2022-2026

State Strategic Plan for Information Resources Management

Accelerating the Next Generation of Technology in Texas

About This Plan

The Information Resources Management Act (Texas Government Code, Section 2054.91-094) requires the Texas Department of Information Resources (DIR) to prepare a state strategic plan for information resources management each biennium.

The plan identifies technology goals for state government over the next five years and guides agencies as they develop their agency strategic plans.

Note: For the purposes of this report, the term "agency" is used to indicate a state agency or a state-funded institution of higher education.

The 2022-2026 State Strategic Plan is available on the Department's website at dir.texas.gov.

Texas Department of Information Resources
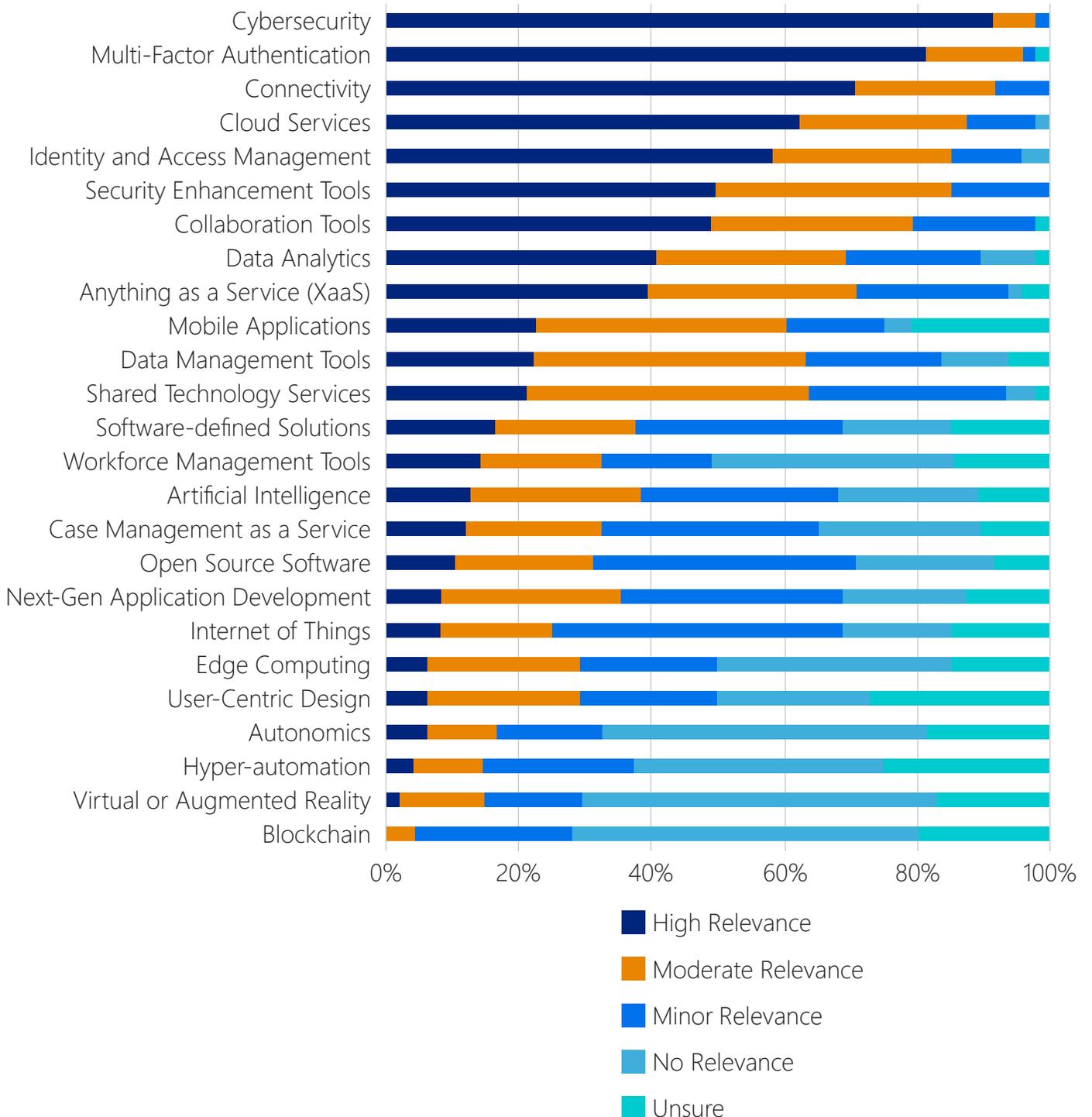P.O. Box 13564, Austin, TX 78711, 1-512-475-4700

