



2020 Biennial Performance Report

Use of Cloud Services and Assessment of Agency IT Infrastructure

This report addresses section 2157.007 of the Government Code which requires the Texas Department of Information Resources (DIR) to report on the use of cloud computing service options used by state agencies¹. It also addresses section 2054.068 of the Government Code which requires DIR to collect information on the status and condition of each state agency's information technology (IT) infrastructure and report on the consolidated information collected.

Background

State agencies must provide secure information and services to both the Texans they serve and the workforce they support. As agencies transition to the next generation of technology, operational and cybersecurity risks within their technology infrastructure remain a challenge. To mitigate these risks, agencies are evaluating investments in legacy systems and considering cloud computing services.

As part of the 2020 Information Resources Deployment Review (IRDR), agencies provided an inventory of their technology infrastructure and answered questions on the agency's technology environment, including the use of cloud computing. Unless otherwise noted, the IRDR is the source of the content presented in this report. This consolidated report includes:


- details regarding the use of cloud computing service options by state agencies,
- information on cloud cost savings and other benefits,
- an assessment of state agency security and operational risks, and
- an analysis for each state agency found to be at higher security and operational risks and their efforts to address those risks².

Findings

- Responses to the 2020 IRDR report that 97% of state agencies have made progress toward cloud adoption.
- The greatest barrier to agency cloud adoption are security concerns, migration costs, and network connectivity between cloud and local servers.
- In Fiscal Year (FY) 2020, vendor-reported information in DIR's Cooperative Contracts program indicate state agency purchases of cloud services totaling over \$96 million, with a cost avoidance of approximately \$12 million on those purchases.
- Regarding IT Infrastructure, DIR conducted an analysis of agencies found to be at higher operational and security risk relative to other state agencies. Many of the low scores were the result of

¹ 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.

² Pursuant to Section 2054.068 (d), this analysis is released to the governor, chair of the House Appropriations Committee, chair of the Senate Finance Committee, speaker of the House of Representatives, lieutenant governor, and staff of the Legislative Budget Board, but is excluded from the public report posted on DIR's website.



incomplete data, lack of understanding of requirements, or changes in agency personnel. All agencies completed remediation plans to address the deficiencies.

Cloud Computing

State agencies are required by section 2157.007 of the Government Code to evaluate and consider cloud computing service options when making purchases for a major information resources project. They are also required to consider cloud computing service options and compatibility with cloud computing services in the development of new information technology software applications. DIR is required to report on the use of cloud computing service options by state agencies.

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.

Three basic cloud service models 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 a different approach to accessing 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.

