International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Cloud Computing Strategy in Sudan

Yousif Eltahir Sharaf Eldin Ahmed

Sudan Academic of Science, Governmental University for Post Graduate Studies, P.O.Box 86, Khartoum – Sudan

Abstract: ***Cloud Computing is a radically new approach to the delivery of ICT services which promises- "anywhere" access to shared computing resources; "freedom" from capital expenditure on back-end computing equipment and software; · the ability to provision computing services very quickly and cheaper than traditional models; and the ability to pay for such services on some form of metered or per-use basis. [1] As Cloud Computing is evolving, there are still considerable challenges pertaining to, between, security, legalities, jurisdiction, availability and reliability, and pricing models that provide definitive and sustained value. Accordingly, the move to Cloud Computing will take time. [1]. This Strategy is based on extensive engagement, research and trials with the ICT field. Notwithstanding the challenges, this Strategy – places Cloud Computing at the heart of our ICT Strategy; sets a course for centralizing and implementing our common ICT needs as a set of shared services; commits to reducing the number of our computer and data centers from potentially hundreds to approximately a few primary facilities; establishes our aim to use external service providers as much as possible in the fulfilment of this approach and to maximize competition in this regard by establishing multi-vendor procurement frameworks; details and timelines lists of ICT activities that we will migrate to Cloud Computing and shared services over a number of phases; and · highlights our need to consider a new ICT organizational structure and new ICT funding and governance arrangements over time. [1] Finally, it makes it clear that the implementation of the measures set out in this Strategy must provide tangible cost savings before they will be advanced [1]***

Keywords: Cloud Computing, Strategy, Service models, deployment models, characteristics

1. Introduction

The purpose of ICT in the public service is to support the effective and efficient delivery of services. In that context, it needs to be:

- Fit-for-purpose in terms of functionality, availability and reliability;
- Delivered in a way that supports the obligation of the government to protect and secure the data and privacy of its citizens and enterprises; and
- Implemented and operated in a way that provides best value-for-money. [1]

As with other governments and large enterprises worldwide, government units have traditionally procured or developed their own ICT infrastructures and solutions and most of them have developed their own ICT functions to manage and operate these. [1]

A range of measures and circumstances are now coming together that provide an opportunity for reconsidering how ICT should be procured, delivered and governed in the public service,

- The current economic circumstances mean that government units must operate with considerably reduced financial and human resources; [1]
- This in turn is compelling government units to concentrate their efforts on their core business and to consider alternative approaches for non-core activities [1]
- Front-end interfaces and devices are becoming more consumer-oriented, more mobile and more intuitive to operate, resulting in an increased expectation and demand for complex services in ever-reducing timescales; [1]
- At the same time, back-end ict infrastructures and systems are increasing in their sophistication and complexity, with commensurate increases in the skill levels required to develop, maintain and operate them; [1]
- The combination of a suspension on recruitment and a general shortage of people with the requisite ict skills makes it difficult for customers to attract and employ sufficient quantities of ict personnel; [1]
- The government has articulated its commitment to rationalizing core
- Processes that are duplicated by establishing shared back office operations or shared services for a range of disciplines including ict;
- A number of government units have already entered formal shared ict service arrangements and have deployed or redeployed staff accordingly; [1]
- Quite a number of government units are co-locating or consolidating their backend ict infrastructure or elements of it in other public service data centers (mainly those operated and managed by the national information center) to reduce hosting costs and to share the costs of power, cooling and basic management; and [1]
- Cloud computing now gives government units the opportunity to consider the consumption of ict services on some form of metered basis as an alternative to traditional provisioning models. [1]

As part of its aim to make National Information center, the consultant of government a leader in Cloud Computing, National Information Center has said that it will promote greater use of Cloud Computing in the public sector. In this context, National Information center dealing primarily with computing power, storage and infrastructural services such as email. These have demonstrated that, while Cloud Computing certainly provides opportunities for efficiencies and cost savings, it isn't yet evolved to the degree required by the public service in terms of security, reliability, service levels, standards, jurisdictional, legal and contractual arrangements, technical interoperability, licensing, dynamic and real-time availability, availability of requisite skills, and commercial models. [1]

