A Public Manager’s Guide to Cloud Computing

Jared Drake
Management
Senior
May 2012

Faculty Mentor – Terry Usrey
Abstract

Before the dawn of cloud computing, government agencies depended on their internal IT staff for their technological projects or gambled by outsourcing the projects to private corporations. In the early 2000s, the Federal Bureau of Investigations invested a very large sum of money into virtualizing their case files by outsourcing the project to a new technology corporation. With the lack of proper project management, the project failed miserably and created serious backlash in a majority of the government agencies against outsourcing any information technology projects.

After a few more large public investment failures in outsourcing IT projects, the governments developed a negative attitude towards outsourcing any IT projects. However, ten years later, our governments are reviewing their budgets due to the financial crisis. Looking to reduce costs and improve productivity, cloud computing appears to be an attractive option. Cloud computing offers many benefits including an increase in productivity, cost reduction, improved cooperation/collaboration, and much more.

However, a manager must also consider the costs of switching to the new technology. It is also important to note that cloud computing is not exactly a term one can define with ease. Cloud computing, simplified, is a term to reference many different possible outsourced IT processes. A comprehensive review of the pros and cons of cloud computing in addition to the possible legal and ethical issues is necessary before converting their IT processes to the cloud.

While many agencies are resistant to change, the framework toward outsourcing IT processes has been laid and hesitant agencies will soon have to embrace the power of this new technology in order to survive in a more accountable government structure. I will examine a few agencies that have successfully transferred some of their IT processes to cloud computing, and a few that encountered various problems along the way. By understanding cloud computing and reviewing how other government agencies successfully switched to cloud computing, managers can utilize its power to cut costs and boost productivity in their organizations.
Introduction

How can a public manager cut costs and improve the productivity of their organization? One possible way a manager can do this is by considering the implementation of a relatively new private sector driven technology called cloud computing. Cloud computing is technology that has the potential to greatly reduce Information Technology (IT) expenses. Agencies can also utilize the collaboration and centralization that cloud computing offers to improve productivity. However, the new technology could have severe disadvantages when dealing with the public's confidential information. A public manager must consider the advantages, disadvantages, and possible legal issues that might arise from this new technology before fully embracing a switch to cloud computing.

Definition and Explanation

What exactly is this great new technology called cloud computing? “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” (National Institute of Standards and Technology, 2011). Cloud computing can link all electronic devices together allowing them to be accessed by each device at any given time. The cloud takes all of those shared files and places them in a centralized location, a collection of servers as depicted in Figure 1. After implementation, any user that has a computer/device with a network connection and privileges to access the files can access them. In order for this resource sharing
To the Cloud 3

service to be successful, some cloud services use a piece of the software to automatically synchronize data on each device. The synchronization that occurs eliminates the problem of outdated versions, and stops users from working on different versions of the document. (IBM)

To understand what exactly cloud computing offers with respect to storage, an individual should examine a business that is offering this service for free. One of the leading businesses for individual cloud storage is Dropbox, and they offer cloud computing storage of up to 2GB for free. Dropbox has an application that an individual can install on any device (shown in Figure 2) such as a laptop, desktop, smartphone, tablet, etc. The application uses an individual’s internet connection to dropbox.com to constantly search the individual’s devices for updated versions of a document. If the Dropbox application finds a newer version of the document, it will upload the document to dropbox.com and synchronize it to any of the individual’s devices as soon as those devices have access to the internet. (Dropbox)
Students working on a group project that requires the group to write a collaborative paper can utilize Google Docs to simultaneously work on the paper. Google Docs is one of the many cloud computing applications that Google has created to allow multiple individuals to work on a document at the same time. As soon as one user finishes typing a single word, Google Docs will save the file locally on its server and instantly update the document for any other users that are working on the document at the same time. (Google) Before Google Docs or any other collaborative cloud application allowed users to work simultaneously on a project, groups generally divided the project into sections and had each individual work on a different part. At the end of the project, one individual would compile the entire paper, but with Google Docs, all of the individuals can write and review the entire paper concurrently without interruption. (Google)

