The Role of Enterprise Architecture in Federal Cloud Computing

Shared Interest Group: Enterprise Architecture

Release Date: January, 2011

The purpose of this report is to provide guidance to Federal IT managers in developing an architected approach to implementing Cloud Computing. It contends that to be fully effective and provide the greatest value to Federal agencies, Cloud Computing must:

• Be architected as an integral part of the agency’s Enterprise Architecture
• Provide for an effective governance mechanism
• Be implemented as services as part of a Service Oriented Architecture

Cloud Computing affects the people, process, and technology of the enterprise and each of these must be dealt with. This report explains the basic elements of Cloud Computing and ties it to solid architectural foundations. The guidance in this report will help enable the benefits of Cloud Computing to be fully realized.
American Council for Technology-Industry Advisory Council

The American Council for Technology (ACT) is a non-profit educational organization established in 1979 to assist government in acquiring and using information technology resources effectively. In 1989 ACT established the Industry Advisory Council (IAC) to bring industry and government executives together to collaborate on IT issues of interest to the government. In 1997 ACT established the Intergovernmental Advisory Board (IAB) to foster communication and collaboration between IT executives at all levels of federal service – Federal, state, local and tribal governments.

The American Council for Technology, in cooperation with the Industry Advisory Council and Intergovernmental Advisory Board, is a unique, public-private partnership dedicated to helping government use technology to serve the public. The purposes of the organization are to communicate, educate, inform and collaborate. ACT also works to promote the profession of public IT management. ACT and IAC offer a wide range of programs to accomplish these purposes.

ACT and IAC welcome the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of information technology. For membership and other information, visit ACT-IAC website at www.actgov.org.

Enterprise Architecture Shared Interest Group

As part of IAC, the EA SIG provides an objective, vendor-neutral and ethical forum to address Enterprise Architecture issues of common interest to government and industry. Our ultimate goal is to help government leaders develop approaches to address the challenges they face in delivering quality products and services to citizens. We are closely aligned with the CIO Council Architecture & Infrastructure Committee (AIC) and the Federal Enterprise Architecture Program Management Office (FEA PMO). We are results focused and driven by pragmatic considerations. We consider the linkage of EA to other management disciplines (strategic planning, budgeting, performance management, portfolio management, etc.) to be of primary importance and strive to collaborate closely with our fellow management disciplines.

Disclaimer

This document has been prepared to provide information regarding a specific issue. It does not – nor is it intended to – take a position on any specific course of action or proposal. Neither is it intended to endorse or recommend any specific technology, product or vendor. The views expressed in this document represent the views of the individuals and organizations who participated in its development. Every effort has been made to present accurate and reliable information in it and to that extent. ACT-IAC assumes no responsibility for consequences resulting from the use of the information herein.

Copyright

©American Council for Technology, 2011. This document may be quoted, reproduced and/or distributed without permission provided that credit is given to the American Council for Technology and Industry Advisory Council.

Further Information

For further information, contact the American Council for Technology and Industry Advisory Council at (703) 208-4800 or www.actgov.org.
The Role of Enterprise Architecture in Federal Cloud Computing

ACT-IAC Enterprise Architecture SIG
January 2011

Table of Contents

1. Introduction ............................................................................................................................ 3
2. Cloud Computing Architectural Framework .......................................................................... 4
3. The Importance of Enterprise Architecture and SOA ............................................................. 7
4. SOA as the Foundation for Cloud .......................................................................................... 7
5. Fundamental Shift in the Organization Model Providing IT Services .................................... 9
6. The Importance of Service Level Agreements ........................................................................ 9
7. Cloud Computing Reference Model/Architecture .................................................................. 9
8. Change in Funding & Cost Models .......................................................................................... 10
11. The Debate Surrounding Cloud Computing ....................................................................... 14
12. Enterprise Architecture: Bringing Clarity to Cloud Computing Decisions ............................ 16
13. Recommendations ................................................................................................................. 18
14. Conclusions .......................................................................................................................... 18
Key Terms .................................................................................................................................. 19
Resources .................................................................................................................................... 20
Key Contributors to this Document .......................................................................................... 20
“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 (Peter Mell and Tim Grance, NIST).

In the Cloud Computing environment, the Enterprise Architect becomes the “orchestrator” to ensure that every service provider efficiently meets the business demands of the service consumer.

1. Introduction

Many Federal agencies are evaluating and implementing Cloud Computing. As agencies take on this transformative technology, they find the transition to Cloud Computing impacts many aspects of their IT environment, including legacy systems, sustaining infrastructure, security and privacy. This document outlines an approach to implementing Cloud Computing that will yield the highest value to agencies. It contends that to be fully effective and provide the greatest value, Cloud Computing must:

- Be architected as an integral part of the agency’s Enterprise Architecture
- Provide for an effective governance mechanism
- Be implemented as services as part of a Service Oriented Architecture (SOA)

In short, Cloud Computing affects the people, process, and technology of the enterprise and each of these must be taken into consideration.

1.1 Intended Audience

This document is intended for chief architects, chief technology officers (CTOs), chief information officers (CIOs), program executives, and other individuals in federal agencies and support organizations who are responsible for leveraging information technology (IT) assets that support mission performance in pursuit of agency business objectives. Italicized passages in this document denote practical tips that practitioners should consider when implementing Cloud Computing.

