggest concern, but certification would help:

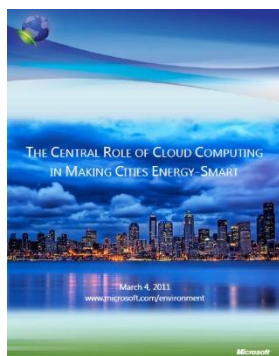
This report examines the implications of these findings on governments, citizens, cloud service providers and IT leaders. Responses from the global business survey of 808 business executives are referenced to provide further context. Throughout, we combine the deep experience of KPMG member firms' professionals with the results of a series of in-depth interviews that were conducted with government leaders from around the world.

The results provide insight into the current state of government cloud and offer an important benchmark for public sector organizations globally.

KPMG (2012) Exploring the Cloud: A Global Study of Governments' Adoption of Cloud.

<https://images.forbes.com/forbesinsights/StudyPDFs/exploring-cloud.pdf>

17 The Central Role of Cloud Computing in Making Cities Energy-Smart



The evolution of urban energy infrastructures is already being enabled by the integration of information technologies that help manage the dynamic, increasingly distributed nature of the supply of and demand for energy. Maturing cloud computing and data management technologies offer new opportunities to address energy management issues on a new scale; one that is needed in a world of increasing energy and environmental constraints. In fact, the evolution of energy infrastructures won't be achieved without information technologies – in particular, applications and services that leverage the computing capabilities of the cloud. All cities will need to leverage systems that are connected and supported by a large volume of real-time data from diverse public and private sources if they are to meet the needs of increasing population.

Microsoft and its partners are working with utilities, universities, governments, building management companies, and leaders in the IT industry to accelerate the development of energy management solutions for our growing cities. Just as Microsoft has nurtured partner ecosystems that have delivered broad portfolios of innovative solutions to advance key industries such as manufacturing, healthcare, education, and many others, it is our intent to apply the same model to energy management systems. We believe this broad approach is critical to accelerate the evolution of energy-smart cities. The scale of this challenge cannot be addressed by one company alone; it needs the breadth of the IT industry to deliver a wide spectrum of solutions for the sustainable design and management of energy across power generation, distribution grids, buildings and transportation systems.

Microsoft (2011) The Central Role of Cloud Computing in Making Cities Energy-Smart, Microsoft Corporation.

http://smartcitiescouncil.com/system/tdf/public_resources/Role%20of%20cloud%20computing%20in%20making%20cities%20energy-smart.pdf?file=1&type=node&id=144

18 Cloud Computing Concerns in the Public Sector



Public sector organizations have much to gain by taking a cloud computing approach to service delivery in their information and communications technology (ICT) environments. But they must have confidence that the benefits can be achieved without compromising core requirements and institutional values.

This paper briefly examines issues that often present barriers to public sector cloud implementation. In particular, it focuses on reliability and resilience, privacy and security, and standards and development. We'll discuss how hybrid clouds are helping to overcome many objections to cloud deployment. We'll also touch on financing models that are making cloud computing more affordable.

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

http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/pscloudconcerns.pdf

19 Study on cloud and service oriented architectures for e-government



Study on cloud and service
oriented architectures for e-
government
Final report



08-12-2011
Document Control no: 00000000-00
Authors: P. Wauters, K. Declercq, S. van der Peijl, P. Davies

The objective of this study is to identify ‘Fundamental Services’ in the context of new “Universal or Global” SOA approaches to the provision of eGovernment services. The key questions which it addresses are: at which level of granularity can ‘Fundamental Services’ be defined? Which ones have the highest potential for reuse? And what are the possibilities for and the potential impacts of delivering public services in line with the concept of a ‘cloud of public services’?

In this context and against the background of significant recent policy and technological developments, the study developed a service taxonomy and methodology in order to identify the ‘building blocks’ of public services delivered online for citizens and businesses. The proposed taxonomy and methodology, which are based on a review of existing SOA-related literature, were then applied via case studies within the scope of the life cycle of a business in three Member States (Sweden, Italy and Belgium) in order to develop a definition of a ‘Fundamental Service.’ Finally, based on real-life approaches to the provision of online public services for reuse by different actors (public administrations and third parties), as well as suggested future scenarios, the study analysed the possibilities for the design of a ‘cloud of public services’ and of the impact of offering public services in this way. The main conclusions of the study are then presented and a number of recommendations for future activities are made.

Wauters, P., Declercq, K., van der Peijl, S. and Davies, P. (2011) Study on cloud and service oriented architectures for e-government, Final report, Deloitte.

<https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/smart2010-0074finalreport.pdf>

20 Establishing a Trusted Cloud Europe



Cloud computing has the potential to bring significant advantages to European citizens, businesses and public administrations, in terms of cost savings, efficiency boosts, user-friendliness, better security, and accelerated innovation. However, access to cloud services in Europe is currently hampered by a number of uncertainties and challenges, which vary from use case to use case. Depending on the type of data, type of service, and need for enforcement, adoption of the cloud may be impeded by legal, technical, operational or economic barriers, as shown through the examples in this document. The Steering Board of the European Cloud Partnership recognises the need to address these uncertainties and challenges through specific and targeted actions, so that Europe can reap the benefits from the shift to cloud computing. Industry, public administrations and cloud users should work on the basis of common templates for similar use cases, which can be adopted step by step in order to improve the functioning of the digital single market for cloud services, and to avoid needless duplication of effort and market fragmentation.

This paper presents two groups of actions in order to reach this objective:

- Firstly, a flexible common framework of best practices needs to be created, at the legal, technical and operational level.
- Secondly, systematic consensus building is required, through public consultations, workshops, coordination groups etc., targeting all stakeholders, including citizens, public administrations, the cloud industry and cloud users.

European Commission (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 Communications Networks, Content and Technology DOI: 10.2759/44445.

<http://bookshop.europa.eu/en/establishing-a-trusted-cloud-europe-pbKK0114281/>

21 Your Cloud in the Public Sector



Your Cloud in the Public Sector

INDUSTRY BRIEF WHITE PAPER

The public sector is adopting enterprise hybrid cloud across governmental and educational institutions with the goal of improving the quality of public services, reducing costs, and increasing responsiveness to risk. This industry brief outlines the common hybrid cloud use cases that are yielding significant benefits for public sector organizations and provides a real-world example that illustrates how agencies are adopting cloud computing to achieve business agility.

VMware (2011) Your Cloud in the Public Sector: Industry Brief White Paper.

22 Cloud Computing Advantages in the Public Sector

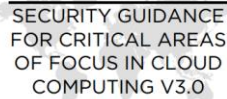


Cloud computing is a disruptive technology model that is changing the way public sector organizations consume information and communications technology (ICT), and how they deploy and deliver services to stakeholders. A trusted network infrastructure is the foundation for any successful cloud implementation. This paper briefly reviews the status of cloud computing in government, education, and healthcare organizations. It also helps make the business case for a cloud implementation by summarizing the chief advantages and business drivers. Case study snapshots describe how public sector organizations have successfully implemented cloud services models in various environments worldwide.

Macias, F. and Thomas, G. (2011) Cloud Computing Advantages in the Public Sector: How Today's Government, Education and Healthcare Organizations Are Benefiting from Cloud Computing Environments, White Paper, Cisco.

http://www.cisco.com/c/dam/en_us/solutions/industries/docs/c11-687784_cloud_omputing_wp.pdf

23 Security Guidance for Critical Areas of Focus in Cloud Computing

The logo for the Cloud Security Alliance (CSA) is located on the left side of the page. It consists of the letters 'CSA' in a bold, blue font, followed by the words 'cloud security alliance' in a smaller, lighter blue font.The cover of the report 'Security Guidance for Critical Areas of Focus in Cloud Computing V3.0' is shown on the left. It features a blue and white design with the title in a bold, sans-serif font.

This is the third and last version of the CSA's flagship report "Security Guidance for Critical Areas of Focus in Cloud Computing." This work is a set of best security practices CSA has put together for 14 domains involved in governing or operating the cloud (Cloud Architecture, Governance and Enterprise Risk Management, Legal: Contracts and Electronic Discovery, Compliance and Audit, Information Management and Data Security, Portability and Interoperability, Traditional Security, Business Continuity and Disaster Recovery, Data Center Operations, Incident Response, Notification and Remediation, Application Security, Encryption and Key Management, Identity and Access Management, Virtualization, and Security as a Service).

CSA guidance in its third edition seeks to establish a stable, secure baseline for cloud operations. This effort provides a practical, actionable road map to managers wanting to adopt the cloud paradigm safely and securely. Domains have been rewritten to emphasize security, stability, and privacy, ensuring corporate privacy in a multi-tenant environment.

In the third edition, the guidance assumes a structural maturity in parallel with multinational cloud standards development in both structure and content. Version 3.0 extends the content included in previous versions with practical recommendations and requirements that can be measured and audited. The guidance does not represent a statutory obligation, but "requirements" was chosen to represent guidance appropriate for virtually all use cases we could envision, and also aligns our guidance with similar well-accepted documents.

CSA (2011) Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance..

<https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf>

24 State of the Cloud Report: Hybrid Cloud Adoption



In January 2016, RightScale conducted its annual State of the Cloud Survey. The survey questioned technical professionals across a broad cross-section of organizations about their adoption of cloud infrastructure. The 1,060 respondents range from technical executives to managers and practitioners and represent organizations of varying sizes across many industries. Respondents represent companies across the cloud spectrum, including both users (17 percent) and non-users (83 percent) of RightScale solutions. Their answers provide a comprehensive perspective on the state of the cloud today.

The 2016 State of the Cloud Survey identified several key findings:

- Hybrid cloud adoption grew significantly.
- Cloud users leverage 6 clouds on average.
- More enterprise workloads shift to cloud, especially private cloud.
- Enterprises increase alignment on role of central IT teams in cloud use.
- Security is no longer the top cloud challenge.
- Cloud cost challenges increase, but optimization efforts lag.
- DevOps grows and Docker spreads like wildfire, especially in the enterprise.
- Amazon Web Services (AWS) continues to lead in public cloud adoption, but Azure (IaaS and PaaS) gain ground.
- Private cloud adoption grows across all providers.

RightScale (2016) State of the Cloud Report, Hybrid Cloud Adoption Ramps as Cloud Users and Cloud Providers Mature.

<http://rightscale%202016%29%20state%20of%20the%20cloud%20report%2C%20hybrid%20cloud%20adoption%20ramps%20as%20cloud%20users%20and%20cloud%20providers%20mature/>

25 Cloud Computing for the Public Sector in Central Europe

Bird & Bird

Cloud Computing for the Public Sector
in Central Europe – the Legal Landscape
by Marcin Górnalski



This paper examines B2G cloud computing services, where an awarding authority or awarding entity (in the meaning of the European Procurement Directives) procures cloud computing services from a private sector provider. We do not discuss the G2G model, where a public sector entity offers cloud type services to other entities from the public sector.

