Executive Summary

Cloud computing marks an evolution in the deployment and management of information technology (IT). Cloud computing will reduce total cost of ownership (TCO) while increasing business agility, flexibility and service innovation. However, realizing the benefits of cloud computing involves dealing with age-old concerns, including security, compliance, privacy, data location, interoperability, service level monitoring, and potential vendor lock-in. To help government IT leaders navigate through the complexity of adopting cloud computing platforms and to maximize the potential benefits, Intel Corporation, in collaboration with the Innovation Value Institute (IVI), presents a Cloud Technology–Capability Maturity Framework* (CT–CMF*). The CT–CMF’s objectives are to offer a standardized approach for government IT leaders, to identify the current status of their cloud computing capabilities, and to provide a systemic path to improvement. As we talked to government IT leaders around the world to understand their views and experiences with cloud computing, Intel also developed a six-point quick-start checklist for government cloud computing programs. The criteria checklist will help promote successful adoption by designing cloud systems that are secure, agile, dependable, open, transparent, and aware. We expect governments to benefit by using the CT–CMF and the criteria checklist in their cloud computing journey to rapidly realize benefits from government cloud computing investments.

Jim Kenneally
Intel Labs
Kieran Mulqueen
Intel Labs
Jimmy Wai
Intel Sales & Marketing

*Other names and brands may be claimed as the property of others.
Introduction

According to CIO.gov, “Cheaper processors, faster networks, and the rise of mobile devices are driving innovation faster than ever before. Cloud computing is a manifestation and core enabler of this transformation. Just as the Internet has led to the creation of new business models unfathomable 20 years ago, cloud computing will disrupt and reshape entire industries in unforeseen ways.”

Technology deployment is increasingly becoming a key component of delivering better public services. The arrival of cloud computing comes at a time when many governments are stipulating that departments and agencies optimize their IT service delivery costs and, at the same time, improve flexibility and responsiveness – in essence, do more with less. The cloud computing model can significantly help organizations and agencies in the public sector grapple with the need to provide highly reliable, innovative IT services quickly despite resource constraints.

Many government departments and agencies are banking on the economics promised by cloud computing to consolidate procurement, optimize expenditures, increase agility, and improve public services. Government departments are increasingly mandated to consider cloud systems first whenever a secure, reliable, cost-effective cloud option exists. To this end, many governments and public-sector bodies are surveying their path toward adopting cloud computing.

Cloud Computing

Cloud computing is an evolution in which IT consumption and delivery are made available in a self-service way via the Internet or internal network with a flexible, pay-as-you-go business model that runs on a highly efficient and scalable architecture. In a cloud computing architecture, services and data reside in shared, dynamically scalable resource pools, often virtualized. Those services and data are accessed by any authenticated device over the Internet or an internal network. The U.S. National Institute of Standards and Technology (NIST) defines cloud computing this way:

*Cloud computing is a model for enabling ubiquitous, 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.*

Furthermore, NIST has identified five essential characteristics of cloud computing as:

1. On-demand self-service
2. Resource pooling
3. Measured service
4. Broad network access
5. Rapid elasticity
Cloud Service Models

Cloud computing architectures are divided into three service models, infrastructure as a service, platform as a service, and software as a service. Each model shares similarities but has its own distinct differences. Choosing a service model typically depends on trade-offs between cost, complexity, and security. Very often, multiple service models are utilized, each suited to satisfying differing needs.

Cloud Deployment Models

Cloud computing architectures are deployed in different ways depending on the organizational structure and the provisioning location. The three basic deployment models are public, private, and community. In addition, these models can be melded to form hybrid models.

International Government Cloud Trends

Until recently, many government cloud deployments were primarily addressing data center consolidation and more efficient provisioning of commodity IT services. However, as the pursuit of greater efficiencies and better public services intensifies, government departments and agencies are becoming increasingly interdependent. This intensification is forcing a shift toward a matrix of shared IT services spanning multiple government departments and agencies. Consequently, governments are seeking to understand how cloud deployment can best support various services that are provided either across government agencies or directly to the general public. From the process of examining national and international trends, distinct patterns and themes are emerging regarding government cloud adoption trends.

Six Key Criteria For Effective Government Cloud Adoption

The six key criteria define the key characteristics resulting from the examination of numerous successful government cloud initiatives. Table 1 provides a quick summary and each criterion is then discussed in length.

