Cloud Readiness Pilot Assessment Report

June 2016

Table of Contents

0 Disclaimer

The Toolkit is a diagnostic and planning tool intended to provide recommendations for action based on existing good practice. It does not constitute technical or legal advice and no inference should be drawn as to the completeness, adequacy, accuracy or suitability of the underlying assessment or recommendations. Without limitation to the immunities and privileges of the Bank under its Articles of Agreement and other applicable laws, the Bank shall not be liable for any loss, cost, damage or liability of any kind as a result of this Toolkit or its use.

1 Introduction

More and more governments are looking to move to a cloud platform. Cloud platforms, when correctly implemented, can potentially provide greater:

- flexibility in terms of allocating and managing resources (both computing and personnel)
- standardization of the overall enterprise architecture, thus simplifying maintenance and future application development
- opportunities for organizations within governments to share data and applications
- opportunities for governments to build up technical skills that can help a country be technology competitive on the international stage

Cloud computing has the ability to level the technological playing field and enable countries with limited infrastructure and digitization to leap frog countries that have a traditional, and less flexible infrastructure and a large number of large, legacy applications.

While having a cloud platform makes it easier to implement major goals of governments, such as eGovernance, it is fundamentally a more flexible, on-demand approach to allocating computing resources. Cloud computing can be a great enabler, but it does not replace needed strategic initiatives or overcome existing processes and regulations. Cloud computing is a fast paced, and quickly evolving area of computing. As such, it can be daunting for governments to implement a true cloud platform, especially as there may be specific and unique concerns around areas such as data security when using cloud technologies.

The World Bank Cloud Readiness Toolkit was used as the input for this report. The toolkit is comprised of two assessments, a country assessment and an application and infrastructure assessment. Each assessment is comprised of a series of questions. The toolkit is designed to provide a baseline for a country. This baseline shows how ready a government is to implement a cloud platform, and provides tailored recommendations based on the gaps identified from completing the assessments. All questions are geared towards the government and the public sector. As such, the toolkit does not assess cloud providers or skills available in the private sector.

The country assessment questions cover the following categories:

Category	Purpose
General	Determine the true level of interest in migrating to the cloud and also the primary benefit that the government hopes to realize.
Resources	Determine if the government has the key skills already available or easily accessible prior to starting a cloud migration.
Security	Determine what kind of security is required, including rules around data retention and security clearances. Perception of security may also impact public adoption of applications meant for use by the citizens of a country.
Regulations	Determine whether there are regulations in place that would prevent the migration of some or all government applications to a public cloud or discourage the creation of local cloud providers.
Governance of Information and Communications Technology (ICT) Systems	Determine whether existing IT processes and procedures have been adapted to a cloud environment. If applications cannot effectively utilize a cloud environment, the government will not fully realize the potential benefits.
Data	Determine how secure a government's data is now and whether there are regulations in place that would prevent the migration of some or all government data to a public cloud and what the overall quality of the data currently is.
Infrastructure	Determine whether migrating to the cloud may be too much of a burden on the existing infrastructure.

The application and infrastructure assessment questions cover the following categories:

Category	Description
General	This section covers questions that are not covered in the other categories, such as which department owns the application.
Architecture	This section covers questions that help determine what kind of cloud computing resources would be needed and how they can be optimized. This category also determines whether the application would benefit from the cloud architecture.
Operation Optimization	This section covers how the application is currently being used and what the potential boundaries for future growth are based on the current infrastructure.
Security	This section covers data security, for example any sensitive data (classified data or information that can be used to identify individuals) or encryption requirements.

The questions are weighted and scored to produce recommendations that offer a conversation starter on the current readiness to implement cloud computing. The questions and weights within the assessment documents can later be updated dynamically to reflect changes in policy or circumstances, which will update the scores and corresponding recommendations. These recommendations are only guidelines, and do not replace detailed assessments and planning that will be needed for a successful cloud migration.

1.1 Contents

The below sections can be found in this report.

1.1.1 What is Cloud Computing?

This report contains a high level overview of cloud. Cloud computing is still a relatively new concept and one that is rapidly evolving to meet ever changing technological demands and needs.

1.1.2 Findings and Recommendations

The World Bank Cloud Readiness Toolkit was piloted in three countries in order to test the toolkit as thoroughly as possible, and then refine the toolkit based on lessons learned. The findings from all three pilots as well as lessons learned are found in this section. Findings include a recommended deployment model and high level roadmap.

1.1.3 Assumptions

This section briefly discusses the assumptions that were incorporated into the toolkit

1.1.4 Public Cloud Vendor Comparison

Vendor selection can be one of the most challenging parts of migrating to the cloud. The number of vendors and their various attributes can be overwhelming. In addition, vendors frequently do not provide the same metrics and attributes making comparisons even more challenging. This section compares two of the largest public cloud vendors in terms of size, global reach, and variety of offerings. This section is intended to provide a guideline for vendor comparisons that governments may undertake.

This report will not:

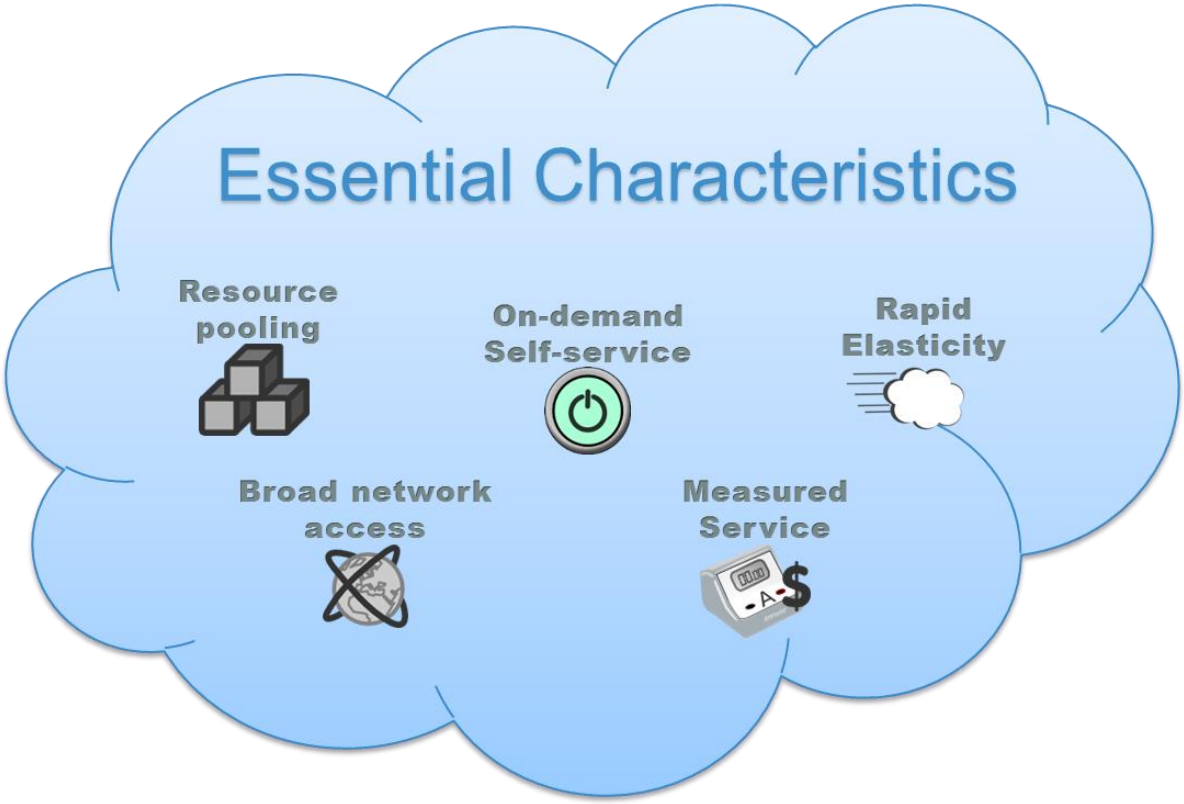
- Replace an in depth assessment or business case
- Provide steps for building a private data center or selecting a public cloud provider
- Provide estimates for migrating to the cloud
- Provide guidance on budgeting for migrating to the cloud
- Recommend a specific cloud provider
- Assess cloud providers
- Assess skills and offerings available in the private sector
- Recommend a service model

2 What is Cloud Computing?

According to the National Institution of Standards and Technology, cloud computing is a model for enabling ever present, convenient, on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (U.S. Department of Commerce, 2011). In other words, cloud computing can also be referred to as on-demand computing. It is a way for users to get continual access to shared computing resources, such as servers, storage, and sometimes services, as needed.

2.1 Essential Characteristics

There are five essential characteristics that define the cloud, as shown in the schematic below.



2.1.1 Resource Pooling

The cloud provider pools all computing resources to serve multiple customers (U.S. Department of Commerce, 2011). These customers can be both external, in the case of a public cloud provider, who might be serving multiple organizations, or internal, in the case of a private data center which may be serving multiple departments. The pooled computing resources are assigned as and when needed, but released and reassigned for other purposes when not being used. Instead of the traditional approach of allocating a single server or amount of space to an application, computing resources are dynamically allocated as needed. This optimization of the infrastructure typically reduces overall infrastructure costs and limits risks such as server failure.

However, the downside to resource pooling is that you have multiple users, groups, or organizations using the same computing resources. This concurrent use of shared computing resources by multiple users, also known as tenants, is referred to as multitenancy. As part of multitenancy, applications still need to be isolated from each other so that problems in one application do not affect others. In addition, access to one application does not mean access is provided to other applications using the same computing resources.

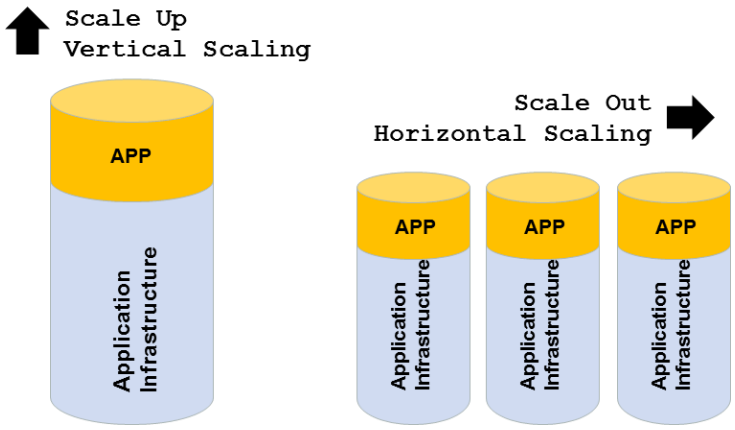
2.1.2 On-Demand Self-Service

Cloud services are provided on request (U.S. Department of Commerce, 2011). Users can request computing resources, such as server time and network storage, as needed, automatically, without requiring human interaction with the service provider. This automation is generally considered more efficient and less error-prone than traditional provisioning processes where requests must be submitted and servers manually set up and configured. The downside is that individuals may request resources whenever they need them, but may not release them when they no longer need them. Automated tools can help with this as well.

2.1.3 Rapid Elasticity

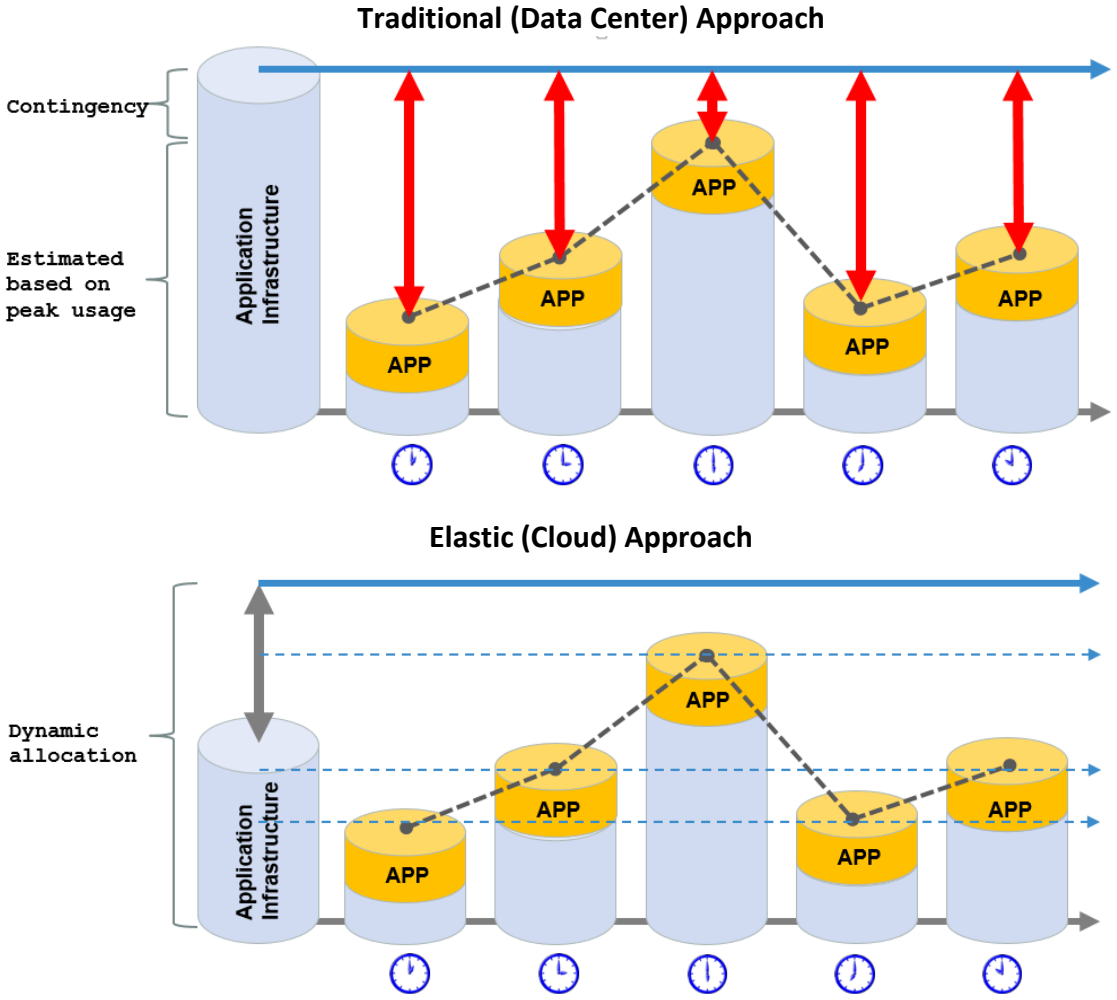
Computing resources can be elastically provisioned and released, in some cases automatically, enabling applications to scale rapidly in line with demand. The computing resources available for provisioning may be requested in any quantity at any time. This enables more effective utilization of the available infrastructure (U.S. Department of Commerce, 2011). To better understand this concept, it helps to understand what it means for an application to scale.

An application can scale either vertically or horizontally. Vertically means the existing application instance is using more of a specific resource, horizontally means adding additional instances of an application or nodes. An example of scaling horizontally would be going from one web server to three and an example of scaling vertically would be going from 4 GB of memory to 16GB.



Traditionally, computing resources have been allocated with additional contingency in case it is needed. Elasticity refers to the ability for a platform to be dynamic and adaptable as opposed to static. A cloud platform is elastic and can adapt to increasing and decreasing utilization by

rapidly expanding and shrinking computing capacity for a given application or application service. In the diagram below the overall application infrastructure that is used is significantly less in the elastic, cloud based approach.



2.1.4 Broad Network Access

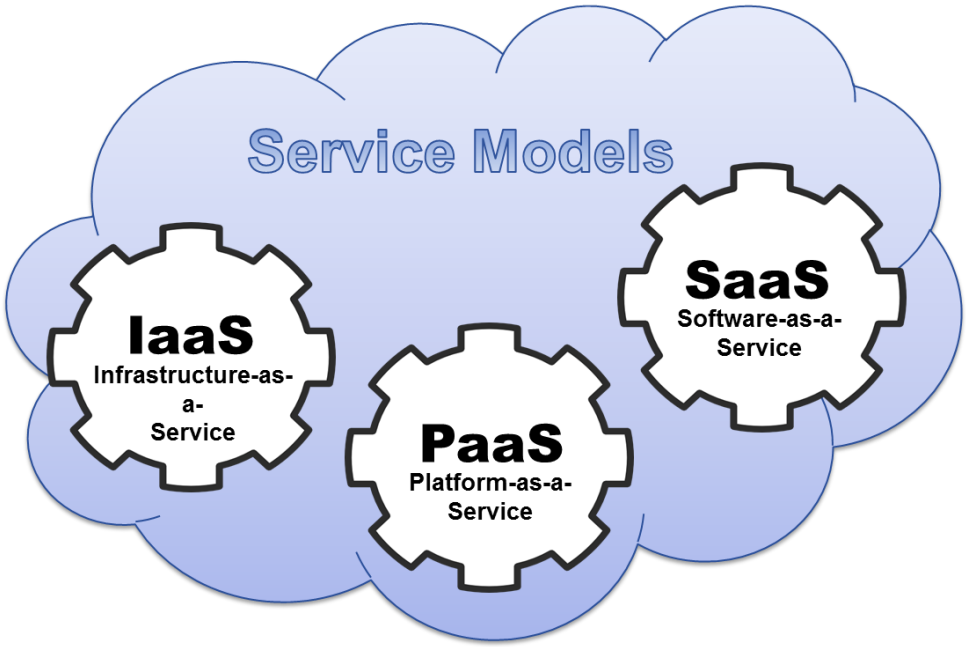
Computing resources are available over the network and accessed through standard devices such as computers or mobile phones (U.S. Department of Commerce, 2011). It is important to keep in mind how a cloud will be reached and what the network availability and bandwidth capacity is before choosing a particular cloud solution.

2.1.5 Measured Service

Cloud systems automatically control and optimize resource use by tracking usage at a level appropriate to the type of service (i.e., storage, processing, network bandwidth, or active user accounts) (U.S. Department of Commerce, 2011). Payment for these services are based on this usage. This is also known as “pay per use”.

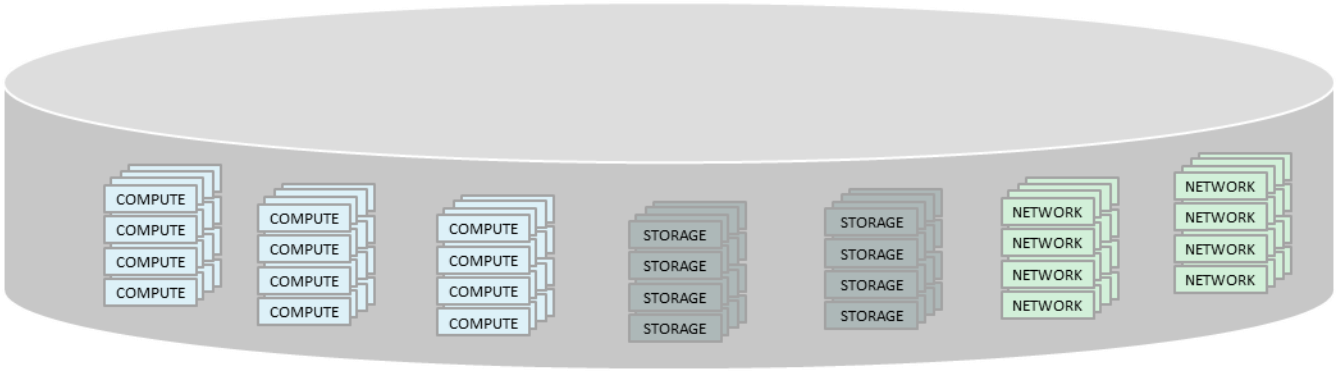
2.2 Service Models

There are three service models in cloud computing: (i) Infrastructure as a Service (IaaS), (ii) Platform as a Service (PaaS), and (iii) Software as a Service (SaaS).



2.2.1 Infrastructure as a Service (IaaS)

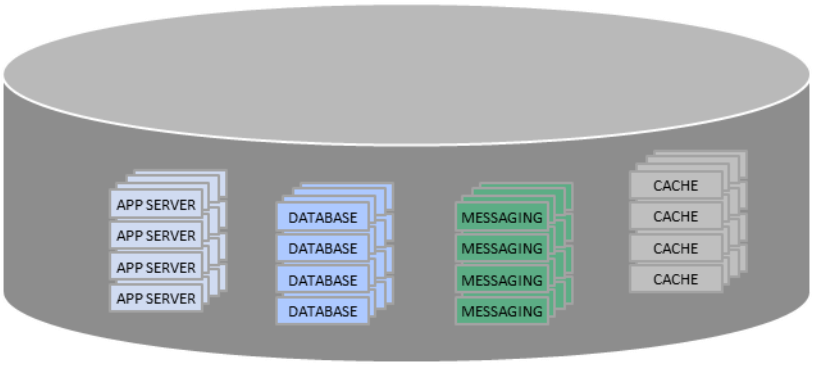
Infrastructure as a Service provides the capability to request (or provision) processing, storage, network, and other fundamental computing resources; the requester is able to deploy and run operating systems and applications (U.S. Department of Commerce, 2011). The requester does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and limited or no control of the networking components (i.e. host firewalls).



2.2.2 Platform as a Service (PaaS)

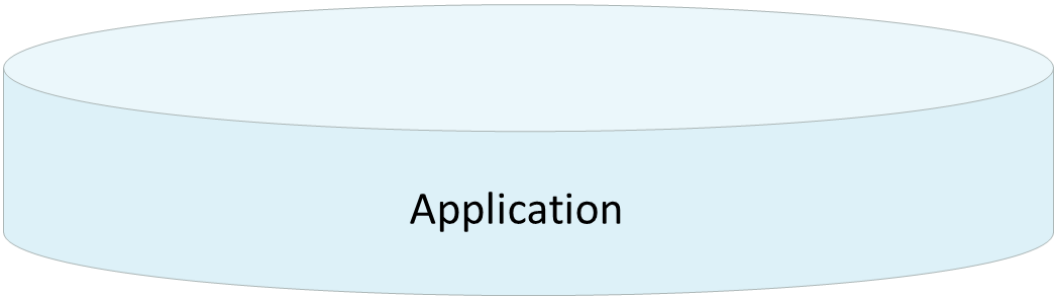
Platform as a Service provides the capability to deploy onto the cloud infrastructure, user-created or owned applications created using programming languages, libraries, services, and tools **supported by the provider** (U.S. Department of Commerce, 2011). The requester does not manage or control the 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. If an application currently resides on an unsupported operating system i.e. UNIX, the application will need to be updated to run on a supported operating system i.e. Linux or take advantage of an IaaS offering where any operating system can be installed.



