The cloud helps government deliver new services quickly. However, selecting, aggregating, integrating, customizing and managing multiple cloud environments is a difficult task. Cloud services brokerage is an emerging approach that can help governments manage the complexity and risks associated with a burgeoning cloud services portfolio.

This paper introduces the brokerage model and explains how organizations can receive the most benefit from it to create a sustainable cloud services model for the future.
Introduction

The cloud helps federal, state and local agencies save money, free up staff and deliver new services quickly. As governments steadily adopt cloud services, however, they are discovering that selecting, aggregating, integrating, customizing and managing multiple cloud environments is an increasingly elaborate task. Cloud services brokerage is an emerging approach that can help government organizations manage the complexity and risks associated with a burgeoning cloud services portfolio. This paper introduces the brokerage model; explains how organizations can receive the most benefit from a cloud services broker (CSB); and looks at how the Texas Department of Information Resources (DIR) has incorporated CSBs into its service model so agencies can reduce complexity, save money and create a sustainable cloud services model for the future.

Cloud Investments on the Rise

Cloud services are gaining traction in the public sector as agencies seek to alleviate staffing shortages; control costs; modernize technology; provide more agile services; and comply with cloud-first, data consolidation, telework and other federal initiatives. IDC Government Insights predicts federal government spending on cloud services will reach $3 billion in 2015 and spending on private cloud services alone will be $5.9 billion by 2018. State and local governments are following similar trends in adoption. According to the National Association of State Chief Information Officers (NASCIO) 2014 State CIO Survey of 52 members, nearly 75 percent of respondents maintain some applications in the cloud and are considering others. Twenty percent described their agency as “highly invested in cloud services,” an increase of more than 300 percent from 2013.

Early adopters have helped organizations understand how to best use cloud services and have eased concerns about procurement, data migration and other issues. In the same NASCIO survey, 86 percent of respondents said they intend to adopt software-as-a-service (SaaS) in the coming year, nearly 67 percent intend to adopt infrastructure-as-a-service (IaaS) and 58 percent intend to adopt platform-as-a-service (PaaS). Email and collaboration (63%), storage (47%) and office productivity applications (47%) were the most commonly identified services to be migrated to the cloud.

The Challenges and Complexities of Cloud

Given cost savings and other motivators, governments are likely to continue their expansion of cloud services. However, as they do so, many are discovering the complexity of cloud services adoption. Janet Gilmore, director of digital government and information resources manager for Texas DIR, has “been there.” DIR serves Texas state and local agencies, school districts, higher education and nonprofit organizations. In 2012, it decided to adopt cloud services for state government because it needed to reduce costs and improve its speed to market for delivering important services.

“We had trouble procuring, deploying and configuring infrastructure and delivering very necessary applications quickly,” she explains. “It didn’t take long for DIR to recognize the complexity of its undertaking. “We were new to cloud services. We didn’t know which offerings were best for a particular need. There were lots of different prices and models for seemingly similar services. There were so many variables; we were just plowing through the choices and thinking that choosing the right approach and the right cloud service would take even more time,” Gilmore says.

Considering public sector organizations often use more than one cloud service, with heterogeneous platforms and different vendors for different services, it’s no surprise
organizations such as Texas DIR are running into the following challenges as they adopt cloud-based solutions:

**Procurement**
- Determining which data, applications and processes to move to the cloud
- Deciding on the right cloud environment for each service (private, public or hybrid)
- Comparing services when features, pricing models and service level agreements (SLAs) are not standardized across cloud services
- Consolidating purchases to obtain more favorable pricing and terms
- Identifying stable, proven vendors that offer the services needed and at the required levels of security, interoperability, availability and support

**Integration and Customization**
- Integrating cloud services effectively so they interoperate with legacy infrastructure and onsite and other cloud services
- Customizing or creating user interfaces, application workflows, and other features and processes to meet the organization’s specific needs

**Management**
- Obtaining a unified picture of the organization’s entire ecosystem of on-premises and cloud-based systems
- Ensuring security, protecting data and complying with government regulations
- Managing licenses, service utilization and costs consistently — and at the best value — across diverse cloud environments
- Monitoring SLAs and handling penalty clauses and other details if SLAs are not met
- Managing bill payment and vendor relationships
- Extending security policies to the cloud to ensure security and privacy across all environments

**Cloud Services Brokerage: A Primer**

To address these challenges and get the most benefit from cloud services, trailblazers such as Texas DIR have turned to CSBs to provide expertise; act as a single point of contact; and help procure, integrate, customize and manage cloud services.