<table>
<thead>
<tr>
<th>TABLE 1: SIX KEY CRITERIA FOR EFFECTIVE GOVERNMENT CLOUD ADOPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SECURE</strong></td>
</tr>
<tr>
<td><strong>AGILE</strong></td>
</tr>
<tr>
<td><strong>DEPENDABLE</strong></td>
</tr>
<tr>
<td><strong>OPEN</strong></td>
</tr>
<tr>
<td><strong>TRANSPARENT</strong></td>
</tr>
<tr>
<td><strong>AWARE</strong></td>
</tr>
</tbody>
</table>
Secure

Security is often the top concern for government departments and agencies considering the move to cloud-based services. Government departments and agencies need to reassess the traditional IT network firewall protection principle in recognition that the movement of data increasingly crosses the IT network firewall. This means building security into data, applications, infrastructure, and hardware layers (i.e., adopting end-to-end layered security) rather than relying on the assumption that the IT network firewall is the first and last line of defense.

Security models and assumptions need to evolve as governments adopt cloud computing. To address such security needs in the move to cloud computing, proactive government departments and agencies are working with industry to define security standards and implementation approaches (e.g., encryption, authentication, authorization, and geo-location capabilities). Initiatives such as the European Union Agency for Network and Information Security (ENISA) aim to improve the public sector’s understanding of the security of cloud services and the potential indicators and methods that can be used during service delivery.

Agile

Cloud computing continues to capture the attention of both the public and private sectors with the promise of improved agility, scalability, and self-service provisioning of IT services. Cloud computing promotes scalability through adoption of common processes within and across government agencies and departments. Furthermore, the cloud computing delivery model offers easier access to the latest technology innovations. Compared to government IT services running on non-cloud infrastructure, government cloud systems can often dramatically reduce setup times for new applications and offer better scalability, resiliency, and service levels when systems are in use.

For example, the U.S. Federal Labor Relation Authority (FLRA) moved its case management system to a cloud-based SaaS solution and reduced total cost of ownership by 88 percent over five years. Additionally, moving to a cloud-based platform provides the FLRA with secure access to case information from any location in the world, supporting rapid decision-making and organizational agility. The U.S. Social Security Administration’s (SSA) Online Answers Knowledge Base uses a highly scalable cloud-based system to meet peak traffic loads without needing additional infrastructure. Nearly 99 percent of its 25 million Web self-service sessions are handled without agent intervention.

Dependable

Dependability is another highly advertised advantage of cloud computing. The highly configurable, virtualized, and managed cloud infrastructure creates an opportunity to enable higher levels of redundancy and resilience when compared to some of the more traditional infrastructure approaches. On the other hand, the shared nature of cloud infrastructure creates more
security, compliance, and service-level variables to be managed. Using cloud technologies and services (either inside or outside government firewalls) increases the need for government departments and agencies to verify that the underlying cloud infrastructure is secure and that compliance policies are enforced. Governments are increasingly using the power of the purse to demand improved quality, dependability, and accountability from their cloud service and component providers. Initiatives such as the U.S General Services Administration's Federal Risk and Authorization Management Program (FedRAMP) standardize cloud security procedures and provide centralized certification of third-party providers of cloud services to government departments and agencies.

Open

Government departments and agencies increasingly mandate that their cloud deployments be based on accepted Internet protocols and use open and interoperable standards. The objective is to guard against technology lock-in and avoid individual vendors securing a disproportionately high share of government business. Furthermore, open and interoperable standards provide a platform for collaboration across government departments, where information can be managed as a single shared asset (where it is allowed by law and policies), improving its consistency and integrity for providing better public services. Governments that actively promote adoption of open and interoperable standards can facilitate a widespread adoption of cloud computing beyond government sectors (i.e., spill-over effects on to the wider economy). One such approach is the European Union's Cloud Computing Strategy, which has as one of its objectives cutting through the “jungle of technical standards” so that cloud users can “enjoy interoperability, data portability, and reversibility.”

Transparent

As government departments and agencies consume cloud services, it is important for them to understand and monitor:

- The quantity of services being consumed
- How the services are being delivered
- Whether the services match pre-defined service level agreements (SLAs)

Cloud service providers, whether internal or external, should provide clear and easy ways for government departments and agencies to monitor, manage, and audit the services being provided or purchased. Such transparency will ease the adoption path for cloud computing solutions by governments. National and regional governments are increasingly engaging various representative groups to simplify the adoption of cloud services for government agencies. This makes it easier to find, review, commission, decommission, and switch cloud services, thus encouraging marketplace competition.