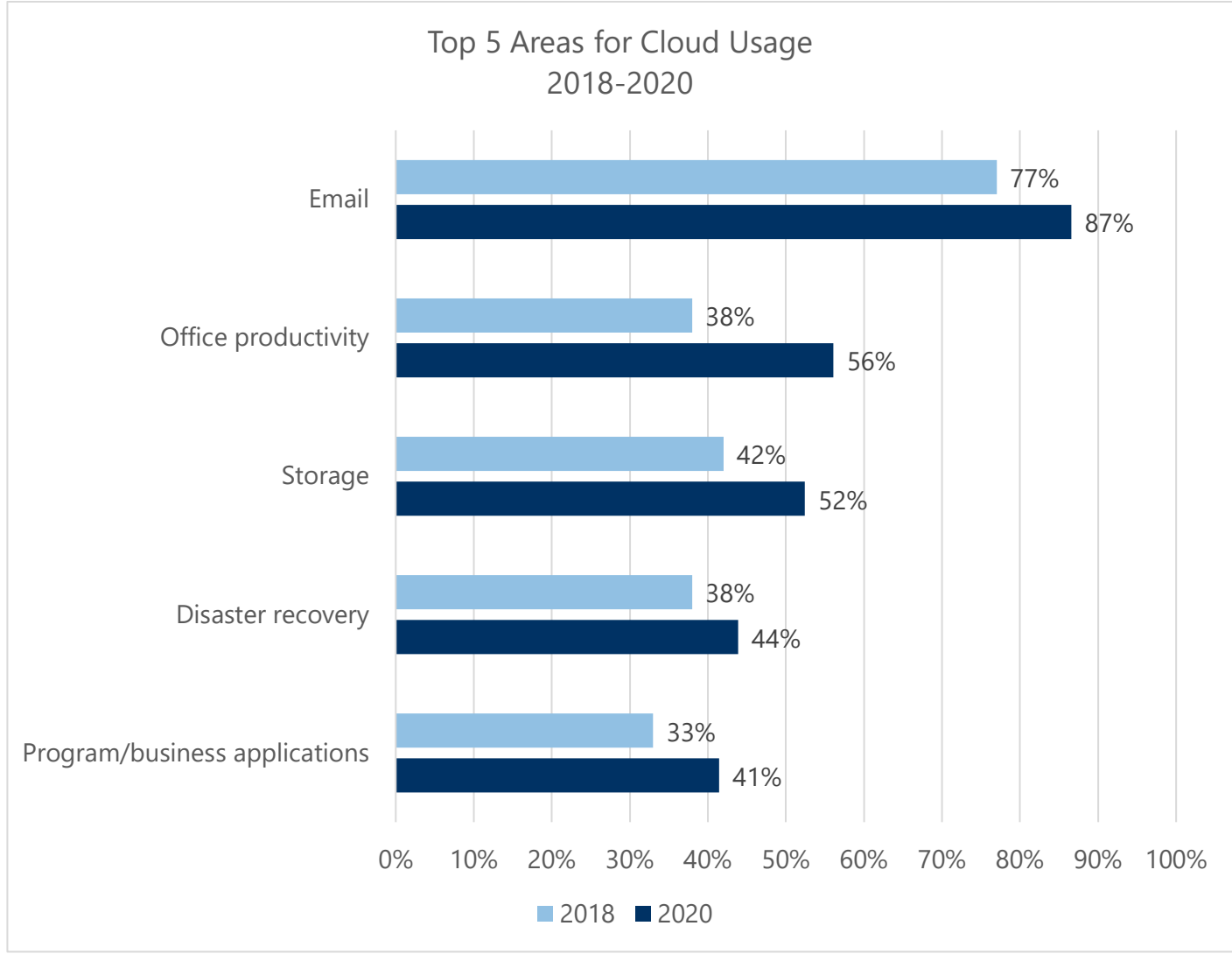
Use of Cloud Computing by State Agencies

The use of cloud computing services is an area of significant progress for state agencies. State agencies have reported to DIR on alignment with and progress toward cloud-related goals established in the State Strategic Plan for Information Resources since 2011, when only 59% reported alignment with cloud goals.