The following issues require particular attention in the context of the public sector procuring cloud services:

- procurement – the impact of public procurement procedures especially in relation to what in the private sector is called “time to market” and the financial value of an award data protection law – primarily processing data in the EU, but also the data processing principles
- budgeting – to what extent are you obliged to predict and budget the costs of cloud computing services especially when you are procuring for a group of public sector entities
- terms & conditions – the conditions upon which the public sector could procure cloud services are yet to be developed, separately for different types of services and the data processed information security – ensuring accessibility, integrity and protecting stored and processed information against unauthorised access
- intelligence and law enforcement – understanding the rights that foreign law enforcement agencies may have to disclose information stored in a foreign cloud; assessing the strategic
- risks of infiltration by foreign intelligence
- EU funding competition – the EU subsidising traditional IT software and hardware purchases which discourages public entities from switching to more efficient cloud computing services

Gawroński, M. (2014) Cloud Computing for the Public Sector in Central Europe – the Legal Landscape, Bird & Bird.

<https://www.twobirds.com/~media/pdfs/brochures/information-technology/bird--bird--cloud-computing-in-central-europe-public-sector.pdf?la=en>

26 Cloud Computing Strategy for Norway



Future growth and welfare in Norway is contingent on continued increase in productivity.¹ Two key factors for growth are innovation and new business development. In order to meet future requirements for public services, we need to make better use of technology. The private sector, particularly service industries, needs to improve at adopting new technology to ensure continued increase in productivity.

Public sector enterprises vary widely in terms of needs, risk profiles, financing and available expertise. One thing they have in common is a responsibility to choose the most appropriate and cost-effective ICT solutions that meet their needs. It goes without saying that the same applies to business and industry.

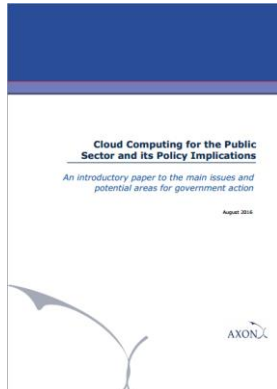
The public sector has a duty to operate as cost-effectively as possible, but it also has a responsibility to properly safeguard citizens' personal data and to protect their interests. It is therefore important that all available solutions be assessed – including cloud computing – when deciding which ICT solutions to procure. Services from the public cloud will suit some enterprises, but not all. The best solution is often a combination of delivery models.

The main objective of the *Cloud Computing Strategy for Norway* is to provide public and private enterprises with more room for manoeuvre when deciding which ICT solutions to use. Provided that other important considerations are not compromised, enterprises should be able to use cloud services wherever they promise the best result and the most cost-effective solution.

Norwegian Ministry of Local Government and Modernisation (2016) Cloud Computing Strategy for Norway.

https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/cloud_computing_strategy.pdf

27 Cloud Computing for the Public Sector and Its Policy Implications



Governments across the world are increasingly considering cloud computing solutions in an effort to provide less costly, more efficient and better public services through a variety of cloud deployment models (private, public, hybrid and/or community clouds).

A typical policy objective driving cloud adoption in the public sector is the improvement and streamlining of 'e-Government services' to meet the demands and expectations of citizens who are increasingly embracing digital and mobile technologies. Better e-Government brings about immediately observable benefits to citizens, but poses the challenge of escalating computing and data processing needs. Cloud computing allows government services to address such increased computing and data processing needs in a flexible, scalable, integrated, cost efficient and secure manner.

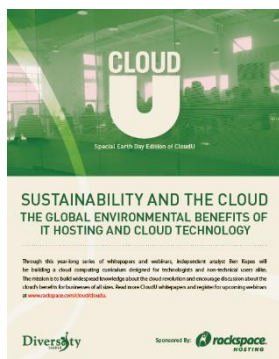
Despite this trend, however, it is still generally common for government agencies to be somewhat reluctant to shift their data to the cloud: erring on the side of caution is a typical and understandable public sector initial response to the challenges of a new, paradigm-shifting, technology.

This paper has been prepared by Axon Partners Group Consulting (Axon Consulting) to provide an introduction to the main policy-related issues concerning cloud computing and to the potential areas for government action. In the next sections this paper, first, provides a high level overview of cloud deployment models. This is followed by a discussion of some common concerns behind cloud adoption. The paper then recommends certain policy and regulatory steps that can help counter these concerns, in light of international experience.

AXON (2016) Cloud Computing for the Public Sector and Its Policy Implications: An Introductory paper to the main issues and potential areas for government action.

<http://www.axonpartnersgroup.com/images/Consulting/News/CloudComputing.pdf>

28 Sustainability and the Cloud



The report details how Cloud Computing, when compared to traditional computing, has multiple positive impacts both economically and environmentally. These benefits are driven by the tendency of Cloud Computing to;

- Reduce total infrastructure allocation
- Increase efficiency by leveraging multi tenancy
- Maximize server utilization rates
- Improve data center efficiency

The report describes how Cloud Computing drives these benefits and why it is the right delivery method to minimize the impact of IT on the planet.

Diversity Limited (2011) Sustainability and the Cloud: The Global Environmental Benefits of IT Hosting and Cloud Technology.

<http://www.diversity.net.nz/wp-content/uploads/2011/04/Earthdayfinal12.pdf>

29 Bringing Cloud Clarity to Public Sector Organisations



Just over three years ago, the UK Government launched its 'Cloud First' initiative. Today, around 24% of departments still don't use the cloud, according to a poll of senior decision makers. When cloud can improve efficiency and security, save costs and help with the digital transformation of the UK's public services, why is it not more widespread? There are a number of myths around adoption of cloud which need to be debunked. The 'Cloud Confusion' that's hindering take-up can only be cleared by a step-by-step analysis of the facts. This white paper highlights these and shines a light on some of the challenges faced by organisations embarking on a cloud journey.

There is sound reasoning behind moving to the cloud. It not only helps reduce IT spend, but can transform the way an organisation works. The report gives an insight into recent research conducted by Kainos regarding cloud adoption of the public sector in UK.

Kainos (2016) Bringing Cloud Clarity to Public Sector Organisations, White Paper.

<https://www.kainos.com/wp-content/uploads/2016/06/Kainos-Cloud-Whitepaper-v04.pdf>

30 State of the art analysis: Cloud solutions in the Public sector



This document contains description of the SUCRE project findings, work and products. This deliverable provides a look into the current state-of-the-art in Open- Source Cloud Computing solutions available for public administrations. Due to the nature of the public sector, most Cloud Computing solutions and service models designed for business use can be also adapted to meet its specific needs. Indeed, to date, many projects address several gaps that exist in the current field of Cloud Computing that range from interoperability to scalability, metrics, optimization and full middleware solutions. Some of those projects promote policy and technology initiatives, while others focus on technical aspects; some solutions are amalgamations of both. Nonetheless, most projects are working to improve interoperability and to provide standards, metrics and platforms that would help to implement a Cloud solution.

The results of the state-of-the-art study reported in this deliverable indicate that, there is still a need for more confirmatory research. Adoption studies are few, and use cases on the use of Cloud Computing in public administrations are generally not publicly accessible. Much of the data presented in this deliverable amount to many possibilities, but evidence of widespread use of Cloud Computing in public administrations is limited or non-existent. Through interviews, aggregate studies and comparative research, the SUCRE project will increase and improve the knowledge of Open-Source Cloud solutions for public administrations.

Mustonen, T. (2013) State of the art analysis: Cloud solutions in the Public sector, Deliverable D1.1, Sucre Project, FP7 -ICT-2011-8.

<http://docplayer.net/1468722-State-of-the-art-analysis-cloud-solutions-in-the-public-sector.html>

31 Thinking About Clouds? Privacy, security and compliance considerations for Ontario public sector institutions

Privacy, security



The use of cloud computing services is increasing in popularity among public sector institutions due to the potential for cost savings and reduced administrative workload that the services entail. While cloud computing may be an attractive option for these and other reasons, the use of this type of service raises concerns about information security, privacy and legal compliance.

This guidance document has been prepared to help institutions evaluate whether cloud computing services are suitable for their information management needs. In particular, it seeks to raise awareness of the risks associated with using cloud computing services and outlines some strategies to mitigate those risks.

Information and Privacy Commissioner of Ontario (2016) Thinking About Clouds? Privacy, security and compliance considerations for Ontario public sector institutions.

<https://www.ipc.on.ca/wp-content/uploads/2016/08/Thinking-About-Clouds-1.pdf>

32 Bringing UK government into the cloud: A guide to cloud computing for the public sector

General



The UK Government is committed to encouraging public sector organisations take advantage of cloud-based computing. The aim is to drive down cost, improve efficiency, and assist the development of service transformation by taking a Digital by Default approach to public services.

In 2012, the UK Government launched the “G-Cloud” initiative. This comprised of a Framework for cloud suppliers and the first CloudStore, allowing organisations from local councils to health authorities browse pre-approved cloud products and services. In May 2013, the Cabinet Office went a step further and announced its Cloud first policy, mandating public sector bodies consider cloud solutions before non-cloud alternatives. The target is for 50% of new public sector ICT spend to be in the cloud by 2015.

There is sound business sense behind this campaign. Moving to the cloud not only helps cut ICT spend but enables dramatic reduction in costs in other areas. It has the potential to transform the way the whole organisation works. It can break down barriers, free people to work more efficiently and effectively and enable members of the public to engage government in ways that suits them best. It can also help you become more responsive and agile and allow you to make better decisions more quickly.

This eBook will show you, step-by-step, how the cloud could help you cut costs, improve performance, collaborate more effectively and empower the public. You'll discover how:

- Wiltshire Council is saving £2 million annually thanks to moving to the cloud and bringing ICT management in-house.
- Local authorities across the country are keeping streets cleaner, while slashing the associated costs thanks to a handy cloud-based Smartphone app.
- How a flexible collaboration tool helped Transport for London staff and volunteers work together to keep London moving during the Olympics.

Microsoft (2014) Bringing UK government into the cloud: A guide to cloud computing for the public sector

http://download.microsoft.com/documents/uk/publicsector/ms_ps_ebook_ukgovcloud_f.pdf

33 The Future of Public Sector ERP: Agile Cloud-Enabled Services (ACES)



The landscape for public sector enterprise resource planning (ERP) system deployments is changing dramatically. Governments are moving away aggressively from highly customized, on-premises solutions toward shared platforms and cloud-enabled managed services. In response, ERP solution providers must offer unprecedented flexibility to meet varying government needs for customization, control and cost containment. Solution providers must also ensure that ERP software, implementation and ongoing operations are tightly integrated to maximize efficiency and accountability. This paper describes the evolving market for public sector ERP deployment models and advocates the need for a flexible ecosystem, named Agile Cloud-Enabled Services (ACES), to serve the diverse requirements of governments of all sizes. We can all use a few more acs in our hand.

While effective ERP systems are needed to manage the business of government, many systems in place today do not have the deployment versatility to deliver adequate functionality. Much attention is now focused on how to deploy modern ERP capabilities in the most efficient manner. Growing numbers of state and local governments are turning to secure, cloud-enabled services for ERP software, platforms and infrastructure so they can stay focused on their mission of serving the public and spend less time managing technology. For example, Maine's move to cloud-enabled ERP has allowed the State to reallocate staff to focus on strengthening policy management as well as internal and fiscal controls on a statewide basis.