Digital Marketplace is a UK government initiative to encourage the adoption of cloud-based services across the entire UK public sector (e.g., Web hosting,
site analytics or document collaboration tools). Its objective is to simplify how the public sector buys and delivers digital services by promoting a common marketplace. Furthermore, to stimulate new entrants into the cloud marketplace, the UK government actively tracks the proportion of its cloud business secured by small and medium-sized enterprises (SMEs).

Government initiatives are also focused on cultivating the necessary legal and regulatory frameworks (including data protection, privacy and portability regulations, electronic signature laws, security audit requirements, computer crime legislation, intellectual property protection, performance and quality of service) to expand the cloud computing marketplace and boost national productivity, growth, jobs, and citizen digital savviness. The European Union believes initiatives like these can deliver a net gain of 2.5 million new European jobs and an annual boost of €160 billion to the European Union GDP (i.e., around 1 percent) by 2020.¹

**Aware**

Applications designed for legacy IT infrastructures (i.e., non-cloud) are based on the assumption that the legacy applications are typically tied to specific (i.e., physical) hardware and, when the hardware fails, that the application running upon it fails. Cloud-architected applications and services are designed to be flexible and agile across a cloud infrastructure (i.e., they are cloud aware). Cloud-aware applications can seamlessly scale up or down to match unpredictable demand patterns or leap-frog onto new infrastructure resources if existing resources falter. This ability can be especially appealing for government services that have seasonal or cyclical demand patterns, thereby optimizing computing and storage capacity along with cost.

The U.S. Administration for Children and Families (a division of the Department of Health and Human Services) migrated its GrantSolutions.gov Web site to a cloud-based infrastructure to support periods of high-volume processing more cost effectively.² With APIs provided by GrantSolutions.gov, third-party developers can build upon government cloud-aware applications to provide citizens with rapid access to innovative services.³ This is especially useful where government agencies have seasonal workloads and limited resources.

Government departments and agencies must deliver cloud-based services that maintain or increase existing levels of security, performance, and manageability. Traditionally, non-cloud-based applications and services were designed for a known type of end-user computing client that accessed services inside government firewalls (e.g., standardized desktops or notebooks). Today, a more flexible service delivery approach is needed to support a continuum of compute devices, from desktops to smart phones, accessing government cloud-based services inside and outside government firewalls. Cloud-architected applications and services are increasingly using capabilities embedded in end-users’ computing clients to deliver on these expectations. This client awareness helps to provide a more consistent user experience and flexibility to realize the potential of cloud-based government services.
Cloud Technology–Capability Maturity Framework (CT–CMF)

To support implementation of the six key criteria for effective government cloud deployments, Intel Corporation and the Innovation Value Institute (IVI) have co-researched and created the CT–CMF. While the six key criteria define the characteristics of successful deployments for government cloud systems, the CT–CMF identifies underlying key capabilities necessary to achieve those characteristics. The CT–CMF reflects the understanding that while organizational structures, technologies, and projects will change, management capabilities are more enduring. CT–CMF’s seven key capabilities are shown in Figure 1. These capabilities are designed to be universally applicable regardless of the combination chosen across cloud service models and cloud deployment models. The principles of CT–CMF can be readily applied internally or stipulated for cloud service providers (CSPs).
The bedrock of every cloud computing platform is management of its compute, storage, and networking capabilities. In addition, cloud computing requires complementary management capabilities in cloud application, security, and orchestration. Finally, capabilities are defined for cross-organization governance, supplier management, value, and innovation management. Table 2 defines each CT–CMF capability. CT–CMF’s objective is to deliver government cloud services that are secure, agile, dependable, open, transparent, and aware (i.e., cloud services that meet the six key criteria mentioned earlier). The CT–CMF is designed to provide a stable reference point across the public sector on the cloud computing adoption journey. To accelerate that journey, the CT–CMF provides step-wise levels of maturity for each capability. Figure 2 illustrates the generic maturity concept.

The five levels of maturity (Figure 2) apply to each of the seven capabilities (Table 2) to define the CT–CMF shown in Table 3. Assessing the maturity of each capability provides a baseline for planning systematic improvements that support successful government cloud deployments.