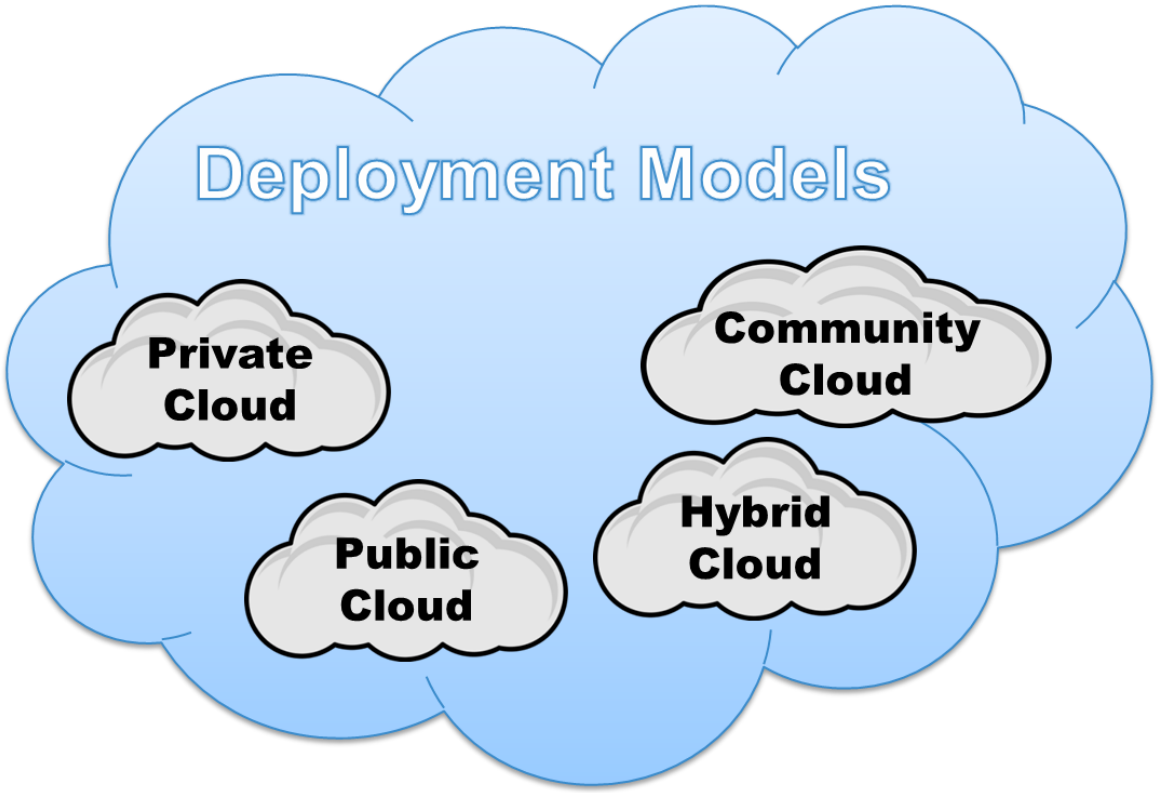
2.2.3 Software as a Service (SaaS)

Software as a Service provides the capability to use the provider's applications running on a cloud infrastructure (U.S. Department of Commerce, 2011). The applications are accessible from various user devices through either an interface, such as a web browser (i.e., web-based email), or a program interface (i.e. Office 365). The requester does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage. Individual applications cannot be altered but there may be user configuration settings that can be adjusted.



2.3 Deployment Models

There are four deployment models to choose from when considering migrating to the cloud.



To understand when to use a particular deployment model as the preferred choice, the models have been compared across five categories – Security, Reliability, Flexibility, Cost, and Vendor Lock-in (degree of difficulty to migrate to a different model if needed in the future). These comparisons are primarily for legacy applications. For each category there is a description and a general score. The score is in relation to the other models.

The table below describes the scoring used in this section.

Icon	Meaning
✓	In comparison to other deployment models, this model is particularly strong in this area.
-	In comparison to other deployment models, this model is neutral or average in this area.
✗	In comparison to other deployment models, this model is weak in this area.

2.3.1 Private Cloud

A private cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple users (i.e. departments). It may be owned, managed, and operated by the organization, a third party, or some combination, and it may exist on or off the premises.

Category	Description	Benefit?
Security	Private clouds are typically more secure than alternatives as the servers are controlled and no other organization has access to them (Pham, 2011).	✓
Reliability	Depending upon the infrastructure within a country, a private cloud, especially if there is a direct line connecting the cloud to the government buildings, may be more reliable than alternatives. For example, if the Internet is frequently slow or unavailable during the day during times of high traffic, then making the internet the primary method of reaching key applications may impact day to day business activities.	✓
Flexibility	A private cloud can be geared towards a particular government's needs. It can be built based on the specific requirements that an agency or department needs.	✓
Cost	Higher setup costs, as all hardware (servers, storage, etc.) must be repurposed or purchased. In addition, all future server maintenance would be performed by the government or third party vendor.	✘
Vendor Lock-in	Once an application is virtualized, it is much easier to move from platform to platform. However, a specific virtualization software must be selected when creating a private cloud. This will create a certain amount of lock-in to a specific vendor, but not significantly more or less than any other cloud option.	-

2.3.2 Public Cloud

A public cloud infrastructure is provisioned for use by any organization that wishes to pay for computing resources (U.S. Department of Commerce, 2011). It may be owned, managed, and operated by a business or outside organization. The infrastructure exists on the premises of the cloud provider rather than the users.

For the purposes of this toolkit, there is also a deployment model called local public cloud. This term applies to a local public cloud provider whose premises are within the country's borders. This may be the only option if a government has strict laws or policies around the storage and transport of data.

Category	Description	Public	Local Public
Security	For governments in particular, there is a risk of having classified or sensitive data located outside the country's borders. There is also the risk of an external threat (cyber-attack). However, there is also the benefit that cloud providers typically have more skilled employees to dedicate to cloud security.	-	✓
Reliability	Depending upon the infrastructure within a country, a local public or public cloud may be more unreliable than alternatives.	-	-
Flexibility	Local public or public cloud providers may limit the operating systems or databases that they provide. This may require that applications be upgraded to a more recent version of some components before being migrated.	-	-
Cost	Minimal setup and maintenance costs as hardware does not have to be purchased or maintained by the government. There will; however, still be licensing fees.	✓	✓
Vendor Lock-in	While there are companies that specialize in enabling users to move from one cloud platform to another, it does require effort. In addition, once the government gets rid of hardware or requests more capacity than they currently have purchased, it is difficult to move all applications back to government data centers without investing time and money. Thus, going with a public cloud provider results in a certain level of vendor lock-in.	✘	✘

2.3.3 Community Cloud

The community cloud is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (i.e., mission, security requirements, policy, and compliance considerations) (U.S. Department of Commerce, 2011). 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. Community clouds are frequently used by government or educational institutions that consist of a number of different entities (i.e. departments or colleges).

Community cloud is a form of private cloud with multiple tenants where all of the tenants are part of the same parent organization. For the purposes of this toolkit, if multiple departments or ministries decide to utilize the same private cloud then private cloud and community cloud are equivalent. For example, if both the Ministry of Finance and the Ministry of Defense want to use the same private cloud, but the Ministry of Defense does not want employees from the Ministry of Finance to have access to the defense data, then you have a private cloud with two tenants. This is now a community cloud. The addition of another tenant does impact the security and flexibility of the offering in relation to a private cloud that is dedicated to a single tenant. A private cloud with multiple tenants must be able to offer the technical architectures both need. For example, if the Ministry of Finance has primarily .Net applications running on Windows servers and the Ministry of Defense has primarily Java applications running on Red

Hat Linux, the private cloud must now offer both platforms. In addition, appropriate security needs to be in place to ensure that access is restricted to the appropriate individuals. This is especially true if any database consolidation takes place.

Category	Description	Benefit?
Security	Typically all the organizations sharing a community cloud have similar types of data and restrictions. It also enables the organizations to combine their skilled employees. However, the more individuals with access to the cloud from other agencies or departments, the greater the risk of an external attack.	-
Reliability	Depending upon the infrastructure within a country and who owns the community cloud a direct line connecting the cloud to the government buildings, may be more reliable than alternatives.	✓
Flexibility	A community cloud can be geared towards a particular group's needs. However, if a large amount of variety is seen in terms of architecture and technologies across the community, some limits and standardization may be required.	-
Cost	Cost is greatly dependent upon whether the community cloud is owned by a member of the community or a third party. Also, if a large amount of effort is required to standardize the platform and applications across the organizations the upfront cost will be higher.	✘
Vendor Lock-in	Whether owned by one of the members of the community or a third party, any time you standardize options across a group you have a certain amount of vendor lock-in, but not significantly more or less than any other cloud option.	-

2.3.4 Hybrid Cloud

A hybrid cloud infrastructure consists of two or more distinct cloud infrastructures (private, community, or public) that remain separate, but are bound together by standardized or proprietary technology which enables data and application portability (U.S. Department of Commerce, 2011). A hybrid cloud is almost always a combination of public and private and is the combination considered in this section. The most common scenario is a predominantly private cloud that "borrows" computing resources from a public cloud when it experiences spikes in data. One example is taxes. Most people submit their taxes within a one month period of time. During the rest of the year there is minimal use of those tax applications. Revenue agencies must have enough computing resources to handle the peak demand before taxes are due. In a hybrid environment, that additional demand is handled by public cloud computing resources. This enables the agency to not have to maintain all those additional computing resources on a day to day basis.

Category	Description	Benefit?
Security	A hybrid approach can combine the strengths of both models, allowing the government to keep data under tighter control, but still get some of the benefits of the public cloud.	✓
Reliability	Depending upon the infrastructure within a country, a private cloud, especially if there is a direct line connecting the cloud to the government buildings, may be more reliable than alternatives. Since the public cloud is only used when needed, infrastructure issues will be minimized.	✓
Flexibility	If applications are also using public cloud computing resources, they typically must be compatible with the public cloud. Since public cloud providers may limit the operating systems or databases that they provide, a hybrid approach may require that applications be upgraded to a more recent version of some components before being able to use the public cloud.	-
Cost	Future setup and maintenance costs will be lower than with a purely private cloud approach, since excess capacity will be freed up. Rather than keep computing resources on hand to deal with peak demand, that additional demand will now spill over to the public cloud enabling temporary increases in capacity (Savvas, 2014). However, setting up the hybrid cloud requires expertise in integration and standardization, which can be expensive in the beginning.	-
Vendor Lock-in	Private clouds still require virtualization software. Moving applications from one software to another is difficult and can be costly so the government could be "locked-in" to the vendor of whatever software is chosen. Changing the public provider once a hybrid solution is setup can also be challenging.	✘

2.3.5 Overview

All four deployment models have different attributes making them better fits for some organizations than others.

Category	Private	Public	Local Public	Community	Hybrid
Security	✓	-	✓	-	✓
Reliability	✓	-	-	✓	✓
Flexibility	✓	-	-	-	-
Cost	✘	✓	✓	✘	-
Vendor Lock-in	-	✘	✘	-	✘

It should be noted that not all organizations should move to the cloud. Before selecting a deployment model, an organization first needs to consider the benefits and risks of moving to the cloud in the first place.

2.4 Benefits

Cloud computing has opened up new possibilities and enables numerous potential benefits, including significant cost savings, faster innovation, and greater flexibility. The following are the common benefits gained from cloud system implementation.

2.4.1 Faster Development of Applications

Cloud computing allows applications to be created and implemented faster. For many governments and organizations it can take weeks, if not longer, to order new servers, set them up, and then build a new application. A cloud system would enable computing resources to be available within hours instead of weeks (Rodier, 2011).

2.4.2 Cost Saving

Infrastructure is expensive to purchase, to operate and to maintain. Cloud services are typically pay as you go, or "on-demand", which allows end-users to utilize computing resources as needed. It maximizes the utilization of computing resources and reduces the operation and maintenance costs especially during non-peak times. Cost savings are impacted by current IT expenditure, current hardware life cycles, and which deployment model is chosen.

2.4.3 Improve Operations (Agility and Scalability)

Limited computing resources can prevent applications from running as quickly as they could or from running at all if the resources are needed for other applications. For example, a government has a processor intensive census program that runs once every ten years and runs on the same server as an application that shows who is eligible to vote. It may not be possible to generate a list of voters and process the census results at the same time. The cloud can help by automatically supplying additional computing resources during heavy system use.

Growth can also exceed a system's capabilities. Perhaps in the past most citizens went to their local government office to apply for benefits or get a driver's license, but with the growth of mobile phones, they can now reach these applications online. This sudden spike of usage may require more processing power than was originally planned for or purchased. Without the cloud, such a spike of usage might cause the system to crash or become inaccessible. With the cloud, additional computing resources are added as needed and removed when no longer required. (Microsoft, 2011)

2.4.4 Disaster Recovery and High Availability

Many public cloud service providers have data centers located in multiple locations. This provides a failover location in the event that the primary location becomes unavailable due to a security event, natural disaster, or human error. This capability keeps the government operating seamlessly.

2.4.5 Modernization

Many governments have servers with a variety of software components on them. There may be multiple versions of Linux or Windows operating systems, the same for different versions of databases, or even programming languages. Moving to the cloud typically gives governments the opportunity to standardize their technology architecture across the government or across a department. This increases the ease of maintenance and the ability to add additional features and functionality to applications going forward.

2.4.6 Technological Advantage or Competition

Governments have a mandate to provide services to their citizens. As part of pursuing this mandate, government may consider implementing a cloud strategy. Alternatively, a government may consider implementing a cloud strategy in order to gain or maintain a perceived technical advantage. This advantage could be in either the public or private sector. A government may work to build demand or skills in the area of cloud computing in order to encourage the development of certain skills or products in the private sector.

2.4.7 Security

Major public cloud service providers have their own security protections against internal and external threats. They also support top-line security protocols commonly used. While anything you put on a public server is at higher risk than a computer not connected to an external network, public cloud service providers have security expertise, operation expertise, and are typically up to date on the latest security technologies.

Private clouds have a certain level of security, especially if they are directly connected to the users they serve rather than accessed via the Internet. However, organizations using private clouds generally have a smaller skilled security team than a public cloud provider would.

2.5 Risks

2.5.1 Cost - No economies of scale

There are economies of scale that come from owning an entire data center. Adding one more server is cheaper than the first one was. In the cloud, every CPU and GB needed will cost the same, whether you use 200 or 200 million. Savings are greatest if there are large spikes in usage that cause storage or servers to sit idle when not in use. In the cloud, you only need to pay for those additional computing resources when used. This can also make it more challenging to predict monthly costs. Sudden increase in usage of an application can result in a sudden jump in costs.

2.5.2 Vendor Lock-In

Whether the decision is to build a private cloud or go to a public cloud, there will be a certain amount of vendor lock-in. The degree of lock-in varies, particularly when it comes to deciding to move out of a public cloud. Once you exceed existing computing resources, it is much harder

to leave the cloud. This should be considered if you think you might need to make changes in the future due to data or other concerns.

2.5.3 Infrastructure

If the network infrastructure is unreliable or is already highly utilized then moving to the cloud may be too much of a burden on the existing infrastructure. It could cause applications to crash or be inaccessible. In such situations the network infrastructure must either be upgraded before considering a move to a public or hybrid cloud or, alternative, a private cloud on a dedicated line should be considered.

2.6 Migrating Applications

An important step in planning for a cloud implementation is deciding which applications to move. Not all applications should be moved to the cloud. There are many attributes that are considered in the application assessment, but some of the most important categories to consider are structure, dependency, connectivity, and reliability.

2.6.1 Structure

A large, single-tiered legacy application typically isn't a good fit for the cloud. In a single-tier application the user interface, business logic, and data storage are all located on the same machine. While these applications are typically the easiest to design, they are also the least scalable. Efficiencies are gained when an application is scalable and the load can be spread over several instances. This also helps with disaster recovery as it enables a failure in one part of the system to be mitigated without affecting other parts of the system.

2.6.2 Dependency

Applications that depend on specific hardware—such as a particular chip set or an external device such as a fingerprint reader—might not be a good fit for the cloud, unless those dependencies are specifically addressed. Similarly, if an application depends on an operating system or set of libraries that cannot be used in the cloud, or cannot be virtualized, that application should not be moved to the cloud.

2.6.3 Connectivity

Applications that interface with or use computing resources that will not be reachable from the cloud, including other applications or storage, are typically poor candidates for migration. For example, if tax data cannot be moved to the cloud, you might not move an application that accesses the tax data frequently throughout the day. In some situations, these issues can be resolved with a custom network setup, but how well this works depends on the chosen cloud environment.

2.6.4 Reliability

Applications by their nature are not perfect, but the more reliable an application is, the longer it can run before encountering a problem. Applications that are known to be unreliable should be

reviewed as a possible candidate for rewriting or replacing, since known functionality issues may become worse when migrating an application to a new platform. Trying to migrate an unreliable application may not only increase the effort required to perform the migration, but also fail to achieve the benefits of moving to the cloud.

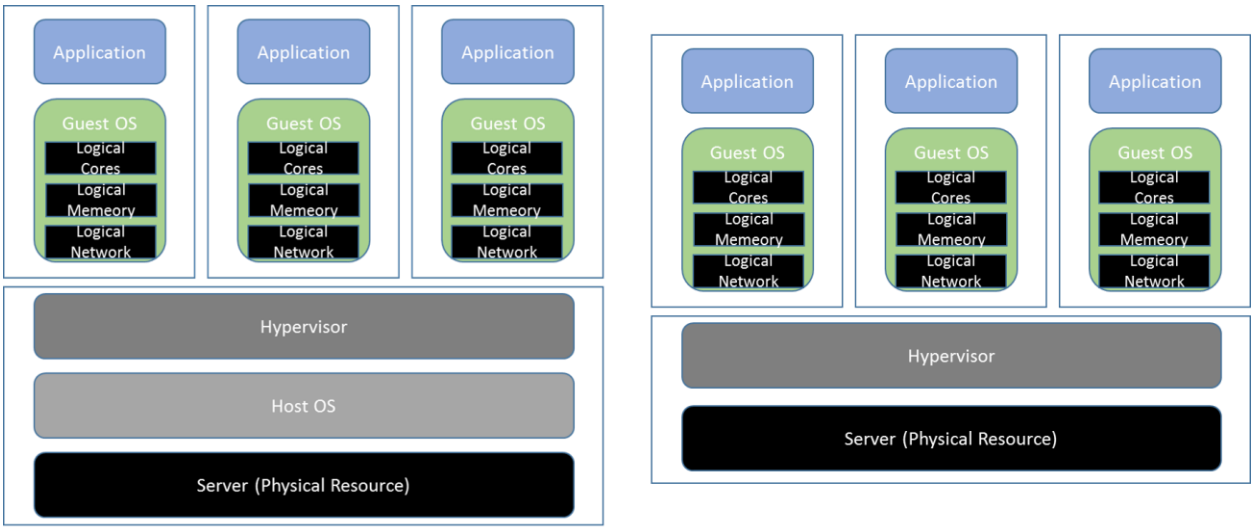
2.7 Virtualization

2.7.1 Overview

Cloud computing is built upon the ability to virtualize applications, regardless of the deployment model selected. Understanding virtualization is key to understanding how pricing works in the cloud. A high level knowledge of this area will enable the creation of more accurate estimates and thus better, and more cost effective, utilization of cloud computing resources. It will also assist with the building of a business case around implementing a cloud computing system.

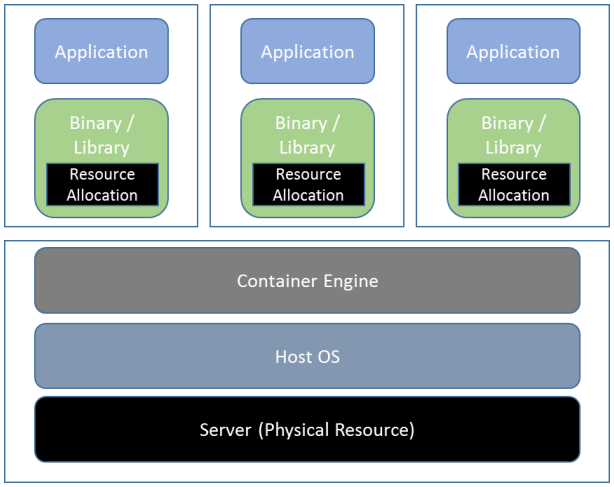
When researching cloud providers and other various cloud service offerings there will be frequent references to virtual central processing units (vCPUs) and virtual cores (vCores). These components differ from their physical counterparts in a manner that is not always very straight forward. NOTE: Amazon Web Services (AWS) uses the term vCPU whereas Azure uses vCore. Conceptually, they are the same.

The main goal when virtualizing a server is to be able to run multiple applications on the same server. Each application has its own space, or virtual machine, on the server. One way to look at this is to think of a physical server as a house. Each room is a virtual machine and each member of the family, or application, gets their own room. The software that enables the creation of these rooms is called a hypervisor. A hypervisor is a piece of software, hardware, or firmware that creates and runs virtual machines. The hypervisor can either be installed directly on the server or on top of the operating system running on the server. The following diagram shows how three applications running on a virtualized server might look, depending on where the hypervisor is installed.



Once a hypervisor is installed, either on the host operating system or directly on the server then the hypervisor manages the physical computing resources (i.e. CPU, memory, etc.) and allocates computing resources to create virtual machines instances upon user request. The guest operating system is installed on the virtual machine instance. Applications can then be installed on the guest operating system and accessed by users.

An increasingly common practice is to take virtualization to the next level and build containers that can easily be moved from server to server. Instead of rooms, the server now has multiple houses and each house can be picked up as a single unit and moved somewhere else as needed. The following diagram shows how container-based virtualization is delivered from a physical server.



Unlike traditional virtual machines, containers do not have a guest operating system installed, but it does require that the physical server have a host operating system. The container itself contains the application in addition to all the components needed for that application and uses the host operating system. This means there is less wasted computing making for a more efficient system, and is also easier to move when needed.

2.7.2 Sizing

When taking applications that currently reside on a physical server and moving them to a virtual machine, it can be challenging to determine how much of various computing resources (i.e. storage, memory, CPUs, etc.) to assign to the application. The recommended approach is to determine what your peak utilization of your current resources over a period of time (ideally 12 months). If that is not possible, then request the same cloud computing resources as the current physical server and monitor the application for the next 12 months to determine utilization, and refine any budget estimates. Based on computing resource usage, the computing resources can be scaled either up or down.

2.8 Conclusions

Increasingly, citizens expect that they can complete tasks online rather than going into an office and waiting in line. In addition, the amount of digital data is growing across the globe and is

expected to continue to do so. The ability to take advantage of this data and use it to help improve efficiencies within the government and provide better services to citizens is driving many governments to consider cloud platforms. Cloud has the possibility to enable government employees to work from anywhere and citizens to get access to information from their phones or homes. It can enable governments to quickly deploy applications and new functionality.

While cloud has the power to connect, it also comes with risks. Moving data outside of secure locations opens it up for attack. This can be especially true if a limited number of employees with skills in security has led to the development of applications that are particularly vulnerable. Legacy applications that were not originally designed for the cloud may have to be updated, a potentially time consuming undertaking.

It should also be noted, that while much focus is placed on the potential cost savings of cloud, much of those savings are difficult to quantify. Many benefits of cloud enable governments to avoid costs in the future. For example, the implementation of a scalable infrastructure can reduce future capacity costs, and faster development of applications reduces development costs. However, these costs do not reduce the current IT budget, and are sometimes overlooked (Neville Cannon, 2015).

The preferred deployment model and path to implementation will be different for every country, and possibly even differ by departments or ministries within the same country. It may be that an agriculture application can move to the public cloud, but a finance application should consider a private cloud. Then the government must decide if everyone should use the same solution or if there should be multiple solutions. A Cloud Readiness Assessment will provide insight into the current state of a country, and will help provide insight into where a country is now, and what recommendations there are for the future.

3 Cloud Readiness Toolkit

Many countries that are interested in implementing a cloud platform are either uncertain where to start or are focused on building a national data center, or equivalent; however, a government may not be ready to leverage the cloud, even if they have one available. In order to assist governments with this gap, the World Bank Cloud Readiness Assessment Toolkit provides a series of questions that determines where a country is in terms of overall readiness, what deployment model they may wish to pursue based on their current regulatory environment, and recommendations on how they can better position their government to take advantage of cloud computing. Once a government is ready to implement a cloud platform, the application and infrastructure assessment can be used to build out a roadmap both at the department/ministry level and the application level.

3.1 Country Assessment

The country assessment is a questionnaire used to assess the government's overall cloud readiness. By answering the questions around regulation, security, infrastructure, etc. the assessment identifies gaps in a country's policies, regulations, or current IT infrastructure that would impact a migration to the cloud or prevent a country from fully realizing the potential of such a migration. Research on government cloud migrations show that countries frequently do not see the full expected savings or benefits when migrating to the cloud due to gaps in readiness.

3.1.1 Methodology

The country assessment is broken down into seven key categories. Each category has a different purpose. Together the entire questionnaire is used to identify key gaps and provide recommendations and a roadmap for the government to consider.