Cloud Services Broker Defined

As defined by NIST, a CSB “is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.”

DIR is one of the first public sector organizations to offer a CSB model. When it began piloting cloud services, it decided a CSB model would “help us explain and normalize the offerings out there — in an ‘apples to apples’ way — and also offer additional support that a provider specializing in infrastructure cloud services might not include in its offering,” says Gilmore. Todd Kimbriel, interim executive director of DIR and state chief information officer, adds “[Cloud brokers] not only bridge the gap, but also provide value-added services. In our case, the purpose of the broker is to actually be a single point of contact for whatever the cloud services are. The idea is that the cloud broker becomes the expert on how to configure and consume those cloud services, how to ensure the service level agreements are held. It’s almost a governance role, as their job is to govern the service delivery from cloud providers.”

As defined by the National Institute of Standards and Technology (NIST), a CSB “is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.” As an intermediary between the organization and the service provider, a CSB helps organizations navigate the complexity of cloud service offerings.

A CSB may have its own cloud platform(s) and resources, or it may simply act as a vendor-neutral go-between for an organization and various cloud service providers. It typically has a catalog of services with rule-based tools that can automatically select services that most closely align with the organization’s pre-defined criteria (e.g., cost, compliance, SLAs). It also has pre-existing relationships with a range of vendors, and may even have pre-negotiated rates and contracts, allowing organizations to save time and money during the acquisition process.
Although many government organizations turn to a third-party CSB to mitigate gaps in expertise, staffing or other resources, some CIOs and IT teams act as CSBs for other business units within their organization. Doing so provides opportunities to consolidate negotiating power and streamline integration and consumption of cloud services.

Cloud Services Broker Roles

Gartner has identified three main roles for CSBs; some specialize in a single role, while others perform multiple roles. These roles correspond to the areas with which many government organizations struggle:

- **Aggregation** — The CSB acts as a reseller, advising an organization on the best solutions, providing budgeting guidance, and procuring and managing multiple cloud services. Frequently, the CSB bundles related services together to offer a single unified service. Aggregation CSBs may also perform monitoring; manage bill payment, vendor relationships and SLAs; and provide other management services.

- **Integration** — The CSB provides integration between cloud services and on-premises services and works to ensure data flows smoothly. By integrating multiple services, it may add new functionality. This role is especially important when an organization is not experienced in cloud migrations, has complex transition requirements or cannot risk mistakes in application deployment.

- **Customization** — The CSB develops additional features or fine-tunes the cloud services to meet an organization’s unique needs.

Benefits

Cloud services brokerage removes many of the barriers to adopting cloud services, allowing government organizations to more fully experience the advantages they offer. A CSB model:

- **Offers expertise.** Many governments are just beginning to adopt cloud services and have not fully grasped all the details related to procuring, deploying, integrating, customizing and managing services in the cloud. CSBs fill in gaps in knowledge and skills.

- **Mitigates complexity.** CSBs alleviate the burden of managing multiple services and working with various vendors.

- **Improves decision-making.** By providing tools and expertise that offer a comparison of service features, prices, SLAs and other variables, CSBs allow an objective and accurate comparison of services and shorten the evaluation process.

- **Enables best-of-breed solutions.** CSBs have vetted a variety of vendors and can help organizations design and acquire the best services solution for their unique requirements.

- **Expedites deployment.** Established relationships with service providers and pre-negotiated contracts and prices shorten the procurement phase, while standardized tools, processes and methodologies accelerate integration, customization and other tasks.

