Transforming Government Services with a Secure, Compliant Private Cloud Environment

Introduction

Today's citizens of national, state, and local governments want and expect services and a secure user experience at every point of need—much like what they have experienced in the private sector.

As a result, governments are under pressure to provide more efficient, secure, and effective citizen-centric applications and services, as well as improve inter-departmental and cross-agency collaboration. To better serve their constituencies, government IT leaders are being asked to transform costly and inflexible legacy infrastructures, increase the productivity of existing workforces, enable cross- agency collaboration, and improve overall organizational agility while balancing economic pressures and security concerns that range from the security of online users and security breaches to the continuity of government and public safety during disasters and crisis.

Cloud computing—IT resources and services that are abstracted from the underlying infrastructure and provided on demand and at scale in a multitenant and elastic environment—offers government leaders the ability to break down aging IT silos with their inefficiencies, high costs, and ongoing support and maintenance issues while improving collaboration and meeting increasing user demand for cost-effective, innovative citizen services on demand across network, computing, and storage resources.

Cloud computing is justifiably called a transformational model for businesses and governments. It transforms IT and the data center as we have known it: dedicated consumption, lengthy hardware procurement, manual addition of new services, manual repair of system failure, provisioning in months, and incremental capital expenditures.

Cloud computing can provide flexibility, efficiency, and democratization around resource allocation, resulting in agile IT service delivery—provisioning in minutes and time to market reduced by more than 50 percent—and cost optimization with higher server and storage utilizations, 50 percent reduction in capital costs, and 25 to 30 percent reduction in operational costs.

And it affects the very way we do business—back office, online citizen services, and public safety, to name a few—and the way and how cost-effectively we engage with government co-workers, partners, vendors, and citizens.

Cloud computing profoundly transforms the way in which information and services are provided to and consumed by citizen users: shared, self-service, scale on demand, automated recovery, provisioning on demand, and pay per use.

In a multitenant cloud environment, cloud security—especially policy control, visibility, testing, auditing, encryption, on-demand security controls, and automated security management for rapid provisioning—becomes increasingly important, as does end-to-end isolation of data, data transmission, and data delivery across the delivery infrastructure—network services, network, computing, storage, and management. In fact, cloud computing can offer some security advantages:

- Cloud homogeneity makes security auditing/testing simpler.
- Clouds enable automated security management.
- Clouds can provide redundancy/disaster recovery services.

In evaluating clouds, government agencies might decide that some applications, data, and services should not be transitioned to any cloud. But they also might shift certain public data to a private cloud to reduce the exposure of internally sensitive data to public access.

As the cost of service delivery and the momentum for "green" initiatives increase, governments must continue to lower infrastructure costs, including security infrastructures, and maximize limited capital and operational spending while evolving their infrastructures.

The U.S. federal government, for example, is in the midst of a major effort to modernize its IT infrastructure. IDC has noted that the government IT modernization effort will require a "rearchitecting of government processes and workflow practices" (Source: IDC Datacenter Centralization and Consolidation at the Heart of Driving Federal IT to Cloud-Computing Economics February 2010).

According to the Federal Data Center Consolidation Initiative outlined in February 2010, the cost of operating a single data center is significant. And that cost has been growing exponentially, due to the explosion in the number of federal data centers from 432 in 1998 to 1,109 in 2009. The initiative memorandum cites cost, inefficiencies, and the lack of sustainability, as well as impact on energy consumption. By June 30, 2010, federal agencies are expected to develop a consolidation plan identifying areas of optimization through server virtualization or cloud computing.

In fact, cloud computing IT services are currently being offered on the Government Services Administration (GSA) website—Apps.gov. According to the website, cloud computing offers scalability, frees up resources, provides service quality, and is easy to implement.

At the state and local level, 45 percent of responding local governments are using cloud computing to maintain applications or provide services, according to an April 2010 survey by Public Technology Institute—a national non-profit technology research organization created by and for city and county governments. Nineteen percent of responding local governments plan to use cloud computing services in the next 12 months; 35% of responding local governments cloud had no plans for cloud. Those not yet interested in moving to cloud cite the cost or lack of business case and security. State and local governments cited resource savings as a primary driver toward cloud—with web hosting/content delivery, collaboration applications, and electronic mail as the top three cloud applications.

