REPORT ON CLOUD COMPUTING AND IT INFRASTRUCTURE

NOVEMBER 15, 2018

Texas Department of Information Resources

2018 REPORT ON CLOUD COMPUTING AND IT INFRASTRUCTURE

Note: In this report "state agency" means a board, commission, office, department, council, authority, or other agency in the executive or judicial branch of state government that is created by the Texas Constitution or by statute. The term does not include university systems or institutions of higher education.

EXECUTIVE SUMMARY

Agencies are facing the next step in modernizing legacy hardware and software, replacing aging systems to move toward a more collaborative, agile, and interoperable state government. As agencies transition from traditional practices to innovative solutions, operational and cybersecurity risks within their IT infrastructure remain. To mitigate these risks, agencies are evaluating current and ongoing investments in legacy systems and considering cloud services and other non-traditional service options.

The 85th Legislature through SB 532 and Article IX of the General Appropriations Act required the Texas Department of Information Resources (DIR) to collect information on the status and condition of each state agency's information technology infrastructure and to submit a report consolidating the information collected. The Legislature also required DIR to report on the use of cloud computing service options used by state agencies. This consolidated report includes:

- Details regarding the use of cloud computing service options by state agencies;
- Use cases that provided cost savings and other benefits;
- An assessment of each state agency's security and operational risks; and
- Analysis for each state agency found to be at higher security and operational risks and their efforts to address those risks through the modernization of information technology systems, use of cloud services, and use of the Statewide Technology Center.

As part of the 2018 Information Resources Deployment Review (IRDR), agencies were asked to provide an inventory of their technology infrastructure as well as other information regarding their technology environment, including the use of cloud computing. This inventory, as well as other information regarding cybersecurity collected from state agencies, is the source of the content presented in this 2018 Report on Cloud Computing and Consolidated IT Infrastructure Report.

FINDINGS

- In FY 2018, state agency cloud services purchases through vendor-reported information in DIR's Cooperative Contracts program totaled over $89 million, with a cost avoidance[1] of approximately $8 million on those purchases.
- According to agency responses to the IRDR, 87% of agencies report to have initiatives aligned with cloud adoption.
- Regarding IT Infrastructure, agencies found to be at higher operational and security risk are smaller agencies; five of these eight higher risk agencies had less than 25 full-time employees.
- Of the eight higher risk agencies, three are outsourcing their IT management to another state entity, indicating constraints on internal agency resources.

[1] As defined by the National Association of State Procurement Officials, cost avoidance is a cost reduction opportunity that results from an intentional action, negotiation, or intervention. For DIR's Cooperative Contracts program, cost avoidance is determined by what customers pay in comparison to other cooperative contract programs.

REPORT ON CLOUD COMPUTING

Cloud computing offers alternatives to traditional IT delivery models and has changed how business is done. The use of cloud services is a top technology priority under the Cost-Effective and Collaborative Solutions strategic goal of the 2018-2022 State Strategic Plan. State agencies are encouraged to evaluate and consider cloud services when implementing new information resources projects. Those agencies who are using cloud are reporting some security and cost saving benefits. Given the wide-ranging functions of the state, each agency will have different uses for the cloud and different requirements for effective and secure migration. As more agencies leverage cloud to fit their unique needs, the state as a whole will be able to identify and develop cloud services in the ways that offer the greatest return to the public.

WHAT IS CLOUD COMPUTING

Cloud computing is a model that enables on-demand network access to resources. It provides convenient, on-demand delivery of information, as well as IT flexibility, efficiency, and cost savings for government. If implementation of cloud services is done carefully and appropriately, it can ease the burden of aging infrastructure and provide flexible, lower-cost, IT service delivery.

There are three basic cloud service models that are useful for different agency needs.

- 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.
- Infrastructure as a Service (IaaS) delivers computing hardware, storage, networking, and backup.

