

Pilot Texas Cloud Offering

Cloud Computing Overview

Cloud computing is an emerging form of delivering information technology (IT) services via convenient, on-demand network access instead of through an organization's own technology infrastructure. Government organizations are using cloud computing solutions as a way to obtain IT capabilities that are flexible, have lower costs, and are quick to implement. In some cases, there is an element of self-service associated with using cloud services.

Cloud computing provides the same access to IT resources—such as email, databases, servers, storage, application software, development tools, and desktop services—as solutions that are procured and maintained on premises. In many cases, cloud computing reduces the need for organizations to incur capital expenses associated with procuring, implementing, and maintaining on-premise resources in exchange for services that are funded with operating expenses.

While the adoption of cloud computing is still relatively low in the public sector, the underlying service delivery model dates back to the advent of mainframe computing. Instead of buying or leasing equipment and hardware for payroll and billing, organizations shared centralized computing resources on an as-needed basis to save on costs.

Cloud computing is enabled through virtualization of IT resources such as computing, storage, network, and software. Virtualization enables the creation of logically partitioned IT resources that share a set of physical resources. These virtual resources are then designed and created through web-based user interfaces that enable simple, quick, and automated provisioning of these resources. Virtualized resources become cloud resources when these resources can be defined and managed for specific organizations and made available with ongoing self-service ability to manage the virtual resources and leverage on-demand access (i.e., public or private Internet). Cloud resources are also centralized, but shared by many groups and organizations to effectively increase use of the physical resources allocated, which can help to reduce overall costs.

There are currently three different deployment models for cloud: *public* cloud, *private* cloud, and *hybrid* cloud.

- In a **public cloud**, the provider delivers common IT capability in a shared environment with great scalability. Demand from multiple customers with similar requirements are pooled together to optimize physical resources. Access is via an on-demand public network capability, such as the Internet.
- In a **private cloud**, IT resources are dedicated and customized with the capabilities, resources, and administration required by a specific organization. Access is generally through a secured or managed network. Private clouds require a data center location, IT physical resources, virtualization, and operations team support. A *virtual private cloud* is characterized by having a specific capacity in a public cloud carved out and dedicated to a particular organization and made available through a secured, managed virtual network.

- In a **hybrid cloud**, the provider blends both private and public cloud features together, with combination preferences usually driven by a particular market niche or consumer group based on an application or system that has partial needs for highly secure or non-virtual resources.

Types of services provided through the cloud include

- **Software as a service (SaaS)** – delivers applications, such as email, customer relationship management, and collaboration software.
- **Platform as a service (PaaS)** – delivers an application framework that supports design and development, testing, deployment, and hosting. PaaS enables organizations to develop custom applications on one platform, but then easily deploy to many hosting environments that support the same platform based on various pricing and service level agreement (SLA) models supported by the instance of that platform environment.
- **Infrastructure as a service (IaaS)** – delivers computing hardware, storage, networking, and other managed services such as backup, monitoring and virtual private network (VPN).

Pilot Texas Cloud Offering

Given the growing significance and maturity of cloud-based services, the Department of Information Resources (DIR) determined it was necessary and timely to gain a deeper understanding of all facets of cloud-based offerings within the public-sector context. Cloud services are generally expected to offer reduced cost and increased efficiency for government organizations. However, the relative uncertainty of the contractual and operational components of cloud services has been a barrier to broad adoption in government.

To develop real and meaningful cloud experience, DIR pursued a pilot, or trial, project aimed at institutionalizing the knowledge needed to successfully enable broad adoption. The Pilot Texas Cloud Offering (PTCO) project focused on infrastructure as a service, but many of the lessons learned can be generalized for government agencies adopting any cloud offering.

The PTCO project was designed to allow a small group of agencies to choose a virtual private cloud-based infrastructure as a service from a marketplace of service providers made available by a *cloud broker*. This approach was selected as it maximized the opportunity to produce the broadest spectrum of experiences for customers. The cloud broker helped to normalize the multiple services available, creating an “apples-to-apples” comparison in pricing and functionality as much as possible. In addition, the cloud broker provided a single, unified web interface for end users to design, procure, provision, monitor, and govern the services. The PTCO allowed DIR and the pilot agencies to gain a greater understanding of cloud infrastructure offerings for state government and document options and issues with provider selection, pricing, access security, data security, credentialing, provisioning time frames, service levels, service remedy options, terms of use, billing models, interoperability, mobility, scalability, capacity management, provider compliance, and monitoring and licensing.