Cloud applications are virtually endless with large corporations, like Microsoft, Google, Apple, and Amazon beginning to focus on developing cloud applications. Microsoft has even begun cloud application packages such as Office 365, which allows an individual to have a virtual office from anywhere they have an internet connection (Microsoft). Amazon has developed Amazon EC2 that allows users to put any application online and run the application virtually, instead of installing the application on every single computer (Amazon). Figure 4 (located at the end of this document) demonstrates the vast scale of private businesses creating various types of cloud based applications. The number of cloud computing applications is increasing at a rapid rate, and managers must understand that these applications just might be the future of IT services. Of course, it is important to understand that all of these applications are only a
third of what constitutes cloud computing. The other two thirds are comprised of platforms and infrastructure. Cloud applications like Dropbox and Google Docs offer many benefits, but it is essential to recognize the other services that the cloud offers. Later in the NIST section, the other services will be discussed.

**Analysis Pros and Cons:**

**Pros:**

One of the greatest benefits of cloud computing is that there is no large initial investment or maintenance costs other than the bandwidth to use it and monthly charges. In the early 2000s, the Federal Bureau of Investigations (FBI) invested a very large amount of money in a corporation to build an application that would allow FBI’s employees to have access to their cases virtually on the employees’ computers (Mueller). However, the project failed miserably because of poor project management. While the whole idea that project management must be improved in government is valid, cloud computing already has established applications that organizations can trial before investing an enormous sum of money into that project.

Many government organizations have their own servers, applications, and networks already created, but they have considerable restrictions. Unlike the cloud, governments traditionally had to purchase new servers and other technologies if they need to handle more information or simply need to use new applications. Normally, an organization would purchase more servers to keep up with the increasing vast amounts of information, but the cost of servers, maintenance, power, and the building for the server’s home will quickly strain the agency’s budget (Microsoft). Cloud computing, on
the other hand, is much more scalable. If an organization has an immediate need to increase their storage, the organization just needs to notify the company, rather than having to purchase new servers that can take up to 6 weeks (Dell).

The cloud allows for easier and quicker improvements. Using a government private network, which are currently being used extensively instead of cloud computing, does have the ability to share files in order to allow for a flow of information and collaboration between users. However, this type of network sharing still lacks the easiness of the cloud. The cloud allows for users to work on the same file at the same time, unlike private networks. A private network is similar to Dropbox, in the sense it allows you to share files with other network users, but the private network is limited by the usability.

Without cloud services, it is very common for users working on a project to have multiple versions of the project. Having multiple versions of a project can lead to backtracking because an individual might update an old version of the file, but neglect to update the newest version. The cloud allows for files to be automatically updated to the most recent version of the file. An employee can actually work on a project from a tablet computer, save the file, and then access the file at the same state on their desktop without losing any of the work (Microsoft). Cloud computing is designed for efficient file-sharing between users, computers, and networks.

Another benefit of cloud computing is the corporate world’s ability to innovate. Why should the government invest in the risk of hiring a company to build cloud service applications when corporations are already creating and taking the risks of cloud
computing? The government can test the cloud computing services before entering into a long term deal, which eliminates most of the risk of cloud computing. Corporations will continue to make technological advances in technology in order to stay ahead of their competition. A government organization can decrease the risk of failure by investing in cloud computing applications that are already created by a corporation, rather than hiring a software developing company to build them a new application. A government organization that is focusing less on IT Infrastructure and more on their core mission is a more effective government entity.

The final benefit for transferring to cloud computing is the ability for an organization to back up all of their data. Cloud computing allows organizations to store all of their data in an external location. It is very possible that an organization could have a natural disaster or a fire destroys all of their servers, thereby, destroying all of their data. However, if an organization also stored their data at a different location by using cloud computing, they could easily retrieve the data and alleviate many headaches. The concept classified as Automatic Disaster Recovery is an invaluable tool when dealing with public information disasters (Kundra, “Federal Cloud Computing Strategy”).