<table>
<thead>
<tr>
<th>TABLE 2: SEVEN CAPABILITIES OF CT–CMF DEFINED</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) COMPUTE</td>
</tr>
<tr>
<td>(2) STORAGE AND NETWORKING</td>
</tr>
<tr>
<td>(3) CLOUD APPLICATIONS</td>
</tr>
<tr>
<td>(4) CLOUD ORCHESTRATION</td>
</tr>
<tr>
<td>(5) CLOUD SECURITY</td>
</tr>
<tr>
<td>(6) CLOUD GOVERNANCE AND SUPPLIER MANAGEMENT</td>
</tr>
<tr>
<td>(7) CLOUD VALUE AND INNOVATION</td>
</tr>
<tr>
<td>MATURITY LEVELS</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>5. Optimizing (Transformational)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>2. Basic (Evolving)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>1. Ad Hoc (Informal)</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
The remainder of this section explores in more detail each of the seven CT–CMF capabilities presented in Table 3.

**Compute:**

*Manage Compute Workloads to Optimize Performance, Cost and Innovation*

Virtualization, the bedrock of cloud computing, improves asset utilization from historically low levels by pooling physical computing resources and sharing those resources efficiently across applications. In addition to maximizing utilization, virtualization helps minimize energy consumption, reduces server footprints within data centers, and provides scalable resources. The capital expenditure (CapEx) savings and the follow-on operating expenditure (OpEx) savings from virtualization create a business case for increasing the scale of virtualization deployments to the point where a virtual server becomes the default build, with special exceptions required for a physical build.

Extending virtualization to the most demanding Tier 1 applications becomes the next goal, using powerful server hardware built from the chip level and up for hardware-assisted virtualization. Furthermore, platform innovations, such as cost-saving power management technologies, increase server utilization and lower energy consumption further. As the compute capability matures in an organization, the ability to support dynamic placement of workloads within and across heterogeneous cloud environments can optimize efficiency, availability, and security. This entails dynamic routing of compute workloads to cloud infrastructures best suited for the job (e.g., different infrastructures for office productivity, mission-critical, highly secure, or location-restricted applications).

At the highest levels of maturity, compute workload placement and execution in the cloud can seamlessly move within and off premises while respecting defined policies such as compute workload priorities or security protocols. That is, cloud architectures provide intelligent run-anywhere execution based on the automated execution of defined policies, instead of stationary-location execution. Individual workloads move in and among private and public clouds across the world based on demand. This provides the ability to optimize performance, cost, location, risk, and benefit (i.e., by taking advantage of arbitrage that may exist between two or more marketplaces or computing environments).

**Network and Storage:**

*Use Improvements in Compute Performance to Manage the Growth of Storage and Network Demands*

As compute capability grows for both client devices and backend infrastructure, corresponding data and storage requirements grow rapidly. As a consequence, there is the increased demand for the network to move that data to where it is needed. Traditional storage solutions often lack the performance and flexibility to handle the growing storage requirements cloud environments demand, while legacy networks can be ill-equipped to accommodate the bandwidth and configurability requirements generated by scalable cloud services, virtual machine (VM) density, and VM migrations, among other factors.\(^{\text{iv}}\)
By summoning the cloud's ability to pool resources and generate efficiencies of scale, government CIOs can reduce costs, floor space, and energy requirements in the data center while gaining the speed, flexibility, and scalability of cloud platforms. However, storage and network modernization require new virtualization policies. Policies around the use of tiered storage architectures, thin provisioning, and storage reduction techniques such as data compression and data deduplication make it feasible to scale capacity on demand and help reduce storage management costs.

Due to cloud architectures' increasing network bandwidth demands, there is growing recognition that traditional network infrastructures are being challenged to keep up. Network strategies for cloud migrations start with upgrading and consolidating LAN ports with high-speed networking technologies such as 10 Gigabit Ethernet (10GbE) and beyond. Converged data and storage networks can then be unified with these high-speed networks. Simplified network infrastructure reduces cable management challenges in the cloud data center, improves airflow and cooling, and drives up data center efficiency.

Software-defined infrastructure (SDI) is an additional layer of abstraction that treats network, storage, and compute capabilities as abstracted resource pools. Software-defined storage (SDS)\textsuperscript{xvi} and software-defined networking (SDN)\textsuperscript{xvii} allow orchestration of storage and network resources similar to virtualized compute resources. These technologies enhance the provisioning, allocation, and management capability of the cloud infrastructure. Moreover, SDI enables policy-based intelligent storage and network resource management that provides automated service assurance for cloud services. The OpenStack Foundation's OpenStack software is one such open-source cloud operating system providing a framework for enabling unified self-service provisioning across compute, storage, and network resources.