National Information Center accepts that Cloud Computing is a major shift in the provision of ICT infrastructure, systems and services. It is acknowledged that it has the

potential to fundamentally change the nature of ICT delivery over time, and to provide benefits in terms of efficiencies, cost effectiveness, speed to market, the leveraging of new opportunities, improving mobility and access, and deploying resources on core activities. As a consequence, it is anticipated that Cloud Computing will be a key part of the strategic future of ICT in the public service, eventually becoming the default and primary delivery mode. [1]

Accordingly, as a general principle, and once the appropriate guidance for evaluation and assessment is in place government units should seek Cloud-based provision as an option for consideration when procuring ICT solutions. [1]

In this context, this Strategy proposes that:

- The use of "private clouds" will be limited to those that receive sanction based on a solid business case and specific, unique requirements; [1]
- Offerings of "public cloud" based provision of solutions need to be subjected to an appropriate application of the criteria for public cloud consideration (annex ii) by the public body concerned; and
- National information center will seek to develop a public service community cloud to negate the necessity for private clouds and to provide another cloud option where the public cloud is deemed not suitable. [1]

2. Public Cloud

While public clouds may be considered by a public body for any requirement, it seems most likely that initial deployments would be most appropriate for:

a) Any public-facing and non-sensitive activity, In other words
- open data initiatives,
- public information repositories,
- public collaboration,
- analytics involving non-sensitive or non-confidential data,
- the front-end elements of online services or apps that do not store sensitive data,
- simulation testing of the availability, robustness and functionality of online services;

b) Developing, piloting and testing new applications or solutions where deep integration with back-end data of a sensitive or confidential nature is not required; and
c) Trailing new approaches that would ordinarily require a considerable capital investment or risk. [1]

3. Public Service Community Cloud

National Information center needs to develop its own Community Cloud for those circumstances where public cloud offerings are deemed unsuitable. [1]

Phase I of a Public Service Community Cloud will seek to evaluate and provision Infrastructure as a Service (IaaS) as follows: [1]

a) Availability only through connectivity with National Networks.
b) It will be coupled with the continuing program of data Center rationalization. In this context, it is anticipated that this IaaS will be provided from data centers owned and managed by National Information Center. However, the use of commercial data centers may be considered subject to evaluation of risk, adequate protections and remedies being provided for contractually, and demonstrable value for money. [1]
c) A public procurement exercise will be conducted to establish a framework of multiple IaaS providers – ideally offering a variety of platforms. While the infrastructure may reside in Government-owned facilities on National Network, the infrastructure would remain the property of the providers, and would be operated, maintained and managed by those providers. They would provide government units with a standardized catalogue of offerings and services and with the required provisioning tools or services. [1]
d) In general, all new infrastructure requirements of government units, such as compute and storage and associated services, would be satisfied through this framework. Each government units would choose its infrastructure provider through mini-competitions within the framework. government units would pay for such infrastructure services on some form of metered basis. Actual charging models and thresholds would be agreed as part of the framework establishment. [1]

Phase II of a Public Service Community Cloud/s will seek to deploy a range of key infrastructural solutions on a centralized multi-tenanted basis, such as, firewalling, web/content filtering, anti-spam, and anti-virus solutions. [1]

Whereas Phase I of a Public Service Community Cloud will ensure a gradual movement away from owned computing infrastructure to the IaaS solutions, [1]

Phase III will seek to develop pilots, proofs of concepts, and live implementations on top of those IaaS platforms, including Platform as a Service (PaaS) solutions. Examples could include: [1]

a) A range of common services/platforms such as –
   - Websites and portals – both in terms of development and hosting,
   - Caching for websites,
   - Database services,
   - Dynamic dr (disaster recovery) based on multi-site provision; and
b) Key infrastructure platforms such as –
   - Directory and federated authentication services,
   - Virtual desktop infrastructure (vdi), and
   - Email. [1]

Phase IV of a Public Service Community Cloud will seek to expand the IaaS environment with Software as a Service (SaaS) solutions such as –

- Analytics with sensitive information;
- Collaboration/content sharing technologies;
- Document management; and
- Case management.