The next wave of the ERP deployment evolution must allow governments to choose where and how each function is best located—whether with the government or a managed services partner. It must also provide a tightly integrated approach to the software and all services required for implementation, operation, hosting and management. Without clear lines of accountability, solutions too easily are derailed.

CGI (2016) White Paper – The Future of Public Sector ERP: Agile Cloud-Enabled Services (ACES)

<https://www.cgi.com/sites/default/files/white-papers/cgi-future-of-public-sector-erp-is-aces-white-paper.pdf>

34 Best Practices for Cloud Security: how security in the cloud can be a better bet than doing it yourself. Bloor Research

White Paper

Bloor

Best practices for cloud security

How security in the cloud can be a better bet than doing it yourself

Bloor Research

The use of cloud-based services is growing rapidly, with the use of software as a service (SaaS), in particular, now becoming mainstream. There are many advantages to be gained through the use of such services rather than deploying and managing technology in-house, and many of those benefits, such as cost savings and flexibility, are well documented. However, as a relatively immature technology delivery mechanism, some originally considered security to be an inhibitor to adoption.

That is something that is changing fast, and many now consider improved security to be among the reasons to subscribe to cloud services. Among the reasons for this is that security can be provided that is often better, cheaper and more effective than that available for in-house deployment—for example, by pushing out mitigation against the very latest threats as they are uncovered to all subscribers automatically. Services are more scalable and are better able to meet modern working demands by extending protection to mobile devices.

Cloud delivery is suitable for a wide range of security services, from basic needs such as malware protection to advanced security services such as vulnerability management, security monitoring, policy compliance, and application security and testing. As well as accessing security services, organisations will also benefit from the service provider taking responsibility for many aspects of security as it must itself have developed a highly secure infrastructure in line with best practice and good governance objectives. These incorporate a wide range of security controls and can attest to the quality and security of its services through management reports and audit trails.

This document discusses how cloud-based security services can benefit organisations of all sizes. However, there are still some issues and challenges that remain to be ironed out. This document aims to provide advice to organisations as to what they should look for when considering cloud-based services and what pitfalls there are to avoid.

Howarth, F. (2012) White Paper – Best Practices for Cloud Security: how security in the cloud can be a better bet than doing it yourself. Bloor Research

<https://www.qualys.com/docs/bloor-cloud-security-white-paper.pdf>

35 Cloud Services and the Government Security Classifications Policy

Cloud Services and the Government Security Classifications Policy



ukcloud | white paper

The UK government has increasingly been encouraging the use of cloud services instead of traditional IT solutions as it seeks to create more cost-effective and agile platforms as part of the Government ICT Strategy. To support this strategy the government has implemented a number of policies and initiatives to make the adoption and use of cloud services easier.

One example is the Cloud First policy, an initiative designed to ensure that central government organisations have a strategy to consume cloud services and deter them from continuing to perpetuate non-cloud solutions. Another example is the G-Cloud framework, established by the government to make it much easier for SME providers to create and sell cloud services, and for public sector organisations to buy them.

The government continues to remove potential barriers to cloud services and enable public sector organisations to evaluate, procure and consume them. The Government Security Classifications Policy (GSCP) replaced the previous Government Protective Marking Scheme (GPMS) in 2014 after a period of parallel running.

This white paper provides public sector organisations with advice and guidance to help them make appropriate use of cloud services without compromising the confidentiality, integrity or availability of the information which makes up their digital and shared services. Because not all cloud services are created equal, this paper explains how public sector organisations can safely select appropriate cloud services, even for the most precious of data assets (eg information that was previously classified at IL4).

UK Cloud Ltd. (2016) Cloud Services and the Government Security Classifications Policy- White Paper.

<https://ukcloud.com/wp-content/uploads/2016/08/UKCloud WhitePaper RGB Digital Government Security Classifications policy.pdf>

36 A guide to strategic cloud adoption for government



This guide is suitable for senior officers within government who are responsible for business and IT transformation, estate management and mapping their organisation's IT to its business strategy. The guide looks in detail at the different stages an organisation needs to work through to adopt cloud and strategically transform its business.

When the UK government formally introduced its Cloud First policy in 2013 it signaled its desire to drive wider adoption of cost-effective cloud computing in the public sector.

This is a laudable aim. What we need to remember, however, is that the Cloud First policy is not just being promoted and mandated for reasons of cost. What it really heralds is the strategic importance of the cloud within the government's vision for how it does business in the future.

"The Cloud First policy will embed the skills a modern civil service needs to meet the demands of 21st-century digital government and help us get ahead in the global race," said Francis Maude, Minister for the Cabinet Office. The message is becoming increasingly clear: while many organisations have experimented with cloud and achieved successful tactical cloud deployments, they are now being asked to do more. The focus is changing and public sector organisations are being asked to start harnessing the cloud to enable more strategic transformation.

But with limited experience beyond tactical deployments, how can you address this need for strategic cloud adoption? This guide seeks to help address that shortfall by detailing a step-by-step journey through a typical strategic adoption. It includes considerations and recommendations that will help you move forward with confidence.

Eduserv (2014) A guide to strategic cloud adoption for government.

<http://www.eduserv.org.uk/~media/Insight/Reports/WEB1350%20A%20guide%20to%20strategic%20cloud%20adoption.pdf>

37 10 Considerations for a Cloud Procurement



Cloud procurement presents an opportunity to re-evaluate existing procurement strategies so you can create a flexible acquisition process that enables your public sector organization to extract the full benefits of the cloud. The document presents procurement considerations as key components that can form the basis of a broader public sector cloud procurement strategy.

Amazon web services (2017) 10 Considerations for a Cloud Procurement.

<https://d0.awsstatic.com/whitepapers/10-considerations-for-a-cloud-procurement.pdf>

38 Cloud UK: White paper sixteen. Cloud adoption trends in the UK public sector.



With its ability to drive efficiencies, improve flexibility and scalability, and reduce costs, Cloud computing has a great deal to offer the UK's increasingly pressurised public sector. But while adoption rates have increased year-on-year, they have not quite kept pace with their private sector counterparts. Progress is, however, progress and, as this report demonstrates, a significant and growing proportion of the public sector is using Cloud, and Cloud Services to help transform the way that their organisations operate, communicate and collaborate.

Public sector organisations harbour many of the same concerns as the corporate world, but it is clear from this and previous research projects that they need a greater level of assurance around the reliability and trustworthiness of Cloud suppliers, SLAs and contractual frameworks. Security, data privacy and data sovereignty hang heavy over procurement decisions, and Cloud Providers face a higher barrier of entry with respect to these issues before they can deliver services to public sector organisations.

Costs and, more specifically, the promise of cost savings, are key drivers in the decision to migrate to Cloud Services, and cost was a recurring theme throughout this research project. However, encouragingly, the flexibility of the delivery model and the need to facilitate innovation are delivering benefits that are more likely to drive initial and subsequent adoptions. This points to a shift in mind set away from seeing the IT department solely as a cost centre to deliver applications and devices, to something that can enable agility and business transformation.

This White Paper sets out to explore the reality of adoption of Cloud Services across the UK public sector and looks into the levels of adoption, the drivers, satisfaction levels with the services being accessed and the concerns that can impede adoption.

OUTSOURCERY (2015) Cloud UK: White paper sixteen. Cloud adoption trends in the UK public sector.

<https://www.outsourcery.co.uk/media/1377/cif-outsourcery-white-paper-16.pdf>

39 Impact of Cloud Computing on Healthcare, Version 2.0.



The aim of this paper is to provide a practical reference to help enterprise information technology (IT) and business (i.e., administrative, clinical, research and teaching) decision makers of the healthcare industry as they analyze and consider the implications of cloud computing for their organizations. The paper includes guidance and strategies designed to help decision makers, who may be new to cloud computing, evaluate and compare cloud services offered by commercial cloud service providers (CSPs); taking into account different requirements from patients, medical practices, hospitals, research facilities, insurance companies, governmental/regulatory bodies, and various other professional and organizational actors. This paper serves as a foundation upon which additional, more detailed whitepapers on specific healthcare and cloud computing topics can be developed in the future.

When considering whether to use cloud computing, healthcare actors must have a clear understanding of the unique benefits and risks relative to the purpose and scope of medical practice and healthcare delivery: optimizing case outcomes while maximizing patient safety and the economy, efficiency and effectiveness of care and treatment. Then they must establish appropriate contractual relationships with the CSPs by means of cloud service agreements and service level agreements (SLAs). Consideration also must be given to the different models of service delivery: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS); because each model includes different requirements and responsibilities. Cloud deployment models – private, public, and hybrid – also impact strategic decisions; so they must be considered carefully.

Throughout this paper, the role that management and IT standards play to improve the flexibility, interoperability and portability of cloud computing environments is highlighted. The paper also identifies other areas where standardization could be effective.

Cloud Standards Customer Council (2017) Impact of Cloud Computing on Healthcare, Version 2.0.

<http://www.cloud-council.org/deliverables/CSCC-Impact-of-Cloud-Computing-on-Healthcare.pdf>

40 White Paper Security in the Cloud: Is it Pie in the Sky?



As cloud computing innovation speeds forward, it's producing new approaches to technology that, while impressive and impactful, are expanding the defensive responsibilities of security leaders. The increased agility that comes with moving to the cloud solves many current technology challenges, but the journey to cloud computing can also accelerate the erosion of perimeter enforcement and trust boundaries. In fact, security is still one of the most commonly cited reasons why Enterprise and Public Sector customers are reluctant to embrace cloud computing, notwithstanding the many benefits it offers in other respects.

This paper will explore reasons behind the perception that cloud computing is somehow less secure than other enterprise computing paradigms, propose ways that organizations can mitigate cloud security risks, and identify how IT leaders can balance the promises of cloud computing with the security needed to safeguard information assets, while ensuring regulatory compliance.

Virtustream (2012) White Paper Security in the Cloud: Is it Pie in the Sky?

http://www.virtustream.com/pdfs/Pie_in_the_Sky.pdf

41 European Cloud Initiative – Building a competitive data and knowledge economy in Europe



The Cloud makes it possible to move, share and re-use data seamlessly across global markets and borders, and among institutions and research disciplines. With the current capacity available in Europe, the data produced by EU research and industry is often processed elsewhere and European researchers and innovators tend to move to the places where high data and computing capacity is more immediately available. At the same time, as Europe is the largest producer of scientific knowledge in the world, it is well placed to take the global lead in the developing of a science cloud.

The European Cloud Initiative builds on the Digital Single Market (DSM) Strategy, which aims, inter alia, to maximise the growth potential of the European digital economy. It aims to develop a trusted, open environment for the scientific community for storing, sharing and re-using scientific data and results, the European Open Science Cloud. It aims to deploy the underpinning super-computing capacity, the fast connectivity and the high-capacity cloud solutions they need via a European Data Infrastructure. Focussing initially on the scientific community, the user base will be expanded to the public sector and to industry, creating solutions and technologies that will benefit all areas of the economy and society. Achieving this will require a collaborative effort open to all those interested in exploiting the data revolution in Europe as an essential component of global growth.

