

DIR Shared Technology Services

STS for School Districts

June 22, 2022



Agenda



- 1. Introductions and STS Overview**
- 2. Public Cloud Manager**
- 3. Texas Private Cloud**
- 4. Managed Security Services**
- 5. Learn More and Join Us**

Introduction and STS Overview

Carrie Davie

MSI Director of Communications, Outreach, and Growth



DIR Shared Technology Services Model



Multi-sourcing Services Integrator (MSI)

- Marketplace
- Service Management
- Business Management
- Operations Management
- Customer Relationship Management

Data Center Services

- Texas Private Cloud
- Public Cloud Manager
- Mainframe Services
- Technology Solution Services
- Print, Mail, & Digitization
- Security Operations

Texas.gov

- Constituent Payment Portal
- Texas by Texas Digital Assistant
- Identity Solutions

Managed Security Services

- Device Monitoring
- Incident Response
- Assessments

Open Data Portal

- Official State Repository of Publicly Available Electronic Data

DIR Shared Technology Services: Data Center Services



Multi-sourcing Services Integrator (MSI)

Capgemini

- Marketplace
- Service Management
- Business Management
- Operations Management
- Customer Relationship Management

- Privileged Access
- Policies & Standards

DCS Security Operations

SAIC

- Active Threat Identification
- Security Incident and Event Management

- Technology Planning
- Reference Architecture

Technology Solution Services (TSS)

Deloitte

- Solution Consulting
- Project Delivery

Application Services

Deloitte

- Application Development
- Application Maintenance
- Legacy Modernization
- Staff Augmentation

Private Cloud

Atos

- Managed Server Compute
- Managed LAN/WAN
- Data Center Facilities

Public Cloud Manager

Rackspace

- AWS, Azure, Google
- Managed Cloud Services
- Email O365
- Geographic Information Systems

Mainframe

Atos

- Managed Mainframe Services

Print, Mail, and Digitization

Xerox

- Managed Print & Mail
- Digitization
- Document Management System

Public Cloud Manager

Joe Nanus, Rackspace



Public Cloud



The Public Cloud Manager will provide computing services, technical and security assurances, and onboarding of public cloud services (commercial and government) through AWS, Azure, and Google.

WHAT'S NEW: Public Cloud service delivery with a focus on aligning the DCS Operating Model with Industry Best Practices. Leveraging Cloud Native tooling, the DCS Cloud Service model is poised to align to the value of Cloud Service Providers by evolving capabilities with investment in Service Evolution of the Public Cloud.

Overall Value

Expanded Public Cloud model to deliver IaaS, PaaS and SaaS services with products and tooling built for and within the Public Cloud to leverage the full benefits of Public Cloud services with the security assurances of DCS.

How you benefit:

- Technical and Security Program assurance of new and existing Services
- Expanded ability to leverage public cloud services
- Cloud center of excellence guidance and support

Choice

Full operational support for IaaS, PaaS and SaaS Offerings to meet the varying support needs by Agency

How you benefit:

- Leverage the best workload hosting strategy for each use case and find the right capability in the right platform at the right Service Tier based on Customer requirements
- Program that will keep pace with cloud service provider evolution of capabilities

Competitive Price

Reduce operating expense by automation, focus on proper service alignment and improved self service

How you benefit:

- Maximize Public Cloud advantage of capabilities and price inherent in Public Cloud use cases
- Standardized Instance Scheduling to turn on/off systems to reduce operating expenses within the Public Clouds
- Daily managed services support rates

Public Cloud Service Tiers



IaaS Sandbox

Benefits & Included Security

- Cloud Native Logging
- Operating System Logging
- MSFT Cloud Application Security
- Verodin Security instrumentation Platform.

Note -
No application layer management

IaaS Semi-Managed

Benefits & Included Security

- Cloud Native Logging
- Operating System Logging
- MSFT Cloud Application Security
- Verodin Security instrumentation Platform.

But wait there's more....

- Armor Anywhere Endpoint Security
- BigFix Patching & Compliance
- CrowdStrike AV

Note -
Customer retains admin rights of OS.
No application layer management

IaaS & PaaS Fully Managed

Benefits & Included Security

- Cloud Native Logging
- Operating System Logging
- MSFT Cloud Application Security
- Verodin Security instrumentation Platform.
- Armor Anywhere Endpoint Security
- BigFix Patching & Compliance
- CrowdStrike AV & HIPS
- Twistlock Container Patching & Compliance (Optional)
- Imperva Web Application Firewall
- Application, Middleware, and Database Monitoring/Support.