Table of Contents

Technology Insights At A Glance

In the 2021 IT Planning Leadership Survey, technology leaders and executives in Texas state agencies and institutions of higher education were asked how relevant the technology developments listed below will be to their organizations and operations in the next two years.

Relevance of Technology Developments

Categories (top to bottom):
- Cybersecurity
- Multi-Factor Authentication
- Connectivity
- Cloud Services
- Identity and Access Management
- Security Enhancement Tools
- Collaboration Tools
- Data Analytics
- Anything as a Service (XaaS)
- Mobile Applications
- Data Management Tools
- Shared Technology Services
- Software-defined Solutions
- Workforce Management Tools
- Artificial Intelligence
- Case Management as a Service
- Open Source Software
- Next-Gen Application Development
- Internet of Things
- Edge Computing
- User-Centric Design
- Autonomics
- Hyper-automation
- Virtual or Augmented Reality
- Blockchain

X-axis: 0% 20% 40% 60% 80% 100%

Legend:
- High Relevance
- Moderate Relevance
- Minor Relevance
- No Relevance
- Unsure

2022-2026 State Strategic Plan for Information Resources Management
Accelerating the Next Generation of Technology in Texas

Vision

The State of Texas will be a leader in the delivery of secure, digital government through well-designed and innovative technology solutions.

Introduction

Over the past biennium, Texans' demand for secure online interaction with government accelerated as the COVID-19 pandemic changed the way agencies operate. At the same time, agencies rapidly implemented the tools that facilitated expanded telework and remote learning, enhanced the use of data analytics, and empowered a more robust technology infrastructure for online government transactions.

While the pandemic highlighted public sector resilience, it also emphasized the importance of planning and meeting future challenges through modernizing technology. Texas agencies continue to face a tremendous sense of urgency to improve internal processes, accelerate collaboration, and provide secure, reliable, constantly-connected technology.

The 2022–2026 State Strategic Plan for Information Resources Management aims to aid agencies as they evolve to meet Texans' expectation that government provide a high level of secure, convenient, and reliable digital service. Each agency can use the strategic goals outlined in this plan to identify actionable objectives for their own strategic planning.

Technology can transform how the state of Texas serves Texans. Proper planning, investment, and management of information technology (IT) resources can help state leaders prepare for and take advantage of the rapid evolution that continues to improve government services.

The Texas Department of Information Resources (DIR) presents this plan to partner with agencies in the advancement of statewide IT goals and deliver the next level of service and value to Texans. By working together toward these common goals, Texas will continue to lead the way.

Goal 1: Secure IT Service Delivery

Goal 2: Advanced Data Management

Goal 3: Strategic Digital Transformation

Goal 4: Proactive Approach to Emerging Technologies

Goal 1:
Secure IT Service Delivery

Objectives

1. Reinforce risk-based security practices, including continuous prediction, prevention, detection, and response to cybersecurity threats.

2. Form a resilience mindset and a vigilant organizational culture through cybersecurity education and training.

3. Develop regional approaches to cybersecurity engagement and response.

4. Create scalable, integrated tactics for cybersecurity based on cost-effective cybersecurity tools.

Goal 2:
Advanced Data Management

Objectives

1. Strengthen data governance by implementing best practices, appointing dedicated data management staff, and maturing data management programs.

2. Enhance data security and privacy with strong controls based on risk and legal requirements.

3. Facilitate better decisions by adopting flexible analytics that provide leaders with business-oriented data.

4. Foster a data-sharing culture where open data is readily available, enabling state leaders and the public to make data-driven decisions.

Goal 3:
Strategic Digital Transformation

Objectives

1. Develop a vision and strategic road map that reimagines how Texas government delivers services.

2. Conduct a collaborative review of agency goals, business processes, and technology to understand the current level of digital maturity.