There are four common cloud deployment models, including public, private, community (government) and hybrid, each with different terms of access to information and resources

- Public Cloud – The cloud provider delivers a common IT capability in a shared environment. Data from multiple customers with similar requirements are pooled together to optimize resources.
- Private Cloud – The cloud provider dedicates and customizes the capabilities, resources, and administration of a defined environment to each organization.
- Community Cloud (Government Cloud)- Deployment is for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. data center services agencies)
- Hybrid Cloud – The hybrid cloud is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by technology that enables data and application portability and interoperability.

DATA CENTER CLOUD COMPUTING SERVICE OPTIONS

Data Center Services (DCS) provides fully-managed and semi-managed IT infrastructure service on DCS private community cloud and public government and commercial clouds. Through the DCS program, customers can manage compute and pay only for what they need. Customers can also take advantage of lower cost infrastructure and support services where it makes technical and business sense. Cloud services are also available to state agencies through DIR Cooperative Contracts and Shared Services. For agencies considering cloud services, DIR offers introductory resources to help guide decision makers in evaluating available options and moving forward with an implementation strategy.

The DCS program continues to evolve to meet customers' growing technology needs, and now offers secure connectivity to multiple public and government clouds. 80% of servers in the DCS program are in the private or public cloud, while the remaining 20% of servers reside in agency-owned legacy data centers or in remote agency business offices. In March 2017, Hybrid Cloud Services were introduced to the DCS program to provide customers expanded cloud and self-management options, while meeting the business, security, and regulatory requirements of Texas state government. Building upon the existing DCS private cloud, the DCS hybrid cloud enables applications and data residing in the state's consolidated data centers to connect directly with applications and data residing in multiple public government and commercial clouds. The hybrid cloud model allows customers to connect their many and varied cloud environments into a seamless virtual data center.

DCS CLOUD OFFERINGS:

STATE PRIVATE CLOUD

- 7400 servers w/capacity on demand
- 3+ petabytes online, 38 petabytes stored
- 40 legacy and 300 remote data centers
- Fully-managed and semi-managed services
- Software currency, automated backup
- CJIS-compliant security
- Disaster recovery with various Recovery Time Objectives
- Auto-provisioning via Marketplace
- Data Centers in Austin and San Angelo

GOVERNMENT PUBLIC CLOUD

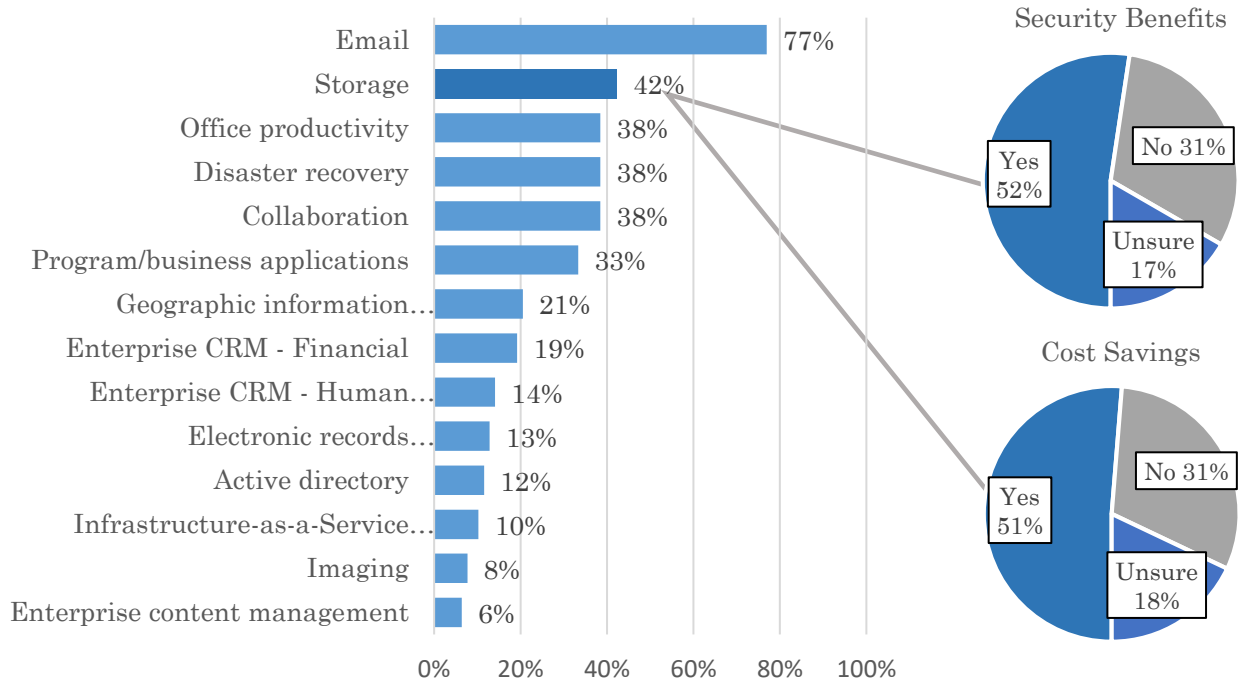
- Integrated Amazon & MS Azure Cloud
- DCS assurances and security
- Self-provisioning via Marketplace
- Fully managed and semi-managed services
- Information Technology Information Library (ITIL) service management processes