1.2 Objectives

The Enterprise Architecture Shared Interest Group of the Industry Advisory Council (IAC EA-SIG) has prepared this document to explain the basic elements of Cloud Computing and to tie it to solid enterprise architectural foundations. Too often in the rush to embrace the latest technological trends, IT managers bypass the architecture and governance processes needed to achieve the touted benefits of those technologies. This document provides guidance that will help organizations that are contemplating a transition to Cloud Computing avoid its potential pitfalls and more fully realize its benefits. Our recommendations are based upon integrating and maximizing the use of Enterprise Architecture, and a leading architectural approach within it, Service Oriented Architecture (SOA), as integral steps in the Cloud Computing transition process. This document emphasizes that to maximize the value to be gained from Cloud Computing, agencies should utilize a service-oriented EA approach to design and implement their future cloud environment. It ties the two concepts together to provide the foundation for effective Cloud Computing.

The role of Enterprise Architect becomes increasingly important to the agency that chooses to implement Cloud Computing. And it is the Enterprise Architect who is positioned to understand which business processes will likely benefit from the elastic qualities of Cloud Computing and help drive the
organizational change (people focus) required to move away from the “server hugging” philosophy of today to one that focuses on agile service delivery.

It is the Enterprise Architect who must understand and demonstrate how to apply SOA and Service Oriented Infrastructure (SOI) to address agency business demand. Finally, it is the Enterprise Architect who must help shape the governance models that monitor, measure, and re-purpose the architecture to ensure it remains efficient and effective in supporting the organization.

1.3 Background

The Obama Administration signaled its intention to continue pursuing a Cloud Computing based IT strategy in the FY2011 budget submission. One of the chief proponents for Cloud Computing is Federal CIO Vivek Kundra. He recently said that the Obama administration’s strategy on Cloud Computing “offers transformational opportunities to fundamentally reshape how the government operates, engages the public and delivers services.” In March 2009 the Federal Chief Information Officer Council named Cloud Computing as a government priority.

There seems to be little doubt that the current administration is intent on using its power and influence to make Cloud Computing an operational standard for government agencies. Their argument for Cloud Computing is that it is a means of achieving a more open, efficient and cost effective government. The administration is utilizing a number of approaches to broaden public support and government buy-in including several initiatives underway within the federal government to explore and define policy, and implement Cloud Computing environments. A number of these initiatives are cited below in Section 10, Government Cloud Computing Initiatives. Several agencies have announced Cloud Computing based programs, however others are still evaluating their options. Many unanswered questions and some prevailing misconceptions about it remain, making the future of Cloud Computing and its application in government not entirely clear. It is therefore crucial to provide context.

Most importantly, it must be noted that it is services that are accessed from the cloud. In fact, it is from a services perspective (functionality accessed via an interface) that Cloud Computing is best understood. In practice, services may be offered or provided by organizations with different goals and objectives and therefore may not be completely compatible with the consuming agency’s requirements. To achieve a model of interoperability, services must be planned and designed to work together. This will not occur by happenstance, but only by design. This is where architecture plays a vital role.

Enterprise Architecture (EA) and SOA, define services in relation to each other – thereby establishing boundaries, enforcing policies and enabling reuse and interoperability. Without the architecture discipline, services anarchy reigns and diminished value results.

The major hurdles for effective use of Cloud Computing are similar to those for using services provided through SOA. Agency cloud environment based on Service-Oriented EA maximizes the value from Cloud Computing.

2. Cloud Computing Architectural Framework

There are three core elements to Cloud Computing 1) essential characteristics; 2) service delivery models; and 3) deployment and consumption models. Together, these elements help Enterprise Architects understand how to best position Cloud Computing to solve the business needs of agencies.

2.1. Essential Characteristics of Cloud Computing
The National Institute of Standards and Technology (NIST) finds Cloud Computing solutions share five characteristics, which include both the business view and technical capabilities of the architecture.

**On-demand self-service** – A cloud consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed, automatically without requiring human interaction with each service’s provider.

**Broad network access** – Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and Personal Device Assistants).

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

**Rapid elasticity** – Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale up and rapidly be released to quickly scale down. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

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

These characteristics are essential in achieving the agility, scalability, reliability, and overall efficiency models that Cloud Computing promises. However, these characteristics do not happen “by magic”. They must be architected into the cloud environment that is being considered regardless of whether they are internally developed or acquired from another source.

### 2.2. Service Delivery Models

Modern IT organizations are moving toward an environment wherein virtually everything is offered as a service. More specifically, these are IT capabilities that are modularized and isolated so that they can be offered and consumed independently of other capabilities. Cloud delivery models reflect this service oriented paradigm across infrastructure, platform, software, as well as supported business processes. A common characteristic of each of the models is that the provider of the service controls and manages the underlying cloud infrastructure supporting them. The consumer basically contracts for these services by either paying for them “by the drink” or obtaining them for a specified period of performance. Each model is briefly described below:

**Software as a Service (SaaS)** – Providing the consumer use of the service provider’s software applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email) – The service provider manages and controls the network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration.
settings. An extension of SaaS is the provisioning of an entire business process, known as Business Process as a Service (BPaaS).

**Platform as a Service (PaaS)** – Providing the consumer the ability to deploy consumer-created or acquired applications using programming languages and tools supported by the service provider’s software applications running on a cloud infrastructure. The service provider manages and controls the network, servers, operating systems, or storage. The consumer has control over the deployed applications and possibly application hosting environment configurations.