- **Lowers costs.** Aggregated purchasing saves money on service expenditures, while offloading procurement and management burdens decrease operational costs.

- **Simplifies operations.** By providing a unified, comprehensive view of an organization’s cloud services, costs and SLAs, CSBs help eliminate redundancies, optimize resource usage and reduce spending, as well as minimize staff time and errors related to managing multiple interfaces.

- **Strengthens security and policy enforcement.** CSBs help ensure cloud services are properly deployed and comply with federal regulations related to security, privacy and law enforcement.

- **Provides flexibility and scalability.** Automated tools help CSBs quickly identify services that best match an organization’s current needs, allowing it to shift workloads and scale capacity and cost as needed.

- **Promotes deep partner relationships.** Strong, long-term partnerships between a CSB and service providers allow a level of collaboration, innovation and problem solving that can be difficult when a single, one-time acquisition is made.

“We definitely experienced a positive speed to market using a CSB, especially when the solution was Web-based and public-facing. We had amazing stories of agencies that were able to deploy critical, public-facing applications from start to finish in less than 60 days.” – Janet Gilmore, Director of Digital Government and Information Resources Manager, Texas DIR
Getting a Cloud Services Brokerage Model to Work for Your Organization

To maximize the potential of a CSB model, government organizations need to first clarify their needs and understand the types of solutions CSBs offer. They need to develop or adapt contracts that clearly spell out terms and conditions, and they need to devise a strategy for evaluating brokers.

Janet Gilmore of DIR emphasizes the importance of distinguishing between the different kinds of CSBs. She says, “It’s important to recognize there are different types of cloud brokers, and you have to know what you’re looking for first. Are you looking for a platform or tool to manage your various cloud services; are you looking for someone to help you architect your solution; are you looking for add-on services; are you looking to put an additional layer between you and SLAs; are you looking for somebody to provide comparisons of re-pricing models and features? You have to decide that first because then you can find a cloud broker that addresses those needs. And in our experience, a cloud broker might be one or more of those things.”

Understanding the Solution Areas

In general, CSB solution areas for the public sector fall into the following categories.

**IT Infrastructure**

Services in this category help organizations migrate their infrastructure to the cloud. This may include provisioning processing (e.g., CPU and memory), networks and other resources that provide a foundation for IT operations. Although IaaS has been touted for its superior performance, scalability and pricing, many IT leaders are finding that is not always the case. Using a CSB, organizations can access and evaluate a wide range of service providers whose core expertise and investments are in data center and infrastructure operations. As a specialist, the CSB can provide guidance on which solutions truly meet the organization’s needs for not only performance, scalability and pricing, but also other important features such as availability and security. The CSB can also work closely with the organization to track usage, anticipate changes in demand and scale services up or down as needed.

**Security and Compliance**

This category includes data protection, identity and access management, incident response and assessment for cloud data and applications. In a Center for Digital Government (CDG) survey of 165 IT professionals in state and local government conducted in May 2015, 62 percent of respondents said security concerns were their biggest barrier to adopting cloud services. CSBs reduce the risk of moving security services to the cloud by vetting vendors to ensure they meet cloud security standards (e.g., encrypting data stored at rest, supporting multifactor authentication, having ISO 27001 certification, prohibiting hosting in embargoed countries) established by the organization, the federal government and organizations such as the Cloud Security Alliance. They also ensure cloud-based security solutions are deployed properly and meet agency-specific policies as well as federal compliance requirements related to the Health Insurance Portability and Accountability Act (HIPAA), the Criminal Justice Information Services (CJIS) guidelines, the Federal Risk and Authorization Management Program (FedRAMP), the Federal Information Processing Standard (FIPS), the Family Educational Rights and Privacy Act (FERPA) and more.