Category	Purpose
General	Determine the true level of interest in migrating to the cloud and also the primary benefit that the government hopes to realize.
Resources	Determine if the government has the key skills already available or easily accessible prior to starting a cloud migration.
Security	Determine what kind of security is required, including rules around data retention and security clearances. Perception of security may also impact public adoption of applications meant for use by the citizens of a country.
Regulations	Determine whether there are regulations in place that would prevent the migration of some or all government applications to a public cloud or discourage the creation of local cloud providers.
Governance of Information and Communications Technology (ICT) Systems	Determine whether existing IT processes and procedures have been adapted to a cloud environment. If applications cannot effectively utilize a cloud environment, the government will not fully realize the potential benefits.
Data	Determine how secure a government's data is now and whether there are regulations in place that would prevent the migration of

Category	Purpose
	some or all government data to a public cloud and what the overall quality of the data currently is.
Infrastructure	Determine whether migrating to the cloud may be too much of a burden on the existing infrastructure.

Each question within a category has its own weight. This weight is based on the impact the answer has on the overall readiness for cloud. Each category sums up to 100%. The answer given for a question determines the value allocated to the overall readiness score and to which cloud deployment model would be the closest fit. The overall readiness score shows where on the path to readiness the country is and aligns with the type of recommendations. A country that falls into a "Ready" category shows that they are on the right path to implement cloud, whereas a score that is in the “Needs Additional Preparation” range, means that a country needs to make some changes before moving forward with a cloud implementation.

Within the document, on the assessment tab, every category is shown, along with the weight assigned to each category. Some categories are weighted more heavily than others based on the impact that category has on overall cloud readiness. For example, Governance of ICT Systems was weighted more because of the impact on the realization of long term benefits of cloud. The category weights are default values based on established methodology and experience, but can be updated to reflect the particular needs and situation of a specific country.

For many questions, an answer of unknown is an option. However, this option should be selected as infrequently as possible. Unknowns typically result in an average score. Having a large number of unknowns might lead to a score that is higher than it should be, thus hiding a lack of readiness or other areas of weakness. Such a score would thus decrease the overall value of the resulting recommendations. The more complete the questionnaire, the more accurate the recommendations and the final score.

3.2 Application and Infrastructure Assessment

The application and infrastructure assessment is a questionnaire used to assess the government’s overall application landscape. By answering the questions for each application being considered for a migration to the cloud, and any servers associated with those applications, the assessment helps determine the fitness, effort and recommended deployment type.

Fitness	Effort	Deployment Model
• Fitness is defined as being a good candidate for cloud • For example, an application that is not going to be retired for years is a better fit than an application that is going to be retired within the next six months • Fitness is assessed on the following scale: Very Low, Low, Moderate, High, Very High	• Effort is defined as the amount of work and energy required to migrate to the cloud • For example, an application that does not follow any coding standards would require more effort than one that does. • There is no direct relation between effort and fitness or readiness • Effort is assessed on the following scale: Very Low, Low, Moderate, High, Very High	• A recommendation of Public, Local Public, Private, or Hybrid is provided for each application

3.2.1 Methodology

While the questions are separated into two groups - application and infrastructure, the questions within each group are split into four categories – General, Operation Optimization, Modernization, and Security. These categories are reflective of the migration drivers that are identified in the country assessment.

Category	Description
Architecture	This section covers questions that help determine what kind of cloud computing resources would be needed and how they can be optimized. This category also determines whether the application would benefit from the cloud architecture.
General	This section covers questions that are not covered in the other categories, such as which department owns the application.
Operation Optimization	This section covers how the application is currently being used and what the potential boundaries for future growth are based on the current infrastructure.
Security	This section covers data security, for example any sensitive data (classified data or information that can be used to identify individuals) or encryption requirements.

Each question has been allocated its own weight based on the level of importance and impact on the 'fitness' and 'effort required' for a cloud migration.

Each category sums up to 100% (total 500%) and the default weight of each category has been set based on the key driver determined during the country assessment.

Category	Driver							
	General Interest	Cost Savings	Faster Development of Applications	Improve Operations (Agility & Scalability)	Disaster Recovery and High Availability	Modernization	Technological Advantage or Competition	Security
General	25%	35%	30%	30%	15%	25%	20%	20%
Architecture	25%	30%	20%	10%	20%	15%	20%	15%
Operation Optimization	25%	20%	30%	40%	35%	35%	35%	25%
Security	25%	15%	20%	20%	30%	25%	25%	40%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

The category weights can be adjusted to meet a specific country's needs.

Each application is assigned a fitness score, and effort score, and a platform recommendation.

Fitness is weighted as per the following criteria:

Category	Description
Very High	Based on the answer, there should not be any issues or risks in migrating this application to the cloud.
High	Based on the answer, there may be minor issues or risks in migrating to the cloud, but there are likely known resolutions.
Moderate	Based on the answer, there may be issues or risks in migrating to the cloud, and workarounds may need to be identified.
Low	Based on the answer, there may be significant issues or risks in migrating to the cloud, and workarounds will need to be identified.
Very Low	Based on the answer, there may be significant issues or risks in migrating to the cloud, and there may be no possible workarounds.

Effort is weighted as per the following criteria:

Category	Description
Very Low	Migration is likely to be as simple as copying binaries. Minimal effort required.
Low	Simple configuration level changes may be required. No source code or functional changes are required.
Moderate	The application may require source code and configuration changes, but they will be changes expected by individuals familiar with migrating to the cloud. No functional changes will be required.
High	The application will require either significant source code and configuration changes or an upgrade to a different operating system, middleware component, or database in order to be compatible with the cloud. In addition, analysis of the code through the use of a tool may be required in order to identify the necessary changes. No functional changes will be required.

Category	Description
Very High	The application will require significant changes including, but not limited to, an upgrade to a different operating system, middleware component, or database in order to be compatible with the cloud or a re-architecting of the application to enable utilization of the cloud architecture.

4 Findings and Recommendations

As part of the Toolkit development, three countries were selected to pilot the methodology and questionnaires – Serbia, the Philippines, and Zambia. These countries were identified and selected based on local government interest, geography, and differences across a variety of country level statistics, as outlined below. The goal of the pilots was to test the toolkit as thoroughly as possible, and then make refinements based on lessons learned.

		Serbia	Philippines	Zambia
Overall	Population	7.13 Million	99.14 Million	15.72 Million
	Country Classification	Upper Middle Income $4,126 to $12,745	Lower Middle Income $1,046 to $4,125	Lower Middle Income $1,046 to $4,125
	Unemployment Rate	17.90%	5.80%	13.30%
	Inflation Rate	1.50%	0.90%	22.90%
	% Population below Poverty Line	24.60%	25.20%	60.50%
Information Statistics	Digital Adoption Index	0.61	0.43	0.33
	Internet Access at Home	66%	18%	13%
	Government – Digital Identification	0.83	0.03	0.58
	Government – Core Administrative Systems	0.73	0.77	0.63
	Government – Online Public Services	0.39	0.48	0.14

4.1 Pilot #1 – Serbia

4.1.1 Summary

This report is meant to be a conversation starter, and provide Serbia with a high level overview of the assessment findings in addition to recommendations on migrating to a cloud platform. The assessment documents are point in time and can be updated dynamically to reflect changes in direction and regulation. For example, if regulations around where data can be stored are put in place, the corresponding assessment questions can up updated to generate revised recommendations and scores. This will enable the toolkit to be utilized throughout the process of selecting a deployment model, implementing the model, and digitizing key e-Government services. This report does not replace a detailed, or in-depth, assessment which should be conducted prior to implementing a cloud platform.

In Serbia, answers were obtained for all but two questions, one of which was marked as unknown. This enabled a more reliable recommendation.

Overall Cloud Readiness Metric

Very Ready	>80%
Ready	65%-80%
Need Additional Preparation	45-64%
Need Underlying Infrastructure	25-44%
Not Ready	<25%

<- Serbia is here

The overall cloud readiness assessment shows that Serbia is a good candidate for cloud. However, Serbia needs to make sure that a solid technology and infrastructure foundation is in place before moving forward on the path to cloud. At this time, given the uncertainty government officials expressed around where data can be hosted the assessment recommends that Serbia pursue a private cloud option which aligns with Serbia's allocation of budget to start construction of a national data center in 2016.

4.1.2 Key Findings

Serbia's overall readiness score is 59%. This puts Serbia towards the higher end of "Need Additional Preparation". Cloud, especially a push towards more e-Services, is considered an important government initiative both at the highest levels of government and by the citizens. In fact, cloud is even being discussed as part of the upcoming election. However, there are still some intermediary steps that Serbia needs to take in order to lay the groundwork for a successful cloud implementation. Serbia has started taking steps in areas – such as defining regulations, but there are still gaps in terms of implementation and moving towards greater interoperability across ministries.

A high risk area identified was that Serbia has no cabinet level ICT organization – in addition, individuals frequently were unable to identify who should be responsible for any sort of overall government ICT or cloud strategy. A contributing factor to this is the reorganization that took place when the current President took office, and many people are anticipating that the government may be reorganized after the upcoming election.

In addition, while Serbia has made strides to put in place certain forward thinking regulations, much of that progress is driven not just by Serbia's desire to move to the cloud, but as part of the country's overall goal of joining the European Union. The European Union requires not only that specific regulations exist, but also encourages a certain amount of interoperability. For example, if the European Union approves a drug for usage across the EU, at some point the Ministry of Medicine and Medical Devices will need to be able to incorporate that into the appropriate government systems.

One of the areas where ministries have started laying the groundwork, but still have further work to do is disaster recovery. Most ministries were quick to identify disaster recovery as a reason to adopt the cloud and stated that they had disaster recovery capability, but then noted that the capability was either within the same building or very close to the original site (i.e. next door). In 2014 a flood did significant damage, raising this as a significant issue. In addition, disaster plans, when they existed, had not been tested.

While a cloud implementation might be successful at this stage, in order to get the most out of the cloud in the long term, Serbia should focus on implementing a government wide cloud strategy and drive adoption of this strategy as it encourages ministries to move to the new platform it is building.

4.1.3 Deployment Model Recommendation

	Overall Readiness	Private Cloud Readiness	Hybrid Cloud Readiness	Public Cloud Readiness	Local Public Cloud Readiness
Readiness Score	59%	70%	66%	0%	0%

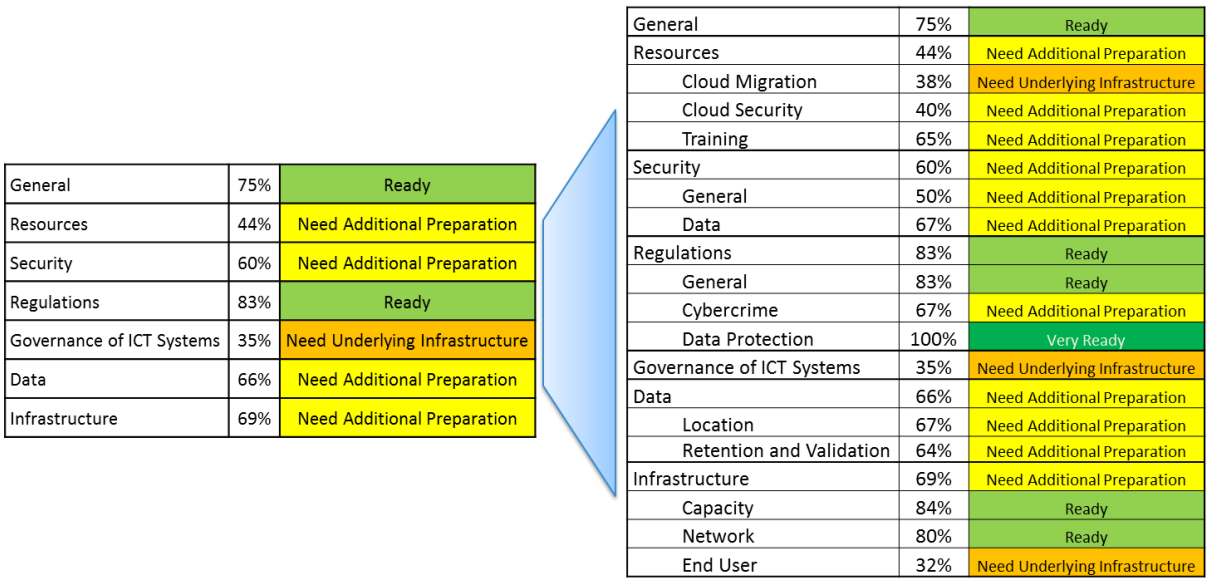
The cloud readiness assessment recommends that Serbia should consider pursuing a private cloud. However, this recommendation was driven by key findings that eliminated public cloud as an option due to restrictions on where data can be stored. The majority of the responses said that data, sensitive or non-sensitive data, could not leave the country nor reside on public servers.

In addition, one other element that drove the deployment model recommendation was a discussion with the major local cloud provider. During the discussion it was determined that no disaster recovery was available for the local provider's cloud offerings. As such, a local public service provider does not exist as a possible alternative for the government at this time.

Serbia may wish to review whether all applications and types of data needs to have the same level of security and protection. That may open up the possibility of public cloud for some subset of data and applications. Also, Serbia should make sure that any private cloud can meet the security needs of all ministries.

4.1.4 Gaps

There are key individuals within the government acting as advocates for cloud and working to get funding in order to build a national data center to provide the basis for a government cloud. This is a key step in the right direction; however, without also focusing on some of the gaps, such as resources, governance, and interoperability; Serbia will only see part of the benefits that they could get from a true cloud implementation.



General	75%	Ready
Resources	44%	Need Additional Preparation
Security	60%	Need Additional Preparation
Regulations	83%	Ready
Governance of ICT Systems	35%	Need Underlying Infrastructure
Data	66%	Need Additional Preparation
Infrastructure	69%	Need Additional Preparation

General	75%	Ready
Resources	44%	Need Additional Preparation
Cloud Migration	38%	Need Underlying Infrastructure
Cloud Security	40%	Need Additional Preparation
Training	65%	Need Additional Preparation
Security	60%	Need Additional Preparation
General	50%	Need Additional Preparation
Data	67%	Need Additional Preparation
Regulations	83%	Ready
General	83%	Ready
Cybercrime	67%	Need Additional Preparation
Data Protection	100%	Very Ready
Governance of ICT Systems	35%	Need Underlying Infrastructure
Data	66%	Need Additional Preparation
Location	67%	Need Additional Preparation
Retention and Validation	64%	Need Additional Preparation
Infrastructure	69%	Need Additional Preparation
Capacity	84%	Ready
Network	80%	Ready
End User	32%	Need Underlying Infrastructure

4.1.4.1 Resources

Serbia has limited local resources in either the public or private sector with skills in cloud migration or security. Turnover is high and skilled IT resources frequently leave the country to pursue other opportunities. In addition, there are no programs currently offered within the government that would help build these skills. Most training is done through external vendors as part of contracts to implement new tools or systems.

In order to address this gap, it is recommended that Serbia review their retention policies to see if they might be able to reduce turnover within the IT sector. In addition, Serbia might consider working with Universities or vendors to develop cloud training to use internally.

4.1.4.2 E-Payment

There were some conflicting responses as to whether e-payment was feasible, but the general consensus was that it was not currently feasible. Some of the barriers seen were around engaging credit card companies and addressing how fees would be paid. Given Serbia's goal of digitizing more and more services, it is recommended that Serbia address the existing gaps in implementing an e-payment service and roll out this capability across the government.

4.1.4.3 Data Location

Most individuals, when asked, said that data should not leave the country; however, when asked if there were restrictions preventing data from leaving the country responded no rules exist. In addition, it was noted that as part of joining the European Union, Serbia will have to pass regulations allowing data to be stored within other European Union countries. In light of the EU regulations, Serbia should review their current data policies and determine if they should be revised or if gaps exist. If gaps are identified, then it is recommended that rules be formalized to address any gaps and that the government work to increase awareness of any existing or future rules around data storage.

4.1.4.4 Governance

Serbia's lowest score was in the area of governance. There are three key recommendations for Serbia in this area.

4.1.4.4.1 CIO

Serbia has no CIO or equivalent cabinet level IT position. This was called out by almost all groups interviewed. Without this there is no designated organization both authorized and responsible for creating and driving a cloud strategy. It is recommended that Serbia create a CIO or equivalent position after the next election.

4.1.4.4.2 Cloud Strategy

Once a CIO or equivalent position has been created, it is recommended that that individual should develop a cloud strategy. The strategy should then be distributed to all the ministries in order to provide direction to future ministry level initiatives.

4.1.4.4.3 Governance of ICT

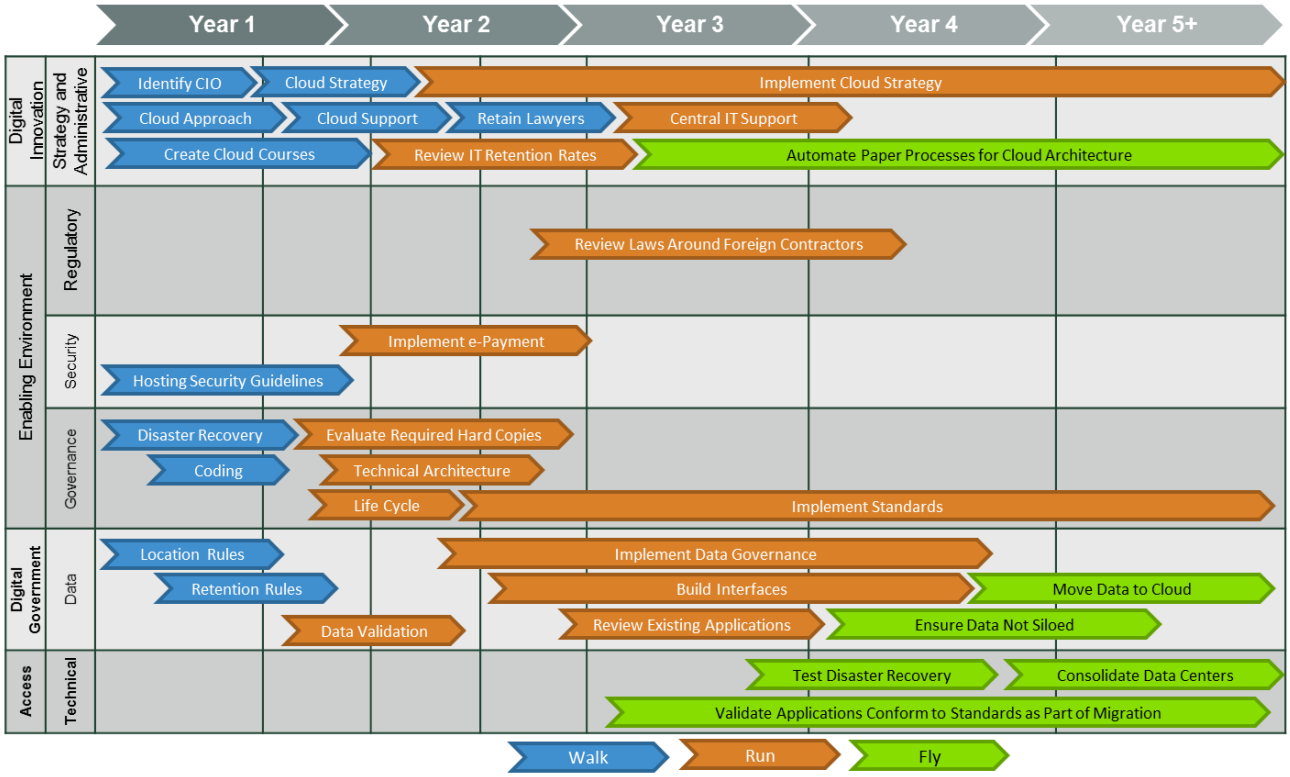
Another critical gap on the path to cloud is in the area of general governance of ICT. Serbia simply does not have certain ICT processes, such as disaster recovery. Serbia also has no technical architecture standards. Implementing technical architecture guidelines would help provide a standard set of technologies being used across ministries. This will make it easier to determine what needs to be supported on the new platform and to migrate applications once it is time to do so.

In addition, for those processes that Serbia does have, such as development life cycle and application documentation, the processes have not yet been updated to include cloud. It is important to make sure that these processes are updated and enforced prior to starting a migration to the cloud. This is key to Serbia getting the greatest benefit out of a cloud platform.

4.1.5 Next Steps

4.1.5.1 Policy Roadmap

Various responses to the questions on the country assessment are associated with a recommendation. Each recommendation has an associated phase, type, and estimated duration. These are used to construct a detailed roadmap. How the roadmap will look will vary based on each country's priorities and needs. However, a sample roadmap has been constructed for Serbia based on the recommendations produced for this report. The recommendations are also outlined in the table following the roadmap. The Digital Development Partnership (DDP) category that most closely aligns to the recommendation has also been noted in both the roadmap and the accompanying table.



The recommendations and roadmap have been split into three phases.

Phase one (walk) focuses on the regulatory and technical infrastructure that needs to be defined before moving to the cloud. This would include defining policies and regulations around data, hosting, encryption, and technical standards. These items should be completed prior to moving onto phase two.

Phase two (run) focuses on defining the next level of policies and regulations, such as evaluating where hard copies of documents are truly needed, what the technical architecture should look like, data validation rules, as well as implementing the policies and regulations created in phase one. These policies and regulations will help standardize the overall environment. A standard environment will make it easier and cheaper to move applications to the cloud. In addition, during this phase, ministries should start to build interfaces to enable the sharing of data across applications. This will simplify data collection and governance.

Phase three (fly) focuses on implementing a true cloud platform. Starting with converting existing manual processes into digital, cloud-based processes and consolidating data centers into the government cloud. A key to a successful implementation of a cloud platform is getting buy-in from various ministries. Encouraging ministries to use the data center as a disaster recovery site might encourage buy-in.

4.1.5.2 Policy Recommendation Table

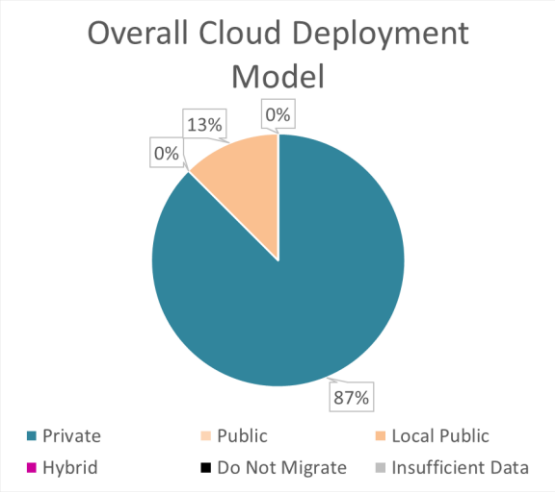
The following table outlines the recommendations, as seen in the country assessment.