Cons:

While there is no large initial costs, cloud computing services will sometimes require more bandwidth for the corporation to utilize it. It is important to note that this requires dependency on this new bandwidth. Increased bandwidth will increase the monthly expenditure to the internet service provider and might be significant for the smaller government organizations to reconsider moving to the cloud. The cloud uploads
or downloads every file any time the file is updated from each individual computer, which can quickly result in increased bandwidth usage (Mell, and Grance). If a manager is considering cloud computing, the manager should be prepared to modify the budget to devote more money to their internet service provider for the increased bandwidth that cloud computing requires. While modifying the budget, the manager may also want to note that benefits, such as less hardware and software maintenance and overhead costs might counteract this negative.

As for the implications of cloud computing on a public organizations budget, a public manager needs to realize that some businesses offering cloud computing do so on a “pay as you go” type system. This system can be very dangerous for a government organization that has absolutely no idea how much it will use cloud computing. It is difficult to create a budget for an expense if they manager has no idea how much their cloud computing expenses will be per month (Mell, and Grance). However, some companies offer cloud computing on a standard fixed contract that would complete eliminates this disadvantage.

Any new technology that is introduced into an organization, there is always an associated cost. Employees must adapt and learn how to use cloud computing, and educating them can cost the organizational a considerable amount of time and resources. If the company or agency did not invest in this new technology, they wouldn’t have to spend the time and resources educating a workforce. (Kundra, Federal Cloud Computing Strategy).
By far, the biggest concern with cloud computing is the security aspect. Government organizations deal with a great deal of information and a considerable amount of the information is confidential information that the public would rather keep private. In many cases, this is actually a legal mandate. The privacy and security of public sector data is dictated by law, but that could be much more complicated to enforce with cloud services. While the openness of cloud computing seems to be in advantage in the field of collaboration, it also puts more information on the internet. With all of that information on the internet, it is much more susceptible to hackers and information leaks to the public (Nelson). However, if the data was only internally accessible on an agency server, the data would less susceptible to hackers and information leaks.

**Evaluation of Pros and Cons**

While there are many great advantages with cloud computing and fewer disadvantages, the disadvantages are very important to consider. If the security of the data becomes compromised, a public agency may very well find a disapproving public and a substantial lawsuit. Organizational change has never been an easy implementation process, especially when the individuals might require training for the change to be successful. If an agency is not carefully monitoring its usage of the cloud services, the agency could possibly have an expense that is not in the budget. The increased demand for bandwidth as required by cloud services could also break an organization’s budget if not properly prepared and create dependence. Security of the data, organizational change, payment based on usage, and increased demand for bandwidth are issues that are not to be taken lightly.
Even with such great disadvantages, the advantages of cloud computing cloud still defeat the disadvantages if it suits the agency’s needs. The increased collaboration offered by cloud computing might be enough itself to legitimize the switch to cloud computing. When looking into the future, cloud computing’s benefits of scalability and synchronized maintenance would definitely reduce costs and labor, while not having cloud computing would only increase these costs. Agencies work with extremely important information, and to protect that information, organizations can use cloud computing as an external storage mechanism to be able to restore data in the event of an unfortunate situation. Cloud computing has a vast number of benefits, but these benefits should be analyzed, by the agency, against the disadvantages cloud computing creates.

**Potential Problems and Solutions**

If and when government agencies decide to make the leap to cloud computing, the public sector will experience many new legal issues. While many legal issues may arise, the primary concern is the security of the public’s data. The government is currently responsible for the information gathered from the public. With cloud computing, private businesses will be contracted to be responsible for the public’s data, but what happens if the private businesses lose the data or files for bankruptcy, while selling the servers with the confidential information on them?