**Data Storage and Disaster Recovery**

This category includes services for storing, backing up, retrieving and recovering data. With ever-growing volumes of data, strict government mandates on storing private information and other data, and the increasing number and ferocity of cyber attacks, government organizations have their hands full when it comes to data storage. CSBs that specialize in this area can help organizations comply with data storage requirements, determine what data to store where (e.g., onsite or in a public, private or hybrid cloud), reduce storage costs by finding the best service for each data type, and help choose a disaster recovery solution that balances risk and cost in accordance with the organization’s business requirements.

**Communication and Collaboration**

This category includes voice over IP (VoIP), instant messaging, email, content sharing, Web conferencing and other productivity applications that are used to conduct business. Email and collaboration comprise the largest category of cloud services adopted by government organizations.
Cloud Services Broker Considerations Checklist

When deciding on a CSB, government organizations should consider the following questions:

- **Services offered.** Does the CSB specialize in specific services? Does it have pre-established agreements with cloud service providers? How do the CSB’s offerings scale?
- **Understanding of public sector requirements.** How well does the CSB understand our unique needs (e.g., for purchasing and compliance with federal requirements for interoperability, portability and security)?
- **Security and privacy.** What minimum levels of security and privacy does the CSB guarantee? What is the CSB’s overall security policy regarding service providers? Does it have personnel with expertise in security and how is that reflected in its offerings? What types of security certification audits does it perform?
- **SLAs and support services.** Who manages support services and service escalations? Who is responsible for SLA governance, including handling penalties for unmet service levels?
- **Infrastructure.** If the CSB provides its own data centers and IaaS, what is its SLA and what is its record for security, performance, availability and scalability? How does it ensure data backup and disaster recovery?
- **Mobile device integration.** Can the CSB support us in enabling services for mobile devices?
- **Customization.** How much customization is available to fit our needs for individual applications and overall integration and implementation, as well as for compliance requirements? What is the additional cost?
- **Tools.** Does the CSB have tools to identify the best cloud services based on parameters such as cost, regulatory compliance and interoperability? Does the CSB offer a portal where we can view and manage all our services from one place?
- **Billing.** Are billing systems integrated with third-party payment gateways? Are bills consolidated for all our services? Does it offer various payment models (e.g., usage based, post-paid and prepaid)?
- **Size and viability.** How long has the CSB been in business, and how long has it been a broker for cloud services? What is its financial standing? How extensive is its partner network?
- **Performance metrics and remedies.** How will we define and measure performance? What are the contract provisions for terminating the relationship?

and many accumulate a sprawling inventory of these services. CSBs with expertise in this area can help government IT leaders develop a unified approach to communication and collaboration, eliminate redundancies, maximize their telecommunications spend and comply with regulations such as the IRS’ Tax Information Security Guidelines for Federal, State and Local Agencies and the Social Security Administration’s Health Care Fraud and Abuse Data Collection Program. They can also help develop solutions that successfully incorporate mobile devices into the organization’s overall communications strategy.

**Tackling Procurement**

Although CSBs help navigate the procurement process, the organization is typically responsible for contracting with the cloud service provider(s) and paying the bills. Government organizations face unique challenges when procuring cloud services. Many organizations are saddled with traditional purchasing rules and practices that are designed for on-premises physical products rather than services that use pay-as-you-go, subscription and other pricing models. They may also be required to comply with federal, state or internal regulations regarding data privacy, transparency and accountability.

In creating agreements and contracts for cloud services, government procurement organizations must be able to explicitly document terms and conditions for service models, data, breach notification, personnel, security, audits and operations. In many cases, they must do so with very limited experience of cloud services and cloud service providers. Meanwhile, many vendors do not fully understand the public sector market and have terms and conditions that government organizations cannot easily meet.

To overcome this challenge, CSBs, technology vendors and public sector organizations are starting to work together to understand each other’s needs, make compromises, and develop contract templates and best practices that can help clarify language and roles, streamline procurement and reduce risks associated with unexpected costs or terms.