At the highest level of maturity, cloud infrastructure will always be available with autonomous self-regulating configurations, allowing the compute workload and cloud services to run continuously without interruption of storage and network services.

### Cloud Security:

#### Evolve the Security Model from Security of the Physical Infrastructure to Full End-to-End Security

The traditional philosophy of security derived from the network firewall won't work effectively for cloud computing, which requires elastic boundaries that can push the perimeter of the enterprise beyond the location of traditional firewalls.\textsuperscript{xviii} Cloud computing makes the network firewall permeable when devices accessing cloud-based services are both inside and outside the firewall. Furthermore, these devices can range from powerful servers and high-performance computing clients to less capable mobile devices, each with independently defined security features and capabilities.
With new usage models, new security models and controls are needed to enforce the protection of virtualized infrastructure, workloads and associated data, and various end-user client devices that access cloud-based applications, as well as protection for data at rest and in motion. A holistic approach is required to evolve the security model beyond traditional assumptions of securing physical infrastructure, standardized devices, and physical insolation in favor of adaptable, end-to-end, multi-layered, and multi-tenant architectures. Security policies, technologies, and controls should encompass data, applications, services, end-point devices, and all aspects of infrastructure. In the case of hybrid or public cloud deployment models, the security model and controls will need to include services and data residing in the public cloud platform.

In some cases, it may be sufficient to have a cloud provider vouch for the security of the underlying infrastructure (e.g., hosting external websites and wikis for non-critical services). However, for mission-critical processes and sensitive data, third-party attestations may not be enough. That is, it may not be sufficient to rely on cloud providers’ logs, reports, and attestations in proving compliance. For example, Intel is collaborating with cloud providers and the IT community on applications of Intel® Trusted Execution Technology (Intel® TXT) in conjunction with other components to provide interoperable, highly secure, tamper-proof measurements of policy compliance and the end-to-end security attestations needed to handle even the most demanding security.

Governments are looking at the centralized certification and accreditation of cloud service providers (CSPs). Certification acts like a security passport that validates a CSP’s credentials. By validating credentials once and to a consistent level, each government department and agency can accept that security passport when a CSP tenders for government contracts. For example, U.S. federal government entities can now utilize Amazon Web Services* (AWS*) infrastructure services after AWS was awarded Federal Information Security Management Act (FISMA) Moderate Authorization and Accreditation. Activities like these can generate wider options for deploying government cloud, speed up government procurement cycles, and help ensure CSPs are evaluated using consistent and rigorous security protocols that prioritize security needs to counter the most serious threats.

At the highest levels of maturity, governments evolve their security models to protect not only the physical infrastructure but also the data and applications (i.e., end-to-end layered security) by striving to provide robust security services that ensure the integrity, confidentiality, and availability of data in a cloud computing environment.

**Cloud Orchestration:**
**Operate with Elasticity, Scale, and Efficiency by Deploying Automated Provisioning and Assurance Models**

Easier provisioning of services is one of the key value propositions for the cloud architecture, where resources and services can be subscribed to and managed by an automated self-serviced portal. Historically, deploying a
new service or application on traditional (i.e., non-cloud) IT infrastructure involves procuring hardware, scheduling the installation in the data center, and configuring and testing the hardware and software – a process often taking weeks or even months. Use of virtualization and standardization in a cloud environment obliterates the traditional project-by-project hardware procurement and infrastructure installation processes, significantly decreasing the time needed to deploy new applications. Fully realizing the business agility and efficiency enabled by cloud computing requires automated services provisioning. With a self-service portal supported by automated provisioning on the back end, government departments and agencies can cut the provisioning time for applications, development environments, or compute infrastructure capacity down to minutes.

Cloud orchestration is not limited to the provisioning of services. Cloud infrastructure - both physical and virtualized – requires solutions for service assurance so that workloads can run efficiently. At advanced levels of maturity, there are likely to be situations when workloads may need to migrate within or across cloud environments (e.g., to maximize data center efficiency or comply with SLA-defined policies such as ensuring that data for workloads running in a secure cloud is not moved to a less secure area). Manual management of such complex and large-scale operations can be prone to human errors or slow reactions to changing demands. To maintain optimized quality of service (e.g., avoiding situations like cloud resource overcrowding), advanced telemetry solutions can help by identifying how variables in a cloud environment change over time and dynamically making decisions on appropriate infrastructure resourcing allocations. Using advanced automated, policy-based workload placement, the orchestration layer can make real-time decisions about where a workload should be optimally placed or relocated if current resources become overcrowded.

