IntelliDyne
EXPERIENCE ABOVE & BEYOND

WHITE PAPER:

STRATEGIC IMPACT PILLARS FOR EFFICIENT MIGRATION TO CLOUD COMPUTING IN GOVERNMENT

IntelliDyne, LLC
MARCH 2012

IntelliDyne
EXPERIENCE ABOVE & BEYOND

STRATEGIC IMPACT PILLARS FOR EFFICIENT MIGRATION TO CLOUD COMPUTING IN GOVERNMENT

Executive Summary

The purpose of this white paper is to introduce IntelliDyne's Five Strategic Impact Pillars to help government CIOs evaluate the right path to cloud computing to achieve efficient use of the government IT infrastructure. One must view "going to the cloud" not as an end goal but as a critical path toward ensuring that cost savings are truly realized and are fully aligned to the agency's long-term business mission. With proper planning, developing the right Service Oriented Architecture (SOA) could yield the critical operational efficiencies for your organization.

The Federal Government's "Cloud First" Mandate: An Imperative Driven by the Need to Cut Costs & Increase Operational Efficiencies.

At present, the Federal Government's IT environments are characterized by several challenges. These include low asset utilization, a fragmented demand for resources, duplicative systems, and environments that are difficult to manage. The Federal CIO's answer is cloud computing — a model that creates a flexible workforce and is almost certain to be an efficiency game-changer for the future.[1]

Many federal agencies are already moving toward the Cloud. In a recent study, 29% of government CIOs indicated that their agencies already use cloud services. That's an increase of ten points from a year ago. Another 29% say their agencies plan to tap into the cloud within 12 months. That means that cloud adoption should surpass the 50% mark at some point in the year ahead.[2]

The Federal cloud computing mandate aims to maximize government IT budgets. According to MeriTalk, the Federal Government spends "$35.7 billion per year supporting older, legacy technologies." With cloud implementations, the government projects savings of $14.4 billion for the first year in government-wide cloud implementations.[3] Thus, it is essential to understand what the cloud is, how it can help, and the steps you need to take in moving toward the model.

[1] Kundra, Vivek. Federal Cloud Computing Strategy. 08 February 2011 http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf
[2] 2011 Federal Government Priorities. *InformationWeek Government*. 02 October 2011.
[3] *MeriTalk* Press Release. 18 April 2011. http://www.meritalk.com/pdfs/MeriTalk_Federal_Cloud_Weather_Report_Press_Release.pdf

The chart below presents a summary of what cloud computing offers:

Efficiency	
Cloud Benefits	Current Environment
• Improved asset utilization (server utilization > 60-70%) • Aggregated demand and accelerated system consolidation (e.g. Federal Data Center Consolidation Initiative) • Improved productivity in application development, application management, network, and end-user	• Low asset utilization (server utilization < 30% typical) • Fragmented demand and duplicative systems • Difficult-to-manage systems
Agility	
Cloud Benefits	Current Environment
• Purchase "as-a-service" from trusted cloud providers • Near-instantaneous increases and reductions in capacity • More responsive to urgent agency needs	• Years required to build data centers for new services • Months required to increase capacity of existing services
Innovation	
Cloud Benefits	Current Environment
• Shift focus from asset ownership to service management • Tap into private sector innovation • Encourages entrepreneurial culture • Better linked to emerging technologies (e.g., devices)	• Burdened by asset management • De-coupled from private sector innovation engines • Risk-adverse culture

Figure 1: Cloud benefits: Efficiency, Agility, Innovation[4]

[4] Kundra, Vivek. Federal Cloud Computing Strategy. 08 February 2011 http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf

Figure 2: IntelliDyne's Strategic Impact Pillars for Efficient Migration to Government Cloud Computing

STRATEGIC PILLAR 1: IDENTIFYING BUSINESS IMPACTS. IS CLOUD COMPUTING RIGHT FOR YOUR AGENCY'S UNIQUE ENVRIONMENT?