The European Cloud Initiative will be complemented by further action under the Digital Single Market strategy covering cloud contracts for business users and switching of cloud services providers, as well as by the Free Flow of Data initiative.

EC (2016) European Cloud Initiative – Building a competitive data and knowledge economy in Europe, Brussels, 19.4.2016, COM (2016) 178 final

<https://ec.europa.eu/digital-single-market/en/news/communication-european-cloud-initiative-building-competitive-data-and-knowledge-economy-europe>

42 Accounting for the cloud



CIPFA, as the leading body advising on public sector accounting, has been asked to look at issues raised by 'accounting for the cloud' on behalf of its members and their employers. This paper, as a first step, explores some of the issues with the aim of inviting comments from interested and informed parties to see if additional guidance would be helpful.

CIPFA (2016) Accounting for the cloud, The Chartered Institute of Public Finance & Accounting

<http://www.cipfa.org/~media/files/cipfa%20thinks/insights/insightsaccountingforthecloudfinal.pdf?la=en>

43 IBM Private, Public, and Hybrid Cloud Storage Solution



This IBM® Redpaper™ publication takes you on a journey that surveys cloud computing to answer several fundamental questions about storage cloud technology. What are storage clouds? How can a storage cloud help solve your current and future data storage business requirements? What can IBM do to help you implement a storage cloud solution that addresses these needs?

This paper shows how IBM storage clouds use the extensive cloud computing experience, services, proven technologies, and products of IBM to support a smart storage cloud solution designed for your storage optimization efforts. Clients face many common storage challenges and some have variations that make them unique. It describes various successful client storage cloud implementations and the options that are available to meet your current needs and position you to avoid storage issues in the future. IBM Cloud Services (IBM Cloud Managed Services® and IBM SoftLayer®) are highlighted as well as the contributions of IBM to OpenStack cloud storage.

This paper is intended for anyone who wants to learn about storage clouds and how IBM addresses data storage challenges with smart storage cloud solutions. It is suitable for IBM clients, storage solution integrators, and IBM specialist sales representatives.

Coyne, L., Dain, J., Gilmer, P., Guaitani, P., Hancock, I., Maille, A., Pearson, T., Sherman, B., Vollmar, C. (2017) IBM Private, Public, and Hybrid Cloud Storage Solution, IBM Redbooks

<http://www.redbooks.ibm.com/redpapers/pdfs/redp4873.pdf>

44 Transforming digital continuity: Enhancing IT resilience through cloud computing



This joint research report, drawn together by the Estonian Ministry of Economic Affairs & Communications and Microsoft, addresses how public cloud computing can enhance government digital continuity. In other words, it looks at the role commercially delivered cloud computing can play in giving a state the capacity to maintain its government services and the data it needs to function, regardless of adverse developments and crises. The aim of this report is to help policy makers and civil servants better understand the policy and technical implications, benefits and limitations of incorporating such public cloud computing into governmental digital continuity plans.

Incorporating public cloud into a state's digital continuity plans presents potential risks and benefits. As states' operations become more data-driven and ICT-centric, ensuring those operations are as resilient as possible becomes increasingly relevant. Governments' options for ensuring resilience have potentially been greatly expanded by the emergence of hyperscale cloud computing infrastructure. Nonetheless, there remain challenges that should be addressed so that this potential can be realized. Alongside the technical complexities of achieving an important government digital service's "failover" into the cloud during a crisis, there are policy complexities to be addressed by any state preparing to transfer its data and/or the data of its citizens outside of its borders (this geographical distribution over multiple data centers in different jurisdictions, indeed across different continents, being one of the fundamental ways the cloud achieves its resilience).

In conclusion, Phase II of the joint research between the Estonian Ministry of Economic Affairs & Communications and Microsoft, successfully advanced both parties' understanding of what is feasible in terms of using commercial, public cloud computing to enhance a state's digital continuity and resilience capabilities.

Estonian Ministry of Economic Affairs & Communications and Microsoft (2016)
Transforming digital continuity: Enhancing IT resilience through cloud computing.

https://www.mkm.ee/sites/default/files/transforming_digital_continuity_-_joint_research_report_finaly_may_20.pdf

45 Eight best practices for public sector cloud adoption



Federal agencies are increasingly turning to cloud technologies to address their software and infrastructure needs, and they are also launching new applications using agile software methods, cloud-based platforms, and containers. Among government agencies:

- 93% run applications on or are experimenting with Infrastructure-as-a-Service (IaaS).
- 72% expect to use Platform-as-a-Service (PaaS) in their organizations within the next five years.
- 93% expect to make new investments in DevOps technologies within the next two years.
- 71% are using or anticipate using containers for cloud applications.

Federal agencies that want the resource efficiencies, scalability, automation, self-provisioning, and agile development capabilities of the cloud should use an open hybrid cloud approach. This aggregates on-premise datacenters and cloud-hosted environments with unified, selfservice management that supports continuous innovation and improves service delivery. With a seamless architecture, open hybrid cloud models deliver improved flexibility and innovation compared to traditional public cloud or on-premise datacenter options.

Redhat (2015) Eight best practices for public sector cloud adoption, Executive brief.

<https://www.redhat.com/cms/managed-files/ps-open-hybrid-cloud-federal-path-to-cloud-inc0437645lw-201609-en.pdf>

46 Secure government collaboration from the cloud



Collaboration as a service is emerging as a transformational model for business IT. Government departments and institutions need to collaborate to increase their productivity and more easily meet targets.

As a method of working, collaboration aligns closely with a key aspiration of modern business; that of bringing together, across sectors, the diverse talents, knowledge and resources available; bringing them to bear efficiently where and when needed, unhindered by boundaries.

The Software as a Service (SaaS) model, sometimes called “cloud computing”, is an obvious means to achieve this. Applications and data are hosted at a highly secure remote location and can be accessed by accredited people using any fixed or mobile device, alleviating the need to install or maintain software or infrastructure anywhere except in the service provider's data centre. This offers technical and operational simplification throughout the application life cycle and has the potential to remove many of the costs and boundaries that impede collaboration between organisations and people.

However, boundaries have often been put in place deliberately to achieve compliance, protect privacy, intellectual property and provide traceability. Some boundaries were created not by design but by incidental physical, political or technical realities – for example the absence of connection between private networks – and whose integrity is assumed by governance, especially in the formulation and implementation of IT security policy. Such boundaries must not be compromised and the innovation promised by the cloud service must offer clarity, control and predictability at the edge.

Atos (2012) Secure government collaboration from the cloud, White Paper.

<https://uk.atos.net/content/dam/uk/documents/your-business/atos-secure-government-collaboration-from-the-cloud-white-paper.pdf>

47 SecaaS Implementation Guidance. Category 1: Identity and Access Management



Identity and Access Management (IAM) includes people, processes, and systems that are used to manage access to enterprise resources by assuring that the identity of an entity is verified, then granting the correct level of access based on the protected resource, this assured identity, and other context information.

This guidance discusses the significant business and technical decisions that need to be considered by an organization seeking to implement the IAM component of Security as a Service (SecaaS) as part of the cloud environment, or an organization that is looking for guidance as to how to assess an IAM offering. This document is intended to assist with the planning, design, implementation and assessment of SecaaS offerings in the area of Identity and Access Management. It is meant to serve as a source of reference for best practices in the industry today.

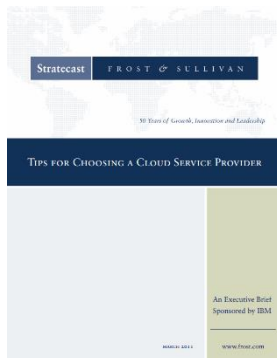
This document addresses personnel involved in the identification and implementation of the IAM solution in the cloud. It will be of particular interest to those with the responsibility of designing, implementing and integrating the consumption of services of the IAM function within any cloud application of SecaaS. Business processes are intended to be shared with stakeholders who have responsibility for ensuring that the solution has full functionality to support the demands of their business. This paper also provides direction for enterprise security stakeholders responsible for ensuring the security of IAM solutions in a corporate IT environment.

This Implementation Guidance documents best practices for the design, implementation and assessment of Identity and Access Management services, especially as they are applied within Cloud Computing.

CSA (2012) SecaaS Implementation Guidance. Category 1: Identity and Access Management, Cloud Security Alliance.

https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf

48 Tips for Choosing a Cloud Service Provider



The biggest myth in technology is the existence of ‘the cloud’. In truth, there are many clouds, each developed and maintained by its own provider, who establishes the definitions and parameters for its cloud offers.

With such a tantalizing assortment of clouds to choose from—and the low barrier to entry—enterprises may consider trying them all, placing different workloads with different providers. But enterprises that go this route soon discover that the strategy creates more problems than it solves. Managing multiple vendors and multiple environments—via multiple consoles and with different pricing schemes, performance parameters, and service level agreements—adds a tremendous management burden to enterprise IT. Furthermore, working with multiple vendors will likely limit the ability to seamlessly perform critical ‘inter-cloud’ functions, such as bursting or backup and recovery. And without the ability to apply security profiles consistently across workloads, the multi-vendor environment can potentially expose the company to risk.

Because cloud is still a new and evolving business model, it can be argued that the decision to select a cloud service provider should be approached with even greater diligence than other IT decisions. Many providers use the same term to define very different services (“hybrid cloud” is one example), making it difficult to compare offers. In addition, the flood of new entrants into the market means that many providers have little to no experience in hosting or application delivery, thus raising concerns not only about today’s service performance but also the ability to evolve their services to meet future needs.

This report provides a list that will help enterprises evaluate their options in two critical areas: the cloud service portfolio and the service provider itself.

Frost & Sullivan (2011) Tips for Choosing a Cloud Service Provider. Stratecast.

http://www-935.ibm.com/services/us/leveragingit/SmartCloud_Choosing_a_Provider_IBM.pdf

49 Oracle Cloud: Modern Cloud for a Modern Government



Public sector organizations are increasingly driven to improve operational efficiency, share information, and integrate processes across operational and jurisdictional boundaries while maintaining control and reducing costs. Recently, cloud computing has captured significant attention as both business and computing model that enables public sector organizations to achieve these daunting objectives.

Adoption and use of cloud computing is now growing at a compound annual growth rate of 26%. Further, cloud computing is expected to account for roughly 20% of the overall global IT market, excluding IT services and client devices, by 2015. Public sector organizations are already at the forefront of this trend. In fact, many major government IT organizations around the world, including the U.S., Canadian, U.K., Japanese, Australian and South Korean national governments, have already defined their cloud strategy and determined to run centralized government clouds, leveraging public clouds where appropriate.

This paper outlines Oracle's cloud computing strategies, solutions and services for public sector customers and partners, and articulates Oracle's value

Mathur, R., Amalfi, F., Erickson, A. and Houchen, D. (2014) Oracle Cloud: Modern Cloud for a Modern Government.