Pilot Networks, which was a corporation specialized in secure web hosting, recently went out of business and many customers simply lost their data. It is worth mentioning that even courts cannot demand businesses to reproduce data that the
private businesses might have already lost (Asprey). If the information is lost, it is lost; therefore, the best way to stop lost data is prevention. Prevention can take a variety of forms ranging from using local backup servers to storing the information with another company to lessen the risk (Asprey). While lost data is a possible problem with cloud computing, a preventive strategy created in collaboration with the agencies technical experts can reduce the risk of losing data.

Private businesses are also responsible for the protection of the public’s data, but what happens when the information becomes compromised by a hacker? Hacking has been around since the beginning of computer networks, which is exactly what cloud computing requires. Hackers groups such as Anonymous and LulzSec have demonstrated the willpower and intelligence that certain hackers now possess. How can a government protect the public information when the information is contained online, where advanced hackers have the capability to steal that information? The government will be responsible from the public’s viewpoint, but the government must impose regulations on the contractor to enforce strict protocols, which is discussed later.

One might easily argue that cloud computing’s greatest disadvantage is the inadequate security that modern cloud computing technology provides. However, one should consider the relative respect of security when compared to the current “noncloud computing” that agencies currently employ. In fact, in September of 2007, one of the United States’ most secretive agencies, the Department of Defense, was hacked by a certain group that they believe was China. (FOXNews). As clearly demonstrated, it seems apparent that data cannot always be secured and that information security is an ongoing process.
National Institute of Standards and Technology

According to the Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB), policy for preventing security issues with cloud computing have already been implemented. With a significant amount of time and resources invested into these policies, they are solid foundational base for any agency that is thinking about outsourcing certain IT processes to begin their own research. A multitude of publications by National Institute of Standards and Technology (NIST) publications have impacted the majority of the policies implemented by FISMA and OMB. To put it simply, government organizations in the United States rely on the NIST’s database of IT security knowledge for protection.

Surprisingly, NIST was created in 1901 by Congress as the federal government’s first physical science research laboratory (National Institute of Standards of Technology). The primary principal the establishment of NIST was the lack of competent measurement system for industrial infrastructure. Germany, England, and many other economic rivals were excelling in developing foundational industrial practices, when the United States realized that America did not have an agency that supported any solid research to influence industrial practices. With the industries innovation surpassing anyone’s expectations, the regulating agencies were less than adequate to serve America’s need for safety with these new innovations.

Today, NIST has been consolidated and supervised by the United States Department of Commerce. With all of the industrial booms and creative commercial innovations in the past century, the ability for one agency to monitor all of these
processes is unimaginable. However, that is exactly what NIST does each and every day. From the smallest nanoparticle created in a laboratory to the structural resistance of our largest buildings against Mother Nature’s powerful forces, NIST has been writing documentation and advising government agencies based on their vast wealth of knowledge in innovation (NIST).

**NIST and the Internet**

The internet is a phenomenon that has changed the way everyone looks at technology. In the early 1900’s, if someone came up with a brilliant idea then obtained a patent, it could be years to decades before the product was integrated into society. However, the advancement the internet has had on communication has absolutely devastated this barrier to entry. Products offered online are almost impossible to regulate to the endless supply of producers and the vastly reduced costs of production and marketing. How can NIST regulate each and every product on the internet? Put simply, NIST cannot regulate every product.

Another predicament the internet has placed on the table is the issue of “nonexclusion”. When patents were developed in the 20th century, the person with the patent was generally deemed to have the most knowledge in the area. With billions of people around the world having access to the internet, the knowledge of how the internet works is probably much higher than the number of people who knew how to build a car. But what is the negative consequence of that many people understanding how the strongest communication system in the world operates? With just a single insecurity in a government’s technology infrastructure, it can be exploited exponential by
the number of people on the internet. It is like trying to keep a secret while having to 
scream in a quiet yet crowded room. Because of these very reasons, NIST has 
changed its model of operations from testing products to crafting idealistic frameworks 
and researching/developing best practices for adoption of new technologies (Bowen 1- 
5).