The cloud transformation requires a shift in how the government thinks of IT. Many organizations see IT as an investment in locally operated applications, servers, and networks. With the cloud, they will have to think in terms of services, commoditized computing resources, and agile capacity provisioning tools, and their collective enabling effect for government agencies and the people they serve. This new way of thinking will have a broad impact across the entire IT lifecycle, from inception through delivery and operations.

The move to the cloud will involve these key considerations:

Selecting services to move to the cloud

Organizations must consider their overall IT portfolios and then create roadmaps for cloud deployment and migration. These roadmaps must prioritize services that have high expected value and readiness to maximize benefits and minimize risk. Defining exactly which cloud services your organization needs is key to developing a sound roadmap to follow.

Identify sources of value

Cloud computing provides three primary sources of business value: efficiency, agility, and innovation. An organization using the cloud increases efficiency through higher computer resource utilization and lower labor costs, while agility gains come in the form of rapid automated provisioning of computing and storage resources. Innovation gains are seen in improved customer satisfaction scores, usage trends, and functionality.

Determine cloud readiness

You must do more than simply assess the potential value of moving to cloud services. Organizations should make risk-based decisions that consider the readiness of commercial or government providers to fulfill their needs. These can be wide ranging, but likely will include security requirements, service and marketplace characteristics, application readiness, government readiness, and the program's stage in the technology lifecycle.

Security requirements

Federal government IT programs have a wide range of security requirements. These include: compliance with Federal Information Processing Standards' agency-specific policies; Authorization to Operate requirements; and vulnerability and security event monitoring, logging, and reporting. The decision to apply a specific cloud computing model must consider these requirements. Federal agencies have the responsibility to ensure that a safe, secure cloud solution is available to provide an IT service, and should carefully consider agency security needs.

STRATEGIC PILLAR 2: BENCHMARK THE BUSINESS AND OPERATIONAL CONSIDERATIONS THAT WOULD IMPACT YOUR CLOUD IMPLEMENTATION

As a federal government agency investigating in cloud solutions, first you must identify the gaps in your current operations and determine if the cloud can help fill those gaps. What are the information and collaboration needs of your providers and users? What aspects of your agency could or should be transitioned to a cloud environment? Will moving to the cloud create the new efficiencies that you want?

Program managers will have to work closely with IT leadership to develop a comprehensive cloud strategy. This will aid in creating a plan of action to ensure that integration points are managed and opportunities for efficiencies leveraged. How well will your current operating model support the cloud migration plan? Organizational process changes are sure to occur. You will have to assess the change management implications and plan for them. You will have to evaluate whether you need to move to a private or a public cloud. The budgetary differences can be significant, and security risks will have to be proactively managed.

Such transitions inevitably involve risk. Risks/reward determinations must be made as you assess your cloud providers' claims. Cost savings will need to be validated and tested against Total Cost of Ownership (TCO). Compliance and change management implications need to be taken into account as well.

Other issues you must consider include integrating your business disaster recovery schema into your cloud migration strategy, and understanding the contracting process—it will change as offerings become more standardized. Service Level Agreement plans must be worked out with the cloud vendor, and the vendor's assurance reporting needs must be determined. Requirements that worked for outsourcing may not work as well in a cloud environment.

Finally, you must fully understand the business integration issues; data architectures must evolve for the cloud. Consider internal audit, security and government regulatory implications of data including privacy, storage, co-location, and governance. You must be sure that compliance requirements are met.

STRATEGIC PILLAR 3: IDENTIFY THE PROPER CLOUD DEPLOYMENT AND SERVICE DELIVERY MODELS THAT UNIQUELY FIT YOUR AGENCY

Cloud computing offers several deployment models. Each provides tradeoffs for federal government agencies that are migrating their applications to a cloud environment. NIST defines the cloud deployment models as follows:[5]

1. **Private cloud.** A cloud infrastructure operated solely for an organization. It may be managed by the organization or a third party and it may exist on-premise or off-premise.

2. **Community cloud.** A cloud infrastructure shared by several organizations and supporting a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and it may exist on-premise or off-premise.

3. **Public cloud.** A cloud infrastructure made available to the general public or a large industry group and owned by an organization selling cloud services.