USE OF CLOUD COMPUTING SERVICES BY STATE AGENCIES

According to the 2018 Biennial Performance Report, 87% of agencies say that they have made progress in cloud adoption. When surveyed, agencies stated they leverage cloud services in a variety of areas, including email, storage, collaboration, disaster recovery, and office productivity, as seen in Figure 1 below.

As part of the 2018 IRDR, agencies were asked whether they experience security benefits or cost savings from using cloud computing services for digital storage. For those agencies that use cloud for digital storage, more than half report that they are realizing cost savings and security benefits, also shown in Figure 1.

Figure 1: Agency Uses for Cloud Services



Source: 2018 Information Resources Deployment Review

Agencies also repeatedly said hosting their agencies' key applications in the cloud was essential to enabling employees to work remotely. Of the state agencies surveyed, 42% state they utilize cloud services or disaster-recovery-as-a-service in continuity of operations or business continuity plans, while 26% reported to be considering it.

Agencies cite security concerns, migration costs, network connectivity between cloud and local servers, and organizational practices as some of the largest barriers to cloud adoption. While security was top of mind, many agencies also report that sensitive work could be

done securely and effectively using the cloud simply by accessing it through a virtual private network. When storing data in the cloud, agencies report the following as their five most essential data security controls: anti-virus software, operating system patching, encryption at rest and in transit, continental US operations only, and network intrusion prevention services.

Through DIR's Cooperative Contracts Program, multiple cloud contracts are offered for cloud services. In FY 2018, state agency cloud service purchases from the program totaled over $89 million. By choosing the cooperative contracting service provided by DIR, agencies realized a cost avoidance of nearly $8 million on those purchases. DIR leverages the purchasing power of the State of Texas to negotiate the most competitive public sector contracts available anywhere.

CLOUD COMPUTING FOR MAJOR INFORMATION RESOURCES PROJECTS

In September of 2018 DIR successfully implemented a new Statewide Project Automated Reporting System per House Bill 3275 (85R), which requires DIR to monitor and report on performance indicators for the entire life cycle of each major information resources project. In general, major information projects are defined as those that whose development costs exceed $1 million and requires one year or longer to reach operations status or involves more than one state agency. The bill requires DIR to create and maintain a user-friendly data visualization tool that provides an analysis and visual representation of the performance indicators for each project on the DIR website. As part of this new system, DIR asks whether an agency has considered cloud computing service options for the specific major information resources projects.