The overall cloud computing market, composed of infrastructure-as-a-service (IaaS), software-as-a-service (SaaS), and platform-as-a-service (PaaS) service models, is growing with estimates of approximately $60 billion by 2012. (See Figure 1.) Infrastructure as a service (IaaS)—a cloud utility architecture—provides an easy cloud entry point for the public sector. In fact, a number of governments are considering the private cloud, in which the data center operates as an infrastructure as a service.

IaaS is a new operational model for accelerated delivery of the new IT high-value services—at reduced cost. For example, IaaS can enable consolidation and virtualization of under-utilized IT computing resources into a virtualized cloud environment with increased flexibility due to IaaS' rapid provisioning capability. IaaS offers a highly attractive, cost-effective solution with its potential to controls costs, deliver better return on investments through multitenancy services, and enable new citizen and cross-agency service offerings and rapid service provisioning and delivery.

Cloud computing can help governments of all types and sizes to continue to lower infrastructure costs, including security infrastructures; maximize limited capital and operational spending; secure the user experience; manage a multi-tenant infrastructure; align and optimize internal processes; enable usage-based per agency or department unit costing; define and rapidly deliver service-level agreements (SLAs) for applications, and help meet the demand for services and rapid service provisioning.

The journey away from traditional IT infrastructures toward cloud computing and IaaS is no small undertaking for governments and their leaders at every level. Governments may benefit from:

- A clear understanding of cloud benefits and limitations
- A well-defined cloud model and architecture requirements
- Identification of needed changes to IT operations and business processes, especially security, governance, and compliance
- An assessment of risk and financial effect
- Reduced risk during a transition
- The resources to make the IT transformation efficient; cost-effective; and, most importantly, of real continuing value to employees, partners, vendors, and customers

The journey's goal is a trusted cloud with the network as the logical platform to bring the existing assets in the data center and new cloud computing approaches together with virtualization, governance and security, and information and applications.

As in any journey, something unexpected can occur. The ease and success of the journey really depend on very good planning and expertise in delivering initiatives of this complexity and magnitude. (See Figure 1.)

Government Leaders Are Asking...

- What is our cloud strategy?
- How do we gain the benefits promised by cloud?
- How quickly can my agency scale to meet citizen or other agency demands?
- How can we assess and track the ROI with cloud computing?
- How does cloud computing affect the security of my government agency or department and my customers?
- How can we become greener in our operations with cloud?
- How can we cost-effectively and effectively serve our constituencies with more and better services?

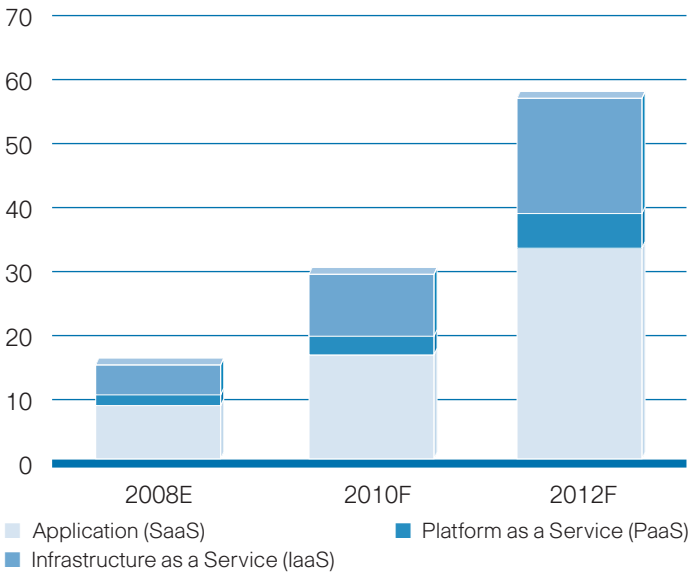
Government CIOs Are Asking...