Category	Recommendation Type	Phase	Recommendation	Duration
Digital Innovation	Administrative	Walk	- Develop skills for managing third party vendors or contractors	6 Months - 1 Year
Digital Innovation	Administrative	Walk	- Work with universities and/or vendors to create cloud courses for government use	6 Months - 1 Year
Digital Government	Data	Walk	- Formalize guidelines around where data can be stored, taking in to consideration cloud technologies	6 Months
Digital Government	Data	Walk	- Establish laws or regulations around the retention of digital data once a server is no longer in use (i.e. a contract has concluded, or a server is being retired)	6 Months
Digital Government	Governance	Walk	- Define coding standards (i.e. best practices) to be followed across the government	6 Months
Digital Government	Governance	Walk	- Define disaster recovery requirements (i.e. frequency of testing procedures, international standards, location and general requirements)	6 Months
Digital Innovation	High-Level Strategy	Walk	- Consolidate strategies into one overall, government-wide cloud strategy	6 Months
Digital Innovation	High-Level Strategy	Walk	- Work with individuals currently using cloud to start standardizing decisions around when to use cloud and then expand that approach	6 Months
Digital Innovation	High-Level Strategy	Walk	- Work with the cabinet in order to get support for adopting a cloud strategy at the highest level	6 Months
Digital Innovation	High-Level Strategy	Walk	- Create a CIO or equivalent cabinet level ICT position in an official capacity	6 Months - 1 Year
Digital Innovation	High-Level Strategy	Walk	- Identify lawyers with knowledge of cybersecurity and ICT that can work with, or for, the government to provide guidance on policy, laws, and regulations	3 Months
Digital Government	Security	Walk	- Establish and implement general security requirements and regulations for digital hosting and cloud service providers (i.e. encryption, data retention, access and ownership, etc.)	6 Months
Digital Innovation	Administrative	Run	- Consider moving IT support for government to a centralized model	6 Months - 1 Year
Digital Innovation	Administrative	Run	- Review IT retention rates in the area of cloud security - Determine if steps to mitigate turnover can be implemented - Establish training for new employees and standards for documentation to enable knowledge transfer	6 Months - 1 Year
Digital Government	Data	Run	- Implement data governance across the government	18 Months +
Digital Government	Data	Run	- Update data retention policies to include cloud based applications	6 Months
Digital Government	Data	Run	- Confirm data governance standards are well documented and distributed - Review existing applications to validate that data will be captured according to the guidelines - Ensure that newly developed applications conform with the guidelines	6 Months - 1 Year

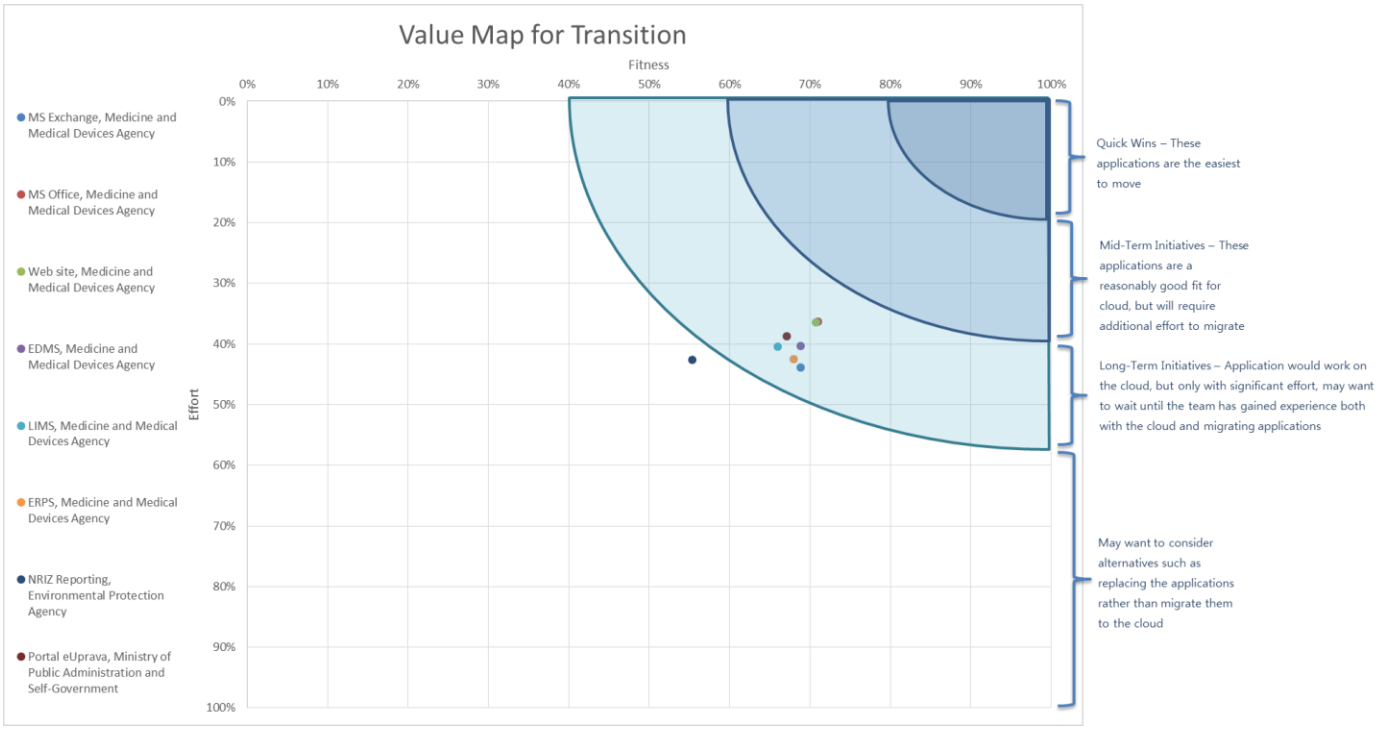
Category	Recommendation Type	Phase	Recommendation	Duration
Digital Government	Data	Run	- Confirm data validation standards are well documented and distributed - Ensure that newly developed applications conform with the guidelines - Review existing applications to confirm that data validation is implemented	6 Months - 1 Year
Digital Government	Data	Run	- Build interfaces to other department, institutions, and ministries to access needed applications and data.	18 Months +
Digital Government	Governance	Run	- Enforce application documentation standards by not moving any applications that do not follow the standards to the cloud	6 Months
Digital Government	Governance	Run	- Adapt the government's life cycle for the cloud	6 Months
Digital Government	Governance	Run	- Define and adopt technical architecture standards (i.e. enterprise standards around application and web servers as well as coding languages)	6 Months
Digital Government	Governance	Run	- Evaluate laws requiring hard copies of specific documents to determine if electronic equivalence is feasible	6 Months
Digital Government	Regulatory	Run	- Review whether exceptions for hiring foreign employees or contractors should be made if the resources are not available locally - Work with local groups to make sure resources are available in the local workforce	3 Months
Digital Government	Security	Run	- Revise encryption standards and requirements to follow international guidelines	6 Months
Digital Government	Security	Run	- Work with local banks or other organizations to enable e-payment, even if in limited capacity, to enable the use of online services	6 Months - 1 Year
Digital Government	Data	Fly	- Start investigating moving data to the cloud for ease of access across departments/ministries	6 Months - 1 Year
Digital Government	Data	Fly	- Ensure data is not siloed and should be maintained by the primary owner	6 Months - 1 Year
Digital Innovation	High-Level Strategy	Fly	- Automate existing paper based processes in a manner architected for the cloud	18 Months +
Digital Innovation	High-Level Strategy	Fly	- Automate existing paper based processes in a manner architected for the cloud	18 Months +
Access	Technical	Fly	- Validate that applications conform to existing standards as part of the migration to the cloud	6 Months
Access	Technical	Fly	- Consider migrating to the cloud as an opportunity to consolidate data centers	18 Months +

4.1.5.3 Application Roadmap

The Medicines and Medical Devices Agency of Serbia supplied information for six of their applications, the Ministry of Public Administration and Self-Government and the Environmental Protection Agency each supplied information for one application. No other application information was provided. This is a living document and can be updated with additional information. This additional information can be used to provide more guidance, analysis, and refined results. Based on the responses from the three Serbian agencies to the assessment, the recommendation for 7 of the 8 applications aligns with the overall country recommendation - private cloud. For one application the recommendation is local public.



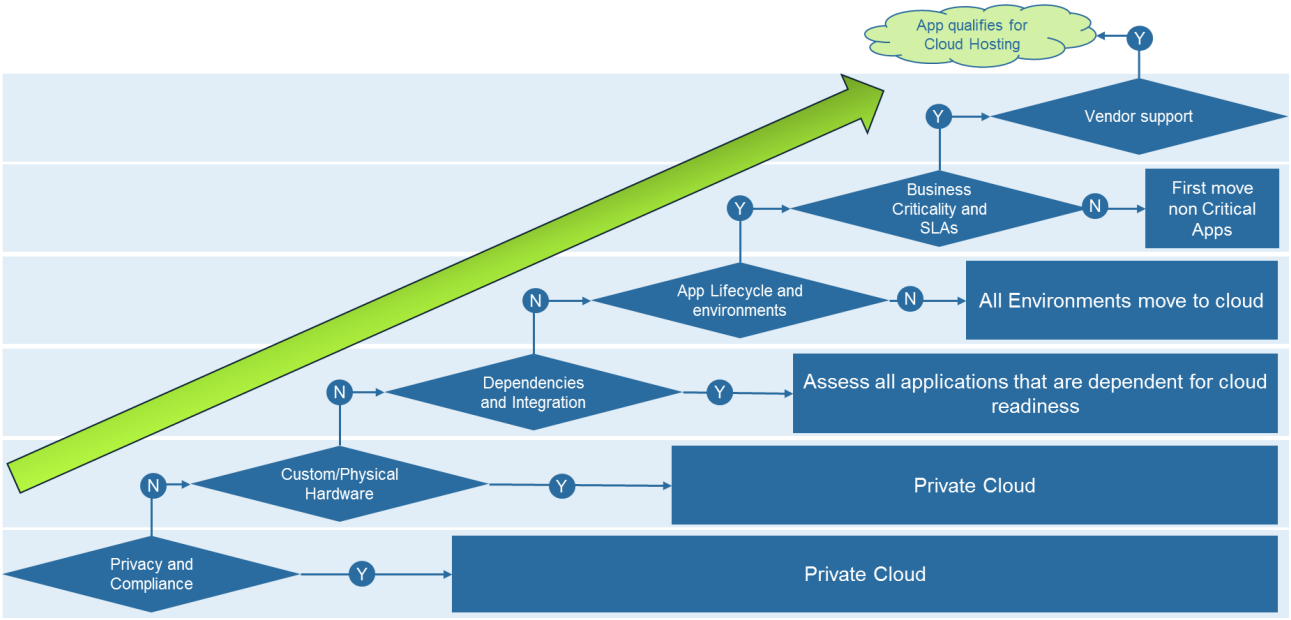
The value map helps show which applications are the closest fit and will take the least amount of effort to migrate. None of the Medicines and Medical Agency of Ministry of Public Administration and Self-Government applications are a strong fit for cloud, but the strongest candidate to start with is EDMS. NRIZ Reporting, the Environmental Protection Agency application, would require the most effort to migrate to the cloud. Due to the level of effort, the Environmental Protection Agency may wish to review NRIZ in further depth to see if it should be replaced, retired, rewritten, or migrated to the cloud.



When starting to plan the roadmap to migrate applications to the cloud, there are numerous attributes that need to be taken into account, including, but not limited to:

- Criticality of the system
- Sensitivity of the data
- Interfaces
- Application dependencies

The below decision tree may help in the creation of an application migration roadmap.



4.2 Pilot #2 – Philippines

4.2.1 Summary

This report is meant to be a conversation starter, and provide the Philippines with a high level overview of the assessment findings in addition to recommendations on migrating to a cloud platform. The assessment documents are point in time and can be updated dynamically to reflect changes in direction and regulation. For example, if regulations around where data can be stored are put in place, the corresponding assessment questions can up updated to generate revised recommendations and scores. This will enable the toolkit to be utilized throughout the process of selecting a deployment model, implementing the model, and digitizing key e-Government services. This report does not replace a full, in-depth assessment which should be conducted prior to implementing a cloud platform.

In the Philippines, answers were obtained for all questions in the country assessment, enabling a more reliable recommendation.

Overall Cloud Readiness Metric	
Very Ready	>80%
Ready	65%-80%
Need Additional Preparation	45-64%
Need Underlying Infrastructure	25-44%
Not Ready	<25%

<- Philippines is here

The overall cloud readiness assessment shows that the Philippines is ready to consider implementing a cloud strategy but requires additional preparation before moving forward. At this time, there are concerns around where the data can be hosted, but there are no regulations that outlined the government's official stance on the matter. As a result, the assessment recommends that the Philippines pursue a private or hybrid cloud option.

4.2.2 Key Findings

The Philippine's overall score is 56%. This puts the Philippines towards the middle of "Need Additional Preparation". There is a clear interest from the government in cloud computing and efforts are underway to implement and standardize a government cloud (G-cloud). However, the Philippines need to make sure that a solid technology and infrastructure foundation is in place before moving forward on the path to cloud. This technology and infrastructure foundation needs to be implemented in a controlled, step by step approach, or it will not be sustainable.

In order to achieve this controlled, step by step approach, the Philippines need to work towards creating an official chief information officer (CIO) or cabinet-level position for ICT. It is noteworthy that at the time of the pilot, there was legislation pending Presidential approval to establish an ICT Department. However, with major elections being held in the next 6 months, the legislation's future is uncertain. The Philippines does have the Information and Communications Technology Office (ICTO) as a de facto CIO which falls under the Department of Science and Technology, but they are not officially recognized as the Department of ICT (or equivalent). Through this department, the Philippines are currently developing an overall ICT strategy. The focus of this strategy is primarily internally driven to improve operations (agility and scalability) and infrastructure which includes an e-Government master plan and a G-cloud. This government cloud, located within a centralized data center, would be used to provide cloud services for individual departments and government agencies, and is currently in the process of being scaled. The Department of Budget Management (DBM) has placed a purchasing hold on hardware for individual ministries and agencies which was done to encourage the use of the G-cloud operated by ICTO and DOST and, long term, prompt the consolidation and retirement of individual data centers. However, there is no official regulator, or enforcement agency, for the creation of these ICT policies and plans but the DBM does have limited enforcement capabilities through budget appropriations which makes policy adoption difficult.

Despite the existence of the G-cloud, concerns over capacity, performance, and reliability hinder adoption by departments. Currently, the G-cloud does not have the capacity for a migration of a department's data center. The current infrastructure is 200 virtual machines (VMs) and they plan to increase the number of VMs to 1,000 by July/August 2016. However, the team received conflicting answers regarding how long it takes to procure a server, which will impact the G-Cloud's ability to scale. ICTO informed the team that it takes 1-6 months to procure a server while other projects and departments stated that it could take 6 months to a year. The team found that the current procurement process sometimes requires additional procedures and can be tedious.

In addition, the G-cloud does not provide service level agreements (SLAs) or a disaster recovery center. It is important to note that drafting a disaster recovery plan is in process but is not planned to be operational for at least a few years. In addition, the limited public sector employees with the relevant skills or experience in cloud services (i.e. cloud modernization, cloud migration and cloud security) further complicates the decision to migrate. This is in part due to the Philippine government facing high turnover rates, which governments as a whole often face. Most resources in cloud migration had less than 18 months of experience while cloud security resources had less than 6 months experience. In both of these fields, the Philippine government saw approximately a yearly turnover rate of 25-50%. This problem had been compounded by the fact that ICTO's original resources came from telecommunications and were not aligned skill wise with the mandate ICTO was given. In terms of future resource development, the University of Philippines has virtualization courses, but no cloud-related courses available. Most of these cloud skills are self-taught through job experience or external vendors and non-governmental trainings. There is a large number of skilled resources, especially in the area of cloud migration, available in the general workforce, although retaining those skills within the government has been challenging. The availability of resources with a strong background in cloud security is less certain. Several responses indicated this was a missing skillset in both the private and public sectors.

As a result of the limitations with G-cloud, departments have taken this as an opportunity to implement their own approach. The assessment found this to be an area of concern as there are limited governance and policies in place for departments to use as guidelines. This has security ramifications as most departments have gone with a combination of Microsoft Azure services and open source products such as Gmail and Google Apps instead of using the G-cloud in attempts to save costs or circumvent the hardware purchasing freeze. In doing so, the departments are open to security and privacy issues. For example, there are no government level encryption standards or any laws or regulations related to digital data hosting.

The Philippines needs to determine whether G-cloud will be able to meet the needs of the government and what those needs are. As part of making this determination, key performance indicators need to be identified that can be applied to the G-cloud so that success or failure can be quantified and measured. The decision to guide all department and government agencies towards a centralized platform that is not ready yet has resulted in departments moving in one of three directions – putting projects on hold pending official direction, moving to a different

cloud provider (typically a public cloud provider) despite no clear guidance on security and regulatory rules, or applying pressure on the G-cloud which isn't operational. In this sense, the Philippines has started to "run" prior to "walking".

4.2.3 Deployment Model Recommendation

The cloud readiness assessment recommends that the Philippines pursue a private or hybrid cloud. This recommendation is a result of the common response around storing data on public servers. Most people said classified data or PII (personally identifiable information) could not reside on a public server which eliminates the public cloud option.

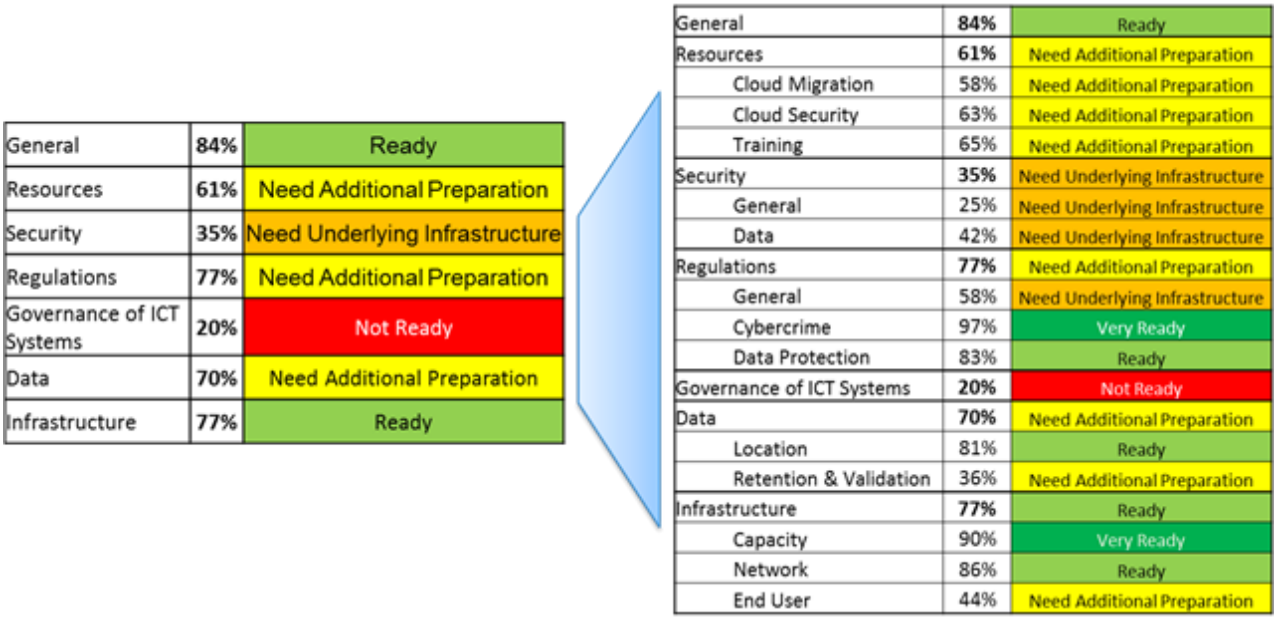
	Overall Readiness	Private Cloud Readiness	Hybrid Cloud Readiness	Public Cloud Readiness	Local Public Cloud Readiness
Readiness Score	56%	65%	63%	0%	0%

However, there are several key decisions that are outstanding and will influence the deployment model.

1. Currently, there are no government-wide standards for several key areas, such as encryption requirements or data hosting standards. When these standards are implemented, will public providers be a viable option and be able to support these requirements?
2. Departments and agencies are hesitant to host classified, confidential, or personally identifiable information on public servers which ruled out the public cloud. However, there are no regulations around data hosting (i.e. geographic local, multi-tenancy, public servers, etc.) enabling departments to decide individually. Would the implementation of data hosting and overlapping ICT regulations add any restrictions to which cloud provider can be chosen?
3. There are limited individuals with cloud skills such as security and migration in the public sector. Would taking advantage of a public cloud provider help mitigate risk, help supplement the existing workforce, or raise security concerns?
4. At a high level, there is a government preference towards local companies over international. If this preference extends to services, are there local cloud providers that meet the government's needs?
5. Do all applications and types of data need to have the same level of security and protection? If not, such a decision may open up the possibility of public cloud for some subset of data and applications.
6. Can a private cloud meet the security needs of all departments? If not, what is the alternative?
7. Would a public cloud provider want to work with the government? There are institutional issues which make working with the government unfavorable for private companies that need to be addressed.

4.2.4 Gaps

Even if the G-cloud was operational and able to meet the service level agreements and capacity requirements of the various departments, there needs to be clear and defined ICT governance and security policies and regulations. Without this, there is no basis upon which to build a cloud strategy. In addition, there was a mindset that "there is no rule preventing us from doing this" which enable departments to implement their own cloud strategy. As a result, the Philippines has significant gaps in security and ICT governance that need to be addressed.



General	84%	Ready
Resources	61%	Need Additional Preparation
Security	35%	Need Underlying Infrastructure
Regulations	77%	Need Additional Preparation
Governance of ICT Systems	20%	Not Ready
Data	70%	Need Additional Preparation
Infrastructure	77%	Ready

General	84%	Ready
Resources	61%	Need Additional Preparation
Cloud Migration	58%	Need Additional Preparation
Cloud Security	63%	Need Additional Preparation
Training	65%	Need Additional Preparation
Security	35%	Need Underlying Infrastructure
General	25%	Need Underlying Infrastructure
Data	42%	Need Underlying Infrastructure
Regulations	77%	Need Additional Preparation
General	58%	Need Underlying Infrastructure
Cybercrime	97%	Very Ready
Data Protection	83%	Ready
Governance of ICT Systems	20%	Not Ready
Data	70%	Need Additional Preparation
Location	81%	Ready
Retention & Validation	36%	Need Additional Preparation
Infrastructure	77%	Ready
Capacity	90%	Very Ready
Network	86%	Ready
End User	44%	Need Additional Preparation

4.2.4.1 Security

There are certain security measures in place such as requiring public sector employees to undergo a clearance process and implement user access and authorization management. However, there are several additional steps required for a secure environment. The assessment shows that there are no government encryption requirements. This would include encryption on data at rest, data in transit or general encryption standards for either a cloud provider or internal hosting. In addition, there are security concerns around using a cloud provider as there are no laws or regulations around data hosting or cloud providers, and no standards around how or when cloud providers are required to discard data. The assessment recommends that this security foundation is built prior to cloud adoption.

4.2.4.2 Governance of ICT

In addition to the security concerns, there is a lack of governance within ICT systems. The assessment found that there are no standards around applications (i.e. documentation, coding standards, development lifecycle, or technical architecture) or disaster recovery. For application related governance, this raises two concerns. First, when moving applications to a new environment such as the cloud, it will be more difficult to migrate an application that does not have documentation that is uniform across the government. In addition, this

documentation would help with the creation of new applications, and standardize the government's application and infrastructure inventory. It is strongly recommended that the Philippines define these standards prior to a cloud implementation through an officially recognized cabinet level ICT office. This office would be responsible with the ICT vision and strategy for the county as well as routinely revising the government-level standards.