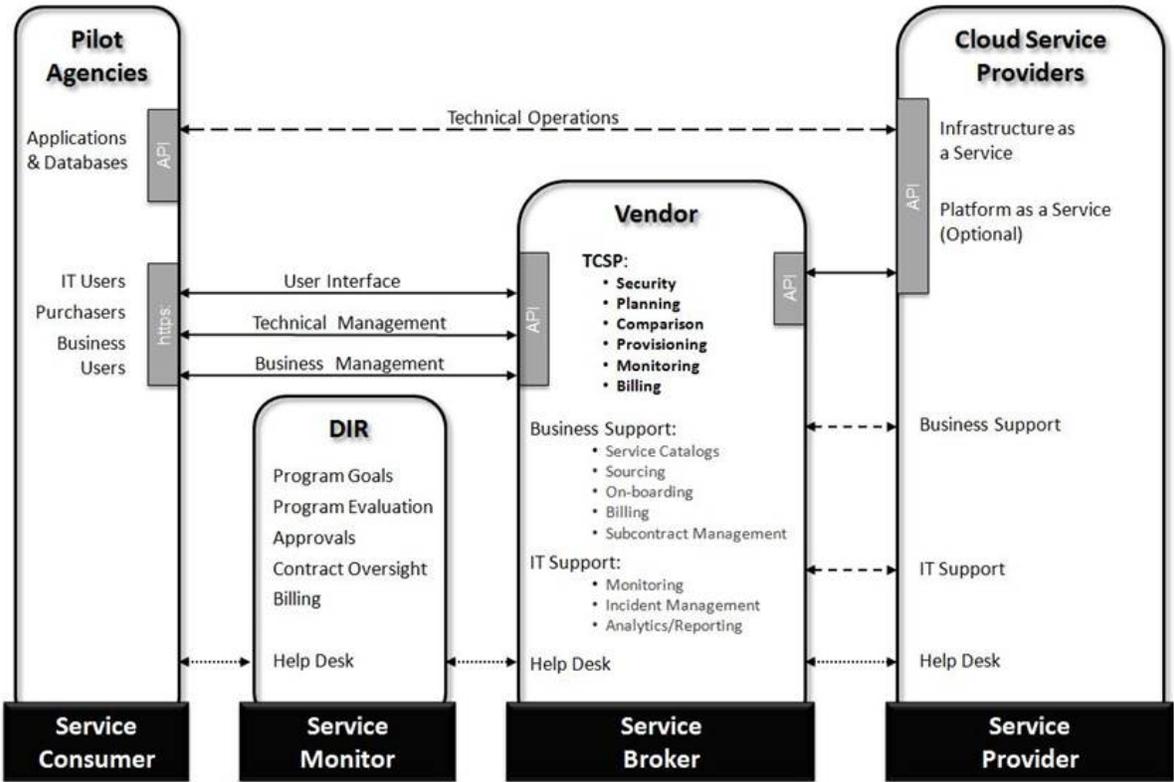
Participating agencies used both large and small applications to investigate the appropriateness of cloud infrastructure hosting for the public sector. Some applications are currently available to the public in production mode while other applications are in development and testing phases. Pilot agencies

included the Office of the Secretary of State, the Texas Water Development Board, the Texas Department of Transportation, and the Texas Department of Information Resources.

Cloud providers were initially chosen by their standing in Gartner’s Magic Quadrant. The terms and conditions were approved by the customers and Savvis, Terremark, Amazon, and Vintage IT Services provided services.

Contractual and technical support was provided by Vintage IT Services and Gravitant, the cloud broker. Gravitant’s self-service web portal, Texas Cloud Self-Service Portal (TCSP), allowed participating agencies to manage and support all phases of the engagement from solutioning to provisioning, operations and capacity management, and decommissioning. Gravitant also provided extensive architecture and solution support. Gravitant, as the cloud broker, established, negotiated, and governed the reseller agreements with the individual cloud service providers. They maintained a catalog of services, line items, and prices associated with each provider, which enabled them to facilitate cloud provisioning across multiple providers—a key feature for government agencies.

Figure 1: PTCO model



PTCO Lessons Learned

Early pilot adopters moved forward with trial and error, figuring things out one step at a time and refining operations based on actual experience. The purpose of this document is to share the collective experiences and lessons learned from the pilot participants. The list of lessons learned resulted from individuals asking and answering questions in the dynamic and collaborative environment created for use during the PTCO.