However, it is acknowledged that some of these may take considerably longer than the proposals at Phase III because of the specific nature of customizations typically implemented in individual organizations. [1]

Phase V of a Public Service Community Cloud will involve the migration of existing legacy and mission-critical systems from traditional platforms. As it is usual to migrate such systems when requiring redevelopment, it seems inevitable that this Phase will take considerable time. [1]

Data Centre Rationalization:

Over the last six years, most of government units have successfully moved elements of their back-end infrastructure, systems, applications and web site to national data center belonging to National Information Center

This consolidation effort will now be formalized as follows:

- Criteria will be developed to identify appropriate data centers/facilities for inclusion in a framework of both fixed and container-based facilities – this framework will incorporate regional distribution for business continuity and DR purposes and is likely to number less than 10;
- The levels and qualities of services to be provided as standard and as value added in these facilities, will be established and catalogued;
- The staffing levels and skills required to operate these facilities and environments and how those should be sourced will be identified;
- Principles for the funding (including if necessary, cost-sharing models) of these facilities will be defined; and
- The appropriate governance structures will be designed and established. [1]

The concentration will be on the consolidation of sites, rather than the consolidation of equipment. The latter will be dealt with over time with the advancement of the Public Service Community Cloud as detailed. While this consolidation program may not result in any significant reduction in equipment, it will remove a great deal of attendant costs in servicing multiple sites with power, cooling, light, networking, maintenance services, and staff supports. [1]

Once these policies have been adopted, and a sufficient level of operation has been established, Government approval will be sought to mandate government units to use the selected data center facilities for all new developments and to migrate existing environments within a defined timeframe. [1]

4. Implementation

In summary, this Strategy support that: [1]

- Cloud-based provision of ICT solutions and ICT shared services will, over time, become the default approach for the public service; government units will then begin to include consideration of Public Cloud offerings in their procurement exercises for ICT solutions;

National information Center will work with government units to develop procurement frameworks for public cloud solutions of universal applicability; [1]

- Existing work in consolidating data centers will be standardized and formalized and the necessary funding and governance arrangements will be defined and implemented;
- A public service community cloud will be developed in phases and coupled with the data center consolidation work underway; [1]
- The exploration, piloting and development of a public service community cloud should encompass solutions from private sector providers, ideally offering different solutions; and
- These approaches will be mandated as they become established and proven to provide best value for money. [1]

Additionally, National Information Center will assess the impact of this Strategy, particularly those aspects relating to the consolidation of ICT environments and the greater centralization or sharing of ICT services, on existing ICT organizational structures in the public service. The National Information Center will bring its assessment through the Public Service Reform governance arrangements to ensure full consideration by senior managers of arising business implications. [1]

It should be noted that, although five phases have been set out for the implementation of the Public Service Community Cloud. [1]

These need not be advanced sequentially. It is anticipated that there will be considerable parallelism in the implementation of these discrete phases. [1]

Additionally, the lists of ICT activities provided for Phases II V of the Public Service Community Cloud are not exhaustive and other services or solutions may, and most likely will, be added as advancements are made and opportunities emerge. National Information Center will maintain an open approach in the determination of targets and the timing of same. [1]

The development of the Cloud Computing Strategy will be monitored and aligned with where appropriate. In this context, support will also be given to the assessment, and where necessary, amendment of existing procurement law to better facilitate the procurement of cloud-based computing resources or solutions, particularly for circumstances such as:

- Unpredictable and irregular use requirements;
- Seasonal or burst requirements;
- Rapid deployments in specific circumstances; and
- Technology trials leading to use. [1]

The National Information Center views this Strategy as a living document which it will keep under review and which it will amend or supplement as Cloud Computing evolves and material information comes to light. [1]

Table A: Timeline for Strategy Activities [1]