**NIST Policy Overview**

The purpose of the NIST involvement in the outsourcing of Governmental IT was 
to ensure that the external organizations were adhering to the same policies and 
procedures as the governments that previously handled those processes and 
information. External subsystems that store, process, or transmit federal information and related 
services are covered in the procedures set forth by the NIST. NIST acknowledges that policies 
and procedures alone are not sufficient to sustain the relationship between public and private 
with respect to handling important IT processes. Trust is crucial in this relationship, but 
sometimes, trust must be conceived only when the government is able to have a 
substantial amount of direct control on the private operating company that is handling 
the information. However, a trustworthy relationship between principle and agent can 
also be based on the duration of the working relationship (Joint Task Force 
Transformation Initiative Interagency). If a company has been aided the government 
organization in IT processes for many years, an excessive amount of direct control is 
usually not necessarily for the protection of the information.
Is Trust Really the Solution?

Why is trust so important when it comes to outsourcing any process and especially a process that has confidential information? When a government organization is outsourcing any process, they are held liable for the contracted work of that outsourced company. Obviously, a tremendous amount of trust is required by the government with the outsourced company. Outsourcing requires trust because another outside organization is doing the operations that the fails in the responsibility of the government that is doing the outsourcing. If governments did not trust their contracted agents, outsourcing would cease to exist, and governments would never be able to reap the rewards of the process.

Literally speaking, it impossible to prevent everyone from doing harm including the employees of the agency. That is to say, if an employee from outsourcing agency’s really wanted to gain a substantial profit by selling confidential information to a foreign country, it would be very difficult for the government to prevent. A government sometimes has to trust the contracted agency with the delicate information or process. Nevertheless, a government should attempt to implement policies within that agency and advise security procedures for the procurement of the documents, which is precisely why the NIST has formulated the frameworks for cloud computing.

Trust: It’s Complicated

Trust is a fundamentally complicated concept in the first place, let alone when the specifics of the issue reside in “net-centric architectures”. Many factors contribute to the difficulty to reach an agreement of trust. With respect to goals of the entities,
Governments focus on the interest of the people, while private companies focus on their stockholders. Of course, this inevitably means that the agencies employed by governments will continue to invest in their infrastructure to maximize future gains, which means that their systems generally are subject to change. The rapid changes require trust on the government’s side because the change is so rapid that a government might not have time to understand the change in information systems that are holding the confidential information (Joint Task Force Transformation Initiative Interagency). Governments maintain confidence in their own organizations because they are comprised of individuals with advanced educations that understand the information that they handle. The rapid change puts the government in the odd situation of not understanding the information systems and practices guarding their information.

The internet is extremely complex.. An individual cannot simply put their finger on where the internet resides or what exactly constitutes it. The same is true with service and application software. The lines of responsibility are quickly blurred by what is owned by each agency. A contracted agency might be utilizing software or services of another company to serve some of its basic IT needs. For example, let’s say the Department of Defense has agreed to use the servers at company X. Company Y created the software and hardware that manages how users interact with the server, such as a router. On Company X’s servers is confidential information about thousands suspected terrorists. While Company Y sent out an update to its systems that accidentally causes their software to crash; therefore, the Department of Defense can no longer access the Company X’s servers. Is it the responsibility of Company X to find another way to deliver the Department of Defense’s information immediately? The complexities of
outsourcing IT services via internet create a very delicate trust issue due to the fact the ownership is often blurred.