Automation is essential for the management of a cloud environment to improve agility and OpEx. However, one key challenge to driving better automation within and across cloud-based infrastructures is successfully breaking down the organizational silos and complex implementation processes across the management of traditional compute, storage, and network platforms. For example, even if capacity is available for provisioning in minutes, agility can be eroded by bureaucratic request-approval processes. Also, data center facilities are often managed independently from cloud infrastructure, potentially impacting automation and efficiency.

To resolve bureaucratic challenges, IT organizations should consider integrating heterogeneous technology platforms, workflows, and management processes as well as security models that govern such processes. This is also an opportunity to redefine existing service provisioning processes by referencing international best practice models. Adapting open standards in cloud infrastructure, software interfaces (e.g., APIs), and service management practices will help turn cloud computing’s automation potential into a reality (i.e., rendering all cloud aspects available to the user without creating IT service requests).
To achieve such a level of maturity, the public sector must continue to build skills and knowledge of cloud technologies and cloud service management and use early wins to demonstrate potential and justify further budget allocations. A centralized management console can monitor cloud resources, capacity utilization, performance, and charge-back for services used. Improved orchestration will allow the IT function to progress toward becoming a broker and integrator of cloud-based services – whether internally or externally sourced.

At the highest level of maturity, cloud services provisioning and infrastructure management are fully automated across the cloud environment, providing an always-on experience to users while optimizing the efficiency across cloud environments.

Cloud Applications:
Enable Applications to be Cloud-Aware and Client-Aware, Taking Full Advantage of Capabilities Present in the Cloud and End-User Computing Clients

Many organizations adopted virtualization to consolidate workloads previously hosted on dedicated physical servers. This transition involved little or no change to the applications themselves, which have traditional expectations and dependencies. Non-cloud-architected applications are tied to the physical hardware infrastructure that hosts them. That is, if the physical hardware fails, the application fails. By contrast, cloud-architected applications are designed with failure in mind. Such applications are cloud-aware when they can migrate across virtualized hardware resources enabling elasticity and protection against hardware failures. That is, their design focus is on minimizing mean time to recovery (MTTR) rather than traditional approaches of maximizing mean time to failure (MTTF).

To deliver cloud-aware applications, government departments and agencies should comprehend the characteristics of legacy applications and make plans for migrating them to appropriate cloud platforms. To optimize for agility, new development guidelines are required for developing new cloud-based applications and for legacy applications migrating to cloud services.

At greater levels of maturity, the API becomes a standard way to expose services and applications running on cloud platforms, thus allowing easier creation of services and optimizing resource provisioning across applications. APIs offer discrete services but also can be rapidly coupled with other services to create more complex applications - accelerating service development by minimizing rework and maximizing reuse. As APIs are exposed as interfaces to the cloud, managing (e.g., policy enforcement, monitoring, and auditing) and securing them will become increasingly important. Widely accessible cloud API management platforms are becoming de facto resources when building new cloud applications and migrating legacy applications to cloud environments. Such platforms take advantage of third-party economies of scale, support agile delivery of cloud-based services, and help handle complexity as the need grows to access more data and generate more services.
Delivering a consistent end-user experience (EUE) and richer quality of service (QoS) from cloud-based applications could be challenging due to variances among end-user computing clients accessing the cloud (e.g., operating systems, form factors, input methods). Rather than sacrificing end-user experiences for the sake of designing to a lowest common denominator, cloud-based applications can be tailored to take advantage of the capabilities present in the end user’s computing client accessing it (i.e., be client-aware). Varying end-user computing client capabilities include operating systems, processors, security patches, network connections, battery capacities, screen size, and input types. Once the relevant capabilities of an end-user’s computing client are made known, a cloud-based application can dynamically optimize the EUE and QoS accordingly, thus maximizing productivity along with safeguarding government department and agency data. As departments and agencies plan their migration to cloud-based services, development guidelines for creating client-aware applications should be part of the core cloud development principles.

At the highest levels of maturity, cloud-architected applications are aware of and utilize the capabilities present in the cloud environment (i.e., are cloud-aware) and end-user computing client (i.e., are client-aware) for agile and optimal services delivery.