<http://www.dlt.com/sites/default/files/sr/brand/oracle/pdfs/Modern%20Government%20Modern%20Cloud.pdf>

50 Cloud 2020 Vision: Keeping the UK at the forefront of cloud adoption



The next wave of the digital revolution is being powered by the Internet of Things (IoT), advanced mobile applications, big data analytics and artificial intelligence (AI). But it is cloud computing that underpins all of these developments. It provides the capability to store, process and manage the vast volumes of real-time data being created through digital innovation.

The UK has a vibrant, fast moving and constantly evolving cloud computing market with multiple cloud providers offering innovative cloud services at the infrastructure, platform and software level. This combination of cloud providers means UK businesses and consumers are able to access a range of and technologically advanced, free to use, and paid cloud services.

The UK benefits from driving innovation in cloud based technologies and driving the use and exploitation of cloud. We can maintain world leading supply-side expertise and world beating demand-side exploitation, accelerating innovation and productivity. But to do all of this we have to keep the UK at the forefront of cloud adoption, techUK has identified six key issues that need to be addressed to ensure this happens.

1. Enabling data portability and system interoperability within the cloud computing ecosystem
2. Building trust in the security of cloud computing services
3. Embracing the change required to optimise the use of cloud
4. Building a coherent regulatory framework for cloud
5. Ensuring effective public sector adoption and usage of cloud
6. Having a communications infrastructure that keeps pace with mass cloud adoption

techUK (2016) Cloud 2020 Vision: Keeping the UK at the forefront of cloud adoption.

https://www.techuk.org/component/techuksecurity/security/download/8064?file=techUK_Cloud_2020_Vision.pdf&Itemid=177&return=aHR0cHM6Ly93d3cudGVjaHVRlM9yZy9pbmNpZ2h0cy9uZXdzL2l0ZW0vODA2NC10ZWNoZWstdmlzaW9uLWZvci1rZWVwaW5nLXR0ZS11ay1hdC10aGUtZm9yZWZyb250LW9mLWNsb3VhLWFKb3B0aW9u

51 Scotland's Digital Future: Scottish Public Sector Cloud Computing Guidance



Scotland's Digital Future: Delivery of Public Services set out an objective of developing a national strategy for the public sector's data storage focusing on consolidation and re-use. This reflected a recommendation of the Review of ICT Infrastructure in the Public Sector in Scotland report by John McClelland which suggested that significant efficiency and energy savings could be achieved through consolidation.

The strategy Scotland's Digital Future: Data Hosting and Data Centre Strategy for the Scottish Public Sector for the Scottish Public Sector sets out how we will deliver on that overall objective and in particular how the public sector will adopt the following approaches for achieving significant efficiency and energy savings: cloud computing, virtualisation and co-location.

This document delivers on the priority action within the strategy to set out the cloud policy for the public sector, and provide the guidance and principles for how Scotland's Public Sector will use the cloud. In assessing the current approach and environments we found that organisations face many options in making arrangements for data hosting but lack both an overall vision and information base for doing so, and need guidance on how best the Scottish public sector use cloud computing.

Cloud computing is a priority option in the overall strategy and organisations must consider how they can adopt the policy and deliver the efficiency and flexibility that this can offer. Cloud computing is an evolving and broad topic on which almost everyone has a perspective and an opinion. Our overall policy position is that cloud computing is part of the strategic future of digital public services in Scotland. It has potential to fundamentally change the nature of digital public service delivery and, when appropriately utilised, can provide benefits in cost effectiveness, energy efficiency and speed of deployment.

The Scottish Government & Digital Scotland (2014). Scotland's Digital Future: Scottish Public Sector Cloud Computing Guidance.

<http://www.gov.scot/Resource/0044/00449265.pdf>

52 Hybrid Cloud: A Catalyst to Driving Efficiencies and Meeting the Digital Aspirations of the UK Public Sector



Given the fiscal pressures on central and local government to deliver better for less, there is a huge opportunity for technology to transform public services to meet the needs of our changing population and deliver efficiencies. There is still some way to go to deliver the wholesale end-to-end transformation that is required, with the ultimate goal being cost effective digital, online, mobile, social, self-serviced, secure, and above all easy-to-use services.

It's of little surprise then to see such high levels of public cloud adoption amongst Line of Businesses (LOB) in UK public sector organisation. Findings from a study from EMC, VCE and VMware show that 85 percent are using some form of public cloud services, whether validated by IT or not. When asked what these public cloud services deployments were used for over a third (36 percent) cited it was used for back-up and recovery services, closely followed by hosting internal applications (35 percent).

Yet against this backdrop, UK public sector organisations face a growing maze of regulations and legislation that both dictate the government structures in which they operate and establish data and privacy practices they must follow. This is putting IT in unfamiliar territory; striving to meet the expectations and needs of a generation of citizens that were not traditionally part of the job.

As public sector organisations across the UK strive to meet the Digital by Default standard (providing better services for millions of users), there is a growing need to have the capacity and technical flexibility to update and improve the service being delivered to citizens on a very frequent basis. Hybrid cloud can facilitate this. It allows IT to set up, test, deploy and take down applications without building any new infrastructure.

vmware, VCE and EMC (2015) Hybrid Cloud: A Catalyst to Driving Efficiencies and Meeting the Digital Aspirations of the UK Public Sector, Public Sector Industry Report.

<https://uk.emc.com/collateral/industry-overview/emc-public-sector-industry-report.pdf>

53 Meeting the digital challenge: How well is the public sector embracing cloud computing?



The cost benefits of moving to cloud computing has dominated much of the recent discussion around public sector IT. Yes, there are undoubtedly huge savings to be made in an era of budget cuts. But this austerity narrative obscures the transformative role that cloud platforms can have in driving more efficient, more effective public sector working practices. This narrative must change if the potential of cloud computing is to be realised.

This paper proposes three points of action to help foster widespread use of cloud platforms and drive forward new ways of working in the public sector:

1. Build awareness and confidence in cloud computing.
2. Get to grips with the government's new security classification system quickly.
3. Embrace G-cloud within your organisations and help employees understand the drivers for working with SMEs.

A rather negative narrative has emerged around the evolution of public sector working practices. The conclusions of this research are much more positive. Cloud computing platforms are an enabler of massive, supportive cultural change and their introduction will take some time and effort. Information security is complicated, but certified commercial platforms can make a pragmatic contribution for Senior Information Risk Owners (SIROs). Finally, digital government, and the more efficient, more effective public sector working practices it promises, is not 'at risk' - it is a racing certainty. Every day the UK government's ambitious goal becomes that bit more achievable, supported by a gradual migration to cloud ICT platforms.

Huddle (2016) White paper - Meeting the digital challenge: How well is the public sector embracing cloud computing?

https://www.huddle.com/sites/default/files/white-papers-files/stateoftheunion-whitepaper-interactive_1.pdf

54 Best Practices for Effective Cloud Computing Services Procurement within the Federal Government



This paper provides public sector organizations guidance on addressing common challenges with cloud computing services procurement and will reflect alignment with the Federal Government's "Cloud First" policy per the Federal Cloud Computing Strategy.¹ Guidance presented in this document is not intended to be prescriptive but to serve as supplemental, as use cases can be quite diverse in regards to purchasing cloud services. For the purpose of illustration this white paper considers a notional cloud acquisition lifecycle approach that reflects common acquisition practice.

While what constitutes a "cloud service" is subject for debate, especially among industry providers, the Federal government generally adopts the cloud computing definition provided by NIST in SP 800-145.3 The essential characteristics in this definition are: on-demand self-service; broad network access; resource pooling; rapid elasticity; measured service.

To ensure the benefits of cloud computing are fully realized and to protect against vendor "cloudwashing" (i.e., overstating the application of cloud services) it is recommended that prospective buyers seek to ensure cloud services meet these five essential characteristics as defined. Typically, this is achieved by evaluating potential services for adherence to these characteristics in the resulting solicitation.

GSA (2016) Best Practices for Effective Cloud Computing Services Procurement within the Federal Government, White Paper.

<http://www.picse.eu/sites/default/files/Cloud%20Procurement%20Practices%20White%20Paper%20FINAL%2001152016.pdf>

55 2016 BSA Global Cloud Computing Scoreboard. Confronting New Challenges



The 2016 BSA Global Cloud Computing Scorecard — the only report to regularly track change in the international policy landscape for cloud computing — shows that global cloud readiness continues to improve in every region of the world. Even so, important exceptions exist in certain countries that threaten to slow economic growth in those markets.

The Scorecard ranks the IT infrastructure and policy environment — or cloud computing readiness — of 24 countries that account for 80 percent of the world's IT markets. Each country is graded on its strengths and weaknesses in seven key policy areas.

Cloud computing democratizes the use of advanced technologies. Cloud computing allows anyone — a startup, an individual consumer, a government or a small business — to access technology previously available only to large organizations. These services in return have opened the door to unprecedented connectivity, productivity and competitiveness.

Countries that offer a policy environment in which cloud computing services can flourish gain in productivity and economic growth. The countries with the most favorable policies are those in which the free movement of data, privacy, intellectual property protections, robust deterrence and enforcement of cybercrime are all important priorities. Many countries also recognize that coordination of national cloud-computing policies with those of other nations will facilitate benefits for all countries participating in the global economy. But countries inhibiting, or failing to support, the use of cloud computing will not keep pace with those embracing the tool.

This year's results reveal that almost all countries have made significant improvements in their policy environments since 2013. But the stratification between high-, middle- and lower-achieving country groups has widened, with the middle-ranking countries stagnating even as the high achievers continue to refine their policy environments.

galexia (2017) 2016 BSA Global Cloud Computing Scoreboard. Confronting New Challenges.

http://cloudscorecard.bsa.org/2016/pdf/BSA_2016_Global_Cloud_Scorecard.pdf

57 A Repeatable Cloud-First Deployment Process Model



Cloud computing is a shared responsibilities model, where different entities are responsible for managing their areas of concern across the entire implementation as appropriate for the specific SaaS, PaaS, or IaaS model that is chosen. Successful cloud initiatives must have top-down support, but just as critically, they need to be viewed as a collaborative effort due to the breadth of subject matter expertise that is required from all parts of the business.

It's important to recognize that cloud-first isn't an initiative that has an end date. In fact, whether the organization decides to move most or all of its infrastructure to the cloud or it starts with just a few SaaS applications, cloud-first is just the beginning of an ongoing process of assessments and decisions that an organization will need to make if it wants to continue to ensure that its best interests are protected.

This paper offers guidance to help organizations establish a systematic and repeatable process for implementing a cloud-first strategy. It offers a high-level framework for identifying the right stakeholders and engaging with them at the right time to reduce the risk, liabilities, and inefficiencies that organizations can experience as a result of ad hoc cloud decisions. The goal of this guidance is to help ensure that any new cloud program is secure, compliant, efficient, and successfully implements the organization's key business initiatives.