**NIST Framework**

While the NIST framework is somewhat vague, the principals crafted into it simplify a very sophisticated issue. For instance, how would NIST handle the situation with Company X? It wouldn’t have because the framework is focused on prevention not reaction. NIST embraces the idea of trust, but defined a framework to ensure that government agencies obtain the essential characteristics of cloud services (Foxwell 5-15). The essential characteristics are **required** if an agency decides to follow the framework.
Framework Essential Characteristics Definitions from NIST:

While all of the essential characteristics are crucial, “On Demand Self-Service” is arguably the most important. Governments must have access to any resource, memory, storage, network, hardware, software, etc. In addition to the resources, the government must also be able to utilize the cloud when needed, in order to maximize productivity while using the cloud. The ability to have self-provisioned access to cloud resources alleviates many of the issues surrounding ownership.
“Measured Service” is another very valuable essential characteristics. People require accountability on governments; therefore, governments must hold their contracted agents and service providers accountable. Measured service provides the capability to have a form of usage metrics for billing and chargeback purposes. The governments can use these metrics to only pay for what services and how much of the services they use. This characteristic also allows governments to avoid paying for services and equipment that are not being utilized because of downtime.

As time progresses, companies and people continuously find creative new ways to access the internet. The tablet and PDAs/smart phones are among the latest ways to access the internet while being extremely portable. “Broad Network Access” allows the government to cooperatively use all instruments that can obtain an internet connection to consume the clouds power. The increased collaboration from “Broad Network Access” is important for the government to be successful in an increasingly mobile world.

“Resource Pooling” is another valuable characteristic that is essential for cloud computing services. Government agencies might like to believe they are independent and powerful, but the truth of the matter is that they must work collaboratively with other agencies in order to serve their people. “Resource Pooling” allows multiple client organizations to share computing resources collectively or independently of each other. It is also great in the ability to manage the resources effectively. If agency A is only using 25% of the cloud services that it thought it would use and agency B began using 150% of its expected cloud resources, “Resource Pooling” would be completely compatible with this situation.
The final essential characteristic of the NIST Framework is “Rapid Elasticity.” It is a complement to the other essential characteristic, “Resource Pooling.” Because of this characteristic, even if both agency A and B used 150% of the cloud services they thought that they would require, the governments would still continue operations on the cloud as normal. The technical term demonstrated here is scalability, and it is a foundational stone in any IT infrastructure. If an organization crafted a system without the ability to scale up or down, it would fail miserably to meet the demands of change.

The NIST Framework is invaluable to future of governments’ IT processes and is critical to apply when considering to transfer services to the cloud. The structure of the framework is based on massive amounts of research done by NIST and other government organizations. Using the NIST Framework creates a proactive approach to cloud computing decision making by depending on essential characteristics to meet the specific needs from a cloud service.

**Successful Transfers to Cloud Computing**

Various organizations have already accepted and applied the NIST Framework to migrate services to the cloud. The Defense Information Systems Agency (DISA), the United States Department of Agriculture (USDA), and the Army Experience Center (AEC) have already successfully migrated to the cloud. While each of them utilized the NIST Framework, they also attribute other factors for their success. The following three organizations have derived many different benefits from switching to the cloud.
Defense Information Systems Agency

DISA is not an agency that one would normally expect to be leading the charge to cloud computing, but nevertheless, the benefits were far too great for them to sit on the sidelines. DISA plays a pivotal role in the Department of Defense by providing global infrastructure to American forces. DISA decided that its defense related computing needs were less than adequate; therefore, they investigated more options. Eventually, they came upon the solution of the Rapid Access Computing Environment (RACE). RACE is DISA’s own infrastructure-as-a-Service (IaaS) solution. As opposed to seeing their infrastructure from an asset management function, they were able to use the unlimited scalability of cloud services. With this new service, they opened the gates to application development, creating and testing hundreds of military applications dealing with satellites to convoy control systems (Department of Defense).

DISA believed that they were lacking efficiency, agility, and innovation, which is precisely what interested them into cloud computing. Due to the extreme importance of confidentiality in this agency, their primary concern was security. Their concern, as shown on the NIST Framework, led them to invest in a private IaaS solution. After migrating to the cloud, DISA claims to have surpassed their expectations in the areas of efficiency, agility, and innovation.