**Infrastructure as a Service (IaaS)** – Providing the consumer the ability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer has control over operating systems, storage, deployed applications, and might possibly have limited control of select networking components (e.g., host firewalls).

As the Enterprise Architect defines these layers, the solution and governance processes focus less on physical characteristics and emphasize delivering the intended service to the consumer. In this manner, Service Level Agreements (SLAs) are essential to the overall architecture.

### 2.3 Cloud Deployment and Consumption Models

The Enterprise Architect may select one or more deployment models to deliver cloud services to the end user community. Industry recognizes four deployment models: Private, Community, Public, and Hybrid. Each deployment model is briefly described below:

**Private Cloud** – The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist either on or off premise.

**Community Cloud** – The cloud infrastructure is shared by several organizations and supports a specific community that has shared interests and concerns (e.g., mission, security requirements, policy, and compliance considerations). It too may be managed by the organizations or a third party and may also exist either on or off premise.

**Public Cloud** – The cloud infrastructure is made available to the general public or an industry group and is owned by an organization selling cloud services.

**Hybrid Cloud** – The cloud infrastructure is a composite of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

IT managers and architects should select the best cloud deployment model based upon a variety of technical and business requirements. The use of Private or Hybrid Clouds may be default choices for many government agencies due to security, privacy and regulatory requirements. Market research indicates that most organizations initially use Private Clouds and move to Hybrid and Public Clouds over time. Many organizations in the health care and financial service industries appear to be adopting the Community Cloud as their preferred deployment model.

A key factor that an organization must consider when selecting a deployment model for each cloud-based service is trust (security and privacy). For example, a Public Cloud is attractive for low impact services and data that require minimal trust. In this model, organizations achieve the lowest cost. In a
Private Cloud scenario, agencies may achieve fewer cost savings but have increased security as data remains inside their organization’s firewall. The management costs may be higher, but the benefits of higher security levels are achieved.

If an organization decides to outsource sensitive high-impact cloud-based services, then they may opt to utilize a Private Cloud managed by an external party. In this model commercial providers offer dedicated environments separated from their Public Cloud offerings both logically and physically. Consumers may access these services through a dedicated government Intranet or virtual private network.

Architects need to base their recommendations of deployment/consumption models on the requirements of the agency which may include (but certainly are not limited to) numerous factors such as security, privacy, sensitivity of information, availability, cost, etc.

3. **The Importance of Enterprise Architecture and SOA**

Cloud Computing has the potential to provide a flexible and scalable platform for delivering services. That flexibility is based on the ability to exchange services within Service Oriented Architecture and the scalability is derived from the virtualization of the platform and the ability to devote additional resources to meet increased demand. This ability to exchange services, in a competitive environment, requires a full understanding and documentation of the service outcomes and interfaces. SOA provides a planned and architected suite of interacting services. A fully articulated services architecture, which is a subcomponent of Enterprise Architecture, is a key feature of a successful Cloud Computing environment.

4. **SOA as the Foundation for Cloud**

The leading SOA methodologies employ a layered architecture of services. The purpose of the layers is to facilitate identifying services, applying the appropriate level of governance and making decisions regarding service sourcing or deployment. Each layer is derived using combinations of Service Delivery Models cited in 2.2 above.

**The Process Layer** is derived from business process analysis (and business process reengineering) and is closely linked to business strategy and performance objectives (BPaaS).

**Core Enterprise Services** are derived from the foundational information that the enterprise requires to meet its mission. Services in this layer are derived from data analysis and represent concepts that are more stable than business processes. Many services will require access to these core data objects.

**Underlying Services** are typically provisioned by wrapping legacy transactions with a façade to expose existing, stable functionality (SaaS).

**Utility Services** are the services that are the most likely candidates for deploying to or consuming from the cloud (PaaS). These technical services (such as Content Management and Logging services) are ubiquitous and have the highest reuse potential (IaaS).

In SOA service layered architecture, virtually any service may be available in a cloud deployment model, cited in section 2.2. However, as Geoffrey Moore pointed out (see Dealing with Darwin, 2005), some
activities are better candidates for standardizing or outsourcing – making them more appropriate to be consumed from the Public Cloud. As Figure 1 depicts, activities can be divided along two dimensions: core vs. context and mission vs. enabling.

Core activities are those that make the organization unique. In the commercial world, these activities produce competitive advantage. Context activities, on the other hand, are those that must be performed but do not define the organization.

The mission critical and enabling activities are derived from Michael Porter’s value chain concept. Mission activities are those that directly produce the output of the organization. Enabling activities are those that indirectly support the mission (such as back office operations).

If we look at these two dimensions together, we observe that there is one class of activities that is ideal for consuming from the cloud – those that are context and enabling activities. They are neither mission-critical nor do they define the organization. As a result they should be considered for outsourcing. The other likely candidate for consuming from the cloud is mission linked to context activities. Although they do directly support the organization’s production, they do not make them unique. As a result these are candidates for standardizing and outsourcing. An example might be the payroll component of a complete HR system that could be outsourced to a payroll service provider such as ADP in the commercial sector or the USDA National Finance Center for government agencies. Activities that are core make the organization unique or special. Organizations typically want to keep them close so that they can innovate and differentiate them to maintain their competitive advantage or in the case of government to maintain organizational effectiveness.