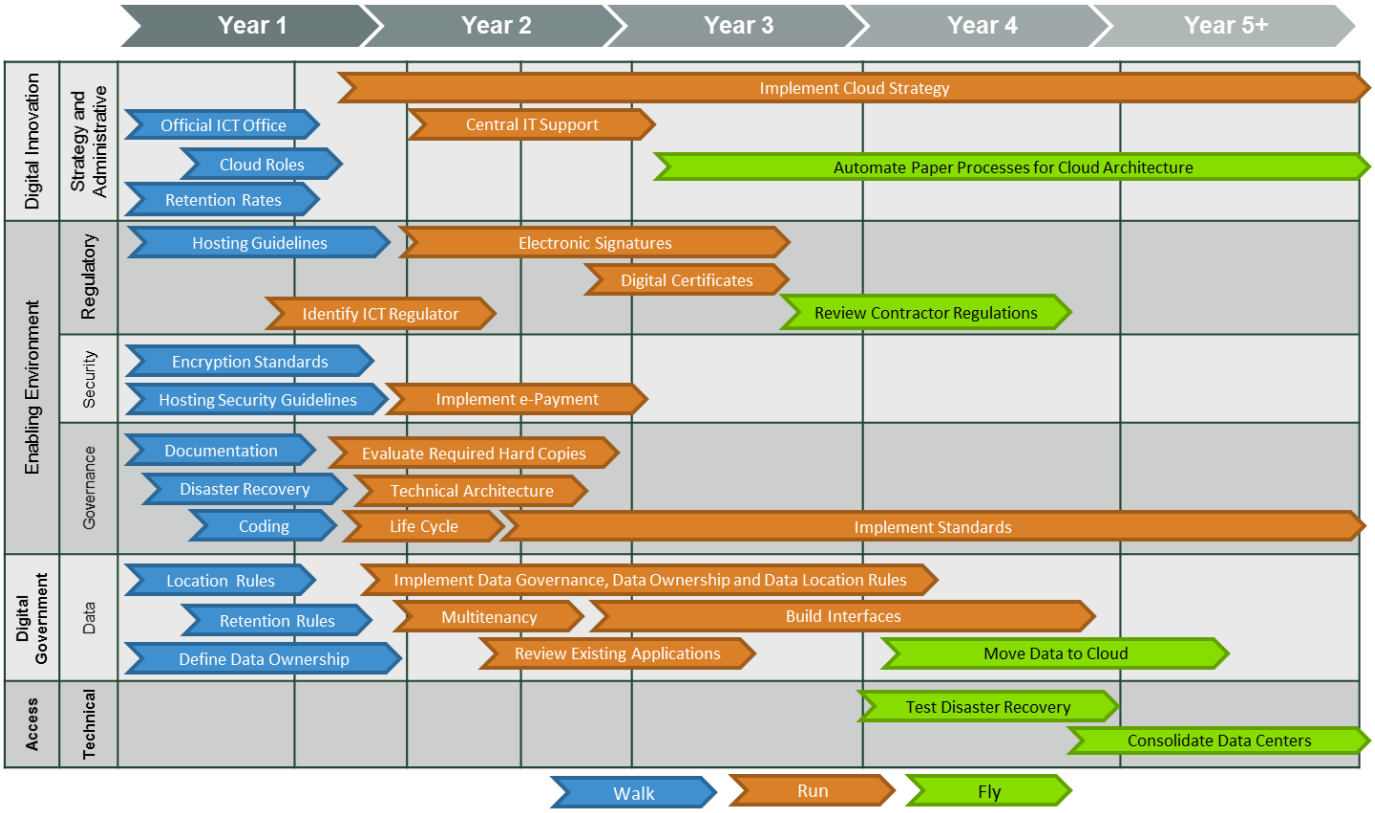
4.2.5 Next Steps

The toolkit provides preliminary policy recommendations and action plans for future steps, but does not replace a full, in-depth assessment of the country's existing regulations, applications and infrastructure.

An ICT policy and vision should be created as well as updated as required. This should not be a static list of recommendations. The Philippines' strategy should be consistently reviewed to ensure the policies align with international ICT best practices.

4.2.5.1 Policy Roadmap

Various responses to the questions on the country assessment are associated with a recommendation. Each recommendation has an associated phase, type, and estimated duration. These are used to construct a detailed roadmap. How the roadmap will look will vary based on each country's priorities and needs. However, a sample roadmap has been constructed for the Philippines based on the recommendations produced for this report. The recommendations are also outlined in the table following the roadmap. The Digital Development Partnership (DDP) category that most closely aligns to the recommendation has also been noted in both the roadmap and the accompanying table.



The recommendations and roadmap have been split into three phases.

Phase one (walk) focuses the regulatory and technical infrastructure standards that need to be defined before moving to the cloud. This would include defining policies and regulations around data, hosting, encryption, and technical standards. In addition, to these standards, an official, cabinet level ICT office should work on defining the government's ICT vision and strategy. These items should be completed prior to moving onto phase two.

Phase two (run) focuses on the implementation of the policies and regulations created in phase one. These policies and regulations will help standardize the Philippine's environment. This standardization can be used to help standardize the offerings provided by the ICTO G-cloud. This would encourage usage, as well as provide guidelines for departments who choose not to use G-cloud as the security and privacy requirements will be clearly defined.

Phase three (fly) focuses on improving services and offerings. The G-cloud will enable departments to provision resources as needed. The G-cloud also provides the government the opportunity to investigate implementing some Software as a Service (SaaS) offerings within the government. For example, there are several software packages, such as email or ERP, which could potentially be provided as a service to other departments. In addition, the Philippines could utilize the G-cloud to turn existing paper based processes into true cloud based offerings.

4.2.5.2 Policy Recommendation Table

The following table outlines the recommendations, as seen in the country assessment.

Category	Recommendation Type	Phase	Recommendation	Duration
Digital Innovation	Administrative	Walk	- Assess applications for which there are no employees with a high degree of familiarity with the application architecture or code to determine if the applications need to be replaced	6 Months - 1 Year
Digital Government	Data	Walk	- Formalize guidelines around where data can be stored, taking in to consideration cloud technologies	6 Months
Digital Government	Data	Walk	- Adopt a data governance approach across the government	18 Months +
Digital Government	Data	Walk	- Define data ownership (i.e. who owns it, where is the master copy, who all should have access, etc.)	6 Months - 1 Year
Digital Government	Data	Walk	- Establish laws or regulations around the retention of digital data once a server is no longer in use (i.e. a contract has concluded, or a server is being retired)	6 Months
Digital Government	Governance	Walk	- Define government-wide application documentation standards	6 Months
Enabling Environment	Governance	Walk	- Define coding standards (i.e. best practices) to be followed across the government	6 Months
Enabling Environment	Governance	Walk	- Define disaster recovery requirements (i.e. frequency of testing procedures, international standards, location and general requirements)	6 Months
Digital Innovation	High-Level Strategy	Walk	- Work with individuals currently using cloud to start standardizing decisions around when to use cloud and then expand that approach	6 Months
Digital Innovation	High-Level Strategy	Walk	- Work with the cabinet in order to get support for adopting a cloud strategy at the highest level	6 Months
Digital Innovation	High-Level Strategy	Walk	- Create a CIO or equivalent cabinet level ICT position in an official capacity	6 Months - 1 Year
Enabling Environment	Security	Walk	- Define encryption standards and requirements (i.e. should sensitive data at rest be encrypted)	6 Months
Enabling Environment	Security	Walk	- Establish and implement general security requirements and regulations for digital hosting and cloud service providers (i.e. encryption, data retention, access and ownership, etc.)	6 Months
Digital Innovation	Administrative	Run	- Consider moving IT support for government to a centralized model	6 Months - 1 Year
Digital Innovation	Administrative	Run	- Review IT retention rates in the area of cloud migration - Determine if steps to mitigate turnover can be implemented - Establish training for new employees and standards for documentation to enable knowledge transfer	6 Months - 1 Year
Digital Innovation	Administrative	Run	- Review IT retention rates in the area of cloud security - Determine if steps to mitigate turnover can be implemented - Establish training for new employees and standards for documentation to enable knowledge transfer	6 Months - 1 Year
Digital Government	Data	Run	- Update data retention policies to include cloud based applications	6 Months
Digital Government	Data	Run	- Confirm data validation standards are well documented and distributed - Ensure that newly developed applications conform with the guidelines - Review existing applications to confirm that data validation is implemented	6 Months - 1 Year
Digital Government	Data	Run	- Create a policy on multi-tenancy	6 Months
Digital Government	Data	Run	- Build interfaces to other department, institutions, and ministries to access needed applications and data.	18 Months +
Enabling Environment	Governance	Run	- Define and adopt technical architecture standards (i.e. enterprise standards around application and web servers as well as coding languages)	6 Months

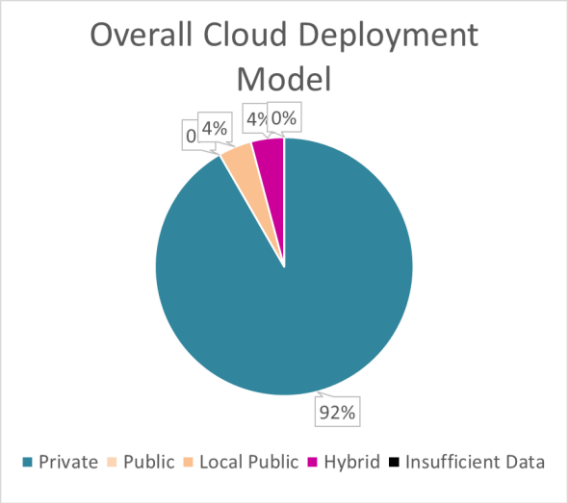
Category	Recommendation Type	Phase	Recommendation	Duration
Enabling Environment	Governance	Run	- Define government-wide life cycle development standards and ensure they align with international standards, especially those that relate to cloud	6 Months
Enabling Environment	Governance	Run	- Evaluate laws requiring hard copies of specific documents to determine if electronic equivalence is feasible	6 Months
Enabling Environment	Regulatory	Run	- Enable government applications to use electronic signatures to increase security of data transfer as well as the confidence of the public and end users	18 Months +
Enabling Environment	Regulatory	Run	- Identify an agency (or regulator) who will be tasked with the enforcement of privacy and related laws and regulations	3 Months
Enabling Environment	Regulatory	Run	- Review whether exceptions for hiring foreign employees or contractors should be made if the resources are not available locally - Work with local groups to make sure resources are available in the local workforce	3 Months
Enabling Environment	Security	Run	- Work with local banks or other organizations to enable e-payment, even if in limited capacity, to enable the use of online services	6 Months - 1 Year
Digital Innovation	High-Level Strategy	Fly	- Automate existing paper based processes in a manner architected for the cloud	18 Months +
Digital Innovation	High-Level Strategy	Fly	- Automate existing paper based processes in a manner architected for the cloud	18 Months +

4.2.5.3 Application Roadmap

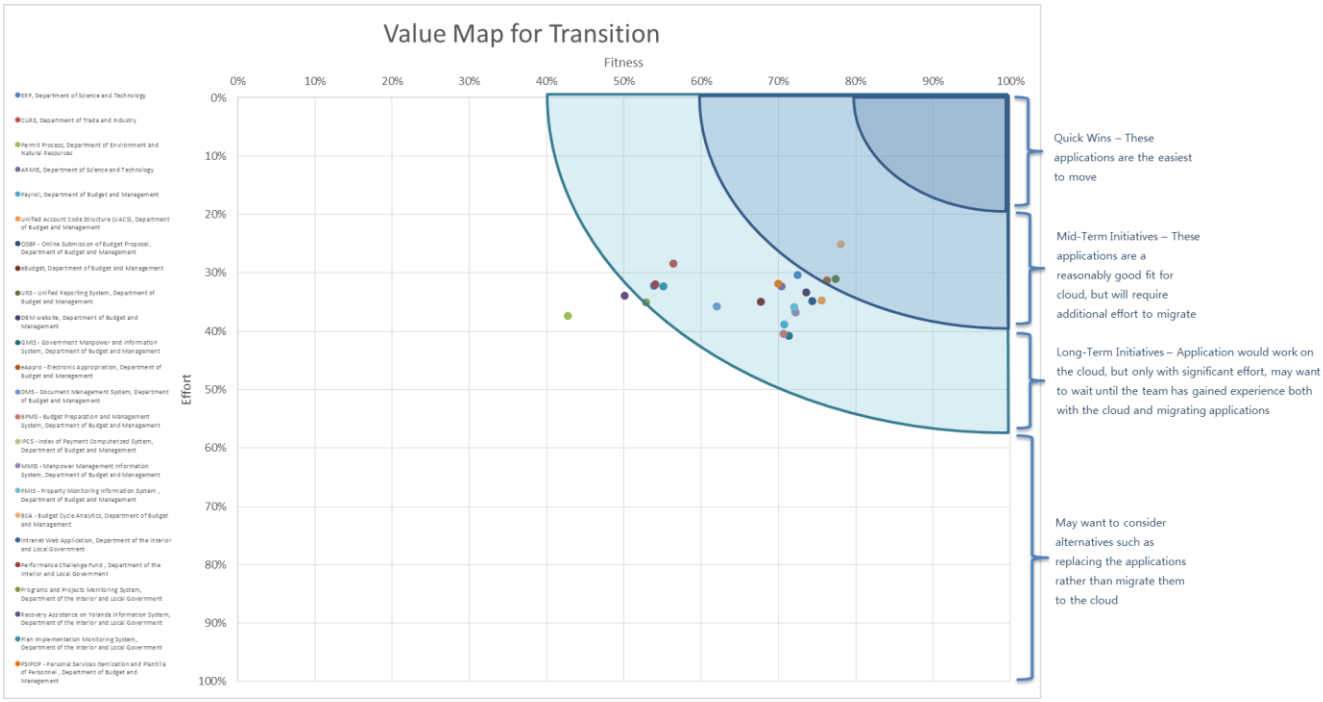
The departments of Advanced Science and Technology Institute, Construction Industry Authority, Department of Science and Technology and the Environmental Management Bureau each provided data for one application. The Department of Budget and Management provided data for 14 applications and the Department of Interior and Local Government provided information for five applications. No other application information was provided. This is a living document and can be updated with additional information. This additional information can be used to provide more guidance, analysis, and refined results.

Based on the assessment responses from the six departments, the recommendation aligns with the overall country recommendation – the majority of the applications are a best fit for private cloud. For the two applications that are not aligned with the overall country recommendation, one application is a best fit for local public cloud and the other is a best fit for hybrid cloud. Hybrid cloud does not differ significantly from the country recommendation. The country assessment found hybrid cloud and private cloud to be only two points apart, a statistically insignificant difference. In addition, local public may be feasible depending on decisions made at the government level. For example, if the government decides to allow this option for certain types of data and applications, this Department of Budget and Management application may be a good candidate.

It should be noted that the assessments for the applications in the Construction Industry Agency was only 70% complete and the infrastructure data for the Department of Interior and Local Government and the Environment Management Bureau applications was not provided. As a result, the recommendation for these applications may change if additional data is provided.



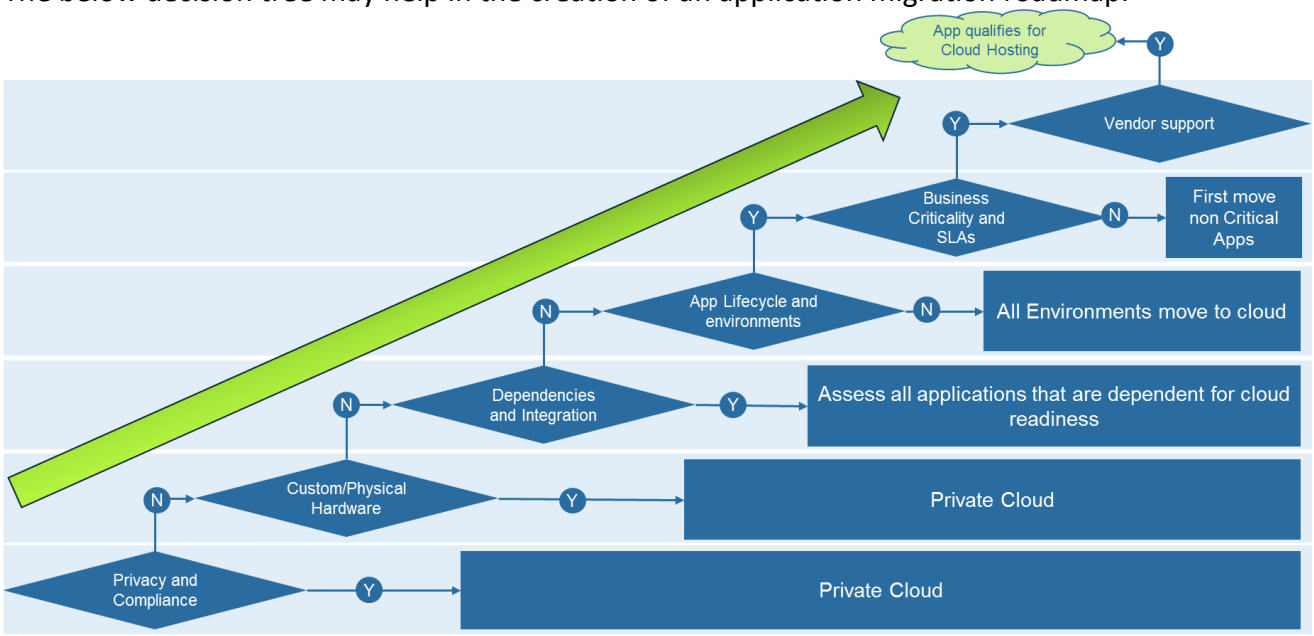
The value map helps show which applications are the closest fit and will take the least amount of effort to migrate. As the graphic shows, the ERP application for the Advanced Science and Technology Institute and the CLiRS application for the Construction Industry Agency are the two closest fits for cloud. The Department of Budget and Management and the Environment Management Bureau may want to consider alternatives such as replacing the applications rather than migrate the Document Management System (Department of Budget and Management) and the Permit Processing (Environment Management Bureau) applications to the cloud. The Philippines needs to provide direction to the various departments, either through lifting the hardware freeze or providing guidance on whether a public cloud can be leveraged.



When starting to plan the roadmap to migrate applications to the cloud, there are numerous attributes that need to be taken into account, including, but not limited to:

- Criticality of the system
- Sensitivity of the data
- Interfaces
- Application dependencies

The below decision tree may help in the creation of an application migration roadmap.



4.3 Pilot #3 – Zambia

4.3.1 Summary

This report is meant to be a conversation starter, and provide Zambia with a high level overview of the assessment findings in addition to recommendations on migrating to a cloud platform. The assessment documents are point in time and can be updated dynamically to reflect changes in direction and regulation. For example, if regulations around where data can be stored are put in place, the corresponding assessment questions can up updated to generate revised recommendations and scores. This will enable the toolkit to be utilized throughout the process of selecting a deployment model, implementing the model, and digitizing key e-Government services. This report does not replace a full, in-depth assessment which should be conducted prior to implementing a cloud platform.

In Zambia, answers were obtained for all but three questions in the country assessment, enabling a more reliable recommendation.

Overall Cloud Readiness Metric		
Very Ready	>80%	
Ready	65%-80%	
Need Additional Preparation	45-64%	
Need Underlying Infrastructure	25-44%	**<- Zambia is here**
Not Ready	<25%	

The overall cloud readiness assessment shows that Zambia needs to put in place their underlying infrastructure before moving forward. At this time, given concerns around where data can be hosted the assessment recommends that Zambia pursue a private cloud option, a path that is aligned with Zambia's recent request to the World Bank for assistance to implement several key ICT initiatives.

4.3.2 Key Findings

Zambia's overall readiness score is 41%. This puts Zambia at the upper end of "Need Underlying Infrastructure". There is strong interest from the highest levels of the government in implementing the "Smart Zambia" vision as outlined by the President. Cloud computing is seen, by the government, as a driver of this overall initiative. While interest within the government is high, there are many key components that are not yet in place. Zambia is taking the steps to make sure that those pieces are in place as they move forward, thus setting themselves up for success if they continue on this path and if they can get support and buy-in from other ministries and departments. A challenge in this area will be enlisting the cooperation of relevant inter- and intra-government officials.

Zambia has an official, cabinet level ICT organization, the Center of Excellence for E-Governance and ICT. All CIOs in other ministries report to the Center of Excellence, and major ICT initiatives

must be coordinated with this department. This mandate was further supported by a memorandum from the President's office encouraging the "coordination and harmonisation of information systems" that noted that all ICT personnel fall under the Center of Excellence and ICT procurement contracts need to be undertaken in consultation with the Center of Excellence. In addition, when we interviewed other departments, they almost unanimously identified the Center of Excellence as the organization responsible for driving ICT policy and direction going forward. This puts Zambia in an excellent position to implement policies and regulations uniformly and from the top down.

Multiple ministries had not only created a disaster recovery plan, but had partially tested them by bringing up applications and switching users over to them. In addition, most disaster recovery sites were a significant distance away, as opposed to being within the same or a neighboring building.

However, Zambia also has some key infrastructure concerns that are not captured within the scope of the cloud assessment, but could impact Zambia's ability to move forward with a migration to the cloud. 99% of Zambia's electricity comes from hydro, but Zambia has been in a drought since 2014. Thus, even though they have the grid and the capacity, they cannot produce enough electricity to provide power to everyone on the grid. While this may be a reason to bring servers that need to run 24/7 into one data center, a lack of power complicates access and availability. Zambia has no clear coordination around the laying of fiber optic cables. This has led to different companies laying cable in the same spot and a lack of a coordinated effort to reach many of the rural areas of Zambia. Lastly, the cost of transmitting data outside the country is much higher than the cost of transmitting data within the country. However, most usage is cross-border, which means that lines leaving the country are on average utilized at 60-70% of total capacity. Also, less than 20% of government buildings within the capital city of Lusaka are connected to the internet. This provides an opportunity to create an exclusive, government owned and operated network that connects to a central data center; however, such an initiative would be time intensive and expensive. These infrastructure concerns are foremost on the government's mind and are a key component of the request to the World Bank for ICT funding.

While Zambia has significant preparatory work to do before they are ready to implement a cloud strategy, they are approaching the problem in a step by step manner that may put them in a better position in the long run than many countries that appear to be further ahead on the path to cloud at this point in time.

4.3.3 Deployment Model Recommendation

The cloud readiness assessment recommends that Zambia pursue a private cloud. However, this recommendation was driven by key assessment findings; primarily concerns around data leaving the country, which eliminated public cloud as an option. However, at least two groups were looking into public cloud as an option, so the government should review the current barriers for public cloud computing and formalize the preferred approach.

	Overall Readiness	Private Cloud Readiness	Hybrid Cloud Readiness	Public Cloud Readiness	Local Public Cloud Readiness
Readiness Score	41%	53%	0%	0%	0%

The most important part of selecting a cloud approach is determining where data can be stored. This question has multiple parts. Can data be stored on a public server? Can government data and applications reside on the same server as non-government data and applications (multitenancy)? Can data leave the country? If so, all countries or just some? Does this rule apply to all data, or just a subset of data, perhaps non-sensitive data? All of these questions need to be formalized so that every ministry handles their data in the same way.

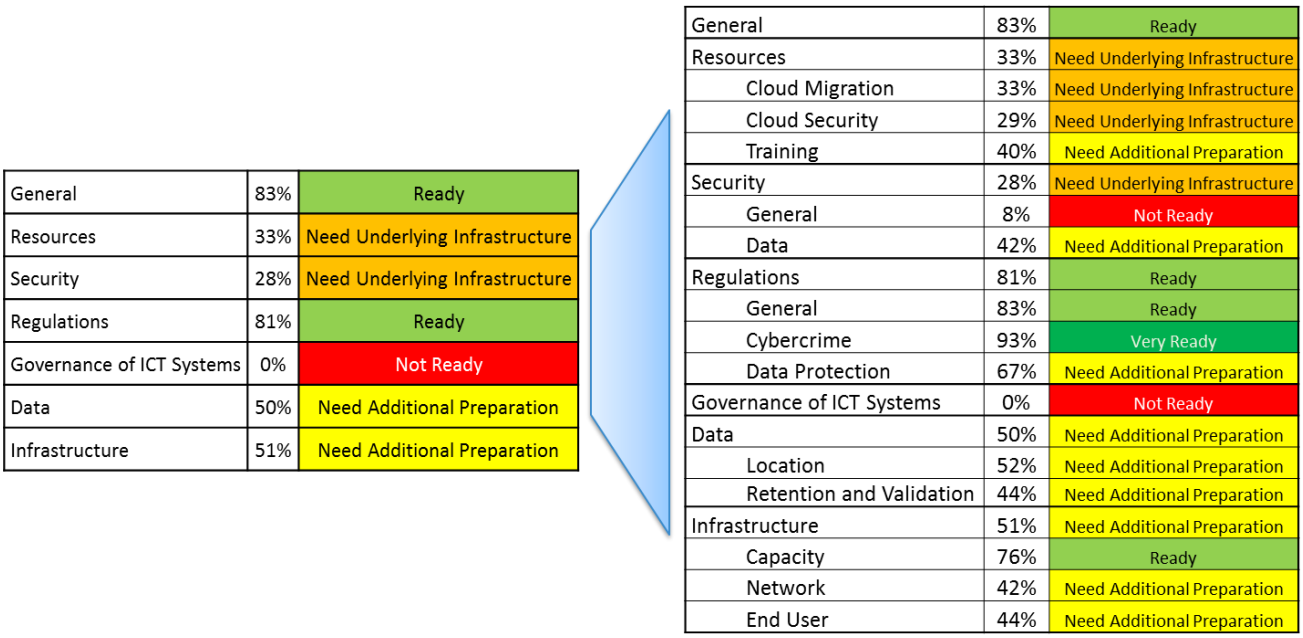
In Zambia, there was general consensus that data, especially sensitive data, could not leave the country and it could not reside on public servers. Data could reside in data centers owned and operated by third parties, but when questioned further, most situations appeared to describe colocation, where the server was owned or exclusively used by the government, regardless of where it resided. This finding drove the recommendation that Zambia pursue a private cloud as a public cloud provider would use public servers that may also be used by non-government organizations. In addition, a non-local public cloud provider would necessitate the storing of data outside of Zambia.