CONSOLIDATED IT INFRASTRUCTURE REPORT

SB 532 and the General Appropriations Act require DIR to assess state agencies' security and operational risk profiles; and, for state agencies found to be at higher security and operational risk, to include a detailed analysis and estimate of the costs to address the risks and related vulnerabilities. DIR must also describe how agencies are addressing security and operational risks through the modernization of information technology systems, use of cloud services, and use of the statewide technology center. The following report provides DIR's assessment of security and operational risks at 78 agencies.

METHODOLOGY

DIR scored agency risk using multiple data sources, all self-assessed information provided from the agency to DIR. The overall score is on a 100-point scale, with 100 being the least risk and 0 being the most risk. There were no penalizing factors, although non-answers result in the lowest score for a given attribute. The following provides an overview of the calculations for each of the contributing factors.

INFORMATION RESOURCES DEPLOYMENT REVIEW – 30 PTS.

Agencies are required by Government Code, Section 2054.0965, to complete a biennial review of their information resources deployment, the Information Resources Deployment Review (IRDR). The 2018 IRDR asks agencies to answer standardized questions about information security and continuity of operations. Every agency subject to this report was required to complete the IRDR by March 31, 2018. DIR selected 13 IRDR questions with varying points assigned to each response option. The sum of each of these questions provides the value for this section and is factored into the overall score.

IT INVENTORY – 20 PTS.

As part of the 2018 IRDR and to meet the requirements of SB 532, every agency was asked to provide an inventory of their IT environment, including server, mainframe, and cloud computing options. Each server instance within the IT inventory requires the agency to input information about the characteristics of the server such as year of deployment, role, type, etc. As part of the inventory process, agencies were asked to provide a 1 (low) to 5 (high) level of criticality/impact and failure probability associated with each instance. The impact of disruption, failure, or a security breach can be determined based on the costs to the agency or the state, both tangible (e.g., human safety or monetary losses) and intangible (e.g., damage to reputation, brand name, or trust). The probability of disruption, failure, or a security breach is the likelihood or frequency that harm will come to the agency or the state because of a weakness or exposure. This can be determined by understanding how easily weaknesses can be exploited, what incentive someone might have to gain access or cause damage to the agency or state's information assets, and the safeguards currently in place to protect the assets. A threat source could be human (e.g., hacker, current or former employee, competitor), natural (e.g., tornado, flood), or environmental (e.g., fire, electrical outage).

AGENCY SECURITY PLANS – 30 PTS.

The 2016 Agency Security Plans required agencies to assess their maturity on a scale of 0 to 5 for 40 security objectives. Agencies can assign maturity levels to different divisions, e.g., 50% of the organization is at a 5, while 25% is at a 4, and another 25% is at a 3.

SECURITY SERVICES – 20 PTS.

Values were assigned to agencies based on the recency of obtaining a security assessment and penetration test. If an agency has not obtained either of these services, they are given a "0" for that category. The assessment and penetration test scores are combined to create the overall security services score.

OVERALL RISK SCORE – 100 PTS.

Each of the factors explained above are then combined to reach the overall risk score for the agency. While there are many additional factors that could be considered in defining a risk methodology, DIR is limited by the availability of data sources, and by the completeness of self-reported data. This methodology provides a basis for making relative judgments concerning risk from the perspective of the state as a whole. Future improvements in the information collected from agencies will result in more conclusive determinations regarding individual agency risk.

IRDR Security & Operations (30%) +
IT Inventory Impact & Probability (20%) +
Security Plan Maturity (30%) +
Security Assessments (20%) =
Overall Risk - 100%

AGENCY OUTREACH

DIR focused outreach for the purposes of this report on the bottom 10% of agencies based on their overall score. This resulted in eight agencies below the overall score of 34. DIR scheduled interviews with each agency and offered them opportunities to provide updates on each of the scoring mechanisms and to highlight their efforts in remediating security and operational risk. The analysis of agency information is represented in Figure 3 below:

Figure 2: Agency Risk Scores

Sources: 2018 Information Resources Deployment Review, Agency Security Plans, Agency Penetration Tests and Security Assessments