To apply this concept, organizations should develop a portfolio management approach based on services and characterize each service in terms of these two dimensions. Using this catalog of services the organization can best determine how to acquire each service. Cloud Computing represents one of the available means to source services.
5. Fundamental Shift in the Organization Model Providing IT Services

Cloud Computing represents another step in the transition to information technology as a service. In order to take advantage of the cloud, IT organizations need to characterize their requirements and offerings as services. It follows that the organization’s EA should also be characterized as a set of well-organized services. It is widely recognized that IT exists to support the business or mission and, as such, should be considered a “customer-support” organization. Many IT organizations are formalizing this concept using Information Technology Service Management (ITSM) and IT Infrastructure Library (ITIL). ITSM and ITIL provide a framework and taxonomy for structuring the services effective IT shops offer and manage. ITIL is a framework of best practices for managing the IT infrastructure; ITSM leverages ITIL with other processes to deliver quality IT services to the business/mission.

In addition to taking a service portfolio approach to identifying required services, organizations adopting Cloud Computing should recognize that the organizational model would change as well. Once IT has been constructed as a set of services, each service can be evaluated in terms of how it should be provided and the performance level it should achieve. The assessment of core vs. context discussed in Section 4 will aid the sourcing evaluation. Performance metrics for each service offering should be developed to clearly delineate the effectiveness and efficiency of the service. These metrics become the basis for establishing SLAs between the consumers and providers of the service. In many cases, IT organizations will become both consumers and providers of services. This will shift the organizations from a paradigm of build and buy to one of consume and offer – with significant organizational implications.

6. The Importance of Service Level Agreements

With Cloud Computing, the IT organization will need to focus on creating meaningful Service Level Agreements (SLAs) as a way of monitoring, managing and incentivizing efficiency at operational and technical levels. SLAs may include the following elements:

- Performance parameters
- Location of data
- Metrics for events
- Backup/recovery and continuity requirements
- Quality of Service
- Cost
- Reliability
- Refresh cycle (releases/versions)
- Penalties for non-achievement of the above

The IT organization will be responsible for establishing SLA performance monitoring over the cloud environment. The governance organizations should work closely with the Enterprise Architects in developing operational contracts, SLAs and incentives for providers to meet service delivery goals. In this role, Enterprise Architects would also measure and document how well cloud service providers meet established technical requirements.

7. Cloud Computing Reference Model/Architecture
Patrick Stingley, CTO of the Bureau of Land Management set forth a model mapping cloud services to that of the FEA Service Reference Model (SRM). At first glance, one can see that these services exist in government data centers today. The difference is that Cloud Computing architecture uses commodity hardware and virtualization to commoditize these services.

**Figure 2. Cloud Computing Reference Model**

Stingley states that this model resembles the IT services found in the ITIL processes. This model of Cloud Computing depicts the service-oriented view of IT creating a generalized form of the ITIL Services Directory. Enterprise Architects can use this model to identify the IT services that may be delivered through Cloud Computing.

8. **Change in Funding & Cost Models**

There are a variety of funding and cost models applicable to Cloud Computing depending on whether the organization is a provider or consumer of cloud services. We expect that most federal agencies will be consumers of cloud services. For agencies that are cloud service providers, decisions must be made about the provisioning level. That is, whether the agency is providing SaaS, PaaS, or IaaS. The following table indicates the tiered possibilities for providing cloud services. As should be evident,
provider of cloud services may be a provider and consumer simultaneously and may have capital investment costs as well as operating costs associated with providing the services.

<table>
<thead>
<tr>
<th>Provider of:</th>
<th>Hosting Method</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software as a Service</td>
<td>• Host own platform</td>
<td>• Consumer of PaaS</td>
</tr>
<tr>
<td></td>
<td>• Own or license the intellectual property (IP)</td>
<td></td>
</tr>
<tr>
<td>Platform as a Service</td>
<td>• Host platform on own infrastructure</td>
<td>• Consumer of IaaS</td>
</tr>
<tr>
<td></td>
<td>• Own or License the platform software</td>
<td></td>
</tr>
<tr>
<td>Infrastructure as a Service</td>
<td>• Host Infrastructure on own hardware</td>
<td>Not a Cloud Provider</td>
</tr>
<tr>
<td></td>
<td>• Own or License the infrastructure software</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3. Organizations Can Be Providers And Consumers of Cloud Services.

For cloud service consumers, the situation is generally simpler. In most cases, the services can be consumed on a metered or usage basis; however, for some platform and infrastructure services, a license agreement (and associated capital costs) may be required.

Many of the benefits of Cloud Computing involve efficiency gains that result in capital and operational cost savings. Regardless of the provider mechanism, substantial savings can accrue from consolidating servers and using virtualization (in contrast to dedicating servers to applications). Virtualization can reduce the cost of requisite hardware while providing scalability (the ability to ramp up the number of users of a service) by treating compute, storage, and network resources as pools and spreading the requirement for multiple applications or services.

Cost restructuring comes about by converting IT capital investments into operating expenses. Using a cloud deployment model lessens the requirement for system administration as the IaaS software automates the provisioning of software patches and upgrades. If an agency chooses to use a Hybrid or Public Cloud model, they can outsource some of the functions (like maintaining servers) that they would otherwise have to perform themselves. While this form of outsourcing may not reduce overall costs, it should allow agencies to increase focus on those areas that are core to their mission and leave some of the non-core activities to others.