CSA (2016) A Repeatable Cloud-First Deployment Process Model, Palo Alto Networks.

https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/cloud-first-now-what

58 Citizen-Driven Innovation



This guidebook aims to bring citizen-driven innovation to policy makers and change agents around the globe, by spreading good practice on open and participatory approaches as applied to digital service development in different nations, climates, cultures, and urban settings.

The effort is born of a Memorandum of Understanding for collaboration¹ between the World Bank and the European Network of Living Labs and their shared interest in applying new citizen centric methodologies for innovation.² These two organizations have pooled their resources to create this guidebook and share their broad set of experiences and know-how with city dwellers and policy makers, hoping to inspire its readers with successful case stories together with guidance on how to apply these approaches to their own contexts.

The following pages explore the concept of Smart Cities through a lens that promotes citizens as the driving force of urban innovation. Different models of Smart Cities are presented, showing how citizen-centric methods have been used to mobilize resources to respond to urban innovation challenges in a variety of situations, objectives and governance structures. The Living Lab approach strengthens these processes as one of the leading methods for 'agile development' or the rapid prototyping of ideas, concepts, products, services and processes in a highly decentralized and user-centric manner. By adopting these approaches and promoting citizen-driven innovation, cities around the world are aiming to alleviate the demand for services, increase the quality of delivery, and promote local entrepreneurship. Citizen driven innovation, however, is best seen in action rather than on paper. This guidebook therefore mixes practical advice with concrete cases of experimentation between city administrators, citizens, and key stakeholders, as the best proof of the methodologies proposed.

Eskelinen, J., Robles, A. G., Lindy, I., Marsh, J., & Muenta-Kunigami, A. (Eds.). (2015). Citizen-Driven Innovation. World Bank Publications.

https://openknowledge.worldbank.org/bitstream/handle/10986/21984/Citizen_Driven_Innovation_Full.pdf?sequence=

59 Cloud Computing Study

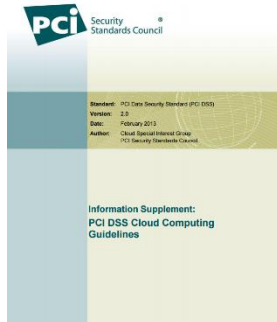


Cloud computing is a new model of computing that could bring substantial benefits to consumers, businesses and administrations, while also creating new risks and challenges. This study provides an overview on cloud computing and how it relates to EU consumer protection and the EU digital single market goals. It demonstrates that cloud computing could induce savings and facilitate innovative online services. However, it finds that barriers to take-up of cloud computing are manifold. It concludes that in order to seize the benefits of cloud computing, priority actions for EU policymakers are addressing legislation-related gaps, improving terms and conditions for users, tackling stakeholder security concerns, encouraging the public sector cloud, and promoting further research and development in cloud computing.

Directorate General for Internal Policies (2012) Cloud Computing, Study. Policy Department A: Economic and Scientific Policy.

<http://www.europarl.europa.eu/document/activities/cont/201205/20120531ATT46111/20120531ATT46111EN.pdf>

60 Information Supplement: PCI DSS Cloud Computing Guidelines



Cloud computing is a form of distributed computing that is yet to be standardized¹. There are a number of factors to be considered when migrating to cloud services, and organizations need to clearly understand their needs before they can determine if and how they will be met by a particular solution or provider. As cloud computing is still an evolving technology, evaluations of risks and benefits may change as the technology becomes more established and its implications become better understood.

Cloud security is a shared responsibility between the cloud service provider (CSP) and its clients. If payment card data is stored, processed or transmitted in a cloud environment, PCI DSS will apply to that environment, and will typically involve validation of both the CSP's infrastructure and the client's usage of that environment. The allocation of responsibility between client and provider for managing security controls does not exempt a client from the responsibility of ensuring that their cardholder data is properly secured according to applicable PCI DSS requirements.

It's important to note that all cloud services are not created equal. Clear policies and procedures should be agreed between client and cloud provider for all security requirements, and responsibilities for operation, management and reporting should be clearly defined and understood for each requirement.

Cloud Special Interest Group and PCI Security Standards Council (2013) Cloud Computing, Study. Policy Department A: Economic and Scientific Policy.

https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

61 Cloud Computing and Government Services



eEnviPer is an EU-funded project aiming to provide an integrated web-based platform for the application, administration and consultation of environmental permits, thereby making the environmental permitting process more transparent, more accessible and more efficient. The platform will be available in early 2014 after intensive field tests in five European countries (Croatia, Greece, Italy, Serbia and Turkey).

eEnviPer uses innovative technical approaches such as public sector cloud services and service-oriented architecture (SOA) to build open, flexible and collaborative egovernment services while at the same time lowering information and communication technology (ICT) costs. The use of an internet-enabled platform such as eEnviPer can be a first step for municipalities and permitting authorities to make their permitting processes more cost effective, transparent and user-friendly. The system offers the possibility for public administrations to easily deploy both new services and existing procedures as shared services. The platform can also access locally available data sources such as geospatial information through industry-standard XML-based interfaces.

This paper examines the cloud computing aspects of the eEnviPer platform in detail. The first section introduces cloud computing, cloud based services and deployment models. The second section analyses the transition and the benefits of government services into cloud implementation. Finally, the last section focuses on features of the eEnviPer platform as a cloud based service.

Yümlü S. (2013) Cloud Computing and Government Services. SAMPAŞ Information & Communication Systems.

http://eenviper.eu/uploads/files/1308_White_paper_IV.pdf

62 Accenture cloud application migration services



Across the world, organizations of all sizes from every sector are moving to cloud computing. And they need help with migration: Yet fewer than half of the organizations moving to cloud are confident in identifying which of their applications could best benefit from the technology.

According to global analyst IDC, spending on public IT cloud services is expected to reach more than US\$107 billion by 2017.

And, according to Aragon Research, moving legacy applications to a hybrid cloud environment may be the most challenging task.

The results of Accenture's High Performance IT research show high performers are combining private and public clouds with existing systems to enhance what each has to offer as they transition to a hybrid environment.

In short, high performers aren't waiting for new technologies to develop or mature before they act.

Accenture (2014) Accenture cloud application migration services: A smarter way to get to the cloud. Accenture.

https://www.accenture.com/t20160728T233018_w_us-en_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_9/Accenture-Cloud-Application-Migration-Services.pdf

63 Migrating Applications to Public Cloud Services: Roadmap for Success



Across all industries, momentum is building to migrate applications to cloud computing. While cost savings, speed of deployment and scalability top the list of business motivations, an increasing number of enterprises view cloud computing as a key enabler of business transformation that can help improve customer engagement, forge new partnerships and drive competitive advantage.

However, the migration of applications to cloud computing must be done in a strategic and methodical manner. Existing enterprise applications must be thoroughly assessed to determine which workloads can benefit most from early migration to the cloud. Key considerations including costs of migration, application redesign, application performance and availability, security and privacy requirements, and regulatory requirements must be taken into account.

The aim of this guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers analyze and consider application migration to cloud computing. The paper focuses primarily on the migration of applications to public cloud services. It includes a list of steps, along with guidance and strategies, that takes into consideration both business and technical requirements.

The section titled “Motivation and Considerations” provides an overview of the potential impact that the migration of enterprise applications to cloud computing will have on new and existing business processes. This section provides guidance on the types of applications that are best suited for migration to the cloud.

The section titled “Migration Roadmap” is the heart of the guide and includes the basic steps of a formalized migration process. It details both strategic and tactical activities for decision makers to develop a business plan and detailed migration plan.

Cloud Standards Customer Council (2013) Migrating Applications to Public Cloud Services: Roadmap for Success.

<http://www.cloud-council.org/deliverables/CSCC-Migrating-Applications-to-Public-Cloud-Services-Roadmap-for-Success.pdf>

64 Planning the Migration of Enterprise Applications to the Cloud



Cloud computing—IT resources and services that are abstracted from the underlying infrastructure and provided on demand and at scale in a shared multitenant and elastic environment—represents a paradigm shift from which both enterprise IT and service providers can benefit.

A cloud can provide IT infrastructure services such as servers, storage, network and network services, or infrastructure as a service (IaaS); an application deployment platform with application services such as databases, or platform as a service (PaaS); or subscription-based software applications, or software as a service (SaaS).

Today, service providers, who already excel at provisioning, managing, and scaling services for multiple customers, are providing offerings based on IaaS in which the enterprise uses the pay-as-you-go compute infrastructure from the service provider. A cloud provided by a service provider is known as a public cloud.

In addition, some enterprises are choosing to build a private cloud—enterprise IT infrastructure services, managed by the enterprise, with cloud computing qualities: self-service, pay-as-you-go chargeback, on-demand provisioning, and the appearance of infinite scalability.

Whether they are considering a private cloud or a public cloud as their services model, enterprises first must consider which of their many applications belong in the cloud and how to migrate them. In the public cloud, service providers also might want to assist enterprises in making the best possible decision about migrating applications. The applications chosen for migration and how you approach the application migration process can affect not only the ease and success of the migration itself but also the user's service experience.

Let us take a look at what is involved in application migration, as well as the business and technical factors behind a decision to migrate applications to a cloud model.

CISCO (2010) White Paper - Planning the Migration of Enterprise Applications to the Cloud.

https://www.cisco.com/en/US/services/ps2961/ps10364/ps10370/ps11104/Migration_of_Enterprise_Apps_to_Cloud_White_Paper.pdf

65 Cloud Computing Applications in the Public Sector



Cloud computing brings key advantages to the governments facing conflicting IT challenges. However, the cloud paradigm is still fragmented and concerns over data privacy and regulatory issues presents significant barriers to its adoption. Cloud computing is expected to provide new ways to run IT in public sector. At the same time, it presents significant challenges for governments, and to make the most of cloud, public sector organizations need to make some important decisions. Governments planning to migrate to the cloud are actively moving to harness digital services but with different focus, reasons, and strategy. However, the degree of cloud adoption by the public sector around the globe varies significantly. Most governments are piloting cloud computing but there are huge differences between each country. This chapter explores the state of the art of cloud computing applications in the public sector; various implications and specific recommendation are also provided.

Manzoor, A. (2016). Cloud Computing Applications in the Public Sector. In Cloud Computing Technologies for Connected Government (pp. 215-246). IGI Global.

<https://pdfs.semanticscholar.org/782f/1dca721c1758e8b2a5835ec1a66c3e5fa39f.pdf>

66 Recommendation of the Council on Digital Government Strategies



This document presents the Recommendation on Digital Government Strategies aimed at bringing governments closer to citizens and businesses. It was developed by the Public Governance Committee (PGC).

The purpose of the Recommendation is to help governments adopt more strategic approaches for a use of technology that spurs more open, participatory and innovative governments. Key actors responsible for public sector modernisation at all levels of government (from co-ordinating units, sector ministries, and public agencies) will find the Recommendation relevant to establish more effective co-ordination mechanisms, stronger capacities and framework conditions to improve digital technologies' effectiveness for delivering public value and strengthening citizen trust. While the level of trust obtained in each country largely depends on its history and culture, the Recommendation can help governments to use technology to become more agile and resilient and to foster forward-looking public institutions. This can increase public trust through better performing and responsive services and policies, and can mobilise public support for ambitious and innovative government policies.