- What is the role of IT in an organization and the effectiveness of IT spend?
- What are the goals of IT over the next year?
- How scalable and flexible is my data center?
- How do I control IT cost spending or cost avoidance and reduce business risk?
- What can I do about server sprawl (leading to power, cooling, space challenges, and overall cost issues)?
- What about disaster recovery of critical computing infrastructure?
- How can I meet governance and compliance requirements and deliver secure operations?
- What about adoption of virtualization or cloud technology?

Government IT Directors Are Asking...

- How quickly can I deploy compute infrastructure to respond to my needs?
- What constraints are keeping the organization from fully utilizing the current compute infrastructure?
- How much would the organization save if it had more robust infrastructure?
- What is the balance between rapid provisioning and secure operations for the organization and citizens?

Figure 1. A Growing Cloud Computing Market—Estimated at ~$60B by 2012



Source: Cisco IBSG; Saugatuck, IDC, Gartner, TripleTree, Deutsche Bank

What Government Leaders Are Asking

Not surprisingly, leaders within government are asking sometimes difficult, though highly relevant, questions about the nature of government IT and the value of the cloud, often based on the role they play in the organization.

Government leaders are seeking competitive advantage and improved time to market for their organizations any time they make an investment in government IT. They want to have a cloud strategy in place that makes sense for their unique needs and citizens. And they want full benefit from any cloud model, especially the ability to scale to meet the needs of the various publics.

Government CIOs and IT managers want to maintain the relevancy and cost effectiveness of IT within the larger organization. They are typically struggling with the rate of growth of their IT infrastructure, the costs of managing it, low resource utilization, and the necessary flexibility to meet the rapidly changing needs and outreach required of the agency or department.

Government CIOs and business unit leaders might be considering what their cloud strategy should be to maximize the public benefit. They are primarily concerned with costs and benefits in addition to strategic direction.

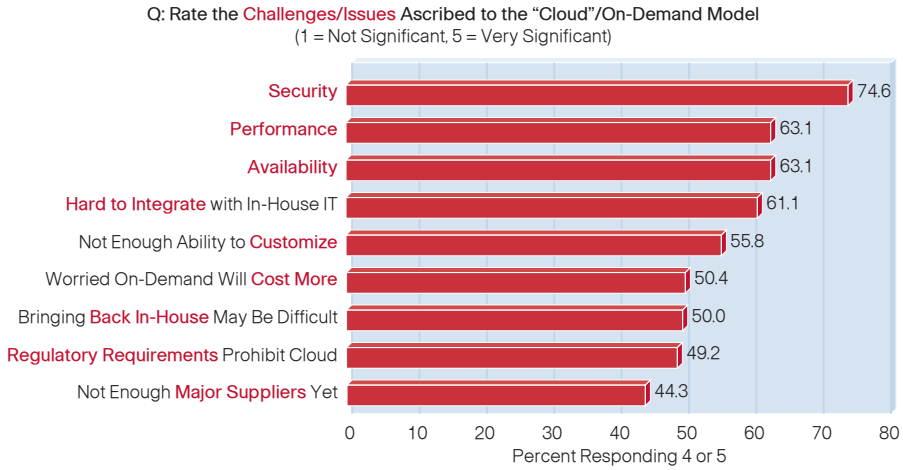
In contrast, IT and data center architects from the network, storage, and computing teams need expertise to help accelerate design and implementation of cloud-based architectures and solutions.

Since architects and solution designers are more focused on design and implementation of an existing cloud strategy, they are more interested in assistance related to the architectural implementation and operational models that cloud services can deliver.

And government IT program managers are focused on maintaining existing infrastructure, not developing IT roadmaps and meeting new organizational needs. They also might be dealing with a myriad of vendors and partners who are involved in current environments and would be required to deliver a cloud-enabled solution.

Unfortunately, there is no one-size-fits-all cloud solution: organization needs as well as network, computing, and storage quality and overall IT complexity differ from agency to agency. Based on Cisco's own research surveying 700 customers in December 2009 (16 percent service providers, 11 percent financial services, 8 percent Government organizations), security, however, is the number one cloud concern. (See Figure 2.)