Activity	Approximate TimeLine
Development of Public Cloud Assessment Criteria (Annex II)	Within 1 year
Development of Public Cloud Procurement Guidance	Within 1 year
Development of Evaluation Criteria for Public Cloud offerings	Within 1 year
Initial Procurement Exercise for Public Cloud Based Solution	Within 1 year
Formalization of Data Centre Selection and Consolidation Criteria	Within 1 year
Consolidation of Data Centers	1 – 5 years
Public Service Community Cloud Phase I	1 – 5 years
Public Service Community Cloud Phase II	Within 2 years
Public Service Community Cloud Phase III	1 – 5 years (dependent on the emergence of interoperable and mature solutions, the availability of the resources needed to advance projects, and the need to extract VFM from existing investments)
Public Service Community Cloud Phase IV	1 – 5 years (dependent on the emergence of interoperable and mature solutions, the availability of the resources needed to advance projects, and the need to extract VFM (Value for Money) from existing investments)
Public Service Community Cloud Phase V	1 – 10 years (dependent on systems development lifecycle, the investment amortization/depreciation timeline, and the availability of interoperable and mature solutions)
Implications on ICT organizational structures	Likely to be ongoing over the entire period

5. Potential Risks and Issues of Cloud Computing

As cloud computing is a new ICT sourcing and delivery model NOT a new technology, many of the risks and issues associated with cloud are also not new. However, as most agency systems were designed to operate in a secure environment, agencies need to fully understand the risks associated with cloud computing both from an end-user and agency perspective and, based on this, adopt principle and risk-based approaches to their strategic planning. Depending upon the cloud model adopted, an understanding and mitigation of the following issues will be required: [2]

Table B [2]

Issue	Explanation
Application design	• There may be less opportunity for customization of applications and services. This may increase complexity when integrating cloud services with existing legacy environments; • Applications (could be either SaaS or Line of Business applications, etc) will need to be treated at arm's length from the infrastructure layer (IaaS); • Applications will need to be designed to accommodate latency; and • Existing software licensing models may not facilitate a cloud deployment.
Architecture	• Moving to a cloud environment will require more emphasis on business design where cloud services will interface/impact business systems; • Prior to making a decision to move to a cloud computing environment, agencies must address the impact on business processes and eliminate any technical barriers; and • Finance recommends agencies use an architectural framework
Business continuity	• Because the cloud is dependent on internet technologies, any internet service loss may interrupt cloud services; • Due to the dynamic nature of the cloud, information may not be immediately located in the event of a disaster; and • Business continuity and disaster recovery plans must be well documented and tested.
Data location and retrieval	• The dynamic nature of the cloud may result in confusion as to where information actually resides (or is transitioning through) at a given point in time; • When information retrieval is required, there may be delays impacting agencies that frequently submit to audits and inspections; and • Due to the high availability nature of the cloud, there is potential for co-location of information assets with other cloud customers.
Funding model	Due to the cloud's pay-per-use model, some part of ICT capital budgeting will need to be translated into operating expenses (OPEX), as opposed to capital expenditure (CAPEX), which may have different levels of authorizations to commit expenses and procure services.
Legal &	• Need to have the ability to discover information under common law;

regulatory	• Need to be aware of data sovereignty requirements; • Need to be aware of legislative and regulatory requirements in other geographic regions, as compliance may be a challenge for agencies; and • Little legal precedent exists regarding liability in the cloud and because of this, service agreements need to specify those areas the cloud provider is responsible for.
Performance and conformance	• Need to ensure that guaranteed service levels are achieved. This includes environments where multiple service providers are employed (e.g. combined agency and cloud environments). Examples include: • Instances of slower performance when delivered via internet technologies; • Applications may require modification; • Monitoring and reporting are adequately delivered for the period between service introduction and exit; and • Failure of service provider to perform to agreed-upon service levels.
Privacy	Risk of compromise to confidential information through third party access to sensitive information. This can pose a significant threat to ensuring the protection of intellectual property (IP), and personal information.
Reputation	Damage to an agency's reputation resulting from a privacy or security breach, or a failure to deliver an essential service because risk was inadequately addressed must be considered for cloud computing applications.
Skills requirements	A direct result of transitioning to a cloud environment means: • Less demand for hardware and system management software product-specific skills; and • More demand for business analysts, architects, portfolio and program and change managers, and vendor/contract managers.
Security	• Must ensure cloud service providers and their service offerings meet the requirements of the Protective Security Policy Framework (PSPF). • With cloud computing, an agency may have limited ability to prescribe the protective security of the cloud environment. Yet agencies will remain ultimately responsible for the information that is stored and/or processed in the cloud. Management must maintain assurance that the security of the cloud service provider is in accordance with the PSPF.
Service provision	• Reputation, history and sustainability should all be factors to consider when choosing a service provider; • Agencies should take into consideration the volatility of the growing cloud computing market; and • Agencies should ensure they address portability of data in the case of service provider failure.
Standards	• Strategies for open standards, interoperability, data portability, and use of commercial off the shelf (COTS) products are required for reducing the risk of vendor lock-in and inadequate data portability. Examples include: • Potential for inadvertent use of cloud services creating "islands" of cloud technologies that will reduce interoperability across cloud types and associated implementations; • A cloud provider decides to no longer stay in business, an agency's data/application/processes must be able to be moved to another provider; and • Certification of projects by vendors for prescribed platforms and versions.