1 – Not all applications are appropriate for the cloud

Some might consider choosing to use cloud computing as a large, complex, all or nothing decision. A more appropriate perspective is considering how cloud infrastructure could contribute to the development life cycle of individual applications and the role it might play in an overall IT portfolio strategy.

In general, the cloud environment should be considered for applications that

- require rapid deployment,
- are approaching a technology refresh and/or the end of contractual obligations to a legacy environment,
- have variable storage needs,
- need bursting capability,
- use virtual servers rather than physical servers (the reliability, performance, or security of dedicated servers are considerably more expensive when procured through the cloud), or
- are based on federal funding with “cloud first” recommendations.

2 – Variety of services and variety of needs create complexity

Migration to cloud infrastructure shares common issues with the technical migrations that have come before it. For example, the migrations from mainframes to PCs and from standalone PCs to distributed networked PCs affected the connectivity, compatibility, and ability of hardware, middleware, operating systems, and databases. Each of these migrations were complex and required architecture and design solutions to work effectively.

In the cloud, as with any hosted infrastructure solution, each requirement has the potential to introduce configuration challenges that are usually overcome through technical troubleshooting. In cloud computing, the cloud service provider may provide subject matter expertise to ease and speed up the troubleshooting.

In general,

- the older, more patched, and complicated an application, the more complex the migration to the cloud infrastructure will be;
- deploying the newest releases of an operating system or VMware may require updates to databases or middleware that are not yet available from third-party vendors;
- multifaceted integrations with other systems increases the complexity of cloud migration; and

- a cloud broker can play a critical role in helping agencies screen their applications for cloud feasibility and prioritizing cloud migrations accordingly.

3 – Variety of services creates opportunity to solve a variety of needs

The variety of services and business models in a cloud infrastructure offer organizations a wider variety of tools for solving problems. For example, cloud infrastructure may help in satisfying a need for immediate (emergency) consumption, resolving a situation for the short-term while a long-term solution is developed separately, and freeing up physical infrastructure for repurposing. Specifically, the flexibility of cloud infrastructure offerings allow an organization to

- **Stand up an application quickly.** For example, the Secretary of State’s office was able to stand up www.votetexas.org, a mobile-enabled, interactive information website built to assist Texans with the complexities of redistricting and voter participation, within two weeks of beginning the sourcing and procurement effort. This was a mission-critical, highly visible, and advertised website that was urgently needed to support the 2012 Texas primary elections. It included a solution design, pricing, approval workflow, provisioning, and system monitoring of the site—all governed from a single web portal.
- **Develop and test multiple applications in a flexible environment** that cannot impact or be impacted by the production environment.
- **Respond to recurring peak business demands with “bursting”** rather than investing in bandwidth and infrastructure that is underutilized in non-peak periods.
- **Host large, publicly accessible datasets separate from more sensitive information** to free up capacity while strengthening and simplifying security requirements.

4 – Costs differ among providers and within each provider’s offering

Cloud model comparison is difficult due to the variables in product offerings, including the business models, service levels, and package inclusions. For example,

- Some providers offer full IT stacks (hardware and software infrastructure, middleware platforms, application system components, and turnkey applications), while others are bare bones offerings with an a la carte menu for each add-on required.
- Technical integration and licensing capabilities vary with each provider (e.g., Active Directory integration, VPN connectivity, Oracle licensing). In some cases, organizations can opt to rent software instead of buying licenses, with renting being inexpensive for short-term need but expensive for long-term need.
- Some business/pricing models assume 24/7/365 availability while others offer “power down when not in use” or “pay by the drink” options more suited for use with development or testing sites.
- Pricing an application architecture deployment design for a particular provider can be a time-consuming process due to low-level pricing models that have to be aggregated for each solution. Even after provisioning, costs are not fully predictable and can vary month to month. This can cause difficulty within government organizations that need to be able to predict monthly, or at least annual, expenses.
- Some of these challenges are addressed by cloud brokers through side-by-side provider comparisons and aggregating the contractual or service elements of the offering across the

participants. Cloud brokers also translate capacity requirements into provider line items, thus allowing for accurate estimation of cloud cost.

- Payment terms can differ greatly and may not always align with statute. It is critical to understand the payment terms associated with a service. For example, can the provider accept purchase orders? Can the provider submit invoices? Can the provider accept payment in arrears? Can service credits be refunded or applied to future services?