Figure 2. Security Research Results (IDC, August 2008)



Source: National Institute of Standards and Technology (NIST): www.csrc.nist.gov/groups/SNS/cloud-computing/index.html.

Exploiting Infrastructure as a Service for Business Benefit

In many governments today, the infrastructure evolution toward cloud computing is under way. Over the last few years, IT has been responding to new user demands and, in the process, laying the foundation for cloud computing with:

- Consolidation of computing resources
- Virtualization of resources, with some 30 to 40 percent of businesses virtualized today
- Reprovisioning resources on demand
- The beginnings of automation with the decoupling of physical assets and services

As more governments explore cloud computing, many government leaders are considering the private cloud, in which the data center operates as an Infrastructure-as-a-service (IaaS) utility. For the first time, virtualization and extending the virtualization architecture beyond the boundary of organization, service-oriented architectures and extending service orchestration, automated provisioning, and unified computing are making IaaS architectures technically and operationally feasible.

Cloud adoption requires an approach that covers the virtualized data center architecture and the IaaS cloud operations management architecture. These architectures must work in conjunction; through cloud service orchestration, changes and updates are made simultaneously to both. The IaaS cloud operations management includes such technologies as cloud service orchestration, which runs an end-to-end workflow; usage-based chargeback mechanisms; service level agreement (SLA) management; and a federated configuration management database (CMDB).

IaaS Benefits for Governments

- Consolidation and virtualization, thus reducing capital expenditures
- Amortization of infrastructure across multiple customers, which translates into cost savings
- Realization of economic efficiencies
- Rapid provisioning of services with immediate relevancy to citizens

In essence, IaaS is a modular infrastructure solution with data services that can be turned on and off based on customer demand and available capacity. Podlike units of network, storage, and computing resources can be right sized for target applications and virtual workloads. This flexible architecture scales up or down, enabling elasticity for customers. It also provides rapid provisioning and end-to-end SLA management capabilities. The data center architecture, which can span many data centers, can provide business continuity and disaster recovery. IaaS also delivers ease of platform migration for workloads, multiuser support, and multiple application lifecycle support.

So not only are there quick deployment, migration, and scaling of applications and associated infrastructure, but the cost advantages for applications from IaaS are significant: low cost per resource; no waste from overdimensioning; and capital expense is converted to operating expense, a variable cost. Most importantly, the rapid provisioning and orchestration capabilities intrinsic to cloud and IaaS transform the user's experience of service delivery, in contrast to traditional service procurement cycles, which could take months rather than minutes.

IaaS also enables:

- Utility computing service and billing model
- Automation of administrative tasks
- Desktop virtualization
- Policy-based services

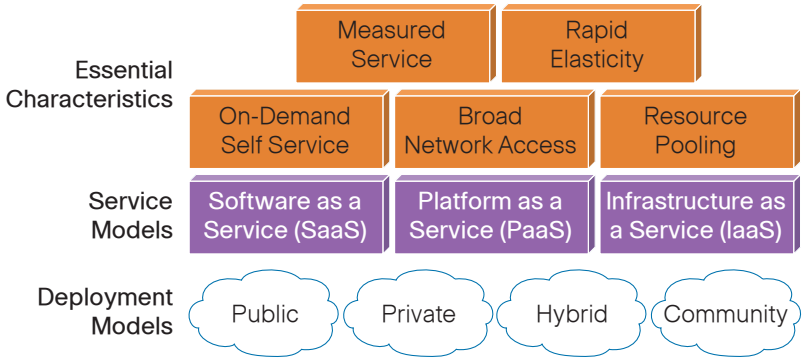
Private Clouds and Other Cloud Approaches

IaaS is one of three major service models in the cloud computing value chain. The foundation of the cloud, of course, is the IT infrastructure.

Software as a service (SaaS) provides applications services delivered over the network on a subscription basis. Cisco® WebEx® and Salesforce.com are two well-known providers of SaaS.

Platform as a service (PaaS) provides software development frameworks and components delivered over the network on a pay-as-you-go basis. Examples include Cisco WebEx Connect and Google Apps Engine. (See Figure 3.)