Note -
PCM retains admin rights of OS.
No application layer management

The background of the slide is a photograph of a field of bluebonnets in bloom. The flowers are in the foreground and middle ground, with some in sharp focus. The sky above is a mix of dark, heavy clouds and lighter, wispy clouds, with a warm, orange and yellow glow from the setting or rising sun visible on the horizon. The overall mood is serene and natural.

Remote File Service

Jason Wicker, Rackspace

Remote File Service



- PCM is now able to provide Remote Cloud Based File Service
 - This replaces the previous remote file offering
- Features include
 - On Prem File Synchronization
 - Multiple levels of storage class (Archive, Hot, Cold, Premium, etc.)
 - Ability to have multiple types of storage pools against a single file source
 - Available in AWS and Azure
 - Built with reference architectures
 - Secure point to point encryption available
 - Low cost to entry, low cost to manage
 - Infinitely scalable - storage pools can be configured to expand automatically



Disaster Recovery

Jason Wicker, Rackspace

Disaster Recovery – Benefits with DCS



DR Classification and Target RPO/RTO times:

Service	Class A	Class B	Class C	Class D	Class E
Type	Active/Active	Regional Standby	Active/Active in Region	Backup/Restore	Sandbox
Description	Replicated data and load balanced environment across multiple regions. All regions actively taking traffic	Replicated data and services in a second region. Second regions is ready to take traffic via load balancers.	Data is load balanced across availability zones. All IaaS have a failover target. PaaS regional or HA available services.	No in region high availability, IaaS with backups and single instance PaaS	Customer Managed. PCM services to restore are best effort and assistance.
Region	Multi (2 minimum)	Multi (2 minimum)	Single Region	Single Region	Customer Managed
Availability zone	Multi (2 minimum)	Single/Multi	Multi (2 minimum)	Single Zone	Customer Managed
RTO	Real Time	< 1 Hour	< 8 Hours	< 5 days	Best Effort
RPO	Real Time	< 15 Minutes	< 4 Hours	< 24 hours	Best Effort

Texas Private Cloud

Margie Powers, Atos



Texas Private Cloud



Texas Private Cloud Atos

- Datacenter
- Server
- (LAN) Network



- Manage **7,500** compute instances in consolidated and 900 remote locations
 - VMWare based converged and hyper-converged architectures
 - Multiple cost-efficient Oracle/database offerings
 - Highly scalable and cost-efficient Disaster Recovery
 - Multiple SAN/VSAN enterprise class offerings
 - Enterprise class Data Protection and Security offerings
- Software Defined Network (SDN) and Software Defined Data Center (SDDC) architectures provide platforms for enterprise level automation
- Manage 2 Tier II data centers based in Texas

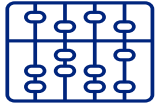
Texas Private Cloud Transformation



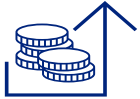
New Technologies Implemented to Date



Software Defined Network with all customer migrations complete; allows IP portability between the CDC's, enabling a seamless failover and failback in a disaster



Enterprise Exadata and Fractional Oracle for cost efficiency with Oracle platforms



Dark Capacity for significantly lower-cost disaster recovery platforms



vRealize Automation for integrations with ServiceNow to provide considerably quicker and seamless availability of self-service items as approved by the Service Evolution Program



UiPath scripting for automation of repetitive human tasks (eg. automation of recovery from backups for DR Class 4 servers)



Ansible scripting for Linux build and patch management, as well as some NW automation activities

Texas Mainframe



Mainframe Atos

- Managed Mainframe Services



- Manage **4,000+** MIPs in 2 consolidated Data Centers
 - State of the Art IBM z15 Technology
 - Physical database management support for multiple database systems
 - All flash, all encrypted at rest, and all fully replicated SAN/DASD Storage
 - Highly scalable and cost-efficient Disaster Recovery
 - Enterprise class Data Protection and Security offerings
- High customer satisfaction and SLA obtainment
- Highly automated environment
- Cost competitive for application usage