6. Potential Business Benefits of Cloud Computing for Sudan Government Agencies

Transitioning to cloud services may offer the following business benefits for Sudan Government agencies – the level of benefit will depend on the cloud model adopted. [2]

Table C [2]

Benefit	Detail
Scalability	Unconstrained capacity allows for more agile enterprises that are scalable, flexible and responsive to change. For example: • Faster responsiveness can benefit government service delivery, and meet the needs of citizens, businesses, employees, suppliers and corporate relations. For example, ability to provision and utilize a service in a single day; • Option of scalability is provided without the serious financial commitments required for infrastructure purchase and maintenance; and • Provisioning and implementation are undertaken on demand, allowing for traffic spikes and reducing the time to implement new services. Agencies, however, need to be aware that when transitioning from legacy systems, data migration and change management can slow down the "on demand" adoption of cloud computing.
Efficiency	Reallocation of IT operational activities offers opportunity for agencies to focus on: • Research and development including new and innovative applications allowing for business and product growth (improved service delivery); • Creating new solutions that were not technically and/or economically feasible without the use of cloud services; • Enabling prototyping and market validation of new approaches much faster and less expensively; • Providing the ability to de-couple applications from existing infrastructure; and • Rationalizing legacy systems.
Cost Containment	**Changes to an agencies cost model can be modified by the following:** • Services and storage become available on demand without the serious financial commitments required for infrastructure purchase and maintenance. Additionally, they are priced as a pay-as-you-go service; • Transfer of costs **from CAPEX to OPEX** • no need to invest in high-cost IT equipment; for example, able to test software solutions without capital investment; **Reduction of operating costs** • reduced energy consumption;

	• less expense in managing IT systems; • less cost and complexity in doing both routine computing tasks and computationally-intensive problems; • reduced associated with time delays; • potential to reduce support and maintenance costs through transitioning legacy systems to new systems; • potential to reduce the demand for data center resources; and • potential to reduce the Government's carbon footprint. Note: agencies will need to compare current costs against potential cloud expenses and consider models for lowering total cost of ownership (TCO) to understand whether cloud services will offer any potential savings.
Flexibility	• Agencies can save time at set-up, as cloud computing becomes functional faster than other systems; • To transition to the cloud, agencies are not required to install additional hardware or software; • Implementation can be undertaken remotely; and • Potential to access latest technology through software applications being automatically updated by cloud providers.
Availability	• Cloud software architectures are designed from the bottom up for maximum network performance – potentially delivering improved application level availability than conventional IT solutions; and • Greater flexibility and availability of 'shared' information enables collaboration from anywhere in the world – all that is required is an internet connection.
Resiliency	• The potential for failure in a highly resilient computing environment is reduced. The failure of one node of a system in a cloud environment will have no impact on overall information availability and reducing the risk of perceivable downtime.

7. Sudan Government Cloud Computing Policy

Policy Statement
The Sudan Government and its agencies may choose cloud based services if they demonstrate value for money and adequate security. [2]

Vision
The vision for a whole-of-government principles and risk-based approach to cloud computing is to enable the government's ICT ecosystem to meet the wide range of agency business requirements in an optimal manner with regard to cost, security, flexibility, and operational reliability/ robustness. [2]

Key Drivers for Adoption:
The key drivers for agencies to adopt the cloud strategy are: [2]

Table D [2]

Drivers	Outcome
Value for Money	• To reduce duplication and cost; • Leveraging economies of scale; • Increased savings through virtualization; • Allow for "measured" payment (pay as you use); • Reduced energy use; • Enable agencies to reinvest in, and concentrate on, core objectives; • Adopt, where fit for purpose, modern technologies and practices that improve ICT effectiveness and efficiency.
Flexibility	• Create a flexible services-oriented environment for agencies; • Rapid provisioning and deployment of services and on demand scalability and elasticity for services and capabilities.
Operational reliability/ robustness	• High resiliency and availability; • Standard offering.