Cloud Governance and Supplier Management: Use Interoperable Standards and Open Innovation

Multiple laws, regulations, and standards call for a complex weaving together of security and privacy mandates, making compliance a potentially complicated issue for government cloud computing. To avoid such potential issues, common governance and procurement principles should be applied across government departments and agencies. These principles should address technical and business risks associated with different cloud services, including data portability and reclamation, service-level reporting, and security protocols. Demanding trustworthy and tamper-proof compliance assurance capabilities will help ensure desired government policies, operation procedures, security, and service levels are maintained. For example, certain privacy laws may require restricting the geographic location for the storage of certain types of data in the cloud. Trusted Geo-location in the Cloud: Proof of Concept Implementation (Draft), a U.S. National Institute of Standards and Technology (NIST) publication, demonstrates how Intel TXT can aid organizations in monitoring and enforcing geo-location restrictions and policies, thus ensuring their workloads based on cloud services are deployed on trusted hardware in known geographies or locations.

Consolidating demand for cloud services across public sectors, together with development of specific procurement vehicles, will help streamline governance, maximize purchasing power, and optimize sourcing decisions. Government departments and agencies can become cloud service brokers by removing internal obstacles and using cloud computing’s economies of scale and capability to innovate rapidly.
At the highest levels of maturity, responsive governance and innovative supplier management will lead to services that are higher performing, more secure, and more affordable.

Cloud Value and Innovation:
Set Clear Business Objectives, Communicate and Realize the Value Proposition for Government Cloud Services

Public sector investments in cloud-based services typically begin with small but crucial projects that can deliver compelling return on investment, build internal expertise, and establish the credibility of cloud computing’s potential for delivering public services. However, to capture the transformative potential of government cloud computing, public sector organizations should define a ubiquitous vision across public services for government cloud adoption along with corresponding deployment roadmaps. The deployment roadmaps require clear government objectives and transparent value propositions for where cloud computing can improve the delivery of better public services. This will help maximize the value of investments and set budget priorities across the public sector regarding expenditure on cloud versus non-cloud infrastructures.

To evaluate the benefits of cloud computing, public sector organizations will benefit from applying consistent methods for measuring and expressing the value of using cloud-based technologies and services. Evaluation of cloud investments should blend tangible and intangible benefits to establish a transparent line-of-sight relationship between investments and forecasted benefits of better government services. Additionally, the ability to trade saved surpluses across public sector budgets and time periods can be a key enabler to funding the next wave of public sector innovation using cloud computing.

At the highest levels of maturity, the adoption of government cloud is transforming delivery of citizen services.

Planning for Innovation and Value

Much of the early attention regarding government cloud computing has focused on infrastructure consolidation and reducing time to provision infrastructure from weeks (or months) to hours (or even minutes). Increasingly, attention is now turning to higher-order opportunities for innovation using cloud computing. This includes massive business intelligence analyses, intermittent or seasonal processing requirements, and new delivery models for public services.

The public sector can deliver on cloud computing’s innovation potential by promoting progressive policies regarding government cloud adoption. Table 4 serves as a useful checklist for proofing government policies and individual programs against the six key criteria for effective government cloud adoption.

Because of the public sector’s collective buying power – estimated to be up to 20 percent of all IT spending in some geographies – governments are
TABLE 4: SIX KEY CRITERIA CHECKLIST FOR EFFECTIVE GOVERNMENT CLOUD ADOPTION