Innovation, as demonstrated above, was clearly an integral benefit derived from the switch. Having access to test and create hundreds of applications is the definition of innovation. However, this would not have been possible without improvements in efficiency and agility. They claim the improved efficiency came from being able to divide
demand into sub parts, which allowed them to remain productive even during peak times of production. In addition to productivity, the ability to provision resources and infrastructure reduces costs by not requiring them to invest time and capital into physically changing the infrastructure. Agility is highlighted by DISA because, as mentioned above in the pros of cloud computing, obtaining a dedicated server environment can take anywhere from 3 to 6 weeks, but with cloud services can less than a day (Kundra, Public Sector Cloud Computing Case Study: Army Experience Center”).

An important lesson to learn from DISA’s successful migration to cloud services is how they handled security. The NIST Framework collectively acknowledges security through its essential characteristics, it is explicitly stated how to handle additional security if an organization should require it. DISA crafted RACE with virtualization to segregate database, applications, and file residing servers. As referenced towards the beginning, virtualization permits one server to be separated and to function as if it was a collection of different servers. Using segregation as a security tool is an extremely valuable lesson when operating from hosted servers as it mitigates the risk of damage (Department of Defense).

After a successful transition, DISA now serves as a liaison for the Department of Defense (DOD) by aiding other DOD agencies into the cloud. DISA continues to actively monitor their cloud services and results, such as wait times for customers utilizing their services. While eliminating many costly IT positions in DISA, they made the decision to institute a new position of a demand manager, who is solely responsible for the monitoring of the results. DISA continues to reevaluate its position with cloud services,
which is a useful practice for any agency after an IT transformation (Department of Defense).

**USDA To The Cloud**

The USDA is the next agency that decided to empower the cloud. After a thorough review of its IT infrastructure and systems, they decided that communication and collaboration systems were less than adequate for their needs. They soon realized the true supremacy of the cloud’s ability to maximize productivity through advanced accommodating communication systems. Before the transformation, the USDA had 21 different email systems, which were difficult to maintain, let alone to use cooperatively. The cloud has an uncanny ability to consolidate what appear to be uncooperative processes. (Hickey)

To make matters worse for the USDA, every one of their 21 email systems were contracted and the applications were considered to be legacy systems. After several meetings and discussions, the USDA decided the cloud was the best plan of action. For USDA, the primary motivation to make the switch was the economic advantage it provides. By eliminating the legacy programs and consolidating the email systems, the USDA estimates that it is saving $6 million every year (Reuters). Of course, the competition between Microsoft and Google helped drive up the savings for the USDA, highlighting the importance of the capitalist advantage of outsourcing to the cloud.

Agility is also credited by the USDA because of its ability to scale up and down on their demand. Just to get an idea of the size of scalability cloud computing services can offer, USDA migrated 120,000 users to the cloud within a few months. To physically
achieve that feat with servers would have taken several years, and a sizable IT staff. An important, yet subtle, key factor, highlighted here, in deciding which company to trust is that company’s history. Microsoft has developed many applications that have shown to be secure and reliable for a number of years; therefore, their products have already been tested over time and have proven useful (Reuters).

Following the transformation of its email and other legacy applications into the cloud, the USDA changed their management attitude. Initially, USDA was concerned with the physical assets required to meet the demands of the organization, which confined them inside a box and caused setbacks in their service. Now, management proudly preaches their service-based attitude, and changes virtual assets with the click of a mouse. Like DISA, the USDA is continuously revisiting and monitoring their cloud services to understand the usage metrics their workforce and customers require (Smith). USDA is a very strong demonstration of the clouds power to consolidate resources, maximize productivity, and drive wasteful IT expenditures into the ground.

The Army Experience Center

The final organization to be discussed about cloud computing is the AEC. In 2008, the Army, an organization that obviously places a high value on security, evaluated the potential of switching. Interestingly, the Army considered the possibility of simply upgrading their current systems, which was priced comfortably around $1 million. However, the price estimate of the SaaS solution would be 90% less than upgrading their old ARISS system (Kundra, Public Sector Cloud Computing Case Study: Army Experience Center*).
Still not convinced the army evaluated the agility of the SaaS solution. Looking at their current ARISS implementation, it was practically impossible to provide regular updates to serve the needs of the AEC. While the AEC did not release a specific amount of time required to update the new SaaS, they gladly stated it was at a fraction of the time it would have taken to update the ARISS. The SaaS solution also was able to provide compatibility across a range of devices in real time to promote a much more advanced sense of collaboration (Kundra, Public Sector Cloud Computing Case Study: Army Experience Center”).