For most organizations, obtaining services from cloud vendors is considerably more cost effective than providing the capabilities themselves, depending on the utilization of the computing capability. This is primarily due to the combination of “virtualization” and economies of scale. In a traditional environment a server is dedicated to each requirement. The level of utilization for each server is typically very low because the capacity obtained is designed to meet the peak utilization. As a result, data centers in industry and government are typically over-provisioned. Virtualization involves the use of collections of servers to meet multiple requirements. Since the peak demands for each requirement do not typically coincide, the total number of servers needed may be considerably less. Thus, virtualization has its own ROI. Cloud Computing can be considered outsourced virtualization. Cloud vendors are able to optimize their infrastructure and software to reduce costs, provide on-demand scalability, and take advantage of massive economies of scale. They are able to provide capabilities at a fraction of the cost that would be incurred by the organizations providing these capabilities themselves. However, cloud vendors typically charge a premium for on-demand scalability. The cost is typically higher than internally provided capability – when it is used. The savings from Cloud Computing arise from the fact that much of the time, the capability is unused and no fee is paid when the services are not in use.

As has been discussed above, Cloud Computing represents a new paradigm for the deployment and delivery of IT services. As such, it should be approached in the same manner as any significant organizational change. Depending on the organization’s objectives for exploiting the cloud, the emphasis on the typical change management success factors (structure, people, process, technology) will vary.

However, regardless of the emphasis, the following factors will be critical to success with Cloud Computing:

- Management processes
- Trust mechanisms
- Competencies
- Structure (Reference Architecture, Governance)

Effective management processes will be required to oversee the transition to Cloud Computing, including adopting processes for Cloud Computing governance, and solution lifecycle management. The rollout of Cloud Computing will be evolutionary and these processes are useful for keeping multiple initiatives and projects synchronized.

Trust must be established at several levels for Cloud Computing to succeed. The primary trust factor is establishing an enforceable contract between consumer and provider, including enforceable security and/or risk management mechanisms. The contract consists essentially of the SLA that specifies the performance parameters for the service and the enforcement mechanisms for ensuring that the performance levels are achieved.

Security is cited as a leading concern for CIOs considering Cloud Computing. The concern is derived from the lack of transparency found in the public cloud environment. In a Public cloud the common audit logging and management controls that have been available in internal data center environments may not be available. Therefore, agencies cannot readily see who has accessed data, where data has resided, and how the data is archived. Many of these concerns decrease or go away in Private, Hybrid and Community cloud deployments. To further support security requirements, NIST and the Cloud Security Alliance organizations are defining the Security Content Automation Protocol (SCAP). The SCAP draft (SP 800-126 Revision 1) has been available for public review and comment since early June, 2010.

The security issues for the cloud are the same as for SOA – where perimeter based security measures are insufficient. Security should be based on a risk management approach and provide for a balance between system performance and security enforcement.

Organizational competencies must be updated to provide the know-how to architect, design and consume services from the cloud. Individuals must be able to execute the acquisition and solution development lifecycle processes for cloud based services.

Finally, the overriding structure for aligning all of these factors is service-oriented reference architecture. An enterprise level architecture with effective governance will ensure that all of the factors are properly aligned.
10. Government Cloud Computing Initiatives

There are several Cloud Computing initiatives underway in Federal government. These early initiatives may provide the Federal community with best practices and lessons learned, as well as reusable services. These initiatives include:

- **NASA Nebula**: A program in extended pilot mode at NASA Ames Research Center integrating a set of open-source components into a seamless, self-service platform, providing high-capacity computing, storage and network connectivity using a virtualized, scalable approach to achieve cost and energy efficiencies. As a hybrid cloud, Nebula will offer cost-effective IaaS, PaaS and SaaS.

- **DoD/DISA**:
  - **RACE (Rapid Access Computing Environment)**: Enables DoD end-users to provision platform and infrastructure services through the Web using a credit card, 24 hours a day. Race offers PaaS.
  - **GCDS (GIG Content Delivery Services)**: Commercially owned, globally distributed computing platform comprised of servers deployed across the Defense Information Systems Network (DISN) and leverages commercial Internet best practices to provide state of the art web content and web application delivery via standard web protocols (i.e., HTTP and HTTPS). GCDS offers PaaS.
  - **Forge.mil**: A family of services provided to support the DoD's technology development community. The system currently enables the collaborative development and use of open source and DoD community source software. Over time it will support the full system life-cycle and enable continuous collaboration among all stakeholders including developers, testers, certifiers, operators, and users. Forge.mil offers SaaS.

- **APPS.gov**: A Federal Web portal (or storefront), which allows agencies to provide government agencies a simplified way to find, research and rapidly procure cloud products and services.

- **DOE Laboratory Cloud Computing Environment**: The DOE National Laboratories are exploring the use of cloud services for scientific computing. In addition, they are exploring hybrid solutions which would give them the ability to maintain control over the user authorization process while using cloud services such as email, calendaring and collaboration tools for instances which require strong authentication of service users.

- **Federal Cloud Computing Program Management Office**: Managed by the General Services Administration, this PMO is responsible for working with the Federal Chief Information Officers to define the Government’s Cloud Computing Strategic direction, facilitating the acquisition of Cloud Computing services, coordinating Federal Cloud Computing efforts, and providing the Federal community with direction and guidance. The PMO successfully completed a competitive acquisition of IaaS. In the future, these service offerings will be expanded to include PaaS and SaaS offerings.