Managed Security Services

Kelly Alagna and Gene Moore, AT&T





DIR Shared Technology Services: Managed Security Services



Multi-sourcing Services Integrator (MSI)

Capgemini

- Marketplace
- Service Management
- Business Management
- Operations Management
- Customer Relationship Management

Security Monitoring & Device Management

AT&T

- End Point Device Management
- Intrusion Detection/Prevention
- Malware Detection/Prevention
- Managed Firewalls
- Security Operations Centers

Risk & Compliance

AT&T

- Penetration Testing Service
- Vulnerability Assessments
- Security Risk Assessments
- Industry Focus Assessment

Incident Response

AT&T

- Security Incident and Response Management
- Response Preparedness
- Digital Forensics



Managed Security Services (MSS)

Cybersecurity Awareness



Key Considerations:

- In recent years, Cyber-attacks have become more common, more sophisticated, disruptive and damaging to organizations.
- A good cybersecurity posture means taking a comprehensive view of all cyber systems and using a layered approach of policies, practices, and people to prevent, protect against, respond to, and recover from a cybersecurity incident.
- Avoid common missteps an organization can make when first responding by utilizing industry best practices

What's Changed:

- **On February 25, 2022, Texas Governor Abbott issued a letter to Texas DIR and DPS stating the following:**

"Over the past year, the State has taken significant strides to bolster its cybersecurity defenses. To further protect Texans from potential cybersecurity threats, I am directing you to use every available resource to safeguard the state's critical infrastructure and to assist local governments and school districts with their needs."

Critical Questions:

- *Do we have a current Cybersecurity Incident Response Plan with documented steps and actions to take?*
- *Are we confident and prepared to handle a Ransomware attack or other Cybersecurity incident this weekend?*
- *Who can we turn to for Incident Response assistance (consultation, triage, remediation, additional cybersecurity professionals)*



Popular Service Offerings by Category

Security Monitoring

- ❖ Security Information & Event Management (SIEM)
- ❖ 24x7 Security Operations Center (SOC)
- ❖ Darknet Intelligence Monitoring
- ❖ Targeted Threat Research
- ❖ Advanced Threat Hunting (ATH)

Device Management

- ❖ Managed Endpoint Detection and Response (EDR)
- ❖ End Point Protection Services (EPP) – Student Devices
- ❖ Intrusion Detection/Prevention Services (IDS/IPS)
- ❖ Malware Detection and Prevention
- ❖ Managed Next-Gen Firewall Service
- ❖ Managed Web Application Firewall Services

Risk & Compliance

- ❖ Penetration Testing Services (Pen-Test)
- ❖ School District Security Assessment
- ❖ Industry Focused Assessment (IFA)
- ❖ Risk and Cloud Compliance Assessment
- ❖ Texas Cybersecurity Framework Assessment (TCFA)
- ❖ Vulnerability and Web Application Scanning Services

Incident Response

- ❖ Security Incident and Response: (IR event support)
- ❖ IR Preparedness - Cybersecurity Incident Response Plan (CIRP)
- ❖ IR Preparedness - Ransomware Table-Top Exercise (TTX)
- ❖ Digital Forensics



Managed Security Services (MSS)

Incident Response Services



Cybersecurity Incident Management

- ❖ Incident Response services provide expert assistance to your organization in the event of a security breach.
- ❖ This service enables you to field a team of information security professionals in response to a security breach, assess the nature and depth of the situation, and remediate the incident.

Cybersecurity Response Preparedness

- ❖ Incident Response Preparedness uses an industry-leading Incident Management Framework coupled with the AT&T's experience in computer forensics and investigations.
- ❖ AT&T Cybersecurity will assess the status of your Incident Management program against a customized version of the framework to develop an incident program and associated roadmap.
- ❖ Option to Develop a Cyber Incident Response Plan (CIRP) and a Ransomware Table-Top Exercise (TTX)

Cybersecurity Digital Forensics

- ❖ Digital Forensics includes the detailed technical analysis that supports the Root Cause of an incident.
- ❖ Using digital tools and proper chain of custody data handling techniques, certified technicians utilize data for Root Cause Analysis.