Figure 3. Visual Model of NIST's Working Definition of Cloud Computing



Source: National Institute of Standards and Technology (NIST)
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

Computing as a Service: Use Case

Business Challenge

- Scalability issues
- Slow end user response times
- Variable capacity demand
- Lengthy provisioning times for new computing capacity
- Difficulty in allocating IT service delivery charges
- Unplanned, escalating capital/operational computing costs at peak demand periods

Solution: Computing as a Service

- Provided by an IaaS cloud
- On-demand, additional computing resources in response to variable service demand

Benefits

- Highly virtualized computing/network/storage for cost-effective capacity expansion
- Share spare capacity depending upon time of day/year
- Rapid service orchestration
  - Next-generation IT provisioning approaches using web-based portal
- Compute resource scalability and elasticity
  - No capacity planned before the need identified
  - Burst capacity easily allocated
- Fewer capital investments for periodic surges

Challenges to Realizing Solution

- Assessing the costs and benefits using financial return on investment models
- Devising the most flexible CaaS architecture with high degree of virtualization
- Extending or replacing your IT systems management tools to deliver the rapid IT services provisioning required to make CaaS effective
- Implementing a highly secure cloudarchitecture
- Devising departmental chargeback strategies to bill according to actual usage

There are several cloud deployment models:

- **Private clouds:** enterprise IT infrastructure services, managed by the organization, with cloud computing qualities such as self-service, pay-as-you-go chargeback, on-demand provisioning, and the appearance of infinite scalability
- **Virtual private clouds:** cloud services that simulate the private cloud experience in public cloud infrastructure
- **Public or external clouds:** cloud infrastructure made available to the general public through web browsers or through APIs but offering limited customer control
- **Community clouds:** cloud infrastructures shared by several organizations and supporting a specific community; for example, several financial service banks join to form a financial community in a cloud
- And, in the future, **hybrid clouds:** cloud infrastructures composed of two or more clouds able to interoperate or federate through networking technologies, across data center/organization boundaries

Governments can use IaaS architectures to offer specialized services:

Computing as a service (CaaS): A pay-as-you-go service that provides customers with rapid access to virtual servers for a wide range of applications. Enterprise decision support systems, for example, require large data sets that are expensive to manage, while seasonal variations and short-term projects stretch capacity. An IaaS solution provides capacity on demand.

Data center as a service (DCaaS): On demand data center capabilities, including service burst capability to business units to meet increased demand. Organizations with computing-intensive data center requirements can utilize data center as a service to provide capacity for processing and storage on the fly. Grid computing, for example, can pose massive short-term requirements, but is a noncore business for most organizations. An IaaS-based solution provides capacity to that level.

Virtual desktop infrastructure (VDI): VDI provides the infrastructure for hosting a desktop operating system within a virtual machine on a central server. Upfront server investment reduces VDI project ROI, while variable utilization can limit potential virtualization benefits. Using IaaS to support VDI increases the security of end user environments and reduces IT service delivery costs.

In CaaS, DCaaS, and VDI, organizations can leverage their secure and virtual infrastructure and tight SLAs for economies of scale and rapid provisioning via service orchestration to provide burst capabilities.

High I/O cloudburst: By combining corporate infrastructure with cloud-based infrastructure, you can create a flexible, highly scalable application hosting environment with rapid access to additional capacity for peaks of demand. ERP financials, for example, impose seasonal resource demands and incur the sunk cost of customizing financial applications. An IaaS service increases organizational agility with lower costs and adjusts for changing or seasonal demand.

Disaster recovery: Today, many disaster recovery systems remain expensive, seldom used cost centers. IaaS offers the capability to consolidate multiple disparate disaster recovery systems into a single virtualized instance, shared across multiple IT applications, to increase asset utilization and reduce cost. Disaster recovery represents a low-risk service for organizations since they still own primary infrastructure. Provisioning is rapid via orchestration automation.

In order to pilot a cloud approach, some organizations are starting with lower risk IT cloud services, for example, software development and test cloud environments. A high degree of virtualization achieves economy of scale and reduces service delivery costs.