Zambia may wish to review whether all applications and types of data needs to have the same level of security and protection. That may open up the possibility of public cloud for some subset of data and applications. Also, Zambia should make sure that any private cloud can meet the security needs of all ministries. It is recommended that the Electronic Communication Transactions Act (ECTA) be revisited and revised, if necessary, to reflect current needs in data transmission and storage from a regulatory standpoint - this will improve the overall desirability and propensity for adopting cloud technologies.

Any changes in regards to data storage might change the cloud deployment recommendation, and the assessment should be retaken.

4.3.4 Gaps

When discussing cloud with various ministries and organizations, there was strong interest in what was meant by cloud and what benefits the assessment team thought Zambia might see from implementing cloud; however, there was also a distinct hesitancy. Individuals would mention that the underlying infrastructure was not ready. To address this, the government has requested funding from the World Bank for various projects, and also mentioned plans to construct a data center that would be the location for the future government cloud.



General	83%	Ready
Resources	33%	Need Underlying Infrastructure
Security	28%	Need Underlying Infrastructure
Regulations	81%	Ready
Governance of ICT Systems	0%	Not Ready
Data	50%	Need Additional Preparation
Infrastructure	51%	Need Additional Preparation

General	83%	Ready
Resources	33%	Need Underlying Infrastructure
Cloud Migration	33%	Need Underlying Infrastructure
Cloud Security	29%	Need Underlying Infrastructure
Training	40%	Need Additional Preparation
Security	28%	Need Underlying Infrastructure
General	8%	Not Ready
Data	42%	Need Additional Preparation
Regulations	81%	Ready
General	83%	Ready
Cybercrime	93%	Very Ready
Data Protection	67%	Need Additional Preparation
Governance of ICT Systems	0%	Not Ready
Data	50%	Need Additional Preparation
Location	52%	Need Additional Preparation
Retention and Validation	44%	Need Additional Preparation
Infrastructure	51%	Need Additional Preparation
Capacity	76%	Ready
Network	42%	Need Additional Preparation
End User	44%	Need Additional Preparation

4.3.4.1 Resources

Zambia has limited to no local resources in either the public or private sector with skills in cloud migration or security. In addition, there are no programs currently offered at the local Universities that would bridge this gap in the future. When meeting with the University of Zambia, it was mentioned that while there is an IT Security degree, there is no cloud component to that course of study due to lack of teachers with the skill set to cover the material.

In order to address this gap, it is recommended that Zambia work to incorporate cloud into existing IT curriculum. There are multiple ways this could be approached, including, but not limited to, sending faculty to cloud training or working with private companies to get guest lecturers to cover cloud topics.

4.3.4.2 Security

There are several areas within security that Zambia needs to focus on; specifically security clearances and e-payment.

4.3.4.2.1 General

From a general security standpoint, Zambia does not require public sector employees to undergo any sort of security clearance. In addition, Zambia has no encryption requirements at the government level, although two of the ministries we talked to required that sensitive data be encrypted in transit. As Zambia moves to digitize more and more processes and data, and enable citizens to use the internet to request government services it will be critical that basic security rules be standardized and enforced across the government. It is strongly recommended that Zambia institute security clearances for all individuals with access to sensitive data and that they review their encryption requirements.

4.3.4.2.2 E-Payment and PKI

Zambia enables e-payment, but only for taxes. The agreements with the banks and other components of the e-payment system are specific to the Zambia Revenue Authority (ZRA). In addition, the ZRA is currently using the digital certificates supplied by the banks. Given Zambia's goal of providing 140 government services electronically, it is recommended that the Center of Excellence formalize both an e-payment and digital signature process that can be used across the government and make it available to all ministries.

4.3.4.3 Data Location

While most individuals, when asked, said that data should not leave the country, most people were uncertain as to whether or not any actual regulations restricted where data could be stored. Some ministries said no such restrictions existed and others said that ZICTA, the regulatory agency, mandated that sensitive data not leave Zambia. To address this gap, it is recommended that if restrictions are in place, then awareness of them should be increased, and if restrictions are not in place, then they should be formalized and the various ministries and impacted companies made aware of any restrictions

In addition, it should be noted that despite the strong response we got when specifically asking if data could leave the country, the vast majority of ministries are in fact using non-government email addresses, such as Yahoo or Google. This means that data is potentially being sent and stored on email servers located outside of the country. In light of this discrepancy, it is strongly recommended that Zambia review this situation and finalize their overall approach. It is also recommended that Zambia consider migrating to a common email platform across the government.

4.3.4.4 Governance

3.5.4.4.1 Cloud Strategy

While one of Zambia's key strengths is that they have a Center of Excellence to coordinate and align ICT activities across the government, they do not yet have an overall cloud strategy. It is recommended that they develop a cloud strategy that can be implemented across the government and provide direction to future ministry level initiatives.

4.3.4.4.2 Governance of ICT

Another critical gap on the path to cloud is in the area of general governance of ICT. Zambia does not have certain ICT processes in place. Cloud platforms do not support all applications. Having guidelines and processes in place for application development will make it easier to determine what needs to be supported on the new platform and to migrate those applications once it is time to do so. As Zambia works to put processes and guidelines in place, it needs to make sure that they are sufficient for the groups with the strictest requirements. If necessary, exceptions can be granted to those groups for which such strict requirements would be too burdensome. However, the reverse situation, where regulations are too lax for some groups, may mean that the cloud platform, when it becomes available, will not meet the needs of

everyone. It is recommended that Zambia formalize the following processes at the government level:

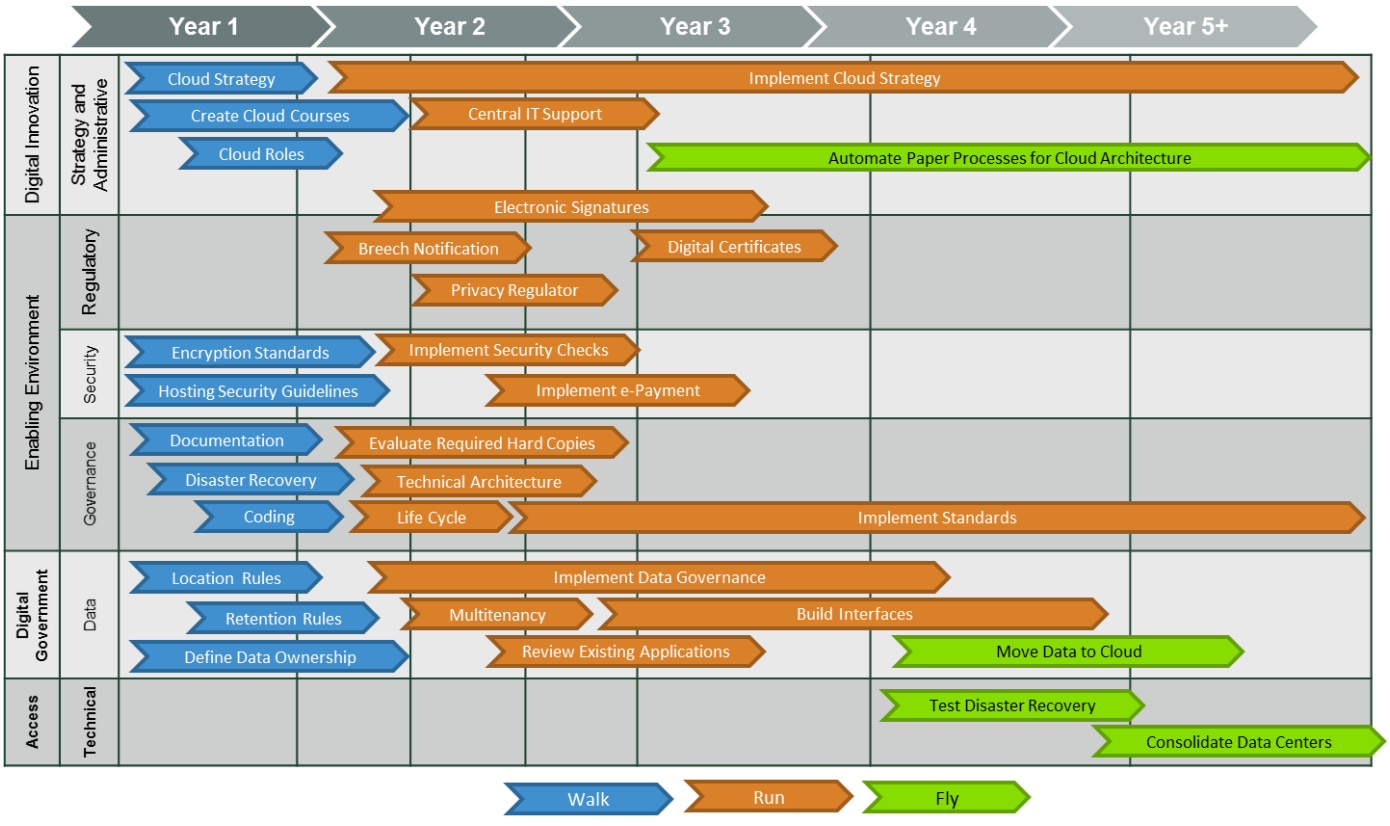
- Interoperability and interconnectivity between ministries
- Technical architecture
- Disaster recovery
- Application documentation

The first two are particularly crucial to getting the greatest benefit out of a cloud platform over time.

4.3.5 Next Steps

4.3.5.1 Policy Roadmap

Various responses to the questions on the country assessment are associated with a recommendation. Each recommendation has an associated phase, type, and estimated duration. These are used to construct a detailed roadmap. How the roadmap will look will vary based on each country's priorities and needs. However, a sample roadmap has been constructed for Zambia based on the recommendations produced for this report. The recommendations are also outlined in the table following the roadmap. The Digital Development Partnership (DDP) category that most closely aligns to the recommendation has also been noted in both the roadmap and the accompanying table.



The recommendations and roadmap have been split into three phases.

Phase one (walk) focuses the regulatory and technical infrastructure needs to be defined before moving to the cloud. This would include defining policies and regulations around data, hosting, encryption, and technical standards. These items should be completed prior to moving onto phase two.

Phase two (run) focuses on defining the next level of policies and regulations, such as multitenancy and technical architecture, as well as implementing the policies and regulations created in phase one. These policies and regulations will help standardize the overall environment. A standard environment will make it easier and cheaper to move applications to the cloud. In addition, during this phase, ministries should start to build interfaces to enable the sharing of data across applications. This will simplify data collection and governance.

Phase three (fly) focuses on implementing a true cloud platform. Starting with converting existing manual processes into digital, cloud-based processes and consolidating data centers into the government cloud.

4.3.5.2 Policy Recommendation Table

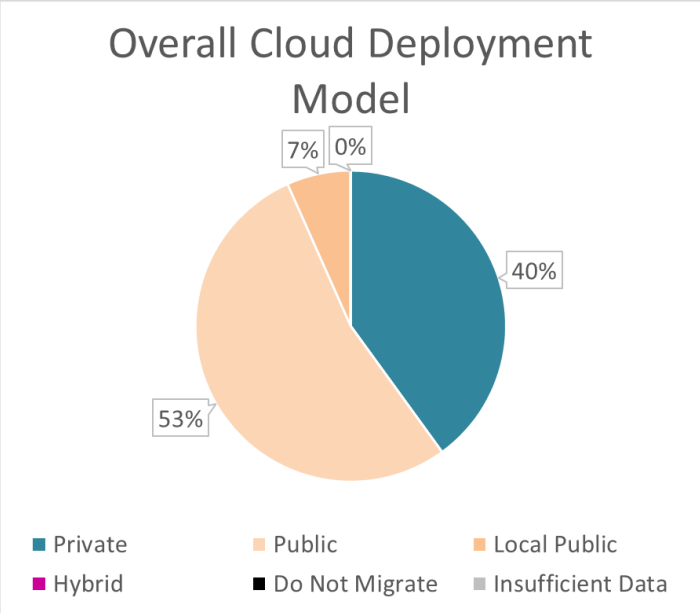
The following table outlines the recommendations, as seen in the country assessment.

Category	Recommendation Type	Phase	Recommendation	Duration
Digital Innovation	Administrative	Walk	- Work with universities and/or vendors to create available and affordable cloud migration courses	6 Months - 1 Year
Digital Innovation	Administrative	Walk	- Work with universities and/or vendors to create cloud courses for government use	6 Months - 1 Year
Digital Innovation	Administrative	Walk	- Work with universities and/or vendors to create available and affordable cloud security courses	6 Months - 1 Year
Digital Innovation	Administrative	Walk	- Work with universities and/or vendors to create cloud security courses for government use	6 Months - 1 Year
Digital Government	Data	Walk	- Formalize guidelines around where data can be stored, taking in to consideration cloud technologies	6 Months
Digital Government	Data	Walk	- Define data ownership (i.e. who owns it, where is the master copy, who all should have access, etc.)	6 Months - 1 Year
Digital Government	Data	Walk	- Establish laws or regulations around the retention of digital data once a server is no longer in use (i.e. a contract has concluded, or a server is being retired)	6 Months
Enabling Environment	Governance	Walk	- Define government-wide application documentation standards	6 Months
Enabling Environment	Governance	Walk	- Define coding standards (i.e. best practices) to be followed across the government	6 Months
Enabling Environment	Governance	Walk	- Define disaster recovery requirements (i.e. frequency of testing procedures, international standards, location and general requirements)	6 Months
Digital Innovation	High-Level Strategy	Walk	- Define an overall government-wide cloud strategy	6 Months
Digital Innovation	High-Level Strategy	Walk	- Work with individuals currently using cloud to start standardizing decisions around when to use cloud and then expand that approach	6 Months
Digital Innovation	High-Level Strategy	Walk	- Formalize cloud responsibilities as part of specific roles within the government	6 Months - 1 Year
Enabling Environment	Security	Walk	- Define encryption standards and requirements (i.e. should sensitive data at rest be encrypted)	6 Months

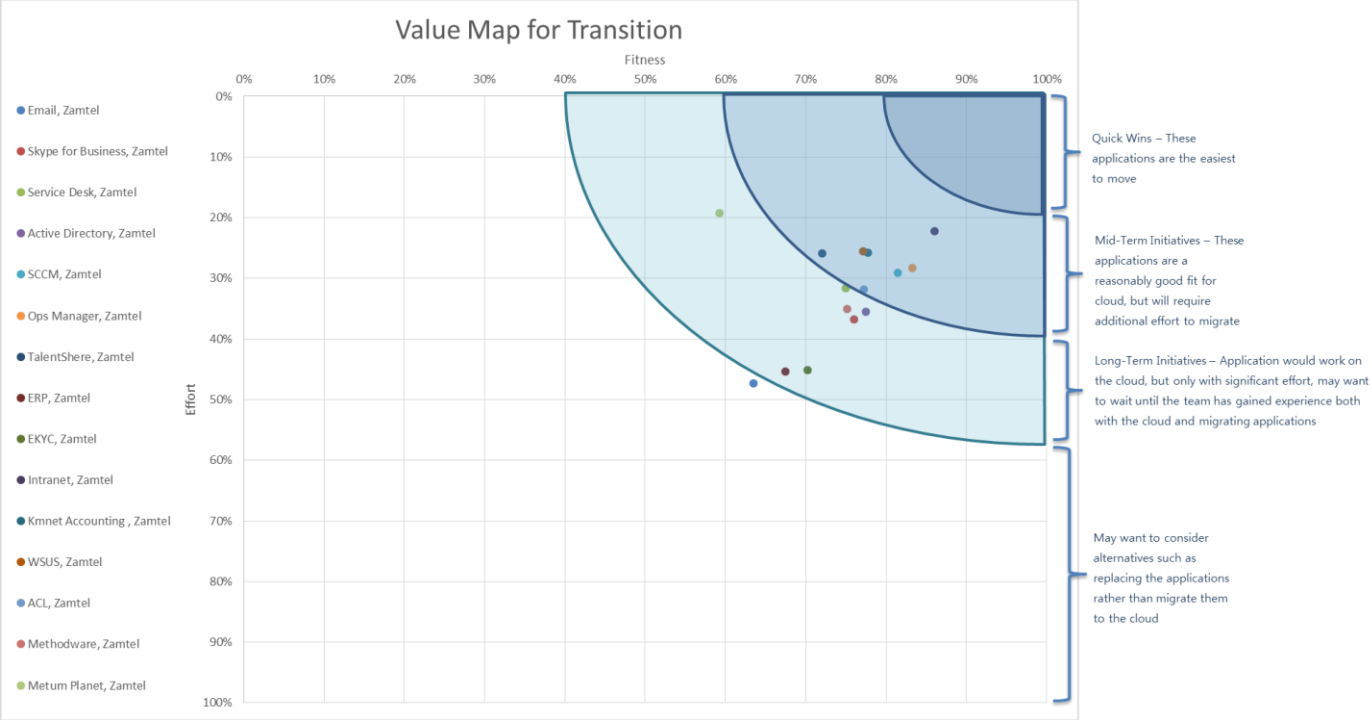
Category	Recommendation Type	Phase	Recommendation	Duration
Enabling Environment	Security	Walk	- Establish and implement general security requirements and regulations for digital hosting and cloud service providers (i.e. encryption, data retention, access and ownership, etc.)	6 Months
Digital Innovation	Administrative	Run	- Consider moving IT support for government to a centralized model	6 Months - 1 Year
Digital Government	Data	Run	- Implement data governance across the government	18 Months +
Digital Government	Data	Run	- Update data retention policies to include cloud based applications	6 Months
Digital Government	Data	Run	- Create a policy on multi-tenancy	6 Months
Digital Government	Data	Run	- Confirm data governance standards are well documented and distributed - Review existing applications to validate that data will be captured according to the guidelines - Ensure that newly developed applications conform with the guidelines	6 Months - 1 Year
Digital Government	Data	Run	- Confirm data validation standards are well documented and distributed - Ensure that newly developed applications conform with the guidelines - Review existing applications to confirm that data validation is implemented	6 Months - 1 Year
Digital Government	Data	Run	- Create procedures and build interfaces to other department, institutions, and ministries to access needed applications and data	18 Months +
Enabling Environment	Governance	Run	- Define and adopt technical architecture standards (i.e. enterprise standards around application and web servers as well as coding languages)	6 Months
Enabling Environment	Governance	Run	- Define government-wide life cycle development standards and ensure they align with international standards, especially those that relate to cloud	6 Months
Enabling Environment	Governance	Run	- Evaluate laws requiring hard copies of specific documents to determine if electronic equivalence is feasible	6 Months
Enabling Environment	Regulatory	Run	- Enable government applications to use electronic signatures to increase security of data transfer as well as the confidence of the public and end users	18 Months +
Enabling Environment	Regulatory	Run	- Identify an agency (or regulator) who will be tasked with the enforcement of privacy and related laws and regulations	3 Months
Enabling Environment	Regulatory	Run	- Create laws that require an organization or agency to notify an individual when their data has been compromised in the event of a security incident	6 Months
Enabling Environment	Regulatory	Run	- Create a process for issuing and tracking digital certificates	6 Months - 1 Year
Enabling Environment	Security	Run	- Implement security checks for individuals working with sensitive systems or data	6 Months - 1 Year
Enabling Environment	Security	Run	- Work to implement a broader e-payment system	6 Months - 1 Year
Digital Government	Data	Fly	- Start investigating moving data to the cloud for ease of access across departments/ministries	6 Months - 1 Year
Digital Innovation	High-Level Strategy	Fly	- Automate existing paper based processes in a manner architected for the cloud	18 Months +
Digital Innovation	High-Level Strategy	Fly	- Automate existing paper based processes in a manner architected for the cloud	18 Months +
Access	Technical	Fly	- Consider migrating to the cloud as an opportunity to consolidate data centers	18 Months +

4.3.5.3 Application Roadmap

Zamtel, the government owned infrastructure/telecommunication service provider, supplied information for 15 of their applications. No other application information was provided. This is a living document and can be updated with additional information. This additional information can be used to provide more guidance, analysis, and refined results. Based on Zamtel's responses to the assessment, the majority of the applications are a fit for public; however, there are several applications that are a fit for private. In the case of those applications that are a fit for public, it is not a viable option at this time unless there are changes to the current data location rules and regulations and a local public cloud provider who has disaster recovery located with Zambia.



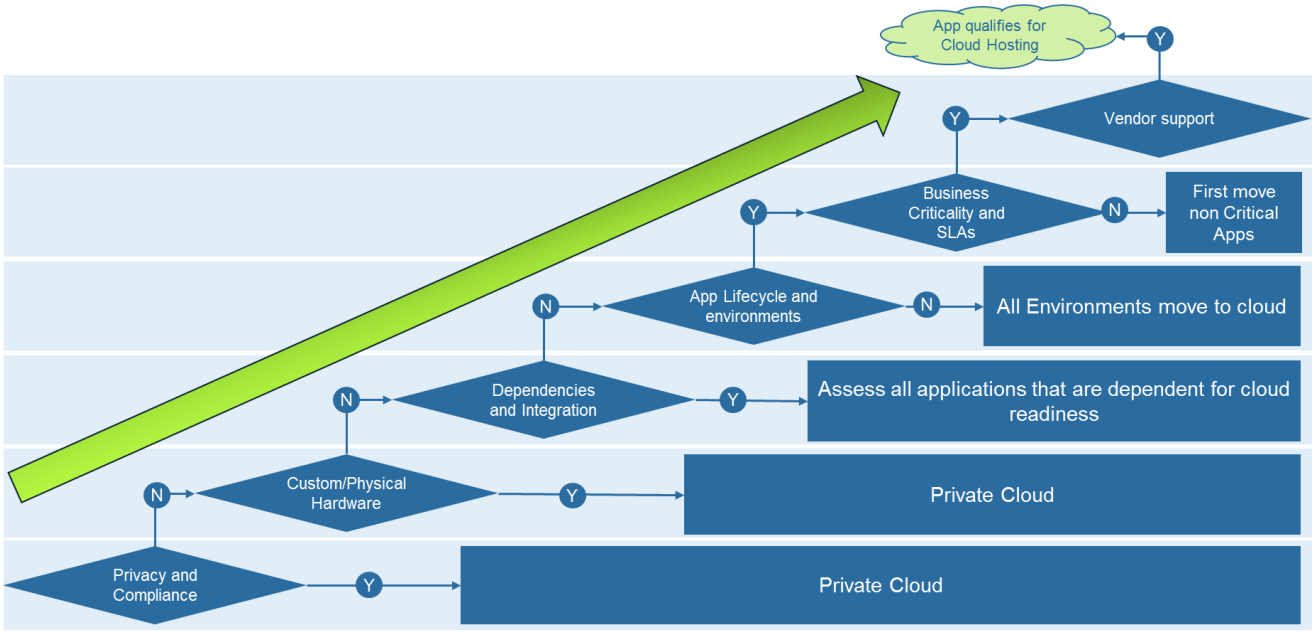
The value map helps show which applications are the closest fit and will take the least amount of effort to migrate. For example, Zamtel's service catalogue application, called Intranet, requires the least amount of effort and is the closest fit. After that, there are several applications that are a reasonably good fit for cloud, but will require additional effort to migrate.