4. **Hybrid cloud.** A cloud infrastructure that is a composition of two or more clouds (private, community, or public). They 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).

Cloud computing is also categorized into service models. These are defined by NIST to be:

- **Cloud Software as a Service (SaaS).** The federal user is able to use the provider's 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 user does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities. One possible exception, however, is limited user-specific application configuration settings.

- **Cloud Platform as a Service (PaaS).** The user has the ability to deploy onto the cloud infrastructure user-created or acquired applications. These applications in general are created using programming languages and tools supported by the provider. In PaaS, the user does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage. Nor does the user control the deployed applications and possibly application hosting environment configurations.

- **Cloud Infrastructure as a Service (IaaS).** The user is able to provision processing, storage, networks, and other fundamental computing resources. In this model the user is able to deploy and run arbitrary software, which can include operating systems and applications. The user does not manage or control

[5] Kundra, Vivek. Federal Cloud Computing Strategy. 08 February 2011

the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components.

Migrating toward the Cloud

Government CIOs must develop a comprehensive cloud strategy and plan of action. This will ensure that critical integration points are managed and that opportunities for efficiencies are leveraged. You must work closely with program leaders to create an enterprise vision and roadmap for the cloud, and identify proof of concept opportunities to leverage.

Steps toward implementing the cloud:

- Educate business and IT management on the cloud's capabilities and potential.
- Deploy competent specialists to study the cloud market and its capabilities, offerings and providers.
- Evaluate the interoperability of cloud solutions against current applications, platforms and infrastructure.
- Re-define the role of the CIO as it evolves from IT provider to Chief Integration Officer who has the opportunity to drive innovation.
- Develop scenario plans for cloud adoption and deployment across each cloud layer and across IT and business operating areas.

Design, develop and deploy operating governance and risk management programs from the IT perspective of cloud computing services.

STRATEGIC PILLAR 4: DEVELOP THE RIGHT SERVICE ORIENTED ARCHITECTURE (SOA) TO GAIN OPERATIONAL EFFICIENCIES

The cloud's shared infrastructure has many benefits, but you should not go to the cloud without closely evaluating your current architecture. One of the reasons a cloud infrastructure is so valuable is that the server, network and database infrastructure are a shared resource available to the entire client user base.

A public cloud implementation can achieve 70-80% utilization of the servers. This is efficient and cost effective. On the other hand, a private cloud's usage may only be in the 30% range.[6] Then ROI can become an issue. For instance, in a stove-piped organizational structure, servers might be operating at 80-85% capacity at times, yet at other times only at 0% capacity. Averaged across a weekly period this leads to a usage of approximately 15%, which may appear to be poor. But the resources required to meet the needs of the organization when they near full load indicate that the organizational IT resources are correctly sized. The key is to have the appropriate architecture in place to reap the cloud's benefits.

To efficiently implement a cloud solution, a Service Oriented Architecture (SOA) is recommended. SOA solves two of the major problems that occur in stove-piped organizations. The first is that organizations often build applications to solve the same problem but in different ways. This creates inefficiencies because users must learn two ways to use IT resources to solve the same problem.

The second issue is that data may be stored in different formats, storage systems and computers around the organization. This lack of planning costs time and money, and in addition duplicates systems and data. The SOA is one method of using standardization as a way to solve such problems. The organization will gain efficiencies such as the ability to reuse data from various sources.

[6] Kundra, Vivek. Federal Cloud Computing Strategy. 08 February 2011 http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf

The diagram below illustrates the components of a SOA, including instituting the correct governance to reap the benefits of the infrastructure.