Development/testing environment: Requirements on testing environments are volatile, with frequent short-term, unplanned resource requests. An IaaS solution enables developers to reduce or eliminate underutilized capacity and equipment and supports all software development phases, including unit test, systems test, and scalability testing to increase responsiveness in responding to development and test environment requests from IT business units.

How to Create a Cloud Approach That Works for Your Government

Many government IT organizations are navigating infrastructure changes involving complex tradeoffs and decisions and then creating design and implementation programs around cloud transitions with only their in-house resources and expertise to guide them and without the benefit of best practices for the wide variety of technologies involved.

With an in-house approach, government organizations could experience some common cloud challenges, such as:

- Limited virtualization around the endpoint computing resources
- Failure to exploit innovative, cost-saving initiatives such as business continuity/disaster recovery into the cloud
- Security inadequately focused at the application or server layer only
- Lack of customer isolation using secure, scalable multitenant services

Since an exclusively internally focused approach to building a cloud would use already stretched in-house resources, one solution is to look to a professional services group that has built and secured data centers, infrastructures as a service, and private clouds; can work with your own in-house expertise in a collaborative fashion; and can draw upon an ecosystem of trusted best-in-class partners.

In addition, it is also possible to construct a government IT wish list for making the transition to the cloud easier, including, for example,

- Choice
- Alignment with business strategy and goals
- A comprehensive, architectural approach
- A full service and solution offering with robust security
- Measurable benefits such as time to market

Based on the organization wish list, then, **choice** would include a **vendor-independent; technology-independent; and open,** customized service and support model delivered by experts.

The service approach and process would require a deep understanding of your data center and organization that is **effectively aligned with your business goals and strategy.**

The service and support solution would embrace all phases of your network, computing, and storage resource lifecycles. In short, your **approach** should be **structured and comprehensive.**

As a corollary to choice, the **products and services** utilized in delivering a cloud model should be **best in class:** provided by an **ecosystem of best-in-class partners.**

Finally, the resulting cloud model must be built upon a **development architecture that aligns with your strategy** and **fits your business needs.**

Business Continuity with Disaster Recovery as a Service (DRaaS): Use Case

Business Challenge

- Devising a cost-effective disaster recovery solution for server-based applications
- One-to-one server redundancy very costly
- Traditional many-to-one schemes might expose business or leave specific applications without capacity

Solution: Business Continuity with Disaster Recovery as a Service (DRaaS)

- Provided by an IaaS cloud

Benefits

- Reduce risk/costs of failure using highly virtualized computing/network/storage for cost-effective backup server provision
- Share spare capacity upon time of day/year
- Rapid service orchestration using next-generation IT provisioning approaches to adjust to necessary capacity
- Avoid additional capital investments that a one-on-one scheme would require
- Enable usage-based billing when disaster recovery needed

Challenges to Realizing Solution

- Assessing costs and benefits using financial return on investment models
- Devising the most flexible DRaaS architecture for required failover coverage
- Extending or replacing IT systems management tools for rapid IT services provisioning required to make DRaaS effective
- Devising departmental chargeback strategies to bill according to actual usage

Government Wish List for Transitioning to Cloud

- Choice: vendor and technology independent, open, secure
- Alignment with your business strategy and goals
- A comprehensive, architectural approach
- A highly secure development architecture for your organization needs
- Rapid time to market

A Comprehensive, Architectural Approach

Let us take a closer look at this recommended approach and how that might work for transitioning your government organization to IaaS or another cloud model. This approach has four basic phases, during which some important questions should be answered.