In this regard, the principles set out in the Recommendation support a shift in culture within the public sector: from a use of technology to support better public sector operations to integrating strategic decisions on digital technologies in the shaping of overarching strategies and agendas for public sector reform and modernisation. The Recommendation hence offers guidance for a shared understanding and a mind-set on how to prepare for, and get the most out of, technological change and digital opportunities in a long-term perspective to create public value and mitigate risks related to: quality of public service delivery, public sector efficiency, social inclusion and participation, public trust, and multi-level and multi-actor governance.

OECD Council (2014). Recommendation of the Council on Digital Government Strategies. OECD.

<http://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf>

67 Factors influencing cloud computing adoption in the public sector: an empirical analysis



Cloud computing is one of the latest Information Technology innovation phenomena that has risen from the idea of sharing, consolidating, and standardizing of resources in a centralized infrastructure and facility. This concept offers many advantages such as cost reduction in both hardware and software investment for organizations. Despite these advantages, cloud computing adoption among organizations is relatively slow with a low adoption rate. As such, this study attempts to bridge the gap by offering insight into possible factors that could influence such adoption decisions. By integrating the Diffusion of Innovation Theory (DOI) and IT personnel characteristics, a conceptual model is developed and tested as a preliminary study to determine the influencing factors of cloud computing adoption by the Malaysian public sector to enhance its service delivery. The results revealed that relative advantage, compatibility, and IT personnel knowledge are the innovation attributes and the human factor for cloud computing adoption in the Malaysian public sector. This study contributes to the knowledge domain of cloud computing adoption literature on theories of IT adoption particularly in the public sector.

Sallehudin, H., Razak, R. C., & Ismail, M. (2015). Factors influencing cloud computing adoption in the public sector: an empirical analysis. *Journal of Entrepreneurship and Business*, 3(1), 30-45.

https://www.researchgate.net/profile/Hasimi_Sallehudin/publication/281336943_Factors_Influencing_Cloud_Computing_Adoption_in_the_Public_Sector_An_Empirical_Analysis/links/55ed334908ae65b6389f439e.pdf

68 White Paper - Cloud Computing



This White Paper is the result of an SATW-sponsored workshop conducted in April 2012 by the ICT topical platform to better understand the opportunities of Cloud Computing for Switzerland, specifically in the education and public sector arenas. We aim to inform the appropriate decision and policy makers to ensure a timely implementation of the recommendations pro-posed herein.

After defining what cloud computing is and describing its many advantages, this white paper presents various examples of successful cloud computing implementations from such diverse fields as education, public administration, business, and industry. All these projects have in common that the cloud solutions resulted in appreciable cost savings and provided better scalability than traditional IT implementations.

An interesting finding is that, in terms of the use of cloud computing in its industry and administration, Switzerland does not rank among the top industrial countries despite the fact that it is one of the countries with the highest ICT expenditures per capita worldwide as a recent study of the Swiss cloud computing landscape revealed. Despite the fact that numerous strategy papers exist, their implementation unfortunately is a long time coming. The reasons are manifold, but the main culprits seem to be a lack of security, a lack of trust in the new technology, and a lack of experts.

The white paper concludes with the recommendation to create a Swiss community cloud for education and research. Such a cloud will not only help advance cloud computing research, but also can be a first step towards addressing the above challenges. Its main use, however, will be that it will provide the stakeholders and players in Switzerland's education and research with a unique environment throughout their educational and professional life.

Brian, O., Brunschwiler, T., Dill, H., Christ, H., Falsafi, B., Fischer, M., ... & Kaiserswerth, M. (2008). Cloud computing. Communications of the ACM, 51(7), 9-11.

http://www.cloud-finder.ch/fileadmin/Dateien/PDF/News/2012-11-06_SATW_White_Paper_Cloud_Computing_EN_1_.pdf

69 Getting ahead in the cloud



Getting ahead in the cloud

The transition to cloud computing will be especially challenging for governments, given their myriad IT systems and their security, budgetary, and organizational constraints. We look at four critical actions they must take.

Executive Summary

Cloud computing is becoming a reality for governments. It offers a number of advantages, including the ability to scale up or down, to share resources, and to reduce costs. However, the transition to cloud computing is not without challenges. Governments must take four critical actions to get ahead in the cloud: 1) Assess their current IT environment, 2) Develop a cloud strategy, 3) Build a cloud-ready organization, and 4) Monitor and measure cloud adoption.

Cloud computing is becoming a reality for governments. It offers a number of advantages, including the ability to scale up or down, to share resources, and to reduce costs. However, the transition to cloud computing is not without challenges. Governments must take four critical actions to get ahead in the cloud: 1) Assess their current IT environment, 2) Develop a cloud strategy, 3) Build a cloud-ready organization, and 4) Monitor and measure cloud adoption.

The transition to cloud computing will be especially challenging for governments, given their myriad IT systems and their security, budgetary, and organizational constraints. This paper looks at four critical actions they must take.

By migrating to the cloud, public-sector organizations will be able to free up IT spend for reinvestment in mission-enabling activities or national objectives such as deficit reduction. With more agile systems and faster deployment times, they will be better at supporting key government operations and providing services to citizens. However, just as the benefits are great, so too are the challenges that must be addressed to achieve them. An investment today in the tools, capabilities, and processes required to surmount the obstacles to cloud migration is likely to yield a significant return in the long term.

Nichols, K., and Sprague, K. (2011). Getting ahead in the cloud. McKinsey & Company.

https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjtY656rXTAhVSYIAKHwBHDjMQFggjMAA&url=https%3A%2F%2Fwww.mckinsey.com%2F~%2Fmedia%2Fmckinsey%2Fdotcom%2Fclient_service%2FPublic%2520Sector%2FPDF%2FMckK%2520on%2520Govt%2FIT%2520Challenge%2520and%2520opportunity%2FMOG7_Cloud.ashx&usq=AFQjCNH4LNSuGOvaWcgxCbLGbwAw7E3jDA&sig2=WUT0OvxUU00KOKrTDYO41w

70 Oracle's Cloud Solutions for Public Sector



Public sector organizations are increasingly driven to improve operational efficiency, share information, and integrate processes across operational and jurisdictional boundaries while maintaining control over costs. Recently, cloud computing has captured significant attention as both a business and computing model that enables public sector organizations to achieve these daunting objectives.

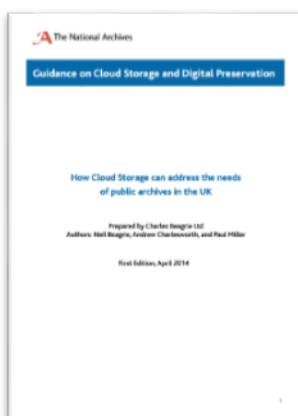
Despite some early market confusion regarding the exact nature of cloud computing, public sector customers and vendors have rallied around the standard taxonomy defined by the U.S. National Institute of Standards and Technology (NIST). This structure has enabled industry analysts to measure cloud computing trends. From its humble beginnings, adoption and use of cloud computing is now growing at a compound annual growth rate of 26%. Further, cloud computing is expected to account for roughly 20% of the overall global IT market, excluding IT services and client devices, by 2015. Public sector organizations are already at the forefront of this trend. In fact, many major government IT organizations around the world, including the U.S., Canadian, U.K., Japanese, Australian, and South Korean national governments, have already defined their cloud strategy and determined to run centralized government clouds, leveraging public clouds where appropriate.

Oracle is a clear and well-positioned leader in public and private cloud computing. Building upon its market leading commercial-off-the-shelf enterprise software, Oracle has enhanced its hardware, software and management capabilities through investments in innovation, strategic acquisitions as well as key partnerships. This paper outlines Oracle's cloud computing strategies, solutions and services for public sector customers and partners, and articulates Oracle's value proposition and key differentiators.

Oracle (2012). Oracle's Cloud Solutions for Public Sector. White Paper, Oracle.

<http://www.oracle.com/us/industries/public-sector/cloud-solutions-public-sector-wp-323002.pdf>

71 How Cloud Storage can address the needs of public archives in the UK



Digital preservation is a significant issue for almost all public archives. There is an increasing demand for storage of both born-digital archives and digitised material, and an expectation that public access to this content will continue to expand. At the same time the UK Government's recent adoption of a 'Cloud First' policy for public sector IT procurement is mandated to central government and strongly recommended to the wider public sector to achieve better value for money in IT services and data storage.

This Guidance is focused on the cloud and its potential role in archival storage. It aims to help public archives in the UK develop an understanding of cloud storage and its potential contribution to their digital preservation activities, and to provide a balanced overview allowing archives to understand potential benefits and risks involved and the range of options available (including not using cloud if it does not meet your requirements).

Whilst primarily targeted at public archives, the aim is to provide information that will be useful within a range of organisational contexts, and overarching advice that can be translated into the private sector where relevant.

The Guidance and case studies have been prepared and selected to be applicable to a broad range of archives. The requirements and key needs in terms of the content of guidance for the sector have been collated via a series of interviews and a focus group with archive representatives.

Beagrie, N., Charlesworth, A., and Miller P. (2014). Guidance on Cloud Storage and Digital Preservation: How Cloud Storage can address the needs of public archives in the UK. Charles Beagrie Ltd.

<http://www.nationalarchives.gov.uk/documents/archives/cloud-storage-guidance.pdf>

72 [ui!] makes urban data usable via cloud technology



“Our platform UrbanPulse brings together the various data sources that any city already collects now, like traffic light sensor data, for example“, explains Christian Müller from [ui!] – The Urban Software Institute. By bundling onto one platform, the data is made usable for any applications based upon them, thus enabling value-added services for the administration of a city or direct service for citizens.”

“Until now, this measurement data has been treated in isolation,” says Müller. By linking the data on the UrbanPulse platform, synergies are achieved. Thus, for instance, street lighting could be reduced at night when sensors register less or little traffic on a particular road. If the traffic volume increases, lighting can be automatically increased again. This way, energy could be saved without jeopardizing traffic safety.

With Urban[traffic!] Pulse, [ui!] has developed an application that processes traffic-relevant data. The solution analyses the sensor data transmitted by traffic guidance systems at intersecting roads and makes them available almost in real time. Since spring 2013, the solution has been in the test phase in Darmstadt and has been continuously providing measurement data to research institutes of Darmstadt Technical University (e.g. traffic planning and traffic technology). City employees also have the opportunity to import information on the extension of road intersections into the system. This information is also used to perform a geo-referencing of the sensors.