3. Understand what Texans need and expect from their government, so that state IT leaders can procure and implement human-centered applications.

4. Promote mobile-first digital experiences that allow Texans to seamlessly access all government services.

Goal 4:
Proactive Approach to Emerging Technologies

Objectives

1. Prioritize investing in platforms and projects that support emerging technologies and help accelerate legacy modernization.

2. Develop flexible and adaptable approaches to procure and implement the innovative technologies needed to meet the modern demands of Texans.

3. Identify opportunities to deploy emerging technologies that improve the day-to-day delivery of government services.

4. Develop a resilient workforce that can adapt to emerging technologies and new concepts of public sector work.

Goal 1: Secure IT Service Delivery

Texans entrust government with some of their most sensitive and confidential information, and government agencies bear the responsibility for ensuring that information is not compromised.

As increasingly complex cyber threats continue to target the public sector, agencies must minimize risks to technology and evolve cybersecurity practices focusing on the human element.

In addition, Texas government must continue to invest in advanced tools for identifying, preventing, detecting, and responding to information security and cyber threats.

Challenges

Cybersecurity threats range widely in sophistication and scope. Increased reliance on third parties creates supply chain risks and the possibility that tools could be used to gain unauthorized access to networks or information.

Advances in technology give rise to new classes of threats almost every day.

Challenges around the human element of cybersecurity are prevalent and drive the need for identity-based, location-independent solutions.

A nationwide shortage of skilled cybersecurity professionals continues to hinder the public sector's ability to recruit and retain people with specialized skills.

Cybersecurity risks are complex and may occur during other disruptions. As a result, there is an increasing need for regional responses and integrated continuity planning.

Desired Outcomes

- Mature, risk-based security programs that safeguard information, reduce harm, decrease third-party risk, provide continuous protection, and increase resilience.

- A cybersecurity-aware culture that can better identify and prevent incidents by sharing threat information throughout cyber communities.

- Sustainable resources to meet security needs, including long-term investment in cybersecurity tools, talent, and training.

- High levels of protection for private and confidential information, reduced exposure to cyberattacks, and regional approaches to preparedness that build resilience.

Objectives

> **1** Reinforce risk-based security practices, including continuous prediction, prevention, detection, and response to cybersecurity threats.

The global pandemic changed the nature of work and created the unique risks of a hybrid workforce.

Agencies must consider the vulnerabilities for remote workers, increased opportunities for human error, and limitations for monitoring virtual workspaces.

Agencies should explore a zero-trust model as a long-term approach to reducing vulnerabilities.

As cloud adoption accelerates, so do the challenges of evaluating and monitoring cloud products and services.

State law now requires agencies to contract with cloud providers that demonstrate compliance with the state's risk authorization and management program, TX-RAMP.

The program will provide standardization for security assessment, authorization, and monitoring of cloud computing services that process Texas government data.

As security risks shift, the public sector must focus on user identity and access management in addition to network-based security measures.

Agencies may want to take advantage of centralized identity and access management solutions to reduce duplication and implement risk-based protections.

92%

of agency leaders agree that **cybersecurity** will be highly relevant to their organization in the next two years.[1]

Source: 1) 2021 IT Planning Leadership Survey.

Objectives (continued)

2 Form a resilience mindset and a vigilant organizational culture through cybersecurity education and training.

As the range of cybersecurity threats evolve, it is critical that agencies provide ongoing education and training to all employees and contractors.

Agencies must reduce exposure and strengthen the first line of defense against phishing, social engineering, and other human-focused tactics used in cyberattacks.

Texas government must implement cybersecurity practices well-suited for the workforce of the future by building internal skills, cross-training staff, and adopting policies that support good cyber hygiene.

Agencies should identify and develop the security skills employees need to support the agency's mission, the types of technology it uses, and the data it creates and maintains.

3 Develop regional approaches to cybersecurity engagement and response.

When cybersecurity incidents, natural disasters, pandemics, or other events disrupt IT systems, a quick response is critical to the restoration of government operations and services.

Agencies should participate in and support regional cybersecurity planning, training exercises, and responses to actual events.