- **Cloud Computing Advisory Council**: The CCAC is a collaborative governance body comprised of over twenty-five Federal agencies. Membership is primarily made up of enterprise architects and IT Infrastructure managers. The purpose of the CCAC is to:
  - Provide Federal agency subject matter expertise in support of the Federal Cloud Computing initiative and strategic direction;
  - Address Federal agency Cloud Computing issues, requirements, and business needs;
o Develop and recommend the Federal Cloud Computing vision, strategy, and plans;
 o Review the Federal Cloud Computing PMO’s deliverables, as appropriate and to provide specific feedback;
 o Execute specific tasks as assigned by the CCPMO or OMB.
 o Enable cross-functional collaboration with other related Federal initiatives – such as TIC, IPv6, FDCC, etc.
 o Share best practices and current activities.

- **Cloud Computing Security Working Group**: The CCSWG is a working group under the CCAC. This group is comprised of IT security professionals and Enterprise Architects working to develop a common Federal Cloud Computing Certification and Accreditation process.

- **Federal Risk and Authorization Management Program**, created by the CCSWG, is a government-wide initiative to provide joint authorizations and continuous security monitoring services for all agencies. It can certify new network security products or services for individual agencies. Those certifications can be reused by other civilian agencies thereby reducing duplicative work and spending.

- **Citizen Enabling Open Government (CEOG)** – a nascent initiative sponsored by the Enterprise Architecture Shared Interest Group. The CEOG offers a vision of agile and adaptive government services that may be offered over the next ten to fifteen years. Most importantly it relies heavily on Cloud Computing to seamlessly integrate suites of services from multiple stakeholders into a “single face” to citizens.

### 11. The Debate Surrounding Cloud Computing

There is an active and ongoing debate around the merits of Cloud Computing for the US Federal government. On one hand there are those who say that Cloud Computing is the wave of the future that will produce an unprecedented set of benefits for government agencies that embrace it. On the other are those who contend that Cloud Computing is merely a recycled mix of technologies and methods that will amount to little more than the latest over-hyped and under-performing technology fad.

Cloud Computing has become part of industry lexicon making it a recurring theme of countless magazine articles and blogs as well as a feature topic of conferences, trade shows, seminars and webinars occurring across the country. This “industry buzz” has created an impetus that is influencing vendor strategies and product offerings; and seemingly overnight the field has become crowded with players offering an array of cloud oriented products and services. This includes some of the industry’s biggest names who are developing innovative cloud solutions and establishing infrastructure, platforms and capabilities that seem to provide viable options for both government and industry clientele. At the same time there are firms that seem to be taking a more reactive approach to the perceived market opportunity - some appear to be hitching themselves to the cloud bandwagon to preserve competitive positions and cash-in on an apparent bonanza. The quality and utility of all these cloud products and services are sometimes difficult to distinguish creating a “cloud of uncertainty” around it.

As discussed previously, GSA has been leading the government’s foray into Cloud Computing by establishing the Federal Cloud Computing Program Management Office to provide technical and administrative leadership, help build confidence and bring clarity to the issue. Apps.gov is an example of their efforts to broaden the use of Cloud Computing in the Federal Government.
Cloud Computing’s proponents say that it will improve data sharing and promote collaboration between various levels of government [federal, state and local] allowing more frequent and efficient interaction with citizens permitting agencies to focus on their core mission functions rather than the acquisition and maintenance of a collection of software systems and supporting hardware. They predict Cloud Computing will save the government billions in the costs of software, hardware, facilities and personnel by enabling the government wide consolidation of data centers, which will create shared resource pools of servers, networks, storage, applications and services.

Cloud Computing is also expected to impact the cost equation for obtaining IT assets and services. It is said to do this by permitting agencies to avoid the capital costs associated with establishing infrastructure and platforms by purchasing them as bundled services on a per-unit consumed basis. It is thought that treating these purchases as operating expenditures rather than capital assets will cut costs by eliminating or reducing many management, accounting and reporting steps now required throughout the typical asset lifecycle (i.e., planning, acquisition, operations, maintenance and disposal).

Its advocates also believe that once it is fully realized Cloud Computing will translate into further costs savings through a reduction in associated energy consumption, which will have the added benefit of reducing the government’s overall carbon footprint resulting in a positive environmental impact.

On the other side of this discussion are Cloud Computing’s opponents and skeptics who say that it is largely unproven and therefore risky. They see many “red flags” around the prospect of exchanging in-house developed systems and capabilities, and the control of sensitive agency data they enable, for a reliance on vendor managed off-site systems and software, the true cost, reliability and trustworthiness of which are difficult to determine. They contend that such uncertainty is reason enough to conclude that the risks associated with Cloud Computing are likely to outweigh its potential rewards.

Such attitudes are somewhat common across government. While there has been a lot of interest in Cloud Computing within government, many agencies have thus far been approaching it rather cautiously. Even though it has roots in familiar technologies and services, Cloud Computing represents a radical departure from business as usual. Just like their private sector counterparts, government business and IT executives are accustomed to the status quo of acquiring, developing and maintaining in-house IT capabilities for applications, hardware, operating systems, system utilities, storage, and networks. Although the traditional love-hate relationship between business and in-house IT still persists as it does elsewhere it does not seem to be reason enough for many agencies to test the Cloud Computing paradigm which is commonly compared to “a leap into the unknown”.