School District Security Assessment



School District Security Assessment

- One Two-Day Onsite Visit
- Interview IT and key department leaders
- Concise Cyber Maturity Scorecard
- Recommendations Prioritized by Risk
- Detailed Full Report for Technical Teams
- Leadership Briefing Provided

Above and Beyond Standard Assessments

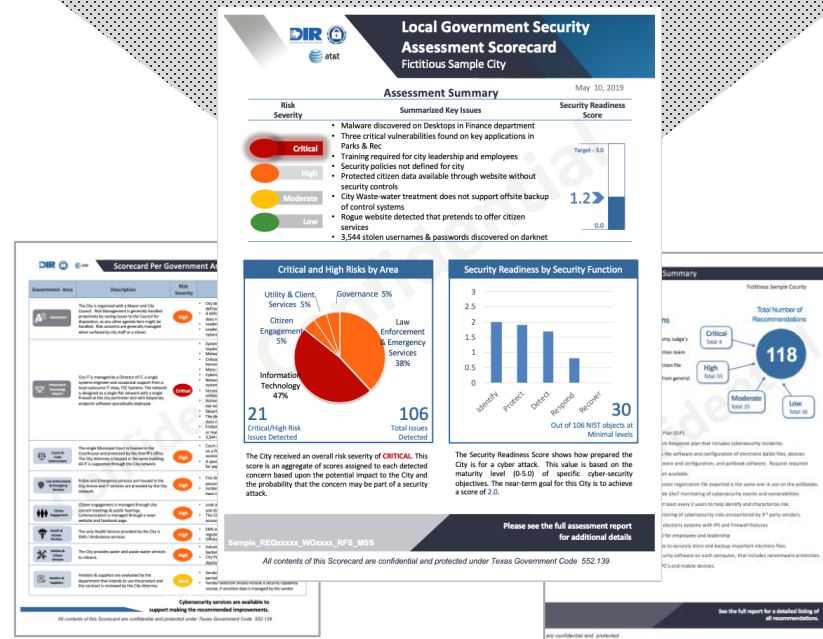
- Conversational Interview Process
- District Process Review
- Student Communication Process Review
- District Building Security Review
- IT Architectural Review
- PII Identification
- NIST CSF-Based Assessment
- Malware Hunting across network
- Internal and External Vulnerability Scans
- Internal Network Scans
- Lightweight Darknet Analysis
- Sample Wireless Network Testing
- Social Engineering Tests

END-TO-END SCHOOL IT EVALUATED AND SCORED

Information
Technology

Student
Access

Physical
Security



* Includes FERPA principals, but is **not** a FERPA Assessment



Managed Security Services (MSS)

In Summary...



We provide *comprehensive IT security services* for Texas agencies and DIR customers in three functional areas, each containing multiple services to meet modern security needs.



**Security Monitoring &
Device Management (SMDM)**



Risk & Compliance (R&C)



Incident Response (IR)

MSS offerings are **billed and branded as DIR solutions** – AT&T is the MSS service provider, complemented by technology from select vendors. For more info, visit the [STS-MSS Offerings](#).

Learn More and Join Us

Elise McCullough

MSI Outreach and Growth Consultant,
Capgemini



STS External Portal

<https://dirsharedservices.service-now.com/dir>

- Designed for prospective STS customers, including governance (city, county, and state) and higher education
- STS Service Offerings catalog with high-level views and drill-down details
- Publications page featuring previous webinars and other helpful articles
- Eligibility details and sample agreements



The screenshot shows the homepage of the STS External Portal. At the top, there is a banner image of a field of blue flowers with the text "Welcome to Shared Technology Services". Below the banner, on the left, is a paragraph about the mission of the Texas Department of Information Resources (DIR). To the right of this paragraph is a search bar. Below the mission paragraph are four blue buttons stacked vertically: "Data Center Services (DCS)", "Texas.gov", "Managed Security Services (MSS)", and "Open Data Portal (ODP)". Below these buttons is a section titled "What is STS?" followed by a paragraph about the objective of the program. Below that is a section titled "STS Values" followed by a bulleted list of three values: "Diverse Technology Solutions", "Assurance", and "Customer Support". At the bottom of the page, there is a footer with the text "Disaster Recovery Webinar" and a small video player showing a person's face with the text "DIR Shared Technology Services" and a "Share" button.