A new state law authorized the establishment of regional cybersecurity working groups, volunteer incident response teams, and regional network security centers that will become cornerstones for these activities.

Agency continuity plans should contemplate scenarios where cybersecurity incidents occur during emergencies or other disruptive events, and cybersecurity response exercises should include regional partners to prepare for complex disruptions.

Objectives (continued)

4 Create scalable, integrated tactics for cybersecurity based on cost-effective cybersecurity tools.

Integrated approaches for cybersecurity and risk management are effective at helping agencies evaluate their current IT infrastructure and make informed decisions about which applications are too costly or high-risk to maintain.

Agencies should apply multiple layers of security tools and strategies to heighten vigilance in protecting confidential and sensitive data.

Leveraging shared security services can help agencies make cost-effective investments in tools that help identify, prevent, detect, and respond to malicious activity.

Examples of such tools include multi-factor authentication, endpoint detection and response, monitoring and reporting tools, breach and attack simulation tools, host intrusion protection systems, and disaster recovery tools.
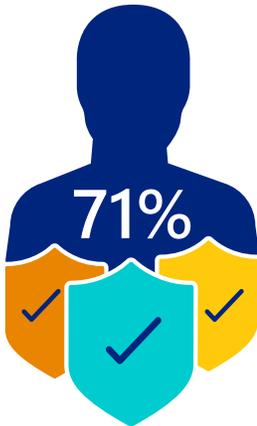
71%

of agency leaders agree that **multi-factor authentication** will be highly relevant to their organization in the next two years.[1]
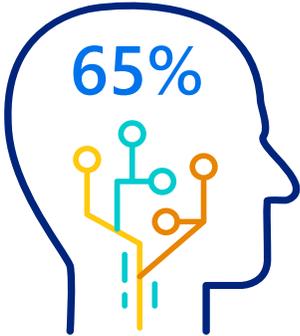
65%

of worldwide government agencies will **use predictive analytics** to identify, contain, measure, and address security risks.[2]

Source: 1) 2021 IT Planning Leadership Survey; 2) International Data Corporation, 2020.

Goal 2: Advanced Data Management

Texas agencies collect, create, and manage vast amounts of data. Because the people of Texas entrust government with so much information, agencies must diligently protect Texans' personal and confidential information and ensure it is properly used.

At the same time, public servants must be able to access and analyze timely, accurate, and high-quality data to deliver effective government services.

Agencies must have strong data governance that balances privacy and security with information sharing and data analytics.

Challenges

Data distributed over many departments can make implementing strong data governance, data and analytics policies, processes, and best practices challenging.

A data-literate workforce and data specialists are both key for data management success. Unfortunately, the state's need for data professionals greatly exceeds the number of qualified applicants applying for these positions.

The volume of data available makes the risk of error or bias greater than ever before. Understanding the strengths and weaknesses of a data set helps avoid decisions based on erroneous insights.

Adhering to retention schedules when creating, cataloging, archiving, and retiring data over its lifecycle is essential to keeping datasets current, useful, and valuable.

Desired Outcomes

- High-quality, timely, secure, and accurate data that is integrated and readily available for decision-making.

- Identification of high-value data assets so agencies can make that data publicly available without compromising confidential or sensitive data.

- Data privacy practices that include data classification and appropriate controls for each specific type of data.

- Mature data management programs with well-defined governance, broad data literacy throughout the organization, and meaningful outcome metrics to measure progress.

Objectives

1 Strengthen data governance by implementing best practices, appointing dedicated data management staff, and maturing data management programs.

Strong data governance guides all aspects of management and control over data assets. Most data governance programs include strategy, policy, standards, oversight, and compliance components.

More mature programs have processes for resolving data issues, initiating data improvement projects, and defining the business value of data.

Agencies can advance organizational change by focusing on people, clearly communicating expectations, and appointing data management officers with the support and commitment of organizational leaders.

Such change requires vision, leadership, and involvement from people at all levels of an organization. It is also essential that staff throughout an organization have a strong understanding of customer expectations, the laws that govern certain data sets, and available data management tools.

Agencies can improve data programs by formalizing employees' data-related roles and responsibilities, cultivating data stewardship, and integrating data governance into business processes.