- **Strategic preparation:** What can cloud do for my government agency or department? How does it affect my resources and costs? What can I expect in ROI? What will be the effect on my processes and operational structure? How does cloud computing affect our security program, security architecture, and customers? What are the gaps between the current security architecture and our targeted cloud security architecture? What is the state of the security architecture of our existing private cloud? What applications, data, and services are suitable for migration to a public cloud? Does our strategy anticipate support for postdeployment (day 2) activities and how we evolve the cloud for greater benefit?
- **Planning and design:** What end-to-end architectural approach is most appropriate to deliver for my chosen cloud strategy? What architecture maximizes virtualization, orchestration speed and design, and chargeback capability? How does cloud computing affect security and our overall technology architecture, including network, services, computing, and storage, as well as our customer-facing security? How can we build a security technology architecture for cloud? How do we plan and design for the evolution of our cloud infrastructure? How do we plan and design for a phased introduction of many cloud models?
- **Implementation:** How do we realize our cloud architecture on time, within budget, and in our environment? How rapidly can we implement the security technology architecture? Does our cloud implementation provide the groundwork for cloud evolution?
- **Optimization:** How do we continue our cloud evolution and ongoing cost reduction? How do we continually optimize our security capabilities?

Strategic Preparation

Experts you trust can help you navigate these phases, helping you to decide on the appropriate cloud computing strategy, ranging from questioning and evaluating whether cloud computing is an appropriate agency, department, or initiative strategy to seeking architecture and security planning and design, implementation, and optimization expertise. Expertise should be based upon extensive experience in designing complex data centers across the multiple technology areas, such as virtualization, service orchestration, automated provisioning, and security that underpin IaaS architectures.

A strategy service should help you evaluate the most appropriate strategy for cloud adoption, including the costs and benefits and operational changes required to successfully benefit from a cloud operational model. Evaluating the current and required services management approach and analysis of how you can transition to a service-driven model occur at this stage and help align subsequent cloud architectural development, tools, and process integration and implementation with business returns.

Strategic preparation should also target security. Government IT experts should evaluate their cloud security risk and architecture security risk and look at protecting access and providing on-demand security options within a services catalog for their users.

In addition, your strategy should take into account your cloud evolution and postdeployment activities in every stage: strategy, planning and design, implementation, and optimization.

Thinking About Security in the Cloud

Security is the number-one issue, according to Cisco's own customer survey results, for government leaders evaluating cloud computing.

Here is a checklist of security issues and capabilities to consider.

- Security based on cloud types: for example, private versus public cloud security
- Security based on the need for an organization security program and security for users
- Refocusing your security policy for the organization and cloud transition
- Role of a dedicated security team to ease the security transition
- Common controls and technical security control overlap
- Policy controls across network, computing, and storage resources
- Visibility controls to address loss of control due to abstraction
- Logging controls:
  - Security dashboard with both policy control and visibility to address logging challenges
  - Secure API access integrated into management and tooling systems to address logging challenges
- Isolation of data, data transmission, and data processing for end-to-end isolation across the delivery infrastructure (including network services, network, computing, storage, and management)
- Encryption:
  - Encrypting access to the cloud resource control interface
  - Encrypting administrative access to OS instances
  - Encrypting access to applications
  - Encrypting application data at rest
- Public version control for SaaS
- Security auditing and testing for compliance
- On-demand security controls within the security catalog for users
- Automated security management to meet the rapid provisioning requirement
- Using existing virtualization as a mechanism for security monitoring and enforcement

Planning and Design

When undertaking IaaS, strategic planning and design can help reduce time to successful deployment and operation of complex IaaS solutions. Cisco Data Center Virtualization Design Services for Cloud, formerly known as Cloud Planning and Design require expert coordination among your team, your partners, and other vendors, as well as a detailed architecture design, data center–specific expertise, and security designed from end to end. The resulting designs and plan - including, for example, an end-to end IaaS architecture blueprint, SLA design, dynamic billing and chargeback design, migration roadmap, facilities, mechanical, and electrical design, a common con-trol framework, a security technology architecture, a user-facing portal design, physical safety and security, and your future cloud evolution—should link back to your strategy and lay the foundation for subsequent implementation and integration.

After the planning and design stage is completed, you are ready for implementing a cloud operational model, which should be a long-term investment opportunity.

Implementation

What is needed to reduce the risk during an IaaS implementation is experience at providing a virtualized architecture, integrated tools, a facilities plan, orchestration integration, workload migration, and staging and validation activities prior to full-scale IaaS implementation. This phase also involves implementing the security technology architecture, the security portal design, automated audit, and physical safety and security designs.