One working group, organized by CDG and consisting of government organizations and leading cloud vendors, has created a guide with model terms and conditions for service models, data, breach notification, personnel, security, audits and operations. In creating agreements and contracts for cloud services, government procurement organizations must be able to explicitly document terms and conditions for service models, data, breach notification, personnel, security, audits and operations. In many cases, they must do so with very limited experience of cloud services and cloud service providers. Meanwhile, many vendors do not fully understand the public sector market and have terms and conditions that government organizations cannot easily meet.

Apart from improving and simplifying the procurement process, part of the value of government organizations adopting...
the DIR contract is they can take advantage of pre-negotiated discounts, terms and conditions. In addition, the contract focuses heavily on finding the most qualified service providers, especially when it comes to security. Shannon Kelley, manager of enterprise contract management for DIR, was part of the team that created the agency’s master bid package and contract for purchasing cloud services. According to Kelley, “Security was the number one concern. We asked subject matter experts throughout the agency for their input into questions about security services, disaster recovery plans and detailed implementation. We had lots of different things that potential providers had to report on, and we evaluated them — based on what they provided — against the published criteria.”

Even with model contracts and templates, cloud services procurement is a complex process. In some cases there is a gap between what a public sector organization requires and what a service provider requires. A CSB with experience in the public sector and in procurement can help smooth bumps in the road — even for states that have advanced CSB models. For example, Texas (like most states) requires that services must be rendered before they can be paid. However, DIR wanted to work with a service provider that requires advance payment for its cloud services. To solve the impasse, instead of DIR contracting directly with the service provider, the CSB held the contract with the vendor and made payments, and then billed CSB on standard net-30 terms once services had been consumed.

Evaluating Cloud Services Brokers

When the pilot team for DIR’s cloud project adopted the CSB model, they had to decide how they were going to solicit CSB vendors. DIR serves more than 200 agencies, so it needed an approach that was comprehensive and flexible enough to accommodate a wide range of requirements. Gilmore explains, “We had to be very flexible with our requirements because we didn’t want to exclude one type of broker over another.” Kelley adds, “We also wanted multiple brokers on contract so customers could have a range of services at various price points.” Instead of requiring specific features or functions, DIR evaluated what each broker provided on its own merit and focused on ensuring a potential offering was secure, vendor neutral and added something of value to agencies. For some questions to consider when evaluating a CSB, see the sidebar on page 6.

Conclusion: Opportunity on the Horizon

Cloud budgets are growing as tax revenues spring back and federal, state and local organizations respond to government mandates for cloud-based services. Government organizations that incorporate a brokerage model could reap several advantages, including mitigating the risk and complexity of cloud initiatives, simplifying governance and management, enhancing data security and privacy and reducing costs. Working with a CSB to securely and effectively utilize their data, applications and other assets in the cloud, organizations can take full advantage of cloud opportunities.

Endnotes

3. Ibid.
4. All information and quotes from CDG interview with Janet Gilmore conducted in August 2015.
13. All information and quotes from CDG interview with Shannon Kelley conducted on August 2015.
DoubleHorn is a leading Cloud Solutions Provider founded in January 2005 and based in Austin, Texas. Their solutions combine products from the leading Cloud providers and are carefully designed to meet emerging technology requirements of the Enterprises & Government. As a Cloud Services Broker, with a simple six step Cloud Transformation Methodology, they advise in selecting the right solution, implement, maintain and offer single source for billing and support of multiple Cloud products. DoubleHorn was awarded the Cloud Services Contract for the State of Texas (DIR-TSO-2518) and Oklahoma (ITSW1022D) covering Cloud Assessment, Cloud Services Brokerage and Cloud Infrastructure-as-a-Service (IaaS). Their comprehensive Cloud catalog includes Cloud IT, Backup & DR, Security, Communications and Collaboration solutions which are capable of meeting all the major Compliance requirements like CJIS, HIPAA, FedRAMP, FERPA, PCI, etc.

For a free estimate of your agencies’ cloud transformation readiness, take advantage of DoubleHorn’s complimentary cloud screening for government at www.doublehorn.com/assessment.