5 – Cloud services may not mean managed services

Cloud utilization does not eliminate the need for system and operating system administration expertise, whether that expertise is available in-house or procured as a value-add service to help architect the solution. Specifically,

- The cloud requires expertise in areas such as software licensing, database integrations, Active Directory integration, firewall rules, VPN connectivity, and network requirements. Existing expertise in these areas help, but new skills are required to know what various cloud service providers can offer or support in each of these areas. Each provider offering may have unique constraints that affect the ability to deploy a complete solution for a particular application.
- Because so much of the emphasis of cloud services procurement and provisioning is on speed, agility, and flexibility, the fundamentals can easily get lost. Security processes and procedures, business continuity and disaster recovery checklists, rosters of qualified back-up personnel, etc., may need to be updated frequently to document changes made possible with the cloud. Customers cannot assume that the cloud services providers will be able to comply with the level of business continuity required, for instance. Appropriate governance processes must be in place to manage these fundamentals and ensure all of an organization's application needs are met.

6 – Costs can be managed through cost model choice

Cloud services providers offer various pricing models for consuming their services. Depending on customer needs, the different pricing models provide choice and flexibility. For example,

- On-demand or pay-as-you-go pricing models provide hourly-based pricing for virtual resources based on various combinations of CPU, memory, storage, and network capacity. These are billed after the resources have been provisioned and allocated for a designated time.
- Subscription pricing models (also known as *monthly package pricing* or *reserved instance pricing*) involve a pre-payment for some fixed capacity (in terms of hours and/or capacity units). This could be a monthly or yearly subscription for the fixed capacity whether it is used or not. The advantage is lower per-hour or per-capacity pricing than the on-demand model since it is pre-paid.
- Reserved capacity (also known as *virtual private dedicated capacity* or *utilized capacity*) pricing models define a specific total amount of CPU, memory, storage, and network capacity that is dedicated and always available to the customer. Virtual machines (VM's) can then be allocated in this total capacity, but the allocation can exceed the total dedicated capacity. Then, only the run-time use of the VM is considered against the reserved total capacity. If all of the VMs allocated use more than the total reserved capacity, then it is considered to "*burst*" and have additional cost. This model has the advantage of providing consistent pricing on a month-to-month basis. In

addition, this model provides flexibility for allocated VMs, which may have low utilization, without incurring additional cost.

In addition, customers should consider the following factors for the most cost-effective cloud services:

- **The provisioning cycle is fast.** Provisioning may happen in hours or days, rather than weeks or months. For many services, the meter starts running as soon as the infrastructure is provisioned, not when the customer configures or deploys it. Therefore, it is important to have a review and approval cycle for an application architecture deployment prior to the actual provisioning. Cloud service providers typically do not provide any review or approval cycles, but this can be a function of a cloud service broker.
- **Customers have the ability to manage their cloud services to maximize best value**, i.e., turning off servers while not in use, etc. These operations can be scheduled and automated based on certain policies such as demand or system usage.
- **The ability to manage costs** to the hour or minute provides flexibility and control for the customer, but also lessens remedies should prices be contested.
- **Leasing vs. owning** places the expense in the operational budget rather than in the capital budget.
- **Most cloud services have a pay-in-advance approach** while governments are used to paying upon delivery. State government payment laws are not consistent with the payment requirements of the cloud providers, which are typically based on the needs of the private sector. It is critical to be on the same page as the provider regarding invoice timing, charge timing, and payment timing. Not all providers understand public sector constraints and they may have to change their billing models to accommodate public requirements.
- **Using cloud services is not always cheaper** and, depending on the application requirements, a lower cost solution might be available. For example, Texas Data Center Services costs were comparable to cloud provider costs in situations where the application did not require a lot of storage.
- In many cases, **the cloud broker serves as the means to regulate payment** across the different entities.

7 – Vendors are learning, too

Cloud services providers and cloud services brokers are simultaneously developing, negotiating, documenting and redeveloping every component of their working business model. The field of cloud services provisioning is so dynamic that terms and conditions, SLAs, and support collateral have very short life cycles of their own. At the same time, breakthroughs to any issue or barrier may occur at any moment.

Vendors are learning that

- The rapidity of change in all cloud service offerings has required cloud service brokers to be in a constant, hands-on education and support mode. To accommodate the very large potential market of government IT, cloud service brokers especially must find a scalable way to keep up with and integrate the changes in the services they broker.
- Cloud providers may have little experience with government procurement methods, standards, regulations, and nomenclature.