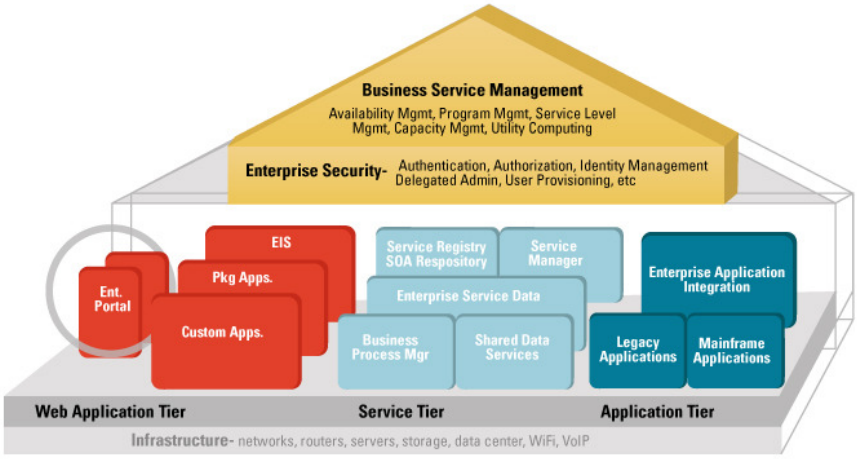

Figure 3: SOA Components

Using Service Oriented Architecture to Manage "Big Data"

By developing an Enterprise Service BUS (a key component of SOA), you can deliver a solution for gathering data from many systems into a layer that allows full manipulation of the data. Thus, it can extend the life of old systems—or, if desired, help to retire those systems. In turn, you'll help your users use their data in the most effective way.

A Service Oriented Architecture helps move data across the network because it eliminates redundant moves. Coordination and governance are key in successfully employing a SOA.

A SOA allows you to build applications that solve a particular problem once, and then you are enabled to propagate the usage of that code across the organization. This reuse of code, as well as having a single structured location to store the data, increases efficiency and eliminates the duplication of code and data in the various silos of the organization.

Once the first application is fielded, as new applications are needed, they can be built using the same structure (and quite possibly the data that is already stored in the application). This way, the new application does not require an entirely new database that must store the identifying information. This is when the SOA architecture starts to bring real value: when the application being developed is more efficient from the start and data storage and computer systems can be reused or used more efficiently. As a result, the organization no longer needs to invest in new hardware, software, database structures and storage. This gain after adding the initial system is much more apparent than it was in the first application. The gain from subsequent applications is the real benefit of the SOA and should be the ultimate goal of the organization.

STRATEGIC PILLAR 5: SELECTING A TRUSTED PARTNER WHO CAN ALIGN YOUR BUSINESS MISSION TO THE RIGHT TYPE OF CLOUD & SERVICE-ORIENTED ARCHITECTURE

The federal cloud mandate represents a dramatic new way to use federal resources. In today's world of tightening budgets and increased scrutiny, the creation of permanent new structures is just not sustainable. The cloud will maximize the Federal Government's resources.

For instance, federal government teams can come together to complete projects and then go their separate ways when the work is done. Resources will be allocated more efficiently. The hope is that federal agencies will be able to reduce redundancies and focus more squarely on their core missions.

Former Federal CTO Aneesh Chopra has emphasized the importance of modernizing the government's tech infrastructure. He said, "We want to make sure there are opportunities for all forms of cloud computing—private clouds, hybrid clouds, commercial clouds — and we've been engaged in the process."[7]

How will *your* federal agency get to the cloud? A trusted technology and business partner can help you through all the steps and processes described in this white paper for getting to the cloud.

Choosing your trusted advisor wisely is critical to your success. The advisor's management and risk strategies must be assessed, keeping aware that IT solutions providers are also going through their own transformation to cloud delivery models.

About IntelliDyne, LLC

IntelliDyne is a consulting firm that enables better business performance through innovative technology solutions. We manage public sector programs that deliver higher operational efficiency and measurable value to clients. We advise, develop, and execute effective solutions in Cyber Security, Cloud Computing, Application Development, Mobile Computing, Business Process Management, Data Center Consolidation, Enterprise Collaboration and Enterprise Infrastructure Management.

For more information, visit our web site at www.intellidyne-llc.com or contact us at cloud@intellidyne-llc.com.

[7] Krill, Paul. *InfoWorld*. 'Obama's CTO Eyes cloud, mobile options.' 01 June 2011. http://www.infoworld.com/d/cloud-computing/obamas-cto-eyes-cloud-mobile-options-684