Proven methodologies, best practices, and deep knowledge of the core systems within the cloud environment can facilitate migration from your existing environment to a cloud utility computing architecture, help assure adherence to plans, and enable on-time delivery of a fully implemented IaaS. During this implementation stage, knowledge transfer also should be an ongoing process and end goal enabling operational confidence for in-house experts.

Since cloud evolution has been anticipated in your strategy, planning and design, and implementation phases, your agency or department is poised to maximize its ROI with optimization of the cloud operational model.

Optimization

Optimization of the cloud operational model, which can accelerate adoption of IaaS, is the point where the true benefits of the private cloud—lower operating and capital expenses, increased security, business agility and responsiveness, and scalability—can be maximized through:

- Architectural reviews
- Security audits, security architecture and posture assessments, and an ongoing security operations office
- Cost reduction exercises
- Process improvements
- Tool customization
- Post deployment or day 2 support

Unfortunately, if you neglect or are unable to take a comprehensive approach to your cloud transition, then you might be at risk of losing competitive advantage through failure to realize a cloud operational model. Additionally, government organizations that embark on a cloud IaaS architecture design, without first detailing the strategic objectives and security and assessing the ROI, might find that their cloud project fails to deliver business benefit. And government organizations that fail to recognize that cloud is an operational model, not just a technology, are more likely to invest heavily in projects that overrun and fail to deliver measureable benefits.

What is crucial to successful realization of IaaS cloud business benefits is to take a comprehensive, architectural approach across strategy, security, ROI-driven architectural decisions, tools, people, and process changes that are required to deliver the promise of the cloud. (See Figure 4.)

Figure 4. Expertise and Services Required for Building a Cloud Operational Model

Five primary criteria for evaluating in-house and outside services should be their ability to deliver a cloud operational model by:

- Developing a financially justified strategy and reducing transition risk
- Aligning IT services management people and processes with your business objectives
- Accelerating the development, implementation, and optimization of a validated and secure IaaS architecture, integrated tool design, and chargeback mechanism
- Creating a phased migration plan to enable a successful adoption of the new cloud operational model and preparing in every stage for the cloud evolution and post-deployment (day 2) activities
- Increasing the time to value of the data center architecture for cloud services creation and delivery

Conclusion

To obtain the very real benefits of cloud computing, government leaders should consider and evaluate all significant issues and tradeoffs around making the transition to a cloud model: service advantage, security, operational change, cost, capital investments, operating expenses, new or evolved technical and business architectures, and risk.

Whether beginning or in the middle of the journey to a next-generation data center and cloud computing, your government organization will benefit from best-in-class team- and partner-based enablement services across your architectures. The experts you choose to guide you should be able to address the entire environment, offer validated designs and industry best practices, and understand the capabilities and feature sets of all network, computing, and storage devices within your environment.

Enablement services also can help you exploit the full capabilities of the cloud model, including the ability to dynamically provision resources; virtualize applications and services; enhance business resiliency; build security into every layer of the virtualized infrastructure for a secure, compliant cloud environment; and, most importantly, evolve your chosen approach or add new clouds for public benefit as opportunities develop in the future.

To make the journey to and beyond your first cloud easier, your cloud approach should include:

- Choice: vendor and technology independence, open
- A development architecture that meets your organization needs and extends services
- A comprehensive, architectural approach that anticipates your cloud evolution in every stage and into the future
- Access to industry best practices, validated designs, and an ecosystem of best-in-class partners
- Expertise in virtualized data centers and end-to-end orchestration, service provisioning, and security across network, computing, and storage resources
- Experience in strategizing for, planning and designing, implementing, and optimizing IaaS and clouds

A secure IaaS cloud approach with infrastructure management tools for rapid orchestration of new services, service-oriented billing and chargeback mechanisms, and IT services management around people and process alignment can help transform government IT service costs, while enabling IT to better meet collaboration and service demand from co-workers and citizens, as well as deliver greater service responsiveness and agility.

For More Information

For more information about cloud computing and cloud enablement services at Cisco, visit: www.cisco.com/go/cloudenablement.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in the USA C11-604242-00 05/10