This may represent one of the key impediments to the widespread adoption of Cloud Computing in government. Anyone familiar with US government operations knows that the responsibility for executing any government-wide strategy, like Cloud Computing, rests on the collective shoulders of these same agency executives who make investment decisions for their respective organizations – therefore getting their collective buy-in will be a critical success factor for Cloud Computing in government. And widespread adoption is precisely what the Obama administration will need for its Cloud Computing strategy to succeed - because only when a critical mass of agencies participate will the sort of cross agency collaboration as envisioned in the cloud strategy become possible. And the same is true for cost - critical mass will be necessary to realize economies of scale which will drive down the per-unit costs of products and services making them a compelling enough value for agency decision makers to justify the switch.

Most agency executives are interested in better performance and lower costs of operations, but how can they know if these promised improvements are reality or merely industry hype? Certainly decisions
as potentially transformational and/or disruptive as decommissioning systems, dismantling data centers, repurposing or downsizing staff and relocating key aspects of agency operations and sensitive data to an outsourced model (all things that took years and untold millions to put in place) are enough to keep most any agency executive up at night.

The debate on Cloud Computing is far from settled. Certainly many of its purported benefits make perfect sense, but at the same time some of the concerns being voiced about it are legitimate. What’s needed is an unbiased method for testing the risks and rewards of the various Cloud Computing options to help determine the optimal path forward before agencies actually commit to it. We believe Enterprise Architecture provides the ideal approach for doing just that.

12. Enterprise Architecture: Bringing Clarity to Cloud Computing Decisions

EA is a structured and comprehensive best practice approach perfectly suited for building confidence and breaking the impasse surrounding Cloud Computing. It provides facts-based decision support that will help reveal where and how, or even if Cloud Computing should be pursued. It is perhaps the best tool available today for charting a course for Cloud Computing in government. EA can help bring clarity to many issues that are of concern to agencies including those related to performance, cost, security, risk, governance and regulatory compliance. It can help provide answers to common questions such as:

- How can we know if Cloud Computing is even appropriate for our agency?
- Which systems, applications and business processes are the best candidates for cloud outsourcing?
- How can we effectively manage the interrelationships between systems, business processes and data we want to outsource with those that will remain in-house?
- What would be the most effective cloud configuration for our agency (private, public, hybrid, community, etc)?
- How do we protect sensitive agency data in the cloud?
- How do we comply with Federal records management requirements in a cloud environment?
- What’s the best way to assess and manage our agency’s risk profile in a cloud environment?
- What are the actual costs of our IT operations today? What cost savings can be expected by transitioning to Cloud Computing?
- How well are our current agency IT investments performing? What performance improvements are possible in a cloud environment?
- What provisions need to be included in service-level agreements (SLA) to meet agency requirements for budgetary and regulatory compliance?
- How do we effectively monitor SLA performance?
- Where do we start? What are the steps to get from where are today to a cloud environment?

Enterprise Architecture is an industry recognized best practice management approach for sorting out many of the challenges of modern organizations. EA’s primary purpose is to provide business and IT stakeholders with better information to facilitate more informed decision-making - the ideal tool for helping agencies, large and small, sort through the complex issues involved in transitioning to a cloud environment.

EA is a holistic approach for understanding the multi-dimensional nature of organizations, the components that comprise them and the connections and inter-relationships between those components. It involves the development of a strategic information repository that defines the
organization’s mission, business strategies, goals and objectives and the capabilities and resources essential for achieving them including its data and information, business processes, and the enabling technical environment (software and hardware). It also includes information about workforce, organization, locations and other assets. Enterprise Architects utilize techniques for modeling an organization’s current and future architectural states and for developing “transition plans” which describe the incremental processes for implementing new technologies and capabilities in response to the changes in its environment or mission needs. They also employ a number of architecture based analytical and simulation procedures in areas such as cost and performance that can reveal valuable insights into the business which are otherwise not easily derived.

Such quantitative analysis creates an information foundation on which agency business executives can develop more detailed and fact-based business cases that support a move to the cloud. It can help identify which parts of the IT infrastructure, applications and services are best candidates for outsourcing through an examination of all current issues related to them. EA supports the development of risk assessments, outlining the potential cost of risk factors and their mitigation strategies. These are not easily defined because they are usually not known until there is a problem or event at which time they become real and quantifiable.

It can also be used to estimate potential cost savings - typically the perceived cost benefits of a cloud as compared to in-house IT costs are usually too simplistic; there are hidden costs and risks including security, compliance, SLA monitoring and maintaining operational efficiency.

EA is also ideal for identifying improvements in performance that might be gained by migrating to the cloud plus the hard and soft benefits these improvements will deliver. Hard benefits include those investments areas that are directly linked to revenue sources, cost savings or mission attainment; while soft benefits are the tougher to measure benefits such as customer, constituent or employee satisfaction.