The Urban Institute (2015). [ui!] makes urban data usable via cloud technology. The Urban Institute.

https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjorPm8LXTAhWKEVAKHf5CDJsQFggvMAA&url=http%3A%2F%2Fsmartcitiescouncil.com%2Fsystem%2Ftdf%2Fpublic_resources%2FMaking%2520urban%2520data%2520usable%2520via%2520the%2520cloud.pdf%3Ffile%3D1%26type%3Dnode%26id%3D2093&usg=AFQjCNHqgLLqvloEmm1-2EPEZ4kZZIYhTA&sig2=T517ED40Bj0cVDWUCEQpQg

73 Irish Public Sector Cloud Computing Strategy



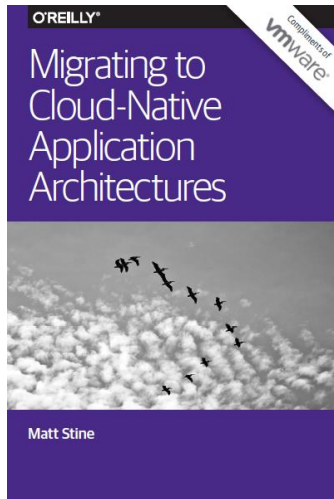
The Centre for Management and Organisation Development (CMOD) is a division of the Department of Public Expenditure and Reform (DPER), mandated to implement policies in the area of ICT and eGovernment. Its role is summarised as having *“among other things, responsibility for monitoring and approving ICT spend in civil and public service bodies, telecommunications policy and infrastructures, eGovernment policy and infrastructures, technology research and policy, central ICT procurements and frameworks, and common IT systems including payroll and HR Management.”*

ICT and cloud computing has been highlighted as key target areas within the Programme for Government, set out by the current coalition Government – *“We will make Ireland a leader in the emerging I.T. market of cloud computing by promoting greater use of cloud computing in the public sector, organising existing State supports for cloud computing into a package to promote Ireland as a progressive place for I.T. investment, establishing an expert group to address new security and privacy issues arising from the use of cloud computing and reviewing the adequacy of current legislation and identify what steps need to be taken to ensure a supportive regulatory environment”*. Against this backdrop, CMOD has published a number of policy documents in the ICT area, which set out strategies to enable the delivery of improved public services. The second of these documents, entitled Supporting Public Sector Reform: Cloud Computing Strategy (the “Strategy”), locates cloud technology at the core of eGovernment. This article discusses Government strategy in the cloud computing area. This article is the second in a three part series assessing aspects of public sector reform. The first discussed public sector outsourcing and the final article will discuss public sector shared services.

Pearse, R. (2013). Irish Public Sector Cloud Computing Strategy. Group Briefing, Arthur COX.

<http://www.arthurcox.com/wp-content/uploads/2014/01/Arthur-Cox-Irish-Public-Sector-Cloud-Computing-Strategy-July-2013.pdf>

74 Migrating to Cloud Native Application Architectures



Stable industries that have for years been dominated by entrenched leaders are rapidly being disrupted, and they're being disrupted by businesses with software at their core. Companies like Square, Uber, Netflix, Airbnb, and Tesla continue to possess rapidly growing private market valuations and turn the heads of executives of their industries' historical leaders. What do these innovative companies have in common?

- Speed of innovation
- Always-available services
- Web scale
- Mobile-centric user experiences

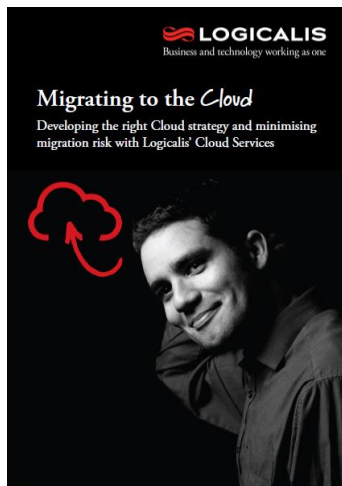
Moving to the cloud is a natural evolution of focusing on software, and cloud-native application architectures are at the center of how these companies obtained their disruptive character. By cloud, we mean any computing environment in which computing, networking, and storage resources can be provisioned and released elastically in an on-demand, self-service manner. This definition includes both public cloud infrastructure (such as Amazon Web Services, Google Cloud, or Microsoft Azure) and private cloud infrastructure (such as VMware vSphere or OpenStack).

This document explains how cloud-native application architectures enable these innovative characteristics.services.

Stine, M. (2015). Migrating to Cloud-Native Application Architectures, O'Reilly

<https://download3.vmware.com/vmworld/2015/downloads/oreilly-cloud-native-archx.pdf>

75 Migrating to the Cloud: Developing the right strategy and minimizing migration risk



Organisations are looking for new ways to deliver IT services and demanding that ICT delivers more with less resources. As a result the traditional data centre has evolved to address these challenges. Cloud services are fast becoming the enabler to meet these business challenges. But how do you get there and how do you do it right?.

As with any IT infrastructure project or architecture, business needs to develop a strategy, assess business and application requirements then carefully plan and execute the solution. Moving to the Cloud is no different; however a cloud methodology is unique to each business. With varying types of cloud such as Public, Private or a mix in a Hybrid Cloud, business needs to adopt an approach that not only meets ever changing business demands but also maintains security and compliance.

The recommended approach to move to the cloud is to use a multi-phase methodology which includes an advisory, an assessment, and a design and implementation phase.

Our cloud services are designed to help you choose and implement the specific cloud solutions that meet your

exact needs and objectives, however diverse they are:

1. Cloud Advisory Service
2. Cloud Readiness Assessment
3. Cloud Design and Migration Service

Logicalis (2015). Migrating to the Cloud: Developing the right cloud strategy and minimizing migration risk with Logicalis's Cloud Services

<http://www.logicalis.com/globalassets/australia/whitepapers/howtoguide-cloudmigration.pdf>

76 Hosting Readiness Assessment Process



EPA's Office of Environmental Information (OEI) is working with Agency System Owners to assess the readiness of IT systems to ensure the advantages of cloud hosting opportunities are realized where applicable. This effort is consistent with the Federal Cloud Computing Strategy (February 8, 2011) and ongoing OEI initiatives to achieve IT cost and performance efficiencies. It is also consistent with the CIO's responsibilities under the Federal Information Technology Acquisition Reform Act (FITARA).

Given the variety of cloud hosting options and models for federal systems, System Owners benefit from consultative services in assessing those options. The decision to stand up a new application or migrate an existing application to the cloud requires decision makers have a deeper understanding of the application architecture, operational requirements, business requirements, and security requirements in order to make the most well-informed decisions.

For these reasons, OEI has developed a comprehensive hosting readiness assessment methodology that captures critical data for making informed decisions. This methodology incorporates a comprehensive alternative analysis and documentation of a business case that aligns with EPA's operational, business, and financial constraints. The hosting readiness assessment process can be used by individual program offices to support Capital Planning and Investment Control (CPIC) decision-making processes and may also be incorporated into Software Lifecycle Management processes that each office uses to review, approve, and manage system development.

Environmental Protection Agency (2015). Hosting Readiness Assessment Process, United States Environmental Protection Agency

https://developer.epa.gov/guide/wp-content/uploads/sites/3/2016/04/conops_epa_cloud_readiness_508_092116.pdf

77 Migrating an existing on-premise application to Windows Azure Cloud



Windows Azure is Microsoft's application platform for the public Cloud. Applications can be deployed on to Azure in various models. Windows Azure is used to:

- Build a web application that runs and stores its data in Microsoft datacenters.
- Store data while the applications that consume this data run on premise (outside the public cloud).
- Create virtual machines to develop and test, or run SharePoint and other out-of-the-box applications.
- Develop massively scalable applications with many users.
- Offer a wide range of services.

With Windows Azure, the focus is on the development, not the infrastructure. Key benefits of hosting applications in Azure include:

- Minimal focus required on the infrastructure.
- No need to buy / maintain any infrastructure.
- Easy scale-up and scale-out available in Pay-As You-Go model.
- Developer(s) having .Net skill can develop and migrate applications on Azure by learning Azure SDK.
- Windows Azure provides SLA 99.95% for the hosted applications.

Typical implementation models available in Windows Azure are virtual machines, Cloud services, websites and mobile services.

Mindtree (2016). Migrating an existing on-premise application to Windows Azure Cloud, White Paper

<https://www.mindtree.com/sites/default/files/mindtree-whitepaper-migrating-an-existing-on-premise-application-to-windows-azure-cloud.pdf>

78 Migrating your existing applications to the AWS Cloud



With Amazon Web Services (AWS), you can provision compute power, storage and other resources, gaining access to a suite of elastic IT infrastructure services as your business demands them. With minimal cost and effort, you can move your application to the AWS cloud and reduce capital expenses, minimize support and administrative costs, and retain the performance, security, and reliability requirements your business demands.

This paper helps you build a migration strategy for your company. It discusses steps, techniques and methodologies for moving your existing enterprise applications to the AWS cloud. To get the most from this paper, you should have basic understanding of the different products and features from Amazon Web Services.

There are several strategies for migrating applications to new environments. In this paper, we shall share several such strategies that help enterprise companies take advantage of the cloud. We discuss a phase-driven step-by-step strategy for migrating applications to the cloud.

More and more enterprises are moving applications to the cloud to modernize their current IT asset base or to prepare for future needs. They are taking the plunge, picking up a few mission-critical applications to move to the cloud and quickly realizing that there are other applications that are also a good fit for the cloud.

We provide three scenarios for each of which we discuss the motivation for the migration, the before and after application architecture, details the migration process, and summarize the technical benefits of migration.

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>

79 Protect Data and Privacy in the Cloud



Microsoft understands that for our enterprise customers to realize the benefits of cloud computing, they must be willing to entrust their cloud provider with one of their most valuable assets – their data. In this whitepaper, Microsoft will outline its approach and processes to ensure that our customers' data in our enterprise services including Microsoft Azure, Office 365, Dynamics CRM Online, and Microsoft Intune, remains private. After discussing the issues surrounding privacy in the cloud, we will discuss the ways in which we ensure our services protect privacy when building our services, to operating the services in the datacenter, to ensuring our customers make informed choices to protect their data privacy in the cloud.

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>

80 Conducting privacy impact assessment: code of practice



Privacy impact assessments (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective PIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. PIAs are an integral part of taking a privacy by design approach.

This code explains the principles which form the basis for a PIA. The main body of the code sets out the basic steps which an organisation should carry out during the assessment process. The practical implementation of the basic principles will depend on the organisation's usual business practice.

The annexes at the back of the code are intended to provide a starting point for the implementation of the PIA. They include a set of screening questions to help organisations identify when a PIA is necessary, and a template which can be used to help produce a PIA report.

The code will be useful for any organisation which is thinking about conducting a PIA. The process described in the guidance is designed to be flexible enough to work for organisations of any size and in any sector. The code will also work with a range of privacy and data protection issues. The ICO will also support sectoral groups who wish to develop a PIA methodology to apply to their particular sector. For example, sectors might find it useful to develop a more specific set of screening questions or identify common privacy risks and solutions.

The Information Commissioner has issued this code of practice under section 51 of the Data Protection Act (DPA) in pursuance of his duty to promote good practice. The DPA says good practice includes, but is not limited to, compliance with the requirements of the Act. Conducting a PIA is not a requirement of the Act, but undertaking one will help to ensure that a new project is compliant.

Ico (2014). Conducting privacy impact assessment code of practice, Data Protection Act, Information Commissioner's Office

<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>