Welcome to Shared Technology Services

The mission of the [Texas Department of Information Resources](#) (DIR) is to serve Texas government by leading the state's technology strategy, protecting state technology infrastructure, and offering innovative and cost-effective solutions for all levels of government. You can use the buttons, to the right or below, to gather more information about some of our service offerings such as Data Center Services or Managed Security Services.

What is STS?

The objective of DIR's Shared Technology Services Program is to supply access to managed IT as a Shared Service, allowing Customers to focus on supporting their mission and business functions rather than directly managing IT services.

STS Values

- Diverse Technology Solutions - Meeting customer needs today while anticipating future demands through proven industry best practices and research.
- Assurance - Services are competitively procured with secure, reliable, and scalable solutions provided by private sector industry leaders and designed to meet customer requirements.
- Customer Support - From procurement through operations, STS solutions offer flexibility, accountability, and agility to meet evolving business needs, while minimizing risk and maintaining business continuity. The STS program provides customers with technical expertise and responsive support using a single platform and enterprise governance structure.

Disaster Recovery Webinar

DIR Shared Technology Services

Share

STS Service Offerings Catalog



Data Center Services (DCS)

Texas.gov

Managed Security Services
(MSS)

Open Data Portal (ODP)

Categories

STS Service Offerings Catalog

Data Center Services (DCS)

Texas.gov

Managed Security Services (MS...)

Open Data Portal (ODP)

STS Service Offerings Catalog

Welcome to the Catalog of DIR Service Offerings. Here, you will find information about the Programs offered by DIR Shared Technology Services. Use the tiles below to navigate through our Services and their Offerings.

Active Threat Identification

Identifying threats to protect our environment

View Details

App Management and St...

Maintain and enhance existing applications or augment your team

View Details

Compute and Storage

An enterprise approach to technology infrastructure

View Details

Darknet Intelligence Asse...

Broad-scale assessment of your brand and infrastructure on the

View Details

Digital Forensics

Detailed analysis of Security Incidents

View Details

Endpoint Detection Resp...

Monitoring platforms and devices for health, performance and activity

View Details

Incident Command Respo...

Ready to respond to security events

View Details

Industry Focused Security...

Security Assessments focused on Local Governments, School Districts and Utilities

View Details

Information Security Polic...

Establishing a framework to keep data safe

View Details

9 of 49

Show More

Want More Information?

- Prospective Customers: Submit our interest form on any offerings page to be contacted by our team.
 - Select all STS Programs or Services of interest.
 - Provide additional information about your needs to help get your request to the right person faster.
- Current Customers: Submit a Request For Solution (RFS) via the Service Catalog or engage your MSI Customer Relationship Manager.

Shared Technology Services Interest Form

Name

Phone number

Email

Title

Organization/Company

* Select all Programs and Services of interest, and we will be in touch!

☐ DCS Texas Private Cloud

☐ DCS Public Cloud Manager

☐ DCS Print, Mail, and Digitization

☐ DCS Mainframe

☐ Texas.gov Payment Services

☐ Texas.gov Application Services

☐ Managed Security Services

☐ Texas Open Data Portal

☐ Please provide any known deadlines or requirements below.

Submit Save Cancel





Eligibility and Contract Requirements

Prior to receiving Shared Technology Services from DIR, all customers must sign either an Inter-Agency Contract (IAC) or an Inter-Local Contract (ILC). In addition, each Program has Terms and Conditions that must be accepted.

Who is eligible?

- State Agencies
- Public Institutions of Higher Ed
- Local Governments
- Public School Districts
- LCRA

Note: Public community colleges are eligible to participate only in Managed Security Services (MSS) and Texas.gov.

Contract Document Previews

- [Shared Technology Services IAC](#)
- [Shared Technology Services ILC](#)
- [Data Center Services Terms and Conditions](#)
- [Texas.gov Terms and Conditions](#)
- [Managed Security Services Terms and Conditions](#)
- [Open Data Portal Terms and Conditions](#)

(Find these on the External Portal's Eligibility page.)

Contact Us

Outreach and Growth Team

outreach.dirsharedservices.nar@capgemini.com





STS is powered by the
following providers:

Atos

Capgemini

NiC
TEXAS

SAIC

xeroxTM

 **AT&T**

Deloitte.

rackspace
technology

 **tyler**
technologies