When starting to plan the roadmap to migrate applications to the cloud, there are numerous attributes that need to be taken into account, including, but not limited to:

- Criticality of the system
- Sensitivity of the data
- Interfaces
- Application dependencies

The below decision tree may help in the creation of an application migration roadmap.



4.4 Overview of Findings

The three countries that participated in the pilot sound very different on paper:

- Serbia is just starting to build a central data center and many ministries have their own small data centers
- The Philippines already has multiple national data centers; however, they handle only a fraction of the government's overall ICT operations
- Zambia has less than 20% of their government buildings connected to the internet and are just beginning to centralize all ICT activities under the aegis of the data center of the Center of Excellence for E-Government and ICT (COEEGICT)

But, the final scores actually find the three countries to be within about 20 points of one another. This is a significant gap, but not as great as might be expected. This is mostly due to the fact that the assessment helps identify gaps that exist in the overall infrastructure and governance framework that could cause future problems. Each country has unique gaps but also similarities such as a large number of paper processes, limited number of available skilled resources, and a major upcoming election. This can be seen in the following SWOT analysis.

	Serbia	Philippines	Zambia
Strengths	- Overall the furthest on the path towards cloud - Organizational culture lends itself towards adopting and implementing a single approach - Good infrastructure and high level of Internet access at home for citizens	- Already have at least three national data centers - In the process of building a government network	- Have a Centre of Excellence and e-Governance that can drive cloud implementation and adoption - Organizational culture lends itself towards adopting and implementing a single approach

	Serbia	Philippines	Zambia
Weaknesses	- No CIO or equivalent cabinet level IT position, thus hindering the ability of the government to drive cloud implementation or adoption - No clear regulations on where data can be stored both geographically and in terms of public verses government owned servers. This currently limits Serbia to a private cloud deployment model.	- No official CIO or equivalent cabinet level IT position, thus hindering the ability of the government to drive cloud implementation or adoption - No clear regulations on where data can be stored both geographically and in terms of public verses government owned servers. Some departments are making these decisions at the department level independent of government direction.	- No clear regulations on where data can be stored both geographically and in terms of public verses government owned servers. This currently limits Zambia to a private cloud deployment model. - No security clearances are required to work on sensitive data
Opportunities	- Cloud is seen as a key initiative by both citizens and government officials - Serbia is pursuing joining the EU and many of the regulations they are looking to implement are also part of that process - Large number of paper based processes that could be automated and architected for cloud	- Department of Budget and Management is enforcing ICTO policies through budgets - Working with Azure to enable that as an alternative cloud offering - Large number of paper based processes that could be automated and architected for cloud	- ICT in general is seen as a key initiative by government officials - Large number of paper based processes that could be automated and architected for cloud
Threats	- Skilled resources frequently leave the country to pursue other opportunities - Upcoming elections	- Current ICTO team does not have the skill set to build a cloud offering - Current data center does not have the capacity or the capability to meet the needs of the various government agencies - Individuals are utilizing alternatives that may not meet the security needs of the government (i.e. Google email) - Upcoming elections	- Lack of stable power grid - Limited access to Internet at home - Unmanaged infrastructure growth (no one is coordinating the laying of fiber optic cables) - Upcoming elections

It should be noted that this report simply recommends next steps for addressing the identified gaps. In addition to implementing these steps, an in-depth assessment based on the findings and conversations generated from the toolkit should be undertaken.

	Serbia	Philippines	Zambia
General	**75%**	**84%**	**83%**
Resources	**44%**	**61%**	**33%**
Cloud Migration	38%	58%	33%
Cloud Security	40%	63%	29%
Training	65%	65%	40%
Security	**60%**	**35%**	**28%**
General	50%	25%	8%
Data	67%	42%	42%
Regulations	**83%**	**77%**	**81%**
General	83%	58%	83%
Cybercrime	67%	97%	93%
Data Protection	100%	83%	67%
Governance of ICT Systems	**35%**	**20%**	**0%**
Data	**66%**	**70%**	**50%**
Location	67%	81%	52%
Retention and Validation	64%	36%	44%
Infrastructure	**69%**	**77%**	**51%**
Capacity	84%	90%	76%
Network	80%	86%	42%
End User	32%	44%	44%
Overall Cloud Readiness Score	**59%**	**56%**	**41%**

4.4.1 Similarities

Despite the difference in scores, there were some similarities seen in all three countries.

4.4.1.1 Defining Cloud

One of the similarities seen across the pilot countries was that most countries interpreted any sort of online application or national data center as meaning that they had cloud. While this is in fact a step towards having a cloud environment, true cloud also has the ability for groups to

request computing resources on demand and be able to handle elastic demand. Neither attribute had been considered by any of the countries where the toolkit was piloted.

4.4.1.2 Elections

The most unexpected similarity was that all three countries will be having a major election within the next six months. In all cases, this has led to a certain amount of uncertainty. In two of the three countries, Serbia and the Philippines, there is legislation pending that would impact cloud adoption, but they only expect the legislation to be signed if there is a change in administration.

4.4.1.3 Lack of Governance

In two countries the creation of a cabinet level CIO or similar ICT position is likely to be determined by the election. The one country that did have a cabinet level CIO position had only created it within the last three months, and has not had much chance to influence policy at a government level. This lack of high level leadership from a Government ICT Champion and direction has likely contributed to the fact that in all three countries, Governance of ICT was the lowest score. Security and information rules were either not very clear, relatively unknown, or did not exist at all. As a result departments were wary of making changes.

4.4.1.4 Resources

Skilled resources were lacking in both the public and private sector in all three countries and turnover amongst those resources with cloud skills was high. In the case of Serbia, when resources gained skills in the public sector through experience they would frequently leave for the private sector. The private sector told us that turnover was equally high in the private sector with individuals leaving the country to pursue other opportunities. In the Philippines resources also frequently left the public sector to take jobs in the private sector, although they were not as likely to leave the country. Although the Philippines did have a bill pending that would increase wages to 80% of market rate. In Zambia, there was a lack of individuals with the skills and limited opportunities for individuals to gain the skills on their own. When talking with the University it was mentioned that cloud components had not been added to any of the IT courses due to a lack of faculty who could teach it. In none of the three countries was there any sort of formal training to build up the skills within the public sector or a plan to decrease turnover of skilled IT resources.

3.6.1.5 Paper Processes

All three countries had a large number of paper processes. In some cases, such as Serbia and the Philippines, there were legal requirements that some documents exist in paper form, in the case of Zambia some ministries had simply not digitized. For example, the Zambian national ID program exists only on paper. This provides excellent opportunities for all three countries to be able to increase efficiencies and improve usability of services by digitizing the processes and creating interfaces between ministries, agencies, and departments that all need access to the same data. No additional work to update or modernize applications is necessary if the new applications are created specifically for use in a cloud environment.

4.4.1.6 Driver

The opportunity to modernize and optimize tie in with what all three countries listed as their key drivers. In the case of Serbia, they selected "modernization", in the case of the Philippines and Zambia they selected "increased agility". All three mentioned cost savings as a secondary driver. However, while the driver for all three countries is similar, the underlying focus came across as very different in the interviews. In the case of Serbia, the key underlying desire is to automate existing government services. In the case of the Philippines the focus was purely internal, services for citizens were never mentioned unless prompted and no services had been specifically identified for automation. In the case of Zambia there is a strong drive to digitize. In addition, Zambia has identified 140 processes as candidates for automation long term.

4.4.2 Differences

These differences seen in focus and leadership, along with organizational differences in approaches to rules and regulations had a direct impact on some of the other key differences seen across the countries.

4.4.2.1 Organizational Approach

How people responded to questions was influenced by each government's organizational approach. For example, in both Serbia and Zambia, when individuals were asked whether things could be done, such as whether data could be stored outside the country, answers defaulted to "no" if there was no official direction. Activities were viewed as restricted until the government determined the high level direction. In the Philippines the opposite was true, individuals assumed that no rule or regulation meant that there was no restriction. In addition, the Philippines took a more consensus approach, so even if a rule did exist, actual enforcement of rules was significantly more challenging as without a restriction in place, rules were followed at a department's discretion.

4.4.2.2 Data Location and Privacy

There was also a difference in organizational approach in how the countries addressed data location and privacy. In Serbia, concerns around data leaving the country seemed to be primarily centered on security and control. If it left the country, who might have access to it? The Philippines overall seemed indifferent to any concerns around privacy. In fact, one group said that if the data needed to be secured, it shouldn't be digitized. In the case of Zambia, a lack of trust was strongly in evidence. Data stored outside of the country was at the mercy of another country and they strongly believed that any outside country would go through Zambia's data. There was also a lack of trust between ministries, citizens, and the government that fed into this concern as well. This will make interoperability more challenging in Zambia versus Serbia or the Philippines.

4.4.2.3 Infrastructure Readiness

The greatest difference between the three countries is in their existing infrastructure. Zambia, with the greatest infrastructure gap, has less than 20% of all government offices in the capital

city of Lusaka connected to the internet. This is a gap they feel strongly about and are working to remedy, but it will take time. In Serbia, buildings are connected and a network is in place, so they are now working to build a data center to start centralizing resources. In the Philippines, they have a multitude of data centers. There are three central data centers as well as quite a few data centers in the basements of various departments. Even so, the Philippines lacks enough capacity to meet demand and all interviews led to the conclusion that without a change in the procurement process or other large change, the Philippines will struggle to meet the capacity demands of the ministries for the foreseeable future.

4.4.2.4 Digital Certificates and E-payment

Security, particularly in the area of digital certificates and e-payment, was also an area where distinct differences in where the countries fell on the path to cloud were seen. Serbia and the Philippines are the furthest along. Serbia has the capability to issue and track digital certificates and Serbia also has existing applications that take advantage of the equivalency of e-signatures to written signatures. However, e-payment was a stumbling block. Ministries have faced challenges around implementing an e-payment system, although some forms of e-banking are currently accepted for some applications. The Philippines has issues close to 1,000 digital certificates and are in the process of testing the use of PKI in their archives and records management information system. In addition, the Philippines also had a partially, but not fully, implemented e-payment process. In contrast, in Zambia, there is no process defined for using digital certificates. The Zambia Revenue Authority (ZRA), the only group interviewed that had looked into digital certificates, were using the digital certificates produced by the banks. So far, the ZRA is also the only organization with the capability to pay online. This is mostly geared towards companies however as there are less than 600,000 registered tax payers in a country of 14 million.

4.4.2.4 Encryption

Encryption is a good example of the overall differences seen in the processes implemented across the three countries. In the case of Serbia, there are encryption standards and they've been defined by a local mathematician. How well they have been implemented is unknown. In the Philippines there are no government level encryption standards, so implementation is ad-hoc. In Zambia encryption is also ad hoc. Amongst those organizations interviewed, only two ministries require sensitive data to be encrypted during transit and only the University was encrypting any data at rest. This discrepancy remained relatively consistent across standards ranging from encryption to application documentation standards and life cycle development. In all of the pilot countries, the standards that did exist had not been adapted for use in a cloud environment.

4.4.3 Recommendations

There were several key recommendations for each category (administrative, high level strategy, data, security, etc.) and phase (walk, run, fly). Those key recommendations have been compiled into the following table.

Category	Type	Phase	Serbia	Philippines	Zambia
Digital Innovation	Administrative	Walk	- Work with universities and/or vendors to create cloud courses for government use	- Assess applications for which there are no employees with a high degree of familiarity with the application architecture or code to determine if the applications need to be replaced	- Work with universities and/or vendors to create cloud courses for government use
		Run	- Review IT retention rates in the area of cloud security	- Review IT retention rates in the area of cloud migration	- Consider moving IT support for government to a centralized model
			- Determine if steps to mitigate turnover can be implemented	- Determine if steps to mitigate turnover can be implemented	
			- Establish training for new employees and standards for documentation to enable knowledge transfer	- Establish training for new employees and standards for documentation to enable knowledge transfer	
	High-Level Strategy	Walk	- Create a CIO or equivalent cabinet level ICT position in an official capacity	- Create a CIO or equivalent cabinet level ICT position in an official capacity	- Define an overall government-wide cloud strategy
		Fly	- Automate existing paper based processes in a manner architected for the cloud	- Start investigating moving data to the cloud for ease of access across departments/ministries	- Automate existing paper based processes in a manner architected for the cloud
Enabling Environment	Governance	Walk	- Define disaster recovery requirements (i.e. frequency of testing procedures, international standards, location and general requirements)	- Define government-wide application documentation standards	- Define disaster recovery requirements (i.e. frequency of testing procedures, international standards, location and general requirements)
		Run	- Evaluate laws requiring hard copies of specific documents to determine if electronic equivalence is feasible	- Evaluate laws requiring hard copies of specific documents to determine if electronic equivalence is feasible	- Evaluate laws requiring hard copies of specific documents to determine if electronic equivalence is feasible
	Regulatory	Run	- Review whether exceptions for hiring foreign employees or contractors should be made if the resources are not available locally	- Enable government applications to use electronic signatures to increase security of data transfer as well as the confidence of the public and end users	- Enable government applications to use electronic signatures to increase security of data transfer as well as the confidence of the public and end users
			- Work with local groups to make sure resources are available in the local workforce		
	Security	Walk	- Establish and implement general security requirements and regulations for digital hosting and cloud service providers (i.e. encryption, data retention, access and ownership, etc.)	- Establish and implement general security requirements and regulations for digital hosting and cloud service providers (i.e. encryption, data retention, access and ownership, etc.)	- Establish and implement general security requirements and regulations for digital hosting and cloud service providers (i.e. encryption, data retention, access and ownership, etc.)

Category	Type	Phase	Serbia	Philippines	Zambia
		Run	- Work with local banks or other organizations to enable e-payment, even if in limited capacity, to enable the use of online services	- Work with local banks or other organizations to enable e-payment, even if in limited capacity, to enable the use of online services	- Implement security checks for individuals working with sensitive systems or data
Digital Government	Data	Walk	- Formalize guidelines around where data can be stored, taking in to consideration cloud technologies	- Formalize guidelines around where data can be stored, taking in to consideration cloud technologies	- Formalize guidelines around where data can be stored, taking in to consideration cloud technologies
		Run	- Build interfaces to other department, institutions, and ministries to access needed applications and data.	- Create a policy on multi-tenancy	- Update data retention policies to include cloud based applications
		Fly	- Start investigating moving data to the cloud for ease of access across departments/ministries		- Start investigating moving data to the cloud for ease of access across departments/ministries
Access	Technical	Prerequisite			- A stable, available network is a key pre-requisite for moving to a cloud environment
		Fly	- Consider migrating to the cloud as an opportunity to consolidate data centers		- Consider migrating to the cloud as an opportunity to consolidate data centers

4.4.3 Lessons Learned

4.4.3.1 Overall Lessons

Many valuable lessons were learned during the three pilots. The most important was that the application and infrastructure assessment is a valuable second step to the country assessment when using the toolkit, as the data needed may not initially be available. Once a country has decided they wish to pursue cloud, the application and infrastructure assessment can be used to identify which departments or ministries would be good candidates to start with, and which applications within those departments or ministries should be looked at first. Overall departments were reluctant to share application and infrastructure data outside of their country, but did see the value in the assessment and may incorporate it into future internal cloud strategic planning initiatives.

The need to emphasize the reusability of the toolkit became apparent. Individuals in all three countries were very quick to note items that were soon to change. Emphasizing that the toolkit was a snap shot in time and could be updated as things changed, thus updating the score and recommendations, helped get more accurate answers during the interviews.

The automated recommendations that are produced by the country assessment were refined during the presentation of the preliminary findings with the country pilot participants. Given the number of categories, the recommendations were aligned with phases (walk, run, fly). Putting recommendations into a more matrix format – broken down by both phase and category - helped give government officials a sense of how the recommendations in different categories worked in parallel to build a cloud platform.

Responses to questions were sometimes unexpected. Some questions had more gray areas within the answers than had been expected and some questions were simply interpreted completely differently from their original meaning. For example, the toolkit did not originally account for the fact that an e-payment system might be only partially implemented. In Zambia, questions around whether there were laws in place around which products could be used almost always immediately raised questions as to whether that included UN sanctions. This feedback was used to refine the wording and response options for questions throughout the questionnaire. Questions where multiple groups gave different answers were always reviewed. Was the difference in answers due to a difference in knowledge, understanding of the situation, or interpretation of the question? Any changes in wording when asking questions out loud were noted and later reviewed to see if the question itself needed to be reworded. This helped identify questions that required additional information or were not self-explanatory.

In addition, new questions needed to be added based on some unexpected discoveries. For example, it was not anticipated that there might be laws mandating that some documents exist in paper form. The importance of an upcoming election on the current situation, a discovery made in Serbia, also had to be incorporated into the toolkit.

4.4.3.2 Serbia

As Serbia was the first pilot country, some missed question areas were identified as well as some questions that were not needed. One example was around cost. There was no knowledge on how much was spent on ICT. The questions around cost were asked as well in Zambia and the Philippines to see if this gap was consistent and it was. The decision was then made to remove all questions around cost. It was also discovered in Serbia how important a cabinet level CIO position was to driving any sort of high level ICT strategy. Questions around such a position were added during this pilot.

4.4.3.3 Philippines

In the Philippines, distinct differences were seen in how questions were answered. In Serbia, the default was to answer in regards to how things stood. Answers were always given in reference to the current state, although explanations might note pending or future changes. In the Philippines, where there seemed to be less differentiation between future and present tense, government officials would imply that things were in progress, but follow up questions in regards to a timeline would show that the activity had not yet been started. To address this some questions were reworded and additional emphasis was placed on the fact that the assessment was a snap shot in time. For example, originally questions around procurement did not focus on timing. Based on feedback that servers could not be procured in a timely manner, even for the organizations running the main data centers, questions were added.

4.4.3.4 Zambia

In Zambia, the wording of new and existing questions from Serbia and the Philippines was tested and relatively few changes were required. The main lesson learned was around the

questions for data location. Additional questions around infrastructure were added when interviews showed that just because a government building is connected to the network, it doesn't mean the network will be available.

5 Assumptions

When designing this toolkit certain standard assumptions were made. These same assumptions were made when translating the assessment results into the final findings and recommendations. The key assumptions are:

- The individuals completing the questionnaires were relatively familiar with the areas covered and thus the questions are as complete and accurate as possible.
- By completing this assessment, it is assumed that there is some interest in identifying and resolving any readiness gaps.
- The government is already using computerized systems.
- The country already has a basic Internet infrastructure, such as copper lines.
- The country has a full time IT team.

6 Public Cloud Vendor Comparison

If a government decides to go with a public cloud setup then the next step is to determine which vendor to select. Vendors usually have multiple offerings, and it can be challenging to compare vendors. Comparisons are typically further complicated by different vendors using different terminology and units. It is recommended that, even if deciding to pursue a private cloud, governments still assess public cloud vendors to determine a baseline of offerings and service level agreements that they may wish to provide. In order to assist with any future comparisons governments may undertake, a vendor comparison can be found in this section for reference.

Azure and Amazon were chosen due to their breadth of services and geographic offerings. This report is not recommending one vendor over another, but only providing an example of a vendor assessment to provide guidance to governments on developing vendor requirements for their own vendor assessments.

Price is a key factor, especially as it can differ per region. Unlike private clouds, public clouds are not fully customizable. Pricing can vary depending upon the components and services provided by the public cloud service provider and also how the government utilizes those computing resources. A rough baseline for public cloud pricing can be found in the tables in this section.

At this time, there is no data center in Africa for Azure or Amazon, so it is recommended that African countries consider either using a data center on the European continent or a local cloud provider. If a local provider is selected, it is recommended the provider be assessed based on the general concepts and specific recommendations outlined in this report. Please be aware that actual pricing can vary based on utilization and contracting (i.e. predicted infrastructure usage, upfront payment, transaction volume, sizing, etc.).

The tables in this section are a representative list of various options and pricing for Amazon and Azure at a specific point in time, it is not comprehensive and further investigation should be done before selecting a provider. January 29, 2016

Key Differences – Azure and Amazon

Type	Amazon	Azure	Advantage
Availability	Amazon supports high availability across data centers Services such as load balancing, virtual network, and auto-scaling spans the region	Azure supports high availability within a data center Services such as load balancing, virtual network, and auto-scaling spans the region	Amazon

Type	Amazon	Azure	Advantage
Load Balancing	Supports load balancing based on IP address (layer 4) and application performance (layer 7) and provides metric-driven load balancing	Supports load balancing based on IP address (layer 4) and application performance (layer 7) and provides sophisticated load balancing policies	Tie
Virtual	Virtual Private Cloud (VPC) which supports Flow Logs which logs relevant traffic for storage and analysis	VNet to VNet (virtual network)	Amazon
Network	Direct Connect provides faster port speed than Azure however Amazon charges extra for a redundant port	Express Route has redundant ports by default	Azure
Auto Scaling	Has auto scaling provisions, terminates instances based on configured policies, and replaces unhealthy instances automatically	Automatically replaces unhealthy instance (service healing). Auto-scaling also supports both time and load-based scale up and scale down.	Tie
Compute	EC2 is billed by the hour	Virtual Machine is billed by the minute, but is slightly more expensive on average	Tie
Storage	Allows requestor to choose the input/output operation per second (IOPS)	Has more predefined IOPS level	Amazon
Security	Provides both server-side and client-side encryption options	Provides both server-side and client-side encryption options	Tie

Map of Major Data Centers – Azure and Amazon

Regional	Amazon	Azure
Asia & Pacific	Tokyo, Japan Beijing, China Singapore, Singapore Sydney, Australia India (Coming soon) Ningxia, China (Coming Soon) South Korea (Coming Soon)	Hong Kong, Hong Kong Singapore, Singapore Saitama, Japan Osaka, Japan Sydney, Australia Melbourne, Australia Pune, India Chennai, India Mumbai, India
Africa	None	None
Europe	Ireland Frankfurt, Germany	Dublin, Ireland Amsterdam, Netherland
North America	Northern Virginia, United States Oregon, United States Northern California, United States Ohio, United States (Coming Soon) Canada (Coming Soon)	Iowa, United States Virginia, United States Illinois, United States Texas, United States California, United States
South America	São Paulo, Brazil	São Paulo, Brazil

General Comparison

Category	Description	Amazon	Azure
Container Support	Container is an image that contains the complete file system in order to run software. It includes code, runtime, system tools, system libraries and all other components you can install on a server. This will allow environment and component consistency.	✓ EC2 Container Service	✓ Azure Container Service
Analytics (Big Data)	This feature will enable the processing and analysis of large amounts of data to reveal patterns, trends, associations, and other information readable by human.	✓ Elastic Map Reduce (EMR)	✓ - HDInsight (Hadoop) - Azure Data Lake
Compute Service	This service provides the computing power. It comes with different operating system and other services such as storage and network.	✓ - Elastic Compute Cloud (EC2) - Amazon Elastic Beanstalk	✓ - Virtual Machine - Cloud Service - Azure Websites and Apps
Desktop Service	This service provides virtual desktop service where you have your desktop computer in the cloud and access it via the internet.	✓ Amazon Workspace	✓ Azure RemoteApp
Hybrid Cloud Storage	This allows on premise applications to access storage which is located in the cloud system. It makes data growth management, data management, and backup (disaster recovery) easier.	✓ AWS Storage Gateway	✓ StorSimple
Load Balancing	A load balancer distributes network or application traffic across a number of servers. Load balancers are used to increase capacity (concurrent users) and reliability of applications.	✓ Elastic Load Balancing	✓ Azure Resource Manager (ARM)
Managed Deployment	This service automates code deployments, enabling you to deploy reliably and rapidly. The service allows you to launch and track the status of application deployments.	? AWS CodeDeploy	? Visual Studio Team Services

Operating System Comparison

Type	Amazon	Azure
Linux	CentOS 6.0+ / 7.0 Debian 8.0+ Red Hat Enterprise Linux 6.0+ / 7.0+ SUSE Linux Enterprise 11+ / 12+ Ubuntu 12.04 / 14.04 FreeBSD 9.0+ / 10.0+	CentOS 6.3+ / 7.0+ CoreOS 494.4.0+ Debian 7.9+ / 8.2+ Oracle Linux 6.4+ / 7.0+ Red Hat Enterprise Linux 6.7+ / 7.1+ SUSE Linux Enterprise 11 SP3+ / 12+ Open SUSE 13.1+ Ubuntu 12.04 / 14.04 / 15.04 / 15.10
Windows	Windows 2003 R2 Windows 2008 R2 Windows 2008 Windows 2012 Windows 2012 R2	Windows 2008 R2 Windows 2012 R2
Virtual Desktop	Windows 7 with MS Office, Trend Micro and utility bundles	Not Supported

Network Comparison

Type	Amazon	Azure	Remark
Virtual Network	Amazon Virtual Private Cloud (VPC)	Virtual Network	This service enables you to establish a private network (closed and security enhanced). This network is logically (rather than physically) isolated from other networks.
Direct Connection	AWS Direct Connection	Express Route	This service enables you to directly connect to the cloud directly from your premises (office or data center) over vLAN which means you can control bandwidth throughput, and keep a more reliable connection than internet-based connections.
DNS	Amazon Route 53	Azure DNS	Domain Name Server (DNS) is used to translate domain names to IP address (like yellow pages). This feature enables users to quickly access applications and infrastructure in the cloud.