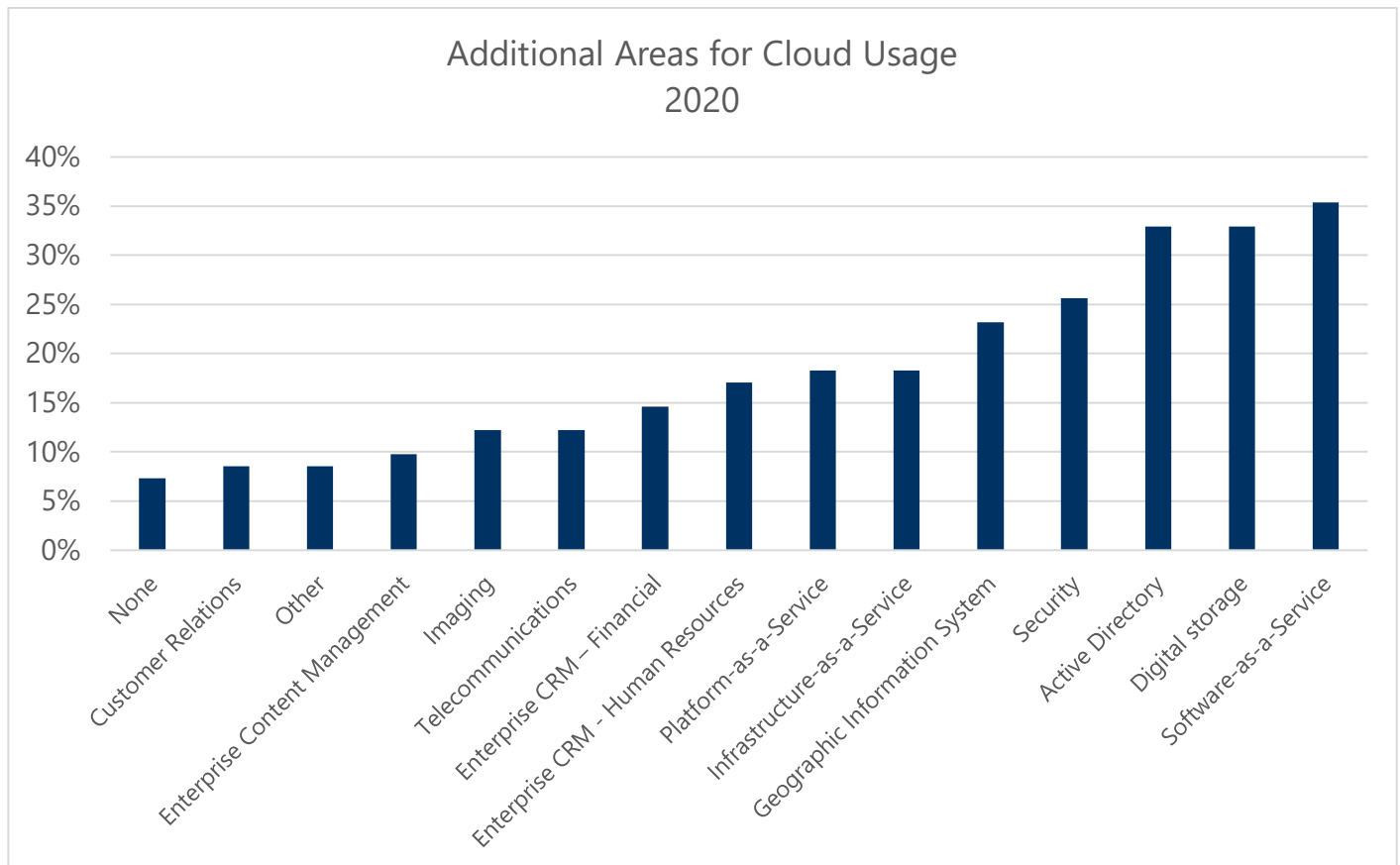
In the 2020 IRDR, 97% of state agencies reported making progress toward cloud adoption goals and 66% report moderate to significant alignment with leveraging shared technology to cost effectively use cloud services. Agencies who are using cloud services are reporting scalability, agility, security, and cost-saving benefits in many of the implementations.

State agencies leverage the cloud for many different services. The chart below shows the percentage of agencies that reported using cloud services for email, office productivity, storage, disaster recovery, and business applications continues to increase.