8. Annex I

The NIST Definition of 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. This cloud model is composed of five essential characteristics, three service models, and four deployment models. [1]

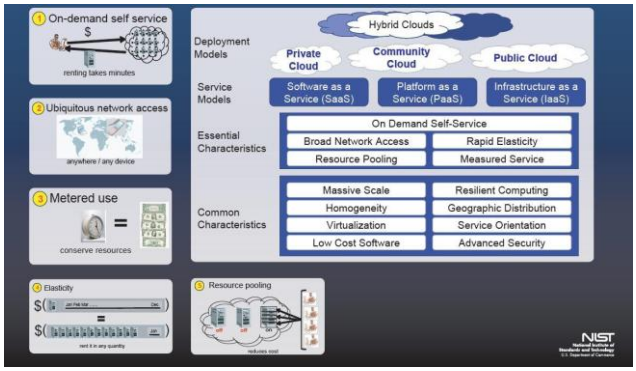

Figure A [2]

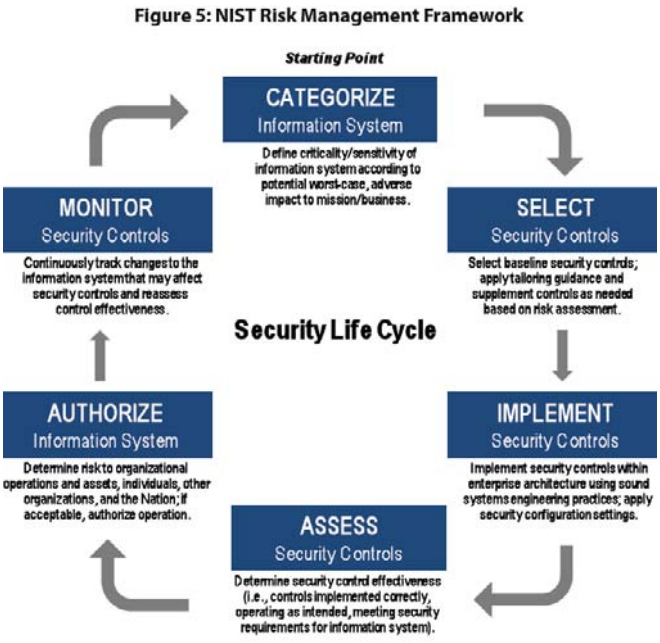

Figure B [4]

Essential Characteristics: [1]

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. [1]

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). [1]

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth. [1]

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time. [1]

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability10 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. [1]

Cloud computing is the result of several technology advances including:

- Reliable, high-speed networks, such as the NBN;
- Very large, global-class infrastructures deployed by vendors like Google and Amazon;
- Virtualization capabilities;
- Commodity server hardware;
- Open source software (e.g. Linux, Apache, and Hadoop), which has slashed the cost of software for data centers; and
- Adoption of open Web 2.0 standards, which has made development of applications in the Cloud much easier and faster. [2]

Figure C: Gartner Hype Cycle for Cloud Computing, 20108, identifies which aspects of cloud computing are in the hype stage, applications/technologies approaching significant adoption, and those that are reasonably mature. While "security as a service" is closer to the plateau of productivity than "virtualization" for example, the former still has 2 to 5 years to mainstream adoption, while the latter less than 2 years. This essentially means that market penetration is higher for virtualization, while maturity of the technology and business models is more advanced for security as a service.