The Cloud Computing strategy is a vision for virtual government operations that will be more lean and responsive to constituent needs. EA can play a key role in that new environment, but it must do so by responding to these new business needs in a more agile and targeted manner; practicing “just in time” and “just enough” architecture. It has often been criticized in the past as an esoteric practice area that takes too long to produce tangible and meaningful results. Many in the government EA community feel their profession is misunderstood and under-appreciated and that EA is not being utilized to its full potential. For EA to provide maximum value it should be repositioned away from compliance and investment reporting to a tool for decision support, strategy development and implementation. It must

---

1 These include cost analytics such as Total Cost of Ownership (TCO) and Return on Investment (ROI) and performance analytics, which use metrics and various key performance indicators to better understand issues such as systems reliability, availability, utilization, behavior, modularity and security. This type of architectural analysis also includes various simulation techniques (i.e., Monte Carlo, Discrete Event, etc) which apply variables (best case, worst case and most likely case) that simulate real life operations to reveal how the new architecture will perform in production.

By benchmarking the “as-is” architecture, enterprise architects can determine how well or how poorly the enterprise IT portfolio is performing towards meeting its current goals and objectives as well as determining the costs of operations. The same procedures are then repeated for various future state or “to-be” architectures, which in the case of Cloud Computing might include the application of SaaS, PaaS, or IaaS. These can then be compared to the current state info using “Gap” or “Diff” analyses techniques to highlight the differences between the current and proposed operating states. Cost-Benefit, What-if, Risk and Impact analyses can then be conducted to see what effect cloud outsourcing decisions will have on the organization and its mission. Lastly various Trade-off analysis techniques can be applied to evaluate the various options and configurations of cloud migrations.
operate in front of the “decision curve” and adopt a results-oriented approach that features a more practical communications style and output that is readily understood and of immediate utility to organizational business stakeholders. This will increase their effectiveness in weighing agency options and making more informed decisions in the world of Cloud Computing.

13. Recommendations

Based on the discussion above, we offer a few recommendations to agencies in the process of adopting or considering Cloud Computing. Each of these needs to be taken in the context of the agency’s Enterprise Architecture:

- Avoid the temptation to rush out and procure cloud enabling infrastructure. Instead, through the use of Enterprise Architecture, identify the program and enterprise services required. Evaluate each for its potential to be consumed from or deployed to the cloud based on core/context considerations, as well as security issues.

- Evaluate the deployment options to determine the role that public, private, community and hybrid clouds can play within your computing environment.

- Enhance your risk management program. Cloud Computing introduces additional risks that must be considered and managed, including security, compliance, monitoring, operational dependency, and others. Risks can be controlled through best practices, technology, and most importantly, effective governance as negotiated in a detailed SLA that meets the organization's goals and requirements.

- Expand your governance program. Managing risk requires policies and compliance enforcement mechanisms (SLAs) to ensure that they are implemented. Where appropriate, monitoring and enforcement can be moved to the cloud (i.e., monitoring as a service).

- Use Enterprise Architecture to benchmark current enterprise costs and performance and to analyze expected improvements from Cloud Computing (gap and impact analysis).

14. Conclusions

Cloud Computing is already making its way into the computing fabric of federal agencies. In some cases, agencies are taking a strategic, enterprise approach to implementing Cloud Computing. In other cases, agencies are taking a tactical, or even ad hoc, approach. The greatest benefits will be derived when a coordinated, architected approach is adopted.

Since Cloud Computing enables the consumption of services from other platforms, it makes sense that service architecture would aid in identifying the appropriate cloud-based services. This will avoid service anarchy where each program consumes services from the cloud that conflict with the services consumed by other programs. EA and its instantiation in SOA provide the foundation for Cloud Computing. Many of the issues that must be addressed to be successful with Cloud Computing are the same issues that must be addressed for SOA.

Cloud Computing can enable a major shift in the funding of IT services and can have a very high return on investment (especially where it reduces the investment needed). Cloud deployments allow investment in innovation vs. operations and maintenance (flipping the 80/20 balance commonly found
in most organizations). However, the cloud brings additional risks that must be understood, evaluated and managed.

An approach to Cloud Computing adoption based on the principles of Enterprise Architecture (with SOA) and effective governance has the greatest likelihood of success in achieving the agency objectives with respect to Cloud Computing.

**Key Terms**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>The means by which the needs of a consumer are brought together with the capabilities of a provider.</td>
<td>OASIS, SOA Reference Model; PGFSOA</td>
</tr>
<tr>
<td>Service Oriented Architecture</td>
<td>A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains.</td>
<td>OASIS, SOA Reference Model; PGFSOA</td>
</tr>
<tr>
<td>Cloud Computing</td>
<td>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.</td>
<td>NIST</td>
</tr>
<tr>
<td>Infrastructure as a Service (IaaS)</td>
<td>Capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.</td>
<td>NIST</td>
</tr>
<tr>
<td>Platform as a Service (PaaS)</td>
<td>Capability to deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider.</td>
<td>NIST</td>
</tr>
<tr>
<td>Software as a Service (SaaS)</td>
<td>Capability to use a provider’s applications (offered as services via interfaces) running on a cloud infrastructure and accessible from various client devices such as a Web browser.</td>
<td>NIST</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Abstraction of a logical capability from its physical implementation. For example, application servers may be provided by a cluster of physical servers rather than each being tied to a single server.</td>
<td>NIST</td>
</tr>
</tbody>
</table>
Resources


Key Contributors to this Document
Dave Mayo (Editor) Everware-CBDI
Scott Dowell CSC
Branko Primetica Global Tech
David Epperly Archangel Information Technologies
Doug Jackson 2MD
Ed Harrington Architecting the Enterprise