- Legacy environment business models assigned a company representative to each agency or large application. This representative knew agency personnel, system expectations, system limitations and was also aware of agency goals.
- Customers may or may not have the skills to perform technical activities through a self-service model and need to consider the impacts of either outsourcing or training.

8 – Fine print still applies

Each cloud service provider has specific terms and conditions that may not accommodate government's rules and regulations. Government procurement includes IT, legal, contract, and financial review and approval requirements. Customer organizations must establish a process and include time in the procurement cycle for ensuring that terms are consistent with their rules and regulations.

Specifically,

- Rules, regulations, policies, and funding sources may have strong preferences regarding the location of hosted environments and support centers that are not compatible with cloud business models; data retention requirements may exceed standard storage timeframes common in cloud hosting environments; and government organizations' security requirements may not be updated to include cloud standards.
- Cloud brokers add value but also add another level of terms and conditions. All parties must understand what is offered, what is covered through the marketplace, and what extra costs are (e.g., solutioning or assisting with a technical integration issue might be an additional service).
- The cloud has its own terminology. This terminology may be used differently by each provider, which complicates contract issues and procurement options (e.g., reserved capacity vs. utilized capacity).

9 – Security is a factor

Security is an important element of cloud services, and the type of cloud solution chosen, whether public, private, or hybrid, impacts the security levels controlled by the customer.

Many of the security risks associated with the use of cloud computing can be managed and prevented. It is incumbent on the agency using cloud services to be proactive in taking the necessary security precautions. Some ways to manage risks are to:

- Design for virtual private networks with private IP addresses, client-to-site and site-to-site VPNs, firewalls, and secure protocols
- Monitor security controls
- Tighten identity and access management
- Virtualize anti-malware
- Provide ongoing validation of security controls
- Be aware of data state and location – know the location of data, processing, and backup
- Update and maintain rules, regulations, and policies that impact cloud solutions
- Test applications for vulnerabilities and patch vulnerabilities if necessary

Conclusion

The pilot has already provided a viable roadmap for future cloud deployments and will be used in any future procurement. Customers are pleased with the pilot and the PTCO will continue through the end of August 2013 so the program can continue to reveal lessons about cloud offerings. ♦

Glossary

Bursting – allows cloud services to exceed planned or allocated thresholds when capacity is maximized

Cloud broker – an intermediary between cloud providers and consumers that make it easier for consumers to choose, provision and maintain cloud services that best suit their needs

Cloud first– federal policy to achieve operational efficiencies by adopting “light” technology and shared services

Logically partitioned – a subset of a computer platform or components of a computer platform, virtualized as a separate logical computers or computer components or a single physical instance subdivided into multiple logical instances

Magic Quadrant – proprietary research tool developed by Gartner Inc. to monitor and evaluate companies in a technology market

Virtual Private Network (VPN) – technology for using the Internet or another network to connect computers to isolated computer networks that would otherwise be inaccessible

Acknowledgements

Customer Contributors

The pilot participants should all be commended for recognizing the importance of offering insight to government organizations that may adopt services offered through the cloud. Thank you to the following state agencies that participated in the PTCO and provided content for this document:

- **Department of Information Resources** – David Smith, Robert Ott
- **Office of the Secretary of State** – Scott Brandt, Frosty Walker
- **Texas Department of Transportation** – Mitch Pope, Kevin Wagner
- **Texas Water Development Board** – Lisa Petoskey, Darryl Lindgens

Partner Contributors

Thank you to the following private partners that participated in the PTCO and provided content for this document:

- **Gravitant** – Manish Modh, manish.modh@gravitant.com, 512-535-7399
- **Vintage IT Services** – Steve Hanes, sahanes@vintageits.com; 512-481-1117, Alex Ladwig, aladwig@vintageits.com, 512-481-1117
- **Savvis** – Jim Gallina, jim.gallina@savvis.com, 630.854.8290
- **Terremark** – Wendell Elms, welms@terremark.com, 214-629-9799
- **Amazon**

DIR Contributors

Jennifer Buas, Vivian Cullipher, Janet Gilmore, Todd Kimbriel, Robert Ott, Ellen Pate, Lorie Ramirez, Joanne Severn, David Smith, John Van Hoorn, Jay Wilbur

Contact

For questions about this report, contact

Janet Gilmore

Assistant Director, eGovernment Services
Texas Department of Information Resources
janet.gilmore@dir.texas.gov
512-463-8447

Published by



Texas Department of Information Resources
300 West 15th Street, Suite 1300 | Austin, TX 78701 | 512-475-4700