<table>
<thead>
<tr>
<th>CRITERIA</th>
<th>DESCRIPTION</th>
<th>QUESTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECURE</td>
<td>Cloud-based services are trustworthy and secure from threats, applying defense in depth to prevent data disclosure (i.e., ensure confidentiality) as well as to prevent data tampering (i.e., ensure integrity).</td>
<td>☑ Are there sufficient end-to-end layered cloud security controls (i.e., defense in depth via secure infrastructure in the data center, secure network connections, secure devices, secure applications, and secure data)? ☑ Do current security models and policies align with new cloud computing deployment and usage models?</td>
</tr>
<tr>
<td>AGILE</td>
<td>Cloud-based services apply dynamic orchestration to rapidly deploy and scale services up or down, dramatically reducing deployment and management time.</td>
<td>☑ Does the cloud-based service include orchestration abilities (e.g., self-serviceability, automation, integration) to dynamically allocate resources, manage service levels, and optimize efficiencies? ☑ Does the cloud-based service use or offer a reusable and modular API architecture and management platform?</td>
</tr>
<tr>
<td>DEPENDABLE</td>
<td>Cloud-based computing performance is reliable, with assured compliance and service levels.</td>
<td>☑ Can failure detection, recovery, and reporting occur with minimal or no manual intervention? ☑ Is service, regulatory, and policy compliance assurance possible using trusted and tamper-proof performance monitoring?</td>
</tr>
<tr>
<td>OPEN</td>
<td>Cloud-based services implement open standards to promote interoperability and portability across heterogeneous environments.</td>
<td>☑ Are open (i.e., vendor-neutral) standards applied to the cloud-based solution? ☑ Are interoperability, portability, and reversibility available for data and services hosted on the cloud computing platform?</td>
</tr>
<tr>
<td>TRANSPARENT</td>
<td>Cloud-based services offered in the marketplace are easily compared, monitored, and audited.</td>
<td>☑ Is the cloud-based service transparently defined regarding comparing, commissioning, decommissioning, and switching cloud providers? ☑ Is tracking of cloud service delivery, consumption, and billing readily available?</td>
</tr>
<tr>
<td>AWARE</td>
<td>Cloud-based services capitalize on the capabilities embedded in the cloud infrastructure hosting them and the end-user computing devices accessing them.</td>
<td>☑ Can cloud-based services capitalize upon both the generic and unique capabilities of virtualized infrastructure resources (i.e., cloud-aware)? ☑ Can the cloud-based service offer secure access and optimal user experience across a continuum of compute devices (i.e., client-aware)?</td>
</tr>
</tbody>
</table>

uniquely positioned to affect the marketplace for cloud computing. Applying the six key criteria checklist (Table 4) together with the CT–CMF (Table 3) will help maximize public sector benefits from government cloud adoption by establishing a common language for goal setting among diverse stakeholders.

Acknowledgements

The authors wish to acknowledge valuable contributions from colleagues across Intel Corporation including Enrique Castro-Leon, Mark Valcich, John Kennedy, Cristian Oliveira and Dawn Olsen.
About Innovation Value Institute

The Innovation Value Institute (IVI) is a not-for-profit entity that aims to transform how public and private sector organizations manage IT for value and innovation. Co-founded by Intel Corporation and Maynooth University, IVI hosts an international consortium of private and public sector organizations that, along with international academic organizations, collaborate on defining management best-practices.

About Information Technology–Capability Maturity Framework* (IT–CMF*)

The Information Technology–Capability Maturity Framework* (IT–CMF*) improves an organization’s capability to deploy and run information services for greater value and innovation. The IT–CMF can be traced back to research originally conducted by Intel Corporation. Since then, IVI and its international consortium have built upon Intel’s original IT–CMF work, enabling public and private sector organizations around the world to systemically improve how they manage IT for value and innovation. Using IT–CMF as part of a continuous IT improvement program is associated with improved IT performance, including optimizing IT costs and higher business value contributions. Find more at www.ivii.ie

About Cloud Technology–Capability Maturity Framework (CT–CMF)

The CT–CMF is co-developed by Intel Corporation and IVI as an add-on extension to the core functionality of IVI’s Information Technology – Capability Maturity Framework (IT–CMF). While IT–CMF encompasses an array of organizational strategies and practices for managing IT for value and innovation, CT–CMF enhances IT–CMF’s core functionality with cloud computing strategies and practices for government organizations.

Endnotes


v. In some government arenas, public clouds are referred to as “private sector” clouds (e.g., a cloud service such as Amazon Web Service (AWS)).


Interoperability is the capability of systems to work together by exchanging information across heterogeneous system boundaries.


An API is an application programming interface that enables software components to talk to one another. APIs are libraries of specifications for objects, routines, and data structures. APIs improve the ability to accommodate changes in the environment rapidly.


A virtual machine (VM) is a software-based emulation of a computer, running on a physical server or client hardware. With virtualization, a single hardware platform can host multiple VMs, increasing resource utilization and manageability.

Software-defined storage abstracts storage from hardware and enables data to be deployed, provisioned, and managed through software controllers.

Software-defined networks separate the control plane (the element of the network used to configure the network) from the data plane (where the actual packet flow and traffic traverse the network), enabling configuration from centralized software controllers.

A firewall is a system (hardware or software) that prevents unauthorized access to or from a private network, forming a barrier between a trusted and an untrusted network.


xxiv. The IT Capability Maturity Framework, Innovation Value Institute, National University of Ireland, Maynooth. 2010.