Database Comparison

Type	Amazon	Azure	Remark
Relational Database	Amazon Relational Database Service (RDS)	Azure SQL Database	Both Amazon and Azure provide Database as a Service (DaaS) options. Amazon provides more database options as part of their DaaS.
NoSQL Database	DynamoDB MongoDB	DocumentDB MongoDB	NoSQL databases do not use tabular relationships to organize data and are mostly used to store large amounts of unstructured data.
Data Warehousing	Amazon Redshift	Azure SQL Data Warehouse	Data warehousing is used to run data analysis and produce reports. It stores current and historical data.

Operating System Pricing Comparison – Azure and Amazon

Data Center Location	Amazon – Linux	Azure - Linux	Amazon - Windows	Azure - Windows
Japan	$0.08	$0.11	$0.10	$0.158
Australia	$0.08	$0.116	$0.10	$0.186
Singapore	$0.08	$0.116	$0.10	$0.174
EU Region #1 – Ireland	$0.056	$0.094	$0.076	$0.15
EU Region #2 - Varies	$0.06	$0.102	$0.08	$0.162
Brazil	$0.108	$0.116	$0.128	$0.178
US West	$0.052	$0.094	$0.072	$0.154
US East	$0.052	$0.088	$0.072	$0.148

- Amazon EU Region #2 - Frankfurt
- Azure EU Region #2 – Netherland
- Amazon - 2 vCPU / 4GB RAM
- Azure - 2 cores / 3.5GB RAM

Storage Pricing Comparison – Azure and Amazon

Data Center Location	Amazon - Storage (500TB)	Azure - Storage (500TB)
Japan	$0.0313 per GB	$0.0228 per GB
Australia	$0.0313 per GB	$0.0251 per GB
Singapore	$0.0285 per GB	$0.0228 per GB
EU Region #1 - Ireland	$0.0285 per GB	$0.0228 per GB
EU Region #2 - Varies	$0.0308 per GB	$0.0228 per GB
Brazil	$0.0387 per GB	$0.0309 per GB
US West	$0.0285 per GB	$0.0228 per GB
US East	$0.0285 per GB	$0.0228 per GB

This table compares S3 storage on Amazon and Locally Redundant Storage (LRS) on Azure

- Azure EU Region #2 – Netherland
- Amazon EU Region #2 – Frankfurt

Network (traffic) Pricing Comparison – Azure and Amazon

Traffic	Amazon – DNS Query	Azure – DNS Query
First One Billion Queries / month	$0.700 per million queries	$0.540 per million queries
Over One Billion Queries / month	$0.350 per million queries	$0.375 per million queries

Traffic	Amazon – Health Check	Azure – Health Check
Internal	$0.50 per health check / month	$0.36 per health check / month
External	$0.75 per health check / month	$0.54 per health check / month

Health check is a process by which network traffic is sent to check if an instance or node is active. This is required in order to setup load balancing and high availability.

Data Center Location	Amazon – Gateway	Azure - Gateway
Japan	$0.062 per hour	$0.036 per hour
Australia	$0.059 per hour	$0.036 per hour
Singapore	$0.059 per hour	$0.036 per hour
EU Region #1 - Ireland	$0.048 per hour	$0.036 per hour
EU Region #2 - Varies	$0.052 per hour	$0.036 per hour
Brazil	N/A	$0.036 per hour
US West	$0.045 per hour	$0.036 per hour
US East	$0.045 per hour	$0.036 per hour

A gateway is a network point that acts as an entrance to another network. It enables the end users to access the system over the internet or enable a hybrid cloud system. This table compares a NAT Gateway in a VPC on Amazon and basic VPN or ExpressRoute Gateway on Azure.

7 Glossary

The following terms appear in this document and in the assessments.

Category	Term	Definition
General	Multitenancy	The concurrent use of shared computing resources by multiple users, also known as tenants
General	Private Cloud	A private cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple users (i.e. departments). It may be owned, managed, and operated by the organization, a third party, or some combination, and it may exist on or off the premises.
General	Public Cloud	A public cloud infrastructure is provisioned for use by any organization that wishes to pay for computing resources. It may be owned, managed, and operated by a business, academic institution, government organization, or some combination. The infrastructure exists on the premises of the cloud provider rather than the users.
General	Hybrid Cloud	A hybrid cloud infrastructure consists of two or more distinct cloud infrastructures (private, community, or public) that remain separate, but are bound together by standardized or proprietary technology which enables data and application portability. Normally, it is a combination of public and private.
General	Community Cloud	The community cloud is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (i.e., 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.
General	IaaS	Provides the capability to request (provision) processing, storage, networks, and other fundamental computing resources, but the requester is able to deploy and run anything they want, including operating systems and applications.
General	PaaS	Provides the capability to deploy onto the cloud infrastructure, consumer-created or owned applications created using programming languages, libraries, services, and tools supported by the provider.
General	SaaS	Provides the capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either an interface, such as a web browser (i.e., web-based email), or a program interface (i.e. Office 365). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.
General	High Capacity Link	Also known as an internet gateway, this is a primary or backbone link outside of a country to the Internet.
General	Internet Service Provider (ISP)	An organization that provides services for accessing, using, or participating in the Internet.
General	Public server	A server that is owned by a third party and accessible via a public network, such as the internet (i.e. AWS or Azure).

Category	Term	Definition
Application	Criticality	**Critical** - the application cannot afford to have more than 2 hours of downtime and there is no alternative for this application. Also, application that is classified as 'critical' by internal policy **High** - the application cannot afford to have more than 4 hours of downtime and there is alternatives for this application (i.e. manual entries) **Moderate** - the application can cannot have more than 12 hours of downtime **Low** - the application can have more than 24 hours of downtime
Application	Single Tier	Single tier, sometimes called one-tier, architecture involves putting all of the required components for a software application or technology on a single server or platform. The alternative is multi-tiered architecture or the three-tier architecture that is used for some web applications and other technologies where various presentation, business and data access layers are housed separately.
Application	Static Attribute	Any source code component that has been hard coded (i.e. hard coded IP address and hostnames).
Data	Personally Identifiable Information	Personal information is data that can be used to identify the individual (i.e. name, passport number, phone number).
Data	Sensitive data	Sensitive data refers to data that is deemed sensitive by the owner of the data (i.e. classified government documents).
Data	User Information	User information is data that belongs to an individual but cannot be used to identify them without additional information (i.e. ID, position).
Functional	Service Level Agreement (SLA)	An agreement that sets maximum or minimum targets for various metrics. For example there may be a service level agreement in regards to how quickly technology support must respond to defects of various severities.
Infrastructure	Demilitarized Zone (DMZ)	A physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet.
Infrastructure	End of Service (EOS)	The expected retirement date of a server based on internal policy or other methods.
Infrastructure	Input / Output Operations Per Second (IOPS)	A common performance measurement used to benchmark computer storage devices such as hard disk drives (HDD), solid state drives (SSD), and storage area networks (SAN)
Infrastructure	Virtual Machine (VM)	An emulation of a particular computer system. Operates based on the computer architecture and functions of a real or hypothetical computer, and its implementations may involve specialized hardware, software, or a combination of both.
Technical Architecture	Central Processing Unit (CPU)	The electronic circuitry within a computer that carries out the instructions of a computer program by performing the basic arithmetic, logical, control and input/output (I/O) operations specified by the instructions.
Technical Architecture	Horizontal scaling	Ability of an application to function across multiple instances or nodes.
Technical Architecture	Vertical scaling	Ability of an application to take advantage of additional computing power, when added (i.e. CPU, memory).

Category	Term	Definition
Technical Architecture	Hypervisor	A piece of computer software, firmware or hardware that creates and runs virtual machines. Sometimes called a virtual machine monitor (VMM).
Technical Architecture	Loose Coupling	Refers to designing a system in which each of its components has, or makes use of, little or no knowledge of the definitions of other separate components.
Technical Architecture	Random Access Memory (RAM)	A form of computer data storage. Stored information is lost if power is removed (computer is shut down).

8 Assessment References

Cannon, N. (2014). *Key Skills Needed for Successful Deployment of Cloud Computing in Government.* Stamford: Gartner.

Galexia Consulting. (2013). *Global Cloud Computing Scorecard.* Retrieved from BSA The Software Alliance: http://www.bsa.org/~/media/Files/Research%20Papers/GlobalCloudScorecard/BSA_Global%20Cloud%20Scorecard_021113.pdf

Kyle Hilgendorf, A. D. (2015). *2016 Planning Guide for Cloud Computing and Virtualization.* Stamford: Gartner.

9 Report References

Microsoft. (2011). *Business Agility and the Cloud.*

Neville Cannon, G. A. (2015). *Government CIOs See Expected Cloud Cost Savings Evaporate.* Stamford: Gartner.

Pham, T. (2011, September 15). *Benefits of Private Cloud Computing: Compliant & Cost-Effective*. Retrieved from Online Tech: http://resource.onlinetech.com/benefits-of-private-cloud-computing-compliant-cost-effective/

Rodier, M. (2011, May 18). *Speed-to-Market Is Biggest Benefit Of Cloud Computing*. Retrieved from InformationWeek WallStreet & Technology: http://www.wallstreetandtech.com/infrastructure/speed-to-market-is-biggest-benefit-of-cloud-computing/d/d-id/1264839

Savvas, A. (2014, May 14). *The benefits of hybrid cloud computing*. Retrieved from ITProPortal: http://www.itproportal.com/2014/05/14/the-benefits-of-hybrid-cloud-computing/

U.S. Department of Commerce. (2011, September). *The NIST Definition of Cloud Computing.* Retrieved from National Institute of Standards and Technology: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

10 Participants and Reviewers

Many individuals were involved in creating and reviewing the toolkit and this report. In addition, many individuals in Serbia, the Philippines, and Zambia participated through interviews, discussions, and feedback during presentations. As many of these individuals as possible are captured in this section.

10.1 Serbia

The individuals listed in the table participated in the interviews and presentations in Serbia.

Group	Name	Role
Additional Contacts	Borislav Srdić	
Additional Contacts	Irena Cerovic	Portfolio Manager at UNDP
Additional Contacts	Jelena Manic Petronikolos	
Additional Contacts	Jelena Tatomirovic	Coming, Network and Security Engineer
Additional Contacts	Marko Filipovic	MS, Serives Delivery Lead
Additional Contacts	Milan Vujovic	Coming, Network and Security Engineer
Additional Contacts	Miroslav Pevac	
Additional Contacts	Radoje Gvozdenovic	
Additional Contacts	Tomislav Ranđić	
Additional Contacts	Vladimir Milosevic	IBM Architect
Additional Contacts	Vladimir Radunovic	Cybersecurity Expert
Directorate for e Government	Dusan Stojanovic	Director
Directorate for e Government	Marija Kujacic	Head of Department
Directorate for e Government	Marija Laganin	PR Advisor
Directorate for eGovernment	Rade Dragović	Head of Department for Development and Standardization
Environmental Protection Agency	Dejan Lekic	Director
Environmental Protection Agency	Elizabeta Radulović	Director of Information System
Environmental Protection Agency	Nikola Pajcin	
General Secretariat	Petar Janjic	Assistant Secretary General of the Government
Institute of Public Health	Dr Ivan Ivanović	Head of Department of Informatics & Biostatistics
Korean Embassy	Hongsik Kim	Korean Embassy / 1st Sec
Korean Embassy	Kichang Park	Korean Embassy / Minister Counselor
Medicines and Medical Devices Agency of Serbia	Igor Pasic	System Administrator, IT engr.
Medicines and Medical Devices Agency of Serbia	Igor Vanevski	M.Sc, grad. Mech. Engineer
Medicines and Medical Devices Agency of Serbia	Tatjana Stojadinovic	Ph.D., IT Group Manager
Ministry of Interior	Dr. Predrag Djikanovic	Assistant Head of Sector
Ministry of Interior	Duško Sivčević	
Ministry of Interior	Goran Perunicic	Assistant Head of Sector
Ministry of Interior	Slobodan Nedeljkovic	Head of Sector, Assistant Minister for Analytics and ICT
Ministry of Public Administration and Self-Government	Dražen Maravić	

Group	Name	Role
Ministry of Public Administration and Self-Government	Irena Posin	Assistant Minister
Ministry of Public Administration and Self-Government	Jovana Vlaškalin	
Ministry of Trade, Tourism and Telecommunications	Dr. Irini Reljin	Head of MTTT, Professor
Ministry of Trade, Tourism and Telecommunications	Zlatko Jelisavcic	Head of Department for Information Society Development
Office of Prime Minister	Ana Šarenac	Prime Minister's Delivery Unit
Office of Prime Minister	Gregor Virant	Prime Minister's Delivery Unit
Personal Data Protection	Lela Rudic	Personal Data Protection
Personal Data Protection	Rodolijub Sabic	
Public Investments Management Office	Sandra Nedeljković	Public Investment Management Office
Public Policy Secretariat of the Republic of Serbia	Djiana Ilic Zogovic	Senior Expert Advisor, Head of Group
Public Policy Secretariat of the Republic of Serbia	Jasna Atanasijević	Director
Public Policy Secretariat of the Republic of Serbia	Siniša Barjaktarević	Senior Expert Advisor
RATEL	Aleksandra Stefanovic	Public and International Relations
RATEL	Nemanja Vukotić	
RATEL	Vladica Tintor	Director
Republic Geodetic Authority	Borko Drašković	Director
Republic Geodetic Authority	Dragan Bogdanović	Head of Department (Info. & Comm.)
Republic Geodetic Authority	Veselin Bakic	
Serbian Business Registers Agency	Branislav Dobrosavljevic	Data Services Manager
Serbian Business Registers Agency	Zvonko Obradovic	Director
Telekom Srbija	Borko Crnogorac	Sales & Marketing Director - SME
Telekom Srbija	Jelena Petrovic	Manager of the Department for Sale to Public Admin.

10.2 Philippines

The individuals listed in the table participated in the interviews and presentations in the Philippines.

Group	Name	Role
Advanced Science and Technology Institute	Bayani Benjamin Lara	Supervising S/R Specialist
Advanced Science and Technology Institute	Denis Villorente	Deputy Executive Director for e-Government
Advanced Science and Technology Institute	Jessi Rubio	
Advanced Science and Technology Institute	Jelina Tetangco	
Bureau of Internal Revenue (BIR)	Carolyn Ann Reyes	
Bureau of Internal Revenue (BIR)	Jocelyn Zabala	
Construction Industry Authority of Philippines (CIAP)	Angelina F Tajon	
Construction Industry Authority of Philippines (CIAP)	Lady Laput	

Group	Name	Role
Construction Industry Authority of Philippines (CIAP)	Lorina S Laurequez	
Construction Industry Authority of Philippines (CIAP)	Sonia T. Valdeavilla	Executive director
Department of Budget and Management (DBM)	Christopher Kuzhuppilly	
Department of Budget and Management (DBM)	Gladys Abellano	OCIO
Department of Budget and Management (DBM)	Mary Jane O. Eucos	OCIO
Department of Budget and Management (DBM)	Michelle Arianne Manza	Executive Assistant, Office of Undersecretary & Chief Information Officer
Department of Budget and Management (DBM)	Richard Moya	Undersecretary
Department of the Interior and Local Government (DILG)	Kieth P. Lagmay	
DOST-ICTO	Toni Torres	Project Manager, i-Govt, ICTO
Environmental Management Bureau (EMB)	Consolacion Crisostomo	
Environmental Management Bureau (EMB)	Herburt Narisma	
Environmental Management Bureau (EMB)	Lexter Maymay	
Environmental Management Bureau (EMB)	Sharmaine Tayco	
Information and Communications Technology Office	Juli Ana E. Sudario	Project Manager, MITHI
Information and Communications Technology Office	Maria Teresa Magno-Garcia	Director
Philippine National Police (PNP)	Felizanrdo Eubra Jr.	Head of Cyber Security
Philippine National Police (PNP)	Mr. Ferrancullo	
University of the Philippines	Rommel P. Feria	
University of the Philippines	Vic Angelo D.S. Mamaril	

10.3 Zambia

The individuals listed in the table participated in the interviews and presentations in Zambia.

Group	Name	Role
CEC Liquid	Kauba Kalungombe	Legal Counselor
CEC Liquid	Marjorie Nalubamba	Chief Sales and Marketing
CEC Liquid	Mwizu Sikanyika	CTO
Centre of Excellence for e-Government and ICT	Dr. Felix Phiri	Director
Centre of Excellence for e-Government and ICT	Chibala	
Centre of Excellence for e-Government and ICT	George Mbasela	
Centre of Excellence for e-Government and ICT	Godfrey Chinyama	Senior Analyst
Centre of Excellence for e-Government and ICT	Joyce Chipwepwe	Acting Head/CPT
Centre of Excellence for e-Government and ICT	Kaluba Shiliya	
Centre of Excellence for e-Government and ICT	Stanley Phiri	Senior Analyst
Ministry of Community Development and Social Welfare	Noel Masese	Assistant Director - ICT

Group	Name	Role
Ministry of Finance	Boyd Lumbwe	Budget Office
Ministry of Finance	Percy Musona	Principal Budget Analyst
Ministry of Health	Virginia Simushi	
Ministry of Health	Chisanga Siwale	
Ministry of Transportation and Communication	Austin Sichinga	Department of Communication
Ministry of Transportation and Communication	Beaton Sibulowa	Department of Communication
Ministry of Transportation and Communication	Nkula Mwanza	Department of Communication
Ministry of Transportation and Communication	Yese Bwalya	Director, Department of Communications
MTN	Clukondi Mwanza	
MTN	Komba Malukufila	
MTN	Linliwe Banda	
MTN	Lubinda Mulikelela	
MTN	Mark Townsend	
University of Zambia	Christine W. Kanyengo	Universty Librarian
University of Zambia	Collins C. Kachaka	Director of IT
University of Zambia	Francina N. S. Makondo	Deputy University Librarian
Zambia Revenue Authority (ZRA)	Daniel Kalunga	Network
Zambia Revenue Authority (ZRA)	Davies Chansa	Senior IT Officer
Zambia Revenue Authority (ZRA)	Enos Ngoma	Business Admin
Zambia Revenue Authority (ZRA)	Halusaka Hamwalla	Assistant Director - IT
Zambia Revenue Authority (ZRA)	Perry Chikwama	Senior IT Officer
Zambia Revenue Authority (ZRA)	Winter Msukwa	System Development
Zamtel	Albert Salima	CIO
Zamtel	Clive Mutentwa	IT Infrastructure Manager
ZESCO	Allan S. Kashimi	
ZESCO	Anthony N. Mwange	Senior Manager
ZESCO	Charity K. Chola	
ZESCO	Mary Chitembo	
ZESCO	Victor Chisemele	
Zambia Information and Communication Technology Authority (ZICTA)	Bernard Banda	
Zambia Information and Communication Technology Authority (ZICTA)	Choolwe Nalubamba	
Zambia Information and Communication Technology Authority (ZICTA)	Elliot Kabalo	
Zambia Information and Communication Technology Authority (ZICTA)	Margaret Muaewda	Director General
Zambia Information and Communication Technology Authority (ZICTA)	Patric Mutimushi	

10.4 Toolkit Reviewers

The individuals listed in the table reviewed the toolkit prior to the start of the pilots.

Name	Company	Role	Reviewed	Country
Dr. Seunghyun Kim	World Bank	Project Manager	Toolkit	USA
Samia Melhem	World Bank	Project Lead	Toolkit	USA
Young Jin Choi	World Bank	Subject Matter Advisor	Report	USA
Clay Lin	World Bank	Subject Matter Advisor	Report	USA
Roman Lerman	Accenture	Subject Matter Advisor	Toolkit	USA
Amanda Jensen	Accenture	Project Manager	Toolkit	USA
Gregory Scheaffer	Accenture	Project Consultant	Toolkit	USA
Anantha Ramadas	Accenture	Cloud Application Transformation Senior Manager	Toolkit	USA
Timothy Aultman	Accenture	Cloud Application Transformation Manager	Toolkit	USA
Chris Scott	Accenture	Lead for Accenture Amazon Business Group	Cloud Comparison	USA
Dominic J. Delmolino	Accenture Federal Services	Managing Director, AFS Infrastructure Agility (Cloud and DevOps)	Country Assessment	USA
Sigurd Myhre	Accenture	IT Strategy	Application Assessment	Norway
Chan Lee	Duzon	President of the Security Division	Toolkit	Korea
Inhyun Bark	Duzon	Senior Analyst	Toolkit	Korea
Jay Lee	Duzon	Subject Matter Advisor	Toolkit	Korea
Nuri Lee	Duzon	Subject Matter Advisor - Cloud Expert	Toolkit	Korea
Dr. Jong Whoi Shin	Microsoft Korea	National Security Officer	Toolkit	Korea
Kyung-ho Son	Korea Internet and Security Agency (KISA)	R&D Center Director	Toolkit	Korea
Dr. Wan S. Yi	Korea Internet and Security Agency (KISA)	Internet Industry Division Director	Toolkit	Korea
Jungjoo Lee	National Information Society Agency (NIA)	Subject Matter Advisor	Toolkit	Korea
Legal	Microsoft	Representative from Legal Team	Toolkit	
Policy	Microsoft	Representative from Policy Team	Toolkit	
Kaja Ciglic	Microsoft	Senior Cybersecurity Strategist at Microsoft	Country Assessment	USA
Stevan Vidich	Microsoft	Azure Expert	Cloud Comparison	
Steve Mutkoski	Microsoft	Government Affairs Director, Microsoft Worldwide Public Sector	Toolkit	
Zaki Khoury	Microsoft	Regional Director - International Organizations - Middle East & Africa	Toolkit	

10.4 Report Reviewers

The individuals listed in the table reviewed this report.

Name	Company	Country
Dr. Seunghyun Kim	World Bank	USA
Samia Melhem	World Bank	USA

Reg Miller	World Bank	USA
John Savageau	World Bank	USA
Natasha Beschorner	World Bank	USA
Oleg Petrov	World Bank	USA
Roman Lerman	Accenture	USA
Amanda Jensen	Accenture	USA
Gregory Scheaffer	Accenture	USA