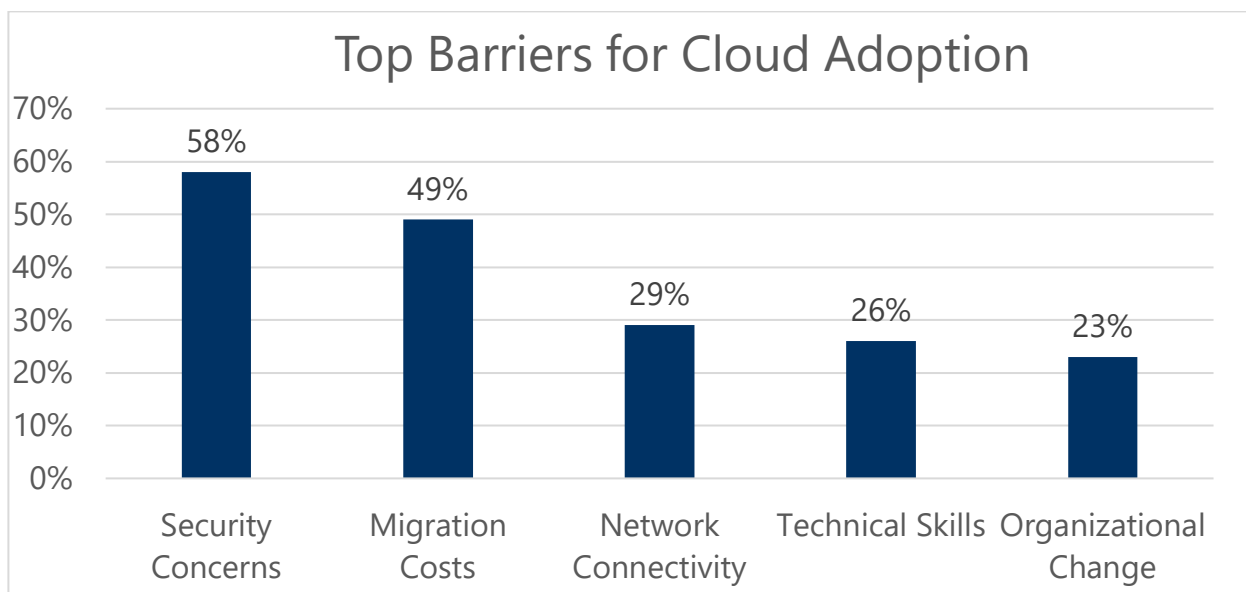




Agencies are also utilizing software-as-a-service, digital storage, active directory, and security.



The greatest barrier to agency cloud adoption are security concerns, migration costs, and network connectivity between cloud and local servers.





Agencies' interest in cloud services continues to grow, with 51% of agencies interested in training or workgroups on cloud services. Cloud brokerage is also a key interest, with 41% considering this as an option in the future.

Cloud Cost Savings and Benefits

State agencies can continue to gain benefits of cloud services by leveraging shared technology services such as those available through the DIR's Cooperative Contracts program and Texas Data Center Services (DCS) public and private cloud infrastructures.

Through DIR's Cooperative Contracts Program, multiple contracts are offered for cloud services. In FY 2020, state agency cloud service purchases from the program totaled over \$96 million³. By choosing DIR's cooperative contracting service, agencies realized a cost avoidance⁴ of nearly \$12 million on those purchases. DIR leverages the purchasing power of the State of Texas to negotiate the most competitive public sector contracts available.

The DCS program, overseen by DIR's Shared Technology Services (STS) program, provides consolidated data services to public entities through an award-winning multi-vendor model. DCS enables Texas state agencies to share costly data center infrastructure and network.

The DCS program continues to evolve with customers' growing technology needs, offering diverse, redundant, and secure connectivity to private, multiple public, and government clouds. The DCS program has expanded the cloud services offered and improved the cloud solutioning process. One new offering is Technology Solutions Services (TSS). TSS provides DIR's customers with strategy management, solution design, and project delivery for both public and private cloud infrastructures. TSS will also provide managed application services to include application development, maintenance, and staff augmentation services for applications hosted in the DCS program.


DCS Texas Private Cloud (TPC)

The TPC is a part of the Texas DCS Program. The TPC employs an enterprise approach to provide secure technology infrastructure compute and storage to DCS customers based on standard reference models and managed services options. As part of the Texas DCS program, participating customers benefit from a high-level, secure suite of offerings supported by Consolidated Data Centers (CDCs), regional, and remote locations. Regional and remote locations are solutioned on a case-by-case basis to meet DCS customer business requirements. TPC offerings include:

- servers with capacity on demand,
- various storage platforms,
- fully-managed and semi-managed services,
- assured software currency, automated backup,
- Criminal Justice Information Services (CJIS)-compliant security,
- disaster recovery with various recovery time objectives,

³ Source: DIR analysis of vendor-reported through DIR Cooperative Contracts program.

⁴ 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.