When the migration to the cloud started, the AEC did not hesitate to take a strong hand approach with emphasis on security. Since the new service is not exactly asset based, management changed their approach to aggressively deal with the contracted services. The AEC poured a mountain of time into crafting a trustworthy relationship with salesforce.com to devise a customized version of their application to meet the needs of AEC.

An excellent point is demonstrated by the AEC and salesforce.com relationship is the ability of contracted cloud services to be customized and tailored to the organization’s requirements. When an average person requests a service, they expect a few options, but those options are generally standardized, similar to a cell phone plan. On the contrary, the cloud is completely open to the organization’s expectations as long as that vendor can make such an adaptation. The top vendors of cloud computer are strong powerhouse technology corporations that have already created most of the commonly used applications, which can be used to the agencies advantage (Kundra, Public Sector Cloud Computing Case Study: Army Experience Center”).
Conclusion

Cloud computing is a relatively new technology that has a wide range of benefits that it can bring to an organization. Outsourcing servers and maintenance to a private organization can reduce technology costs for an agency. The increased collaboration and scalability offered by cloud computing would improve productivity and reduce future headaches. With all of these benefits and no large initial cost, it appears to make sense for a public manager to make the switch to cloud computing.

However, a manager must hesitate and consider the disadvantages before jumping into the cloud. Security is among the top concerns with respect to moving an agencies technological infrastructure to the cloud. Implementing the switch cloud computing can also cause serious human resource problems with the agency’s employees. An agency manager must also consider the legal implications of having outsourced confidential information.

Policies and suggestion are already in place by NIST and other agencies for any organization to utilize. NIST serves as a fundamental backbone for all new industrial and commercial technology advice to federal agencies. Managers should consider using the advice provided by NIST to make informed decisions about cloud computing. While NIST has provided a foundational structure, the NIST framework, to aid managers in making informed decisions about cloud computing, it is essential that organizations understand that there is and always will be an element of trust in their relationship with the outsourced cloud services company.
It is definitely not too late to jump on the cloud computing bandwagon. In fact, it is the perfect time to get on the bandwagon, since managers can see how others successfully migrated to the cloud. DISA needed more efficiency, agility, and innovation in their IT architecture. Using the power of the cloud in combination with virtualization, DISA was able to create one of the most praised IT systems in the entire federal government, RACE. The USDA was battling with inefficient legacy software that was hampering productivity and costing well more than it was worth. Cloud companies were able to consolidate the USDA’s old email systems to provide a more collaborative environment, while saving the USDA $6 million every year. Being very hesitant to outsource private information, the AEC performed a full evaluation of cloud services. Implementing a SaaS Solution allowed the AEC to maintain security, while increasing the compatibility of all devices that required AEC’s services. As demonstrated by the previous three agencies, it is possible to successfully outsource IT infrastructure and services to the cloud and obtain benefits provided by the cloud.

Before an agency embarks on its journey to the cloud, the public manager must decide whether cloud computing would be beneficial to the organization. If the manager believes cloud computing would benefit the organization and has performed a cost/benefit analysis, the manager should take advantage of the policies and frameworks put forth by other federal agencies, especially the NIST Framework. A manager should then communicate with the IT experts of the organization in order to formulate a strategy to counteract the information security and legal issues associated with cloud computing. The public manager must focus on preventative measures. Cloud computing can provide an agency with the desired benefits of reduced costs and
improved productivity if the appropriate strategy is implemented to counteract the disadvantages that can also be associated with cloud computing.
Works Cited


Figures