Due to cloud computing being at the peak of the hype cycle, agencies that seek to transition to a cloud computing arrangement may have to consider increased risks at this time. [2]

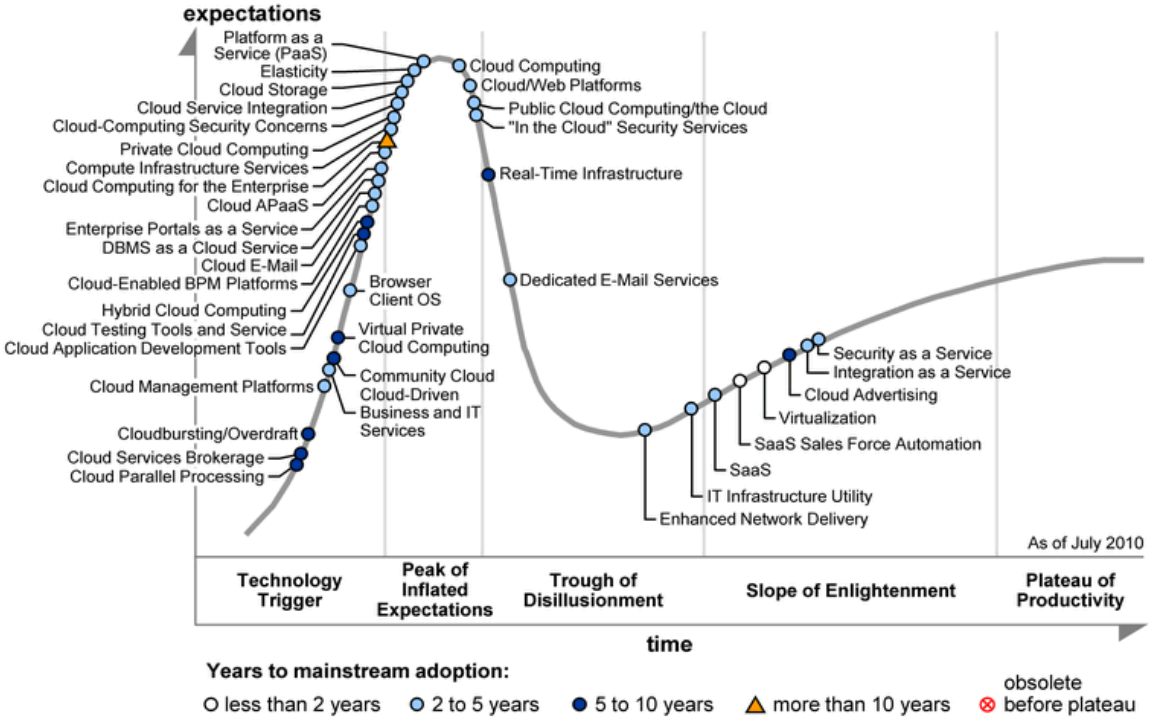

Figure C [2]

Note: The above Hype Cycle Graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. [2]

Advanced Virtualization
Advanced virtualization is a technology rather than a cloud delivery model. It can be defined as a virtual ICT infrastructure that has automated management. [2]

The cloud characteristics that are not intrinsic in virtualization are:
- Capability to undertake usage based billing and invoicing;
- On-demand self-service, at least for end-users (to some extent);
- Broad network access; and
- Rapid elasticity (to some extent).

Advanced virtualization has been included to provide a complete set of information for agencies. [2]

Service Models:

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure11. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. [1]

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.12 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. [1]

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). [1]

Deployment Models: [1]

Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. [1]

Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). [1]

9. Annex ii

Criteria for Public Cloud Consideration [1]
1. Application Design
2. Architecture
3. Business Continuity and Disaster Recovery
4. Commercial and Pricing Model/s
5. Data Location and Retrieval
6. Legal and Regulatory (incl. data protection, governing laws, intellectual property, termination)
7. Performance and Conformance
8. Privacy
9. Reputation
10. Security
11. Security Standards
12. Service Provision (incl. SLAs, transitioning)
13. Staffing and Skills Requirements
14. Technology Lock-In – Migration and Interoperability
15. Technology Standards
16. Value for Money

References

[1] *per.gov.ie/wp-content/uploads/Cloud-Computing-Strategy.pdf*
[2] http://www.finance.gov.au/files/2013/04/final-_cloud_computing_strategy_version_1.1.pdf
[3] https://www.nist.gov/sites/default/files/documents/itl/cloud/cloud-def-v15.pdf
[4] https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf