Cloud
Standards
Customer
Council

Practical Guide to Cloud Computing
Version 1.0

September 26, 2011

Contents

Acknowledgements

The *Practical Guide to Cloud Computing* is a collaborative effort that brings together diverse customer-focused experiences and perspectives into a single guide for IT and business leaders who are considering cloud adoption. The following participants have provided their expertise and time to this effort.

Workgroup Leaders

Melvin Greer (Lockheed Martin) – Workgroup Chair
Gurpreet Singh (Ekartha) – Introduction Leader
John McDonald (CloudOne Corporation) – Vision Section Leader
Amy Wohl (Wohl Associates) – Rationale Section Leader
John Meegan (IBM), Dave Russell (IBM), Keith Prabhu (Confidis) – Roadmap and Key Summary Points Section Leaders
Elizabeth Woodward (IBM) – Lead Technical Editor

Core Workgroup Members

The workgroup leaders wish to recognize the following individuals for their outstanding efforts to provide content, share their expertise and ensure completeness of the *Practical Guide to Cloud Computing*: Anna Gabrielli (AGDesign), Larry Hofer (Cloud and Security Services), Richard Miga (Synergistic Solutions), Rick Warren (Real-Time Innovations), Nasir Balouch (IBM), Christopher Ferris (IBM), Susann Keohane (IBM), Walden Leverich (Tech Software), Yves Le Roux (CA Technologies), Kumar Pappu (VeriAgile Consulting Inc.), Dave Russell (IBM), and Steven Woodward (Cloud Perspectives).

Extended Workgroup Members

The workgroup leaders also wish to thank the following for taking time to provide feedback and share their perspectives on early versions of this white paper: Gurvinder Ahluwalia (IBM), Rizwan Ahmad (University of Auckland), Claude Baudoin (cebe IT & KM), Sourav Dutta (IBM), Sridhar Iyengar (IBM), Sarvani Kondeti (Mahindra Satyam), Heather Kreger (IBM), Ilina Manova (Rila Solutions EAD), Bob Marcus (ET-Strategies), Chris McCarthy (State Street Corp.), Dirk Nicol (IBM) , Bala Peddigari (TCS), Keith Prabhu (Confidis Advisory Services), Oya Sanli (PayDeg), Akash Saxena (Independent Consultant), Amy Schneider (IBM), Don Sheppard (ConCon IT Consulting), and Prasad Yendluri (Software AG).

Additional Reviewers

The following reviewers provided feedback on the *Practical Guide to Cloud Computing*: Daniel Berg, Brian Butte, Pamela Isom, Anshu Kak, Georgios Michalakidis, Wendy Perilli, Andi Snow-Weaver, Sriram Subraramian, Patricia Sullivan, and Shunguo Yan.

Introduction

The aim of this guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers adopt cloud computing to solve business challenges. The emergence of cloud computing, like any new technology model, has the side effect of flooding the market with information and jargon that adds to the confusion and uncertainty amongst decision makers. The *Practical Guide to Cloud Computing* aims to remedy this by providing comprehensive and actionable information in a single reference. The guide explains in nontechnical language the key concepts of cloud computing, and how best to adopt cloud solutions to solve specific enterprise problems.

The *Practical Guide to Cloud Computing* contains a set of guidelines, and strategies to help decision makers in all major activities related to implementing cloud solutions. For example, the "Rationale for Cloud Computing" section explains the different types of cloud service models (Infrastructure as a Service, Software as a Service, and Platform as a Service) and deployment models (private, public, community, hybrid). This section also describes specific costs and benefits of each cloud model with respect to enterprise business challenges. The "Cloud Computing Vision" section looks in to the future evolution of the cloud. It provides a vision on the potential uses and benefits of cloud as the technology matures further. The "Roadmap to Cloud Adoption" section is the heart of the guide. It details both strategic and tactical activities for decision makers implementing cloud solutions. It also provides specific guidance to decision makers on the selection of cloud service and deployment models. All the activities and recommendations in the roadmap take into account the different sizes and IT maturity of the organizations, and will act a useful template for both large enterprises and small-and-medium businesses (SMBs). Furthermore, for enterprises new to cloud computing, the guide highlights key elements and steps to increase the likelihood of a successful cloud implementation.

Readers should note that despite the guidelines provided in this white paper, the ultimate selection of cloud solutions and their success depend upon the judgment of IT and business decision makers and their organizational realties.

The process used to develop this guide ensures that it is valid, reliable, and provides significant value for enterprise decision makers. The contributors to this guide represent an array of experienced industry participants. Also, members of the working group have rigorously reviewed the guide, sought widespread review of iterative drafts, and obtained final approval from the Cloud Standards Customer Council Steering Committee.

A Rationale for Cloud Computing

Why is Cloud Computing Important?

Cloud computing offers a value proposition that is different from traditional enterprise IT environments. By providing a way to exploit virtualization and aggregate computing resources, cloud computing can offer economies of scale that would otherwise be unavailable. It can also offer opportunities to immediately exploit installed hardware and software, rather than using time and resources to design, deploy and test a new implementation.

Because virtual instances can be provisioned and terminated at any time and the user organization pays only for the computing resource they are employing, costs can be lower. Likewise, fee structures need to be adequately clarified and understood to estimate future costs.

Definitions of Cloud Computing

The National Institute for Science and Technology (NIST) defines cloud computing as follows:

> *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.*

This cloud model promotes availability and is composed of five essential characteristics**,** three service models, and four deployment models.

Essential Characteristics

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

- *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and personal digital assistants (PDAs).

- *Resource pooling.* Cloud computing pools a provider's computing resources to serve multiple consumers using a multi-tenant model, with different physical and virtual resources assigned and reassigned according to consumer demand. Cloud computing provides a sense of location independence. Customers generally have no control or knowledge of the exact location of the resources. But, they may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

- *Rapid elasticity.* Resources can be rapidly and elastically provisioned, sometimes automatically, to scale out quickly, and rapidly released to scale in quickly. To consumers, the resources often appear to be unlimited and can be purchased in any quantity at any time.

- *Measured Service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction suitable to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Providers and consumers can monitor, control, and report on services with transparency.

Cloud computing does not exist in a vacuum. Most organizations will have a broad variety of applications already running in their data center. For most, cloud computing will extend their existing infrastructure. Cloud computing can be dedicated to particular tasks. It can be used mainly for new projects. Or an organization may use it for overflow, guaranteeing a certain level of performance for enterprise computing.

NIST Defines Three Cloud Service Models[1]

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure, typically through a pay-per-use business model. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

NIST Also Recognizes Four Deployment Models

- *Private cloud*. A private cloud in which the cloud infrastructure is utilized by just one organization, though not necessarily operated by that one organization.
- *Community cloud*. A community cloud whereby several organizations with common concerns share a cloud.
- *Public cloud*. The public cloud provided by the private sector for all comers, such as Amazon's EC2 service.
- *Hybrid cloud*. A hybrid cloud in which two or more cloud types are discrete but networked together such that a burst of activity beyond the capabilities of one cloud is shifted for processing to another.

It should be noted that the deployment models do not reflect where the resources are actually hosted. For example a private cloud can be hosted internally (on-site) or externally (outsourced). The deployment models in conjunction with hosting need to be recognized and considered.

The Benefits of Cloud Computing

Cloud computing permits the expense of infrastructure and its management to become an operational expense rather than a capital investment. This can be beneficial for the business both from a tax perspective, and also because it allows the organization to conserve capital for other purposes.

[1] Additional service models exist that can be categorized under one of the 3 NIST service models. Examples include Storage as a Service, Communications as a Service, Database as a Service, etc.

Cloud computing offers a centralized, remote facility for computing, leading to economies of scale in both the use of hardware and software and a reduction in required resources for administrative management.

Cloud computing is also enabling business agility. In fact, a December 2010 survey of 170 attendees of Gartner's Data Center Conference indicated that 55% view agility and speed as the main driver for moving to private clouds (Bittman, 13). Cloud computing provides the ability to make use of computing resources on an immediate basis, rather than a need to first invest time and skilled resources in designing and implementing infrastructure (hardware and middleware) and then implementing and testing it. This leads to faster time to value which may mean enhanced revenue, larger market share, or other benefits.

Although there are a number of benefits to cloud computing, cloud computing is not an answer for every problem. Where the user organization requires very high levels of control and/or security, cloud computing may not provide an appropriate computing environment.

Cloud computing is not necessarily cheaper than conventional computing environments. It is the mix of computing workloads and their cost in both traditional and cloud computing environments which will determine if savings can be made. For example, if highly secure environments are required, it might be possible to implement a specialized private–internally (on-site) hosted cloud, but the cost might be prohibitive.

If a completely custom application is required, a SaaS cloud will not be appropriate, although a PaaS or IaaS cloud might be a viable alternative.

What is the Importance of Standards-Based Cloud Computing?

Standards-based cloud computing ensures that clouds can readily interoperate, based on open standard interfaces.

Standards allow workloads to be readily moved from cloud to cloud and services created for one cloud computing environment to be employed in another cloud computing environment, eliminating the need to write redundant code.

Many organizations who are contemplating the use of cloud computing are behaving as if interoperability, portability and integration already exist. In fact, we are at a relatively early stage of cloud computing and many different standards have been proposed. Some permit interoperability, others support limited interoperability, and others are, in fact, proprietary environments. Once a proprietary environment is selected, an organization will experience vendor lock-in. This means that integrating applications or services across differing proprietary cloud platforms will be possible but will require extensive, expensive, and time-consuming work.

Some of the proposed standards are based on open-source environments. This has the advantage of making all the code transparent, available for inspection, and more readily suited for an interoperable environment. However, whenever a new technology is attracting a great deal of attention, neither vendors nor customers are likely to wait for mature standards or rich open source environments. They will leverage the advantage of early adoption of emerging technology at the price of having to move to a standard (and perhaps an open source) environment at a later date.

Cloud Computing Vision

Cloud computing will have future implications in the following areas:

- Economics
- Elasticity
- Globalization
- IT as Service Broker
- Catalyst for Innovation
- Inclusive Computing

Economics

Today, most of the organizational cost savings from implementing the cloud is coming from reduced capital and operations costs because of increased efficiency gained when consolidating certain aspects of IT infrastructure to specialized organizations. The economic gains from the cloud will come from matching infrastructure dynamically to the changing levels of usage inherent in real projects and initiatives. In "*The Three Stages of Cloud Economics*," Forrester Research VP and Principal Analyst James Staten writes:

> *"The key to cloud economics is using cloud computing optimally, understanding the behavior of the applications and services deployed by the business."*

However, consolidation/specialization also implies the need for new and different human resource skills, thus traditional IT roles will change, some IT roles will be reduced in number, while other new roles will be defined in the future.

Elasticity

Information Technology (IT) organizations/areas will need to be more flexible in their business and operational processes, legal agreements and financial obligations. In the future, with standardized service level agreements (SLAs), efficient market-driven pricing and diversified offerings, and an IT operations staff familiar with cloud-delivered services, companies will be able to more quickly adjust infrastructure in response to changing business needs. In his November 2010 whitepaper "*The Economics of the Cloud*", Microsoft's Director of Corporate Strategy, Rolf Harms, writes:

> *Elasticity is a game-changer because, as described before, renting 1 machine for 1,000 hours will be nearly equivalent to renting 1,000 machines for 1 hour in the cloud. This will enable users and organizations to rapidly accomplish complex tasks that were previously prohibited by cost or time constraints. Being able to both scale up and scale down resource intensity nearly instantly enables a new class of experimentation and entrepreneurship.*

Elasticity in cloud computing in not limited to the operations, but can also include the elasticity of the services deployed within the applications.

Globalization

Because a cloud can be instantly global in nature, meaning that it becomes accessible to anyone invited with a minimum of ceremony and process, it frees companies from the bounds of the traditional Internet and intranet barriers. In the future, public clouds, hybrid clouds, community clouds and virtual private clouds will enable individuals and organizations to participate in projects who aren't traditional employees/organizations, or who have transient or geographically diverse relationships to the sponsoring organization.

This free-flow of control, data, information and human participation is a significant challenge to geopolitical barriers. Legal standing might jeopardize the ability for cloud computing to catalyze this transition more rapidly. As *The Economist* said in the article "*Computers without Borders":*

> *"This illustrates the political tensions that will arise with the cloud. In one way it is the ultimate form of globalization: vast virtualized computer systems and electronic services know no borders. Yet governments are likely to go to great lengths to avoid losing even more control."*

In fact, cloud computing drives a unique global political challenge: when there are no longer technical barriers to location and access of data and systems, how do individual country laws and restrictions need to change? Indeed, a worldwide agreement on data security, privacy policies and data interconnection is a necessary element of encouraging cloud diffusion.

IT as Service Broker

In the future, IT will change from a "provider" of all information technology function to a "broker" of best-of-breed services for the organization's business needs.

In their December 2010 report, "*On Demand: From Capacity to Capability,"* Gartner analysts Richard Hunter, Partha Iyengar and Andrew Rowsell-Jones write:

> *The high fixed costs of IT infrastructure and operations are an increasingly heavy burden for many CIOs and their enterprises. Current efforts to address this problem by enabling <u>capacity</u> on demand represent the first steps toward provision of complex business <u>capabilities</u> on demand. In the next decade, this state of affairs will bring profound change to enterprises, IT practitioners and the software industry.*

Thus, companies might retool their own best-of-breed capabilities into cloud-delivered services that would turn what is traditionally a cost center into a profit center.

Catalyst for Innovation

The heart of innovation is collaboration, drawing the best ideas and constructive feedback from diverse participants in a common conversation. In the future, the global, elastic and service-broker nature of clouds will enable organizations to assemble project teams from diverse sources. Organizations will be able to efficiently provide a common, collaborative infrastructure instantly available through mobile and traditional devices. As a result, those organizations will be able to address a new business challenge or opportunity with full collaborative value from all participants.

The cloud enables smaller organizations to develop, market, compete and sell their products on a global scale, like much larger companies but for a much lower cost, thus facilitating a more innovative and dynamic business environment. As VentureBeat.com writes, *"A slew of new offerings in the cloud are helping even the tiniest of businesses look and act like big companies."* Here, too, realization of this commonwealth of services that enables all companies to think globally hinges on a worldwide commonality of rules and laws.

Inclusive Computing

In the future, cloud computing will provide a significant opportunity to improve an organization's ability to meet the accessibility needs of users, such as those who are disabled or aging, or face language or communication barriers. By considering accessibility during design, development and testing of cloud implementation and deployment solutions, organizations can simplify consistent provisioning and release of accessible platforms, infrastructure and services. Such cloud solutions will be able to align with legal requirements and to meet the needs of a diverse set of users. Cloud computing is also delivering assistive technologies such as screen readers for the blind, screen magnifiers for the visually impaired, speech-to-text converters for the deaf and language translators for non-native speakers (Kelley).

For example, the Tottori Prefecture in Japan drove the creation of a cloud-based system where visually impaired people can report difficulties in seeing web images or charts (Morimoto & Takagi). A reviewer then loads additional descriptions or alternative text, which on the next page load marries the new helper content to the original material, allowing the next impaired user to better understand the meaning of the original page. By placing the interpretation into the cloud the original website remains unchanged, which allows for complex, detailed and expansive metadata to be made available without wholesale and time-consuming changes by web designers.

Future Impact

This is by no means a comprehensive list of possibilities, but they represent the most promising of future cloud implications. While economics and elasticity are probably the best understood today, globalization, innovation, adaptation and the retooling of IT as a service broker have potentially the greatest possible future impact.

Roadmap for Cloud Computing

This section provides a prescriptive series of steps that should be taken to ensure a successful cloud deployment from the perspective of a cloud consumer. It takes into account differences that result based on the size of the organization and its IT maturity level. The following steps are discussed in detail:

1. Assemble your team
2. Develop business case and an enterprise cloud strategy
3. Select cloud deployment model(s)
4. Select cloud service model(s)
5. Determine who will develop, test and deploy the cloud services
6. Develop a proof-of-concept (POC) before moving to production
7. Integrate with existing enterprise services

8. Develop and manage SLAs
9. Manage the cloud environment

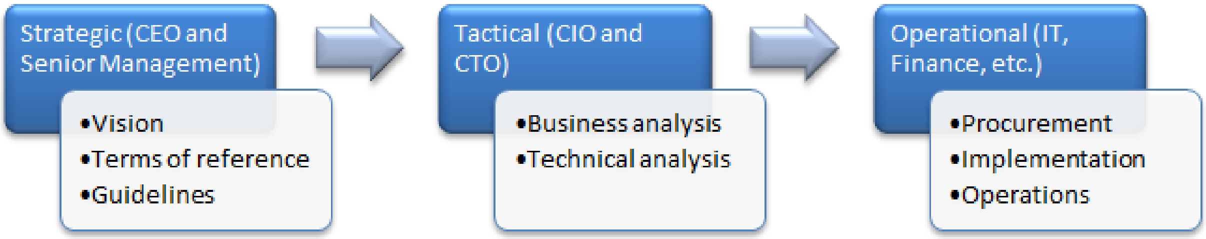
Depending on the maturity of the enterprise and their adoption of cloud computing the entry point will change for each new service being evaluated.

Step 1: Assemble your Team

It is important that the cloud consumer[2] establish a clearly defined team to develop and approve a strategy and implementation plan for cloud services that will be part of the total IT environment. In the past, the recommendations, design, development, deployment and maintenance of the IT environment was primarily driven by the IT department. Cloud computing is creating an evolution where the business leaders are getting engaged because they see cloud as a tool to get closer to their customers and increase sales/revenue.

Adoption of the cloud is viewed as a strategic business decision that allows business not only to improve IT efficiency but also help in achievement of more global business goals like streamlining of the supply chain and extending the business processes to make them more accessible by third parties. Hence, it is logical that the adoption of the cloud should be led by senior management including the CEO and CFO with the CIO and CTO playing the role of key enablers. In essence, resources must be drawn from IT, business (sales and marketing), finance, legal and the administrative areas of the enterprise to build a team that can address the various aspects of adoption.[3] Different skills are required at the different phases of cloud adoption—strategic, tactical and operational.

Figure 1. Three phases of cloud adoption



[2] Note that this section focuses on the cloud consumer. Points of contact between the cloud consumer and cloud brokers, carriers and providers are covered in the later steps of this section.

[3] The mix of the roles may change as one goes from the cloud consumer to the cloud provider, however, there needs to be a direct link between the cloud consumer and the cloud provider to ensure a successful partnership for cloud services.

Strategic Phase

During the strategic phase of cloud adoption, CEOs and the senior management team lead the organization to establish the vision, terms of reference and guidelines.

- *Vision*. The CEO and senior management team should define the overall vision for cloud adoption. It's critical that all levels of the enterprise, particularly the executive levels, buy in to the vision.

- *Terms of reference.* It is important to define the terms of reference early in the cloud adoption process to ensure that the adoption stays focused on the target business goals.

- *Guidelines.* Based on the culture of the business, it is important for senior management to provide broad guidelines for cloud adoption, including security posture, privacy and security concerns etc.

Tactical Phase

During the tactical phase, typically led by the CIO or CTO, the organization performs both a business and technical analysis.

- *Business analysis.* This phase requires the oversight of senior business managers, IT including the CIO, CTO and lead architects, and legal representatives to review and communicate laws which must be adhered to. The overall goal is to build a business case and the supporting long-term enterprise strategy for the transition to cloud computing that delivers sufficient return on investment. It's critical that all levels of the enterprise, particularly the executive levels, buy in to the strategy.

- *Technical analysis.* This phase requires the attention of IT including the CIO, CTO and lead architects, operations personnel, and senior business managers. The goal of this phase is to develop a technical strategy for cloud deployment taking into account the various service and deployment models that are possible. As part of the technical analysis, the business case for building versus buying would be developed which would be presented to the strategic team for their approval.

Operational Phase

During the Operational phase, leaders from various operations groups work through procurement, implementation and establishment of ongoing operations for the cloud deployment.

- *Procurement.* This phase includes negotiations with potential cloud providers and requires the procurement team, finance, legal, senior business managers, and IT including the CIO, CTO and lead architects to be engaged.

- *Implementation.* This phase includes the development, customization and configuration of services which will be deployed in the cloud environment and requires the attention of IT including lead architects, developers and testers as well as operations personnel.

- *Operations.* This phase addresses ongoing operations and management of the cloud infrastructure and deployed services. Operations personnel, customer support, and IT including developers and testers are required in this phase.

Step 2: Develop Business Case and an Enterprise Cloud Strategy

To ensure a smooth transition to cloud, an enterprise should develop an overarching cloud strategy which creates the foundation for project-specific adoptions.

Cloud computing presents interesting business model opportunities to enterprises of all sizes. As enterprises implement cloud computing they may find that their capital expenses and labor costs decrease and their revenues increase from improved speed to market for new services. As part of developing a strategic plan for cloud computing, each new cloud service will need to be evaluated against the current cost of delivery. For example, reduced capital costs will need to be weighed against cloud service charges. The enterprise must also determine whether to train internal resources to use the new cloud technologies or pay for external services to provide those resources temporarily or more permanently.

When developing an enterprise strategy for cloud computing, the considerations highlighted in the following table should be taken into account.

Table 1. Key elements of strategic planning

Element of Strategic Planning	Strategic Planning Activities
Educate the team	• All team members (IT, business, operations, legal and executives) must be educated on what cloud computing is and what it is not. • Establish a common definition of cloud (including terminology) for the entire enterprise so everyone is in synch. • Cloud is an iterative process in which new services build on previously implemented services adding value to existing IT environment.
Consider the existing IT environment	• Develop a complementary cloud adoption strategy with a focus on integrating and leveraging existing technologies and standards. • Develop a strategy to ensure that any existing services to be migrated to the cloud will continue to comply with standards. • Leverage reusable internal services to improve delivery efficiency of customer facing services
Understand required services and functionality	• Determine business case and potential ROI and/or potential new revenue opportunities • Leverage enterprise architectures, standards and industry frameworks to help accelerate the collection of service information and improve consistency. • Customer facing services (SaaS, for example) require separate

	categorization and analysis from internal services (PaaS, for example).
Identify required skills	• Map required skills against available skills. • Develop a plan to enhance internal skills to address potential gaps. • Consider external skills as an option for addressing gaps.
Establish both short and long term plans	• Create an enterprise-wide master blueprint and roadmap for adoption. • Map cloud benefits against existing business problems to identify potential solution areas. • Anticipate the variety of disruptions that may occur both inside and especially outside IT (accounting, tax, HR, legal, vendor management, etc.). • Leverage long term planning to reduce risk of vendor lock in by considering interoperability, portability and ease of integration up front.
Identify clear success goals and metrics to measure progress	• The team sponsoring the project must include the success factors in their proposal. • Metrics need to be agreed to by executives making the final decision to proceed with the project. • Define benchmarks for the existing service before launching the new service in order to determine its impact. • Clearly identify trigger points to be measured.
Understand Legal/Regulatory Requirements	• Consumers and potential consumers of cloud provider services must understand the responsibilities associated with their respective national and supra-national obligations for compliance with regulatory frameworks and ensure that any such obligations are appropriately complied with. Some examples of legal/regulatory constraints upon electronically stored information are as follows: • Physical location of the data • Data Breach • Personal Data Privacy • Data destruction when the corporation no longer wants the relevant data available or transfers it to a different host

	◦ Intellectual Property, Information Ownership ◦ Law Enforcement Access ◦ Service Availability • Be aware that migrating services to the cloud can render services inaccessible. With over 150 countries having ratified the United Nation's Convention on the Rights of Persons with Disabilities and an increasing focus on accessibility regulations, it is important to establish a plan for ensuring compliance.
Track results for an extended time	• Reinforce the objective of implementing the new cloud based service has been achieved • Identify any trends that may need to be addressed to improve the existing service or contract for a new service to take advantage of the trend

Step 3: Select Cloud Deployment Model(s)

The various cloud deployment models are introduced in the Rationale section above. In order to determine the deployment model(s) that best suits your company's business requirements you must take into consideration the critical factors highlighted in Table 2[4].

Table 2. Considerations for selecting a cloud deployment model

Consideration	Private (On-site)	Private (Outsourced)	Public
Criticality of cloud services	Private (On-site) is appropriate for mission critical, security sensitive services	Private (Outsourced) is appropriate for mission critical, security-sensitive services	Public is appropriate for services that are not mission critical and that do not require access to security sensitive information[5]
Migration costs	With a Private (On-site) deployment model, installing and managing cloud software may incur significant cloud software costs even if free	Private (Outsourced) has lower migration costs than Private (On site) since resources are provisioned by the provider. Main	Public clouds have low upfront costs to migrate into the cloud. The implications are similar to the outsourced private cloud scenario

[4] The information in this section is based on information from the NIST Cloud Computing Synopsis and Recommendations document, Special Publication 800-146. The Community deployment models are not called out explicitly in this section since they are similar to the Private deployment options.

5 SMBs may be more inclined to test the Public cloud waters sooner than most enterprises but must thoroughly consider security implications.

	hardware already exists within a consumer organization. Expenses may be mitigated if the enterprise has adopted a service oriented architecture environment and moves to an expense formula for internal departments.	additional startup costs relate to negotiating the terms of the SLA and possibly upgrading the consumer's network to connect to the outsourced private cloud.	except that additional security precautions may need to be taken into account.
Elasticity	With Private (On-site), limited resources are available since computing and storage capacity is fixed and has been sized to correspond to anticipated workloads and cost restrictions. If an organization is large enough, it may be able to provide elasticity to clients within the consumer organization.	With Private (Outsourced), extensive resources are available since a consumer can rent resources in any quantity offered by the provider.	Public clouds are generally unrestricted in their size. Additionally, they can generally use multi-tenancy without being limited by static security perimeters, which allows a potentially high degree of flexibility in the movement of consumer workloads to available resources.
Security threats	With Private (On-site), consumers have the option of implementing appropriately strong security to protect resources against external threats to the same level of security as can be achieved for non-cloud resources.	Private (Outsourced) is similar to Private (On- site). The main difference is that the techniques need to be applied both to a consumer's perimeter and provider's perimeter, and that the communications link needs to be protected.	With a Public model, consumers have limited visibility and control over data regarding security. The details of provider system operation are usually considered proprietary and not available for examination by consumers.
Multi-tenancy	With Private (On-site), risks are mitigated by restricting the number of possible attackers: all of the clients would typically be members of the consumer organization or authorized guests or partners.	The implications for Private (Outsourced) are similar to those for Private (On-site) cloud.	With a Public model, a single machine may be shared by the workloads of any combination of consumers. In practice, this means that a consumer's workload may be co-resident with the workloads of competitors. This introduces both reliability and security risk, and a failure or attack could be perpetrated by any consumer or virtual machine.

Useful hybrid cloud configurations are also possible. For example, "cloud bursting" is a concept in which a consumer uses on-premise IT resources for routine workloads but optionally accesses one or more external Private or Public clouds during periods of high demand.[6] Using one type of cloud to provide backup resources to another is another hybrid possibility as well as using one cloud for disaster recovery for a second.[7] Different cloud deployment variants may also be appropriate for particular organizational functions or roles. For example, an organization may elect to process sensitive data such as payroll information in an outsourced private cloud but use a public cloud for new software development and testing activities.

The IT maturity of an organization along with its size will have a significant impact on the service deployment decisions that are made. Larger enterprises with mature IT environments may lean initially towards Private (On-site) deployments and may transition to Private (Outsourced) and Public deployments over time for primarily non-critical workloads.

SMBs will be apt to transition more aggressively to Public deployments. SMBs have much to gain in terms of cost savings, IT capacity and application functionality that was not available to them previously. Security and reliability issues with Public deployment must be taken into consideration. As a result, SMBs are advised to initially consider Hybrid deployments, moving non-critical applications to Public deployment in the early transition phases.

Step 4: Select Cloud Service Model(s)

While the business value of cloud computing is compelling, many organizations face the challenge of staging a gradual adoption of cloud capabilities, incrementally advancing their IT environment. There are a variety of ways that organizations today are leveraging the benefits of cloud computing. Many patterns of implementation start with an infrastructure virtualization project to establish a foundation that enables future cloud adoption. Conversely, some companies are simply consuming business or IT solutions from a public cloud outside their organization. The three most common cloud service models are IaaS, SaaS, and PaaS as described in the “Rationale” section of this white paper. In order to determine the service models that best suit your company’s business requirements, the potential benefits and issues of each model must be given careful consideration. In addition, the IT maturity of an organization along with its size will significantly impact the service model decisions that are made.

Infrastructure as a Service (IaaS)

The incentives for an enterprise to transition to an IaaS environment differ based on the size and IT maturity of the enterprise. For SMBs, the primary motivation for considering IaaS is capital expense

[6] Note that it is important that mission-critical workloads be transferred to external cloud environments that provide appropriate security controls. In many cases, Public cloud environments are not appropriate for mission-critical applications.

[7] It is important that the cloud environment providing backup support offers identical quality of service that the source environment provides (in particular, security support).

reduction and access to IT capacity that would otherwise not be available. For large enterprises with potentially several data centers and departmental silos in different geographical locations, there are additional incentives for considering a move to IaaS. Incentives include addressing low server utilization, high administrator-to-server ratios, data center sprawl, proliferation of ad-hoc IT solutions, and desire for improved, more centralized control of IT assets.

While many enterprises today are using virtualization to consolidate their IT infrastructures, hardware consolidation is only one piece of virtualization's benefit. Organizations that move beyond virtualization with IaaS capabilities such as integrated service management, automation and rapid provisioning can realize significant benefits:

- Reduction in IT operating expenses and capital expenses by improving resource utilization and administrator-to-server ratios
- Faster time to market through increased efficiency and automation of standardized solutions
- Simplified, integrated management, including real-time monitoring and high-scale low-touch provisioning
- Greater visibility into business processes and system performance to identify redundancies and bottlenecks
- Scaled operations that can meet market dynamics and business strategy

Approaches for Adoption of IaaS

Organizations with mature IT systems already have significant investments in both infrastructure hardware and in-house IT management skills. As a result, they will initially look to refactor these assets as they transition to cloud computing.

Organizations with nascent IT systems, especially SMBs, may not have made significant investments in their IT systems. As a result, they will be incented to transition more rapidly to infrastructure services that are delivered and managed by an external cloud provider.

Table 3. IaaS Adoption Approaches

IaaS Adoption Approach for Large Organizations	IaaS Adoption Approach for SMBs
The following steps provide a recommended approach for IaaS adoption by large organizations: 1. Analyze IaaS offering in terms of total cost of ownership (TCO)/return on investment (ROI) and risks such as vendor lock in, interoperability and existing IT infrastructure. 2. Define a clear IaaS strategy for both private and public implementations before adopting	The following steps provide a recommended approach for IaaS adoption by SMBs: 1. Analyze IaaS offerings in terms of TCO/ROI, risk (vendor lock in/interoperability/existing IT infrastructure). 2. Define an IaaS strategy for both private and public implementations before adopting the IaaS offerings.

specific IaaS offerings.

3. Start with an infrastructure virtualization project to establish a foundation that enables future cloud adoption.

4. Consider moving to a Private (On-site) deployment model which provides a good initial transition to IaaS with relatively low risk.

5. Consider Private (Outsourced) and Public deployment models which can potentially deliver added business value. Closely consider security and reliability issues as well as integration with existing enterprise services.

6. For Public deployments, consider moving only non-critical applications in the early transition stages.

3. In many cases, the Private (On-site) deployment model will not be feasible given insufficient ROI associated with consolidating a relatively small number of existing IT assets.

4. Consider the Public deployment model which provides access to computing and storage capacity at the lowest cost.

5. For Public deployments, consider moving only non-critical applications in the early transition phases.

6. Consider Private (Outsourced) deployment to handle spillover of mission critical workloads during periods of high demand or as a backup resource for disaster recovery.

7. Application migration and administration costs must be taken into account for Public and Private (Outsourced) options.

Large enterprises should consider the following types of projects as good candidates for a transition to a Private (On-site) cloud-enabled data center include:

1. *Consolidate and virtualize your infrastructure*. Realizing the benefits of cloud computing begins with the foundation—efficient and effective consolidation and virtualization across server and storage platforms—to begin building a cloud infrastructure.
2. *Leverage image management.* Image management addresses the visibility, control and automation of virtualized images to reduce operational costs associated with virtualization proliferation in the data center and allows clients to better utilize virtualization as an enabler of high-quality service delivery. When clients implement effective image management, they are better suited to progress into a cloud computing model.
3. *Manage the virtual environment.* Organizations can expand beyond infrastructure virtualization with integrated service management, automation, provisioning and self service to more quickly deploy IT services, improve visibility, increase resource utilization and better manage their cloud environments.

Software as a Service (SaaS)

SaaS is an evolved version of the cloud concept that makes computing a utility that businesses can easily adopt. SaaS allows businesses to benefit from the "pay-as-you go" concept in addition to being highly scalable, offering flexibility to companies to provision and de-provision based on business needs.

While IaaS and PaaS are important service models, SaaS gives businesses complete freedom from managing IT infrastructure and enables them to concentrate on using the features of software to achieve their business objectives. Business solutions on cloud provide customers the flexibility to choose the approach that is best for their company by making it possible to consume and execute business processes, analytics and applications in the cloud.

We can categorize SaaS under two broad headings:

- *Horizontal SaaS offerings.* These are SaaS offerings that are typically applicable to organizations across sectors. Some of the common SaaS applications are in the areas of email, customer relationship management (CRM), productivity, collaboration, analytics, etc.

- *Sector-specific offerings.* With the proven success and maturing of the horizontal SaaS offerings, sector specific SaaS offerings are emerging. These include applications in the areas of logistics, supply chain management (SCM), etc.

SaaS has the following key features:

- SaaS offerings are easily accessible over the public Internet through an Internet browser which makes it very easy to roll them out to a large audience within a short period of time.

- SaaS works on a usage-based pricing model which enable businesses to subscribe to only those services that it needs and for the required number of users.

- SaaS typically offers a standard feature set which allows some level of configuration for individual customers but typically no customization.

- Organizations can reduce their capital expenditures (CAPEX) towards procurement of software licenses by adopting SaaS offerings on a subscription basis.

- Implementation of SaaS offerings can take as little as 1 – 2 weeks in comparison to packaged solutions which typically take anywhere from 2 weeks – 6 months. This enables businesses to capture any short “window of opportunity” that may present itself.

- SaaS upgrades are typically instantaneous and are the burden of the provider. They get tested prior to deployment and the process is transparent to the users.

- SaaS offerings are typically scalable as vendors plan for scalability in their cloud solutions. This enables businesses to scale up rapidly if the business needs dictate.

- Availability of the solution is taken care of by the provider thereby eliminating the need for users to maintain their own disaster recovery solution for these solutions.

Approaches for Adoption of SaaS

The approach for adopting SaaS offerings will differ based on the IT maturity of the organization. For simplicity, two approaches are described below: one for large organizations and one for SMBs. However, given that each organization is unique with its own challenges, it is recommended that organizations evaluate both options and come up with a strategy that addresses their unique requirements.

Organizations with mature IT systems already have implemented in-house packaged applications. Having spent years with these systems and making significant investment in hardware, software and management of these systems, they are reluctant to let go of these systems which have stood the test of time. These applications often have the highest costs per unit of functionality to enhance, support and operate, so therefore significant cost reductions can be realized. Unfortunately, migrating this class of application (legacy or non-virtualized) will incur higher project costs.

Organizations with nascent IT systems, especially SMBs, may not have made significant investments in their IT systems. The reasons for this could vary from cost concerns to complexity in managing such deployments in-house. However with the emergence of subscription based SaaS offerings, such organizations now have an option to adopt SaaS solutions for business needs which was not possible earlier.

Table 4. SaaS Adoption for Large Organizations

SaaS Adoption Approach for Large Organizations	SaaS Adoption Approach for SMBs
Large organizations can take the following approach to SaaS adoption: 1. Analyze SaaS offerings in terms of TCO/ROI and risks such as vendor lock in, interoperability, and existing IT infrastructure—especially network. 2. Define a clear SaaS strategy for both private and public implementations before adopting specific SaaS offerings. 3. Consider SaaS for non-critical business functions that would deliver improved ROI in a cloud environment. 4. Consider SaaS for rapidly evolving business environments where new requirements are likely to emerge, such as social business and Web campaigns. 5. Evaluate SaaS offerings when packaged applications need to be renewed due to a	SMBs can take the following approach to SaaS adoption: 1. Analyze SaaS offerings in terms of TCO/ROI and risks, such as vendor lock in, interoperability, and existing IT infrastructure—especially network. 2. Define a SaaS strategy for both private and public implementations before adopting specific SaaS offerings 3. Reevaluate business processes and identify those that can be enhanced through use of applications that can help improve competitiveness with larger organizations 4. Identify availability of SaaS offerings for these specific processes 5. Evaluate the various SaaS offerings from a business and technical perspective

software or hardware refresh which involves additional purchases.

6. Adopt new disruptive SaaS solutions (perhaps sector-specific) to maintain or extend competitiveness.

Platform as a Service (PaaS)

PaaS leverages an integrated development and runtime platform for creating, deploying and managing cloud applications. Based on the standardization and automation of a common set of topologies and workloads, the platform provides elasticity, efficiency and automated workload management. A PaaS environment dynamically adjusts workload and infrastructure characteristics to meet existing business priorities and SLAs

PaaS helps eliminate the need for developers to work at the image-level, enabling developers to completely focus on application development. It also helps reduce software design steps and enables faster time-to-market using predefined workload patterns.

The incentives for an enterprise to transition to a PaaS environment differ based on the size and IT maturity of the enterprise. For large enterprises, a key motivation for considering PaaS is the ability to quickly and inexpensively develop and deploy new applications. Large enterprises have additional incentives for considering a move to PaaS. PaaS provides:

- A highly standardized and automated provisioning of predefined workloads
- An integrated development and runtime platform for specific workloads
- A consistent pattern-based deployments for most common workloads
- In Integrated workload management for SLA enforcement, dynamic resource management, high availability and business priorities
- Awareness and optimization of workloads based on business priorities and SLAs
- Consolidation of workloads under a simplified management system

Approaches for Adoption of PaaS

Organizations with mature IT systems already have significant investments in their development and runtime platforms along with significant investments in human resources associated with solution development and testing. As a result, they will initially look to refactor these assets as they transition to cloud computing.

In many cases, SMBs do not possess the resources to invest significantly in development and runtime platforms and they lack the in-house human resources to develop and test home-grown applications. Many SMBs are dependent on ISVs to deliver their application functionality. As a result, they are dependent on an external cloud provider to support a PaaS environment that is consistent with their ISVs' applications.

Table 5. Approaches for Adoption of PaaS

PaaS Adoption Approach for Large Organizations	PaaS Adoption Approach for SMBs
The following steps provide a recommended approach for PaaS adoption by large organizations: 1. Analyze PaaS offerings in terms of total cost of ownership (TCO) / return on investment (ROI) and risks such as vendor lock in/interoperability/existing IT infrastructure. 2. Define a clear PaaS strategy for both private and public implementations before adopting specific Paas offerings. 3. Identify early offering candidates based on specific criteria (for example, low risk to the business). 4. Consider starting with either the Private(On-site) or Private(Outsourced) deployment model which provides a good initial transition to PaaS for both mission critical and non-mission critical workloads with relatively low risk. 5. For Public deployments, consider moving only non-critical applications in the early transition phases 6. Consider a platform that leverages existing expertise – i.e., a development team experienced in Java will likely gravitate to a Java-based platform.	The following steps provide a recommended approach for PaaS adoption by SMBs: 1. Analyze PaaS offerings in terms of TCO/ROI and risks such as vendor lock in, interoperability and existing IT infrastructure. 2. Define an PaaS strategy for both private and public implementations before adopting specific PaaS offerings. 3. Determine if there's sufficient in-house development resource to justify the expense of a PaaS environment – if not, SaaS may be the best alternative.

If sufficient in-house development resources exist, both the Private (Outsourced) and Public deployment models are viable options. Selection will be dependent upon the mission criticality of the services being developed and deployed.

Here are a few specific projects that large enterprises should consider to get started on the transition to a PaaS environment:

- *Deploy and manage application infrastructure.* Virtualize, standardize and automate provisioning and management of runtime services to reduce operational costs, speed time-to-value, and better utilize hardware resources.

- *Deliver development and testing environments.* Standardize the delivery of development and test tools that conform to enterprise processes and instantly deliver to a globally-distributed team.

- *Develop and deploy new web applications.* Create, deploy and manage new web applications in a simple, fast and "low touch" way through a virtual application pattern.

As illustrated in this section, there are numerous considerations that need to be taken into account when selecting a service model that best meets your company's business requirements. An effective initial approach is to identify a contained, non-critical business area where cloud could be impactful, identify one or more cloud service models that could be effective in addressing the requirement, and initiate a proof of concept to assess the feasibility and ROI of the alternatives.

Step 5: Determine Who Will Develop, Test and Deploy the Cloud Services

Determining the most effective method to design, develop and deploy new cloud services can be a struggle. In many cases, there is no right answer. The direction will be based on the needs and capabilities of the enterprise. There are essentially four options for the enterprise to consider[8]:

- In house development and deployment
- Cloud provider development and deployment
- Independent cloud service development provider
- Off the shelf purchase of a cloud service

Table 6 examines the pros and cons of the various options for acquiring a new service.

[8] The design of the cloud service is omitted since that should originate from the enterprise and will require the efforts of the IT, business and administrative teams. The new service must have functional capabilities which meet the requirements of the target users and will have also a positive ROI. Designing a cloud service is an extended discussion which will not be covered here, other than to state that ensuring that the design process is followed will be critical to the development and deployment activities.

Table 6. Options for acquiring a new service

Options for acquiring a new service	Skills	Startup considerations	Updates to services	Testing and deployment
In house development and deployment	In house development and deployment is dependent on internal skills and availability of in house resources to develop new services.	In house development and deployment should reduce the learning curve on how to link to legacy services.	With In house development and deployment, the enterprise owns the cloud service and can add updates on the enterprise timetable.	In house development and deployment offers potentially tighter controls during the testing process. In house test managers are able to work closely with other IT and business leaders to ensure complete testing is done.
Cloud provider development and deployment	When using a cloud provider, the cloud provider's area of expertise is cloud computing which should translate into a shorter development and deployment timeline especially with the first cloud service.	A cloud provider needs to be educated on the legacy services which need to be linked to the cloud service (APIs, data formats, etc.).	If the cloud provider does the maintenance for new features, the enterprise needs to understand costs and the expected responsiveness to complete requested updates.	Using a cloud provider creates a potential challenge for testing of the cloud service. It requires cooperation between the enterprise development and operations teams with the cloud provider development and test teams.
Independent cloud service development provider	An independent cloud service development provider should have expertise on the specific cloud service which is being contracted for, thereby reducing development, testing and deployment costs.	The independent cloud service development provider would need to be educated on the legacy services which need to be linked to the cloud service.	The independent cloud service development provider would need to interface with the enterprise implementation team and also the cloud provider implementation team in order to test and deploy the cloud service.	With an independent cloud service development provider, ongoing updates and testing could be more complex and costly as well as take longer given the need to coordinate three parties as opposed to two.

Off the shelf purchase of a cloud service	If using an off the shelf cloud service, ensure that the service meets all the business requirements for the enterprise's cloud service and all the open standards and API requirements of the enterprise.	If using an off the shelf cloud service, determine how easy it will be to map the off the shelf data formats to the enterprise's data formats.	If using an off the shelf cloud service, determine who will be responsible for the modification, testing and deployment activities.	Ensure the initial cost of the off the shelf service offsets the costs for modification. If the time to deployment is significantly shorter then off the shelf option should be considered.

Selecting a methodology for implementing a cloud service can vary depending on whether the consumer is a large enterprise or a SMB. Typically, the skills available within an SMB are targeted towards existing services and it may make more sense to consider contracting for resources from a cloud provider. Large enterprises may have the flexibility for re-assigning internal skills to a cloud project and accommodating the transition to cloud internally.

As is evident from the above analysis, there are tradeoffs for each option. Ultimately, the enterprise needs to take its own unique requirements into account in order to make a decision that best meets their business needs. This also can translate into leveraging several of the options in parallel, based on the needs of a particular cloud service.

Step 6: Develop a Proof-of-Concept before Moving to Production

Once there is agreement that cloud is a viable option and the promise of a positive ROI can be established, it is important to get senior management approval. There needs to be a review of the proposal, projected costs, timeline, risks and resulting benefits with the senior management team. Assuming there is agreement, the next (recommended but optional) step is to assemble a proof-of-concept (POC) team which includes the following:

- *Information Technology*. The team includes architects, systems administrators, development, and customer support (help desk).
- *Functional representative*. The team includes a designated individual within the enterprise who can represent business user expectations.

Assuming that the POC is successful and meets or exceeds expectations, a production implementation of the cloud service can be delivered. Implementing a new cloud service requires the same discipline as implementing a non-cloud service. The implementation team needs to ensure the following activities are completed:

- Verify the cloud service delivers required functionality in a test environment
- Verify that all processes continue to work - end users simulate transactions
- Verify data recovery activities

- Ensure that the help desk can address questions and problems quickly
- Develop a back out plan should there be an unexpected problem in the early stages of production so as not to impact users

The POC can be implemented either in-house or directly on a public cloud. While a public cloud provides benefits like quick provisioning and scalability, it is important that organizations perform testing using representative rather than production data to ensure data security. It is also important to recognize that there may be differences between the POC and target cloud environments that will have to be addressed upon migration to the production environment.

Once all the testing has been completed and all of the stakeholders have signed off that their area is working properly, the new cloud service can be put into full production when the following activities are completed:

- Business contracts agreed to and in place
- SLA agreed to and in place
- Customer support (help desk) educated and in place. Help desk can either be within the enterprise or with the cloud provider
- Post implementation management plan completed

Step 7: Integrate with Existing Enterprise Services

Cloud computing is usually not seen as a total replacement for existing services within the enterprise. Particularly for many large enterprises, a significant investment has been made in existing services including compliance with government legislation and industry standards. In many cases, the existing enterprise services have also adopted infrastructure standards (such as web services standards) to increase interoperability and portability. Further, organizations seek to adopt the cloud to extend their business processes so that they become more accessible to others in their business ecosystem, for example, suppliers and business partners.

There are several ways of establishing seamless links between cloud services and existing services. If the enterprise has already established a direction of adopting open infrastructure standards, then the cloud services should build on what has been already implemented. This increases the opportunity for achieving interoperability between the cloud and the enterprise services.

If the enterprise has not implemented a discipline of adopting open infrastructure standards, then the new cloud services can be used to set the baseline. A clear plan for adopting open standards will ensure interoperability and portability for all cloud services and simplify the process of integrating new services, independent of where or how the new cloud service is acquired.

Integrating open standards into the enterprise can be managed through the use of standardized Application Programming Interfaces (APIs). These APIs will be the conduit between the open standards supported by the cloud services to the existing enterprise services. These APIs will capture data transferred from the cloud services and translate it into a format which can be consumed by legacy services. Conversely, if the legacy services need to transfer data to the cloud service, a similar API will be used.

The most costly method of integrating new cloud services into the enterprise will be to initiate a project to develop custom code for each new cloud service as it is implemented. If this process is followed there are many downsides:

- Increased development costs and time to market for the new cloud service
- Increased maintenance costs to add new capabilities
- Reduced flexibility to integrate new services using the same legacy service
- Increased costs and time to move a cloud service to a new cloud provider
- Higher costs to establish a disaster recovery plan

The security aspect should not be ignored when integrating existing enterprise services with the cloud. Necessary interface controls should be implemented to ensure secure transfer of data.

Step 8: Develop and Manage Service Level Agreements

Creation of an SLA is important to clearly set expectations for service between the cloud consumer (buyer) and the cloud provider (seller). Each cloud entity engaged by the enterprise should have a SLA defined, including: cloud provider, cloud carrier, cloud broker and even cloud auditor. Consideration must also be given to the different types of service models (IaaS, PaaS and SaaS) as each model brings different requirements. This section will focus on the SLA details between the cloud consumer and cloud provider.

The SLA establishes responsibilities for specific activities and allows each party to understand the risks before entering into an agreement. The SLA sets expectations for when issues must be resolved, and spells out any penalties and an exit strategy should the cloud provider not be able to meet the terms of the SLA. As part of the SLA, a service availability target from the cloud provider should be included. The level of service is dependent on the criticalness of the information being processed. If the data being processed is related to account processing (i.e. user is accessing their bank account) it may make sense to monitor for outages and develop a callout process to restore service. If the service is for inquiry only and is tied to non-critical data (i.e. catalog information), the level of service may be lower.

When developing a SLA for cloud services, the considerations highlighted in Table 7 should be taken into account.

Table 7. Key elements of SLA management

Key Element of SLA Management	Key Considerations
Assign core SLA team	• The team should consist of members from IT, business, operations and legal. • The organization should identify an SLA focal point to interface with cloud provider on ongoing basis

	• Team must be fully educated on what cloud computing is and what it is not. • Team must also understand the expectations of the cloud service.
Develop SLA for contracted service	• The core SLA team should identify elements which are critical to protecting the ongoing operations of the enterprise including, but not limited to: • Security and privacy of sensitive data • Proof of origin/geographic location • Adherence to government and industry regulations (i.e. accessibility[9]) • Service performance and availability guarantees • Data recovery plans in the event of a catastrophic failure including offsite data storage • Migration plans in case the provider goes out of business • Agreement on whether subcontracting to another cloud provider is permissible • The SLA sets expectations for when issues must be resolved, and spells out any penalties and an exit strategy should the cloud provider not be able to meet the terms of the SLA.
Define critical processes with the cloud provider	• The cloud provider should identify a person to interface with the cloud consumer to address any and all concerns on the provided service. • The cloud provider must provide scheduled reports on service performance and activity. • The organization should define a process to ensure issues which cause service to perform outside of the agreed to performance levels are resolved in a timeframe consistent with the SLA. • The organization should define an escalation process to elevate the visibility of issues, depending on impact, to the appropriate parties in both the cloud consumer and cloud provider organizations.

[9] The requirement for Information and Communications (ICT) accessibility has intensified in Government, Public Sector, Education and University sectors in the United States and other countries, including Canada, U.K. and Australia. Indeed, there is a global increase in ICT accessibility due to new disability laws and regulations worldwide. Over 150 countries, including the United States, have ratified the United Nation's Convention on the Rights of Persons with Disabilities.

Schedule regular review meetings with key stakeholders within the enterprise	• The SLA focal point within enterprise leads the meetings. • The main objective of scheduling regular review meetings is to review SLA status on an on-going basis. • Review meetings become more important as more cloud services are being implemented and/or the number of cloud providers increases.
Schedule regular checkpoint meetings with cloud provider	• Establishing an ongoing dialogue ensures that problems are addressed before they become major issues. • Checkpoint meetings help establish a trail on the status of the elements of the SLA. • The enterprise can use the information from checkpoint meetings to terminate the SLA if the cloud provider cannot resolve problems consistent with the expectations of the SLA.
Maintain a continuous level of responsibility	• An SLA does not absolve the cloud consumer of all responsibilities. • Ongoing vigilance is required to ensure that enterprise users continue to receive the expected level of service. • Maintain a continuous level of responsibility by receiving direct feedback on level of performance and be aware of any additional features which may be needed.

The SLA is the written agreement used to settle disputes over the delivery of service. Investing the time to develop a comprehensive SLA will help eliminate disagreements in expectations between consumer and provider, and help ensure that satisfactory service levels are delivered.

Step 9: Manage the Cloud Environment

The responsibility within the enterprise for the successful operation of cloud services is shared by the CIO, who has overall responsibility, and the manager of customer support who manages the day to day operational challenges. Any problems which cannot be resolved must be escalated to the CIO to ensure that all avenues to resolve the problem have been executed. If the problem cannot be resolved then the options written into the SLA can be invoked.

The technical and customer support requirements vary based on the service model, deployment model and hosting option selected:

- For a Private (On-site) cloud, the management of the cloud will be consistent with the management of the existing services within the enterprise.

- For Private (Outsourced) and Public clouds, the responsibility for management of the cloud service(s) will be laid out in the SLA. The SLA will establish processes for identifying a problem, who is responsible and depending on the impact of the problem, what resources are brought to bear to resolve the problem (from both consumer and provider).

A disaster recovery process must be defined and implemented to protect the enterprise and its digital assets. The disaster recovery process must be verified prior to putting the cloud service into production. When required, the customer support manager within the enterprise is responsible for initiating the disaster recovery process. There must be a trained individual in both the cloud provider and the cloud consumer areas who can ensure that the recovery process is completed properly and can verify no data loss. Again, it is strongly recommended that the disaster recovery process be tested and verified before it is needed.

There must be a documented agreement (SLA) between the cloud consumer and the cloud provider as to the process for problem reporting and response to the individual reporting the problem. Each problem should have a severity assigned to it to reflect the impact and the resulting urgency for resolution. If an individual within the enterprise cannot get a problem resolved through the cloud provider, the issue should be escalated to the customer support manager. The customer support manager will assess the severity of the problem and take the appropriate action.

In addition to technical and customer support, management of the cloud environment also entails handling of change requests made by the business to meet its changing requirements. An effective change management process needs to be implemented to ensure that business needs are gathered, validated, tested and deployed. Further, in the likely scenario of having multiple cloud vendors, vendor management processes need to be clearly defined to obtain optimum results.[10]

Summary of Keys to Success

Table 8 summarizes a few of the critical keys to success for any organization embarking on a cloud computing journey.

Table 8. Summary of keys to success

Key to Success	Summary
Establish executive support	• Senior management team must understand and take responsibility for the successful adoption of cloud solutions. • Pressures will come from three key players in any cloud decision: IT, finance, procurement, and the user community. • The IT community is most concerned about the global accessibility and impact on things like networks, security, user performance, etc. The key to their

[10] For services offered in a public cloud environment there may not be the ability to request customization of a service as the offering is used by more than one consumer and only the data is segregated.

	support is a globally-aware architectural plan for cloud implementation. • Finance and procurement are most concerned about saving money. The key to executive support is a well-thought ROI rationale and calculation. • Users are often most concerned scaling the environment in lock-step with changes to the business. The key to executive support from this group is to demonstrate higher elasticity from the cloud.
Address organizational change management	• Management must understand and address the pressures introduced by cloud computing on the organization. • Cloud will introduce change to the normal IT development and deployment processes, breaking down many organizational barriers and norms. • At the heart of change is fear of loss—primarily, loss of control. The change must have a well-managed, well-planned process for mitigating fear of loss. • Embracing change is critical to success.
Establish commitment	• The organization must be fully committed to developing and executing a strategic plan for cloud computing within the enterprise. • Adoption of the cloud should be led by senior management including the CEO and CFO with the CIO and CTO playing a role of key enablers.
Develop a Service Level Agreement which meets the needs of the business	• Do not shift bad workloads to the cloud and expect that they will become good workloads. • Do not use SLAs for a fundamentally broken system that cannot meet the expectations being set. The SLA is a shared responsibility and simply moving a service to a cloud provider does not mean that the service will magically work. • Buy service, not servers. Look for complete managed services where you rely on the cloud provider to integrate all the parts into a complete solution. • A properly negotiated SLA will ensure there is a partnership between the consumer and provider for the overall success of the service.
Address federated governance	• Cloud by nature is distributed, but most command-and-control systems for managing IT are hierarchical. • To succeed, some degree of distributed control and federated governance is necessary to match the model of cloud delivery. • Before making a decision on a cloud provider, it is important to understand how the cloud service will be managed and what processes need to be

	integrated into the existing IT environment.
Rationalize security and privacy	• At the heart of security is trust. Often cloud providers have a deeper awareness of what is required to provide good security than the consumers they serve. However, the consumer and cloud provider must work together to establish a trust relationship and to establish the security and privacy required. • Document the level of security required to properly protect the service and data and let the provider confirm how the requirements will be met. Objectively measure the provider's true security capabilities. • It is critical that sensitive information does not find its way into the wrong hands. The provider is responsible for ensuring the privacy of the data is maintained, consistent with the requirements of the SLA
Comply with legal and regulatory requirements	• An enterprise must be aware of and plan for adherence to legal and regulatory requirements, including those related to security, privacy and accessibility. Failure to comply can derail the cloud effort and result in costly lawsuits.[11]
Define metrics and a process for measuring impact	• There is truth in the old adage that "People do what you inspect, not what you expect." • Create operational metrics which define steady state success - define how the metrics will be measured. • Use metrics to assess cost savings and revenue enhancement, and to validate SLA compliance, including elasticity, availability, performance globalization, etc. • By measuring results, there will be a baseline from which to make better decisions for future cloud services with the goal of continual ROI improvement.

Cloud computing offers a value proposition that is different from traditional enterprise IT environments. With proper focus on the key success factors, the promise of the cloud can be realized.

[11] Private citizens with disabilities, the National Federation of the Blind and the American Council of the Blind, and US States Attorney Generals have raised focus on IT accessibility by pursuing legal action against Target, Federal Government of Canada, Universities, and others.

Works Cited

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing (Draft): Recommendations of the National Institute.* Gaithersburg: National Institute of Standards and Technology. http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf This white paper defines cloud computing, the five essential characteristics, three service models, and four deployment models.

Staten, J., Kark, K., & Chi, E. (2011). *The Three Stages Of Cloud Economics: How To Maximize Savings And Increase Profits For Your Organization.* Cambridge: Forrester Research. http://www.forrester.com/rb/Research/three_stages_of_cloud_economics/q/id/59165/t/2 This paper describes cloud economics as a three-stage discipline, how you can use performance analysis to move to the second stage and business model profiling to move to the third stage.

Bittman, T. Private Cloud Computing: Driving a Strategy. Gartner Analyst Report. January 20, 2011. http://www.gartner.com/it/content/1504100/1504116/january_20_private_cloud_tbittman.pdf. This presentation describes the prevalent private cloud computing strategies expected through 2015.

Hunter, R., Iyengar, P., Rowsell-Jones, A. (December 1, 2010). *On Demand: From Capacity to Capability.* Gartner Analyst Report. http://www.gartner.com/DisplayDocument?id=1508715. This paper explains how cloud computing can provide CIOs with the on demand capacity and capabilities needed and anticipates the trend for the next ten years.

Kelley, M. (June 25, 2011). *ALA Annual 2011: Helping Disabled Patrons Gain Access through the Cloud*. Library Journal. http://www.libraryjournal.com/lj/communityala/891140-448/ala_annual_2011_helping_disabled.html.csp. This article provides an example of how cloud is being used to support inclusive computing.

Morimoto, H., & Takagi, H. (2011). Collaborative Web Accessibility Improvement System: A Real-World Deployment. CSUN 2011. http://www-03.ibm.com/able/news/downloads/IBM_Web_Accessibility_Improvement_System_CSUN_2011.pdf.This presentation describes a cloud-based system where visually impaired people can report difficulties in seeing web images or charts.

The Economist. (October 23, 2011) *Computers without Borders: The cloud may be the ultimate form of globalisation*. http://www.economist.com/node/12411854. This article discusses the political tensions that will arise with the cloud and explain why cloud computing with its virtualized computer systems and services that know no borders may be the ultimate form of globalization.

Additional References

Cattteddu, D. & Hogben, G. (November 2009). Cloud Computing: Benefits, risks and recommendations for information security. European Network and Information Security Agency. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment. This white paper provides security guidance for potential and existing users of cloud computing.

Cloud Security Alliance. (August 15, 210). *CSA GRC Stack including CCM v1.1.* https://cloudsecurityalliance.org/research/initiatives/grc-stack/ This is an integrated suite of four CSA initiatives: CloudAudit, Cloud Controls Matrix, Consensus Assessments Initiative Questionnaire and the CloudTrust Protocol.

Cloud Security Alliance. (December 2009). *CSA Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.* https://cloudsecurityalliance.org/csaguide.pdf. The focus of this white paper is on the central issues of cloud computing security.

Cloud Security Alliance. (March 2010). *Top Threats to Cloud Computing V1.0.* https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf This white paper provides best practices to secure cloud computing across 13 domains of concern.

Daskala, B. & Marinos, L. *EFR (Emerging and Future Risks Framework, Introductory Manual*. (March, 2010). European Network and Information Security Agency. http://www.enisa.europa.eu/act/rm/files/deliverables/efr-framework-handbook. This handbook provides the documentation of the EFR Framework which consists of a scenario-based process model developed in order to assess and manage emerging and future risks.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media. http://www.amazon.com/Cloud-Security-Privacy-Enterprise-Perspective/dp/0596802765. Insight from knowledgeable experts including a former Chief Security Strategist for RSA on how to keep your virtual infrastructure and web applications secure.

Forrester Research, Inc. (April, 2011). *Myth Buster – Deploying Virtualization Technology Does Not Automatically Create A Private Cloud.* http://resources.idgenterprise.com/original/AST-0036901_Myth_Buster-Deploying_Virtualization_Technology_Does_Not_Automatically_Create_A_Private_Cloud.pdf This report maintains that IT must first achieve a minimum maturity level with virtualization, infrastructure, and process standardization to reach to achieve the value of a private cloud.