- 
- auto-provisioning via DIR’s customer portal “Marketplace,”
 - Information Technology Information Library (ITIL) service management process,
 - diversity and redundancy options with data centers in Austin and San Angelo,
 - consistent and modern security policies, baselines, and standards, and
 - round-the-clock monitoring and security incident command and coordination activities.

DCS Public Cloud Services

DCS Public Cloud Services offers customers the choice of service tiers and support models. The DCS Cloud Services model is poised to align to the value of Public Cloud Service delivering IaaS, PaaS, and SaaS services with products and tooling built to leverage the full benefits of Public Cloud Services with the security assurances of DCS. Supported services include Office 365, Texas Imagery Services, Salesforce as a Service, Disaster Recovery, Backup Solutions, Remote File Service, and Database Services. Cloud offerings include:

- integrated Amazon Web Services, Microsoft Azure and Google Cloud Platform,
- public and government cloud environments,
- DCS assurances and security oversight,
- self-provisioning via DIR’s customer portal “Marketplace,”
- fully managed and semi-managed services,
- ITIL service management process, and
- round-the-clock monitoring and security incident command and coordination activities.

DCS hybrid cloud offerings enable applications and data residing in the state’s consolidated data centers to connect directly with applications and data residing in these 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.

Conclusion

State agencies continue to report progress for cloud adoption and consider cloud computing services for solutions. While security continues to be a concern for cloud adoption, agencies are using a variety of cloud security controls and express interest in cloud training. They can accelerate the benefits of cloud services by leveraging shared technology services like those available through the DIR’s Cooperative Contracts program and Texas DCS public and private cloud.



Consolidated IT Infrastructure Report

Section 2054.068 of the Government Code requires DIR to inventory state agency information technology infrastructure. DIR is required to analyze and assess state agencies' security and operational risks. For a state agency found to be at higher security and operational risks, DIR must include a detailed analysis of agency efforts to address the risks and related vulnerabilities.

Methodology

The agency risk was scored using multiple data sources, including all self-assessed information provided (or not provided) by agencies to DIR. The overall score is based on a 100-point scale, with 100 being the least risk and 0 being the most risk. The following provides the breakdown of the risk score and an overview of the calculations for each of the contributing factors.

Information Resources Deployment Review – 30pts

Section 2054.0965 of the Government Code requires agencies to complete a biennial review of their information resources deployment, the Information Resources Deployment Review (IRDR). The IRDR asks agencies to answer standardized questions about information security, continuity of operations, disaster recovery, digital storage, agency hardware and software, and legacy applications. DIR selected 16 of the IRDR questions and assigned varying points to each response option.

Agency Security Plans – 30pts

Section 2054.133 of the Government Code mandates agencies develop and periodically update an information security plan for the agency. The 2020 Agency Security Plans require agencies to assess their maturity on a scale of 0 (non-existent) to 5 (optimized) over 40 security objectives. The combined average of all security objectives determined the agency score for this section.

Security Services – 20pts

The following values of 3 to 10 were assigned to agencies based on how recently the agency obtained a DIR-provided Texas Cybersecurity Framework Security Assessment and external network penetration test within a range of plus or minus .05. If an agency had not obtained these services, they were given a "0" for that category. The assessment and penetration test scores were combined to create the overall security services score.

Monthly Security Incident Reporting – 10 pts

Administrative Rules 1 TAC 202.23/1 TAC 202.73 require each agency and institute of higher education to submit monthly security reports to DIR no later than the nine calendar days after the end of the month. These security reports include a summary of security-related events and incidents. To determine the score for this section, DIR reviewed the period from September 2019-August 2020 and assigned a value based on the number of each report submitted on time.

IT Inventory – 10 pts

Sections 2054.068 and 2054.0965 of the Government Code require state agencies to complete an IT inventory as part of the IRDR. Agencies were provided a 1 (low) to 5 (high) level of criticality/impact and failure probability associated with each server instance. The average probability and impact scores were multiplied to determine a general risk score for agencies' servers.



Agency Risk Score Distribution

The distribution of agency scores had an average score of 63.72 and the median score was 64.67. Agencies found to be at higher operational and security risk relative to other state agencies completed remediation plans.