Agencies can go beyond the fundamentals by fostering shared responsibility with strong executive leadership support to increase data governance maturity.

76%
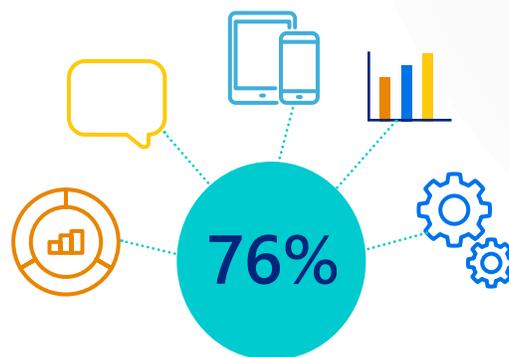
of agency leaders ranked
data governance
as a top initiative.[1]

Source: 1) 2021 IT Planning Leadership Survey.

Objectives (continued)

2 Enhance data security and privacy with strong controls based on risk and legal requirements.

Privacy laws and business practices should form the roadmap of an organization's security practices.

Legal standards, business concerns, and stakeholder expectations should determine appropriate levels of protection and access to data.

Data classification is critical to ensure confidential and sensitive data is identified and have the proper controls applied.

In Texas, data classification follows standards set in statute and defined in the Texas Administrative Code.

Agencies should develop cross-functional teams made up of information security experts, data management officers, legal professionals, and risk and compliance staff to classify data, identify data privacy issues, and assign risk levels.

3 Facilitate better decisions by adopting flexible analytics that provide leaders with business-oriented data.

A strong data analytics program can transform how an agency does business by providing insight into agency operations.

In order to make such insights easy to identify and use, agencies should adopt best practices for data visualization.

Agencies can utilize tools like machine learning or artificial intelligence to optimize their analytics and should explore opportunities to procure solutions that enhance their data programs.

Through adaptive analytics, an agency can predict issues before they arise.

These insights make government more efficient and effective, saving the public time and money.

Objectives (continued)

4 Foster a data-sharing culture where open data is readily available, enabling state leaders and the public to make data-driven decisions.

Open data in government is important for public access, oversight, and trust.

It has the potential to reduce fraud, waste, and abuse while reducing the need for formal requests under the Texas Public Information Act.

The Texas Open Data Portal (ODP) is the state's official data-sharing platform where data can be accessed and consumed.

Through use of the ODP, agencies can foster a sharing culture across all levels of government based on common governance and secure infrastructure that improves efficiency, reduces costs, and increases transparency.

Agencies should proactively identify open data and make it available to Texans through easily accessible sources that empower the public to be more engaged with state government.

500
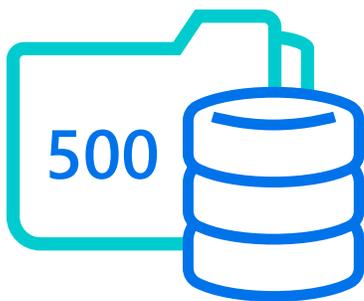
high-value data sets
posted on the Texas
Open Data Portal.[2a]

$25.1 million

estimated **opportunity
cost savings** through public
information request reductions.[2b]

Source: 2a) and 2b) Texas Chief Data Officer, 2021.

Notes: 2a) Agencies self-report that they have published over 500 high-value data sets on the Texas Open Data Portal as of September 1, 2021.; 2b) Estimated is based on assumption that 30% of the total data views and downloads were a result of a public information request redirect for the 14 agencies currently publishing on the Texas Open Data Portal.

Goal 3: Strategic Digital Transformation

In recent years, Texas agencies have increasingly provided a more digital government experience.

As agencies pivoted to remote work during the pandemic, the transition to more digital capabilities accelerated. To keep up this momentum, the public sector must reexamine how Texans consume government services and conduct government transactions.

Agencies should use that information to adjust government business processes and technology tools accordingly. Digital transformation requires leadership and business units working together to integrate the right technology with the people, processes, and tools that make up an agency.

Agencies must take a strategic approach to the adoption of digital technologies in order to fundamentally change how Texas government delivers value to Texans.

Challenges

Demonstrating that new digital capabilities are worth the investment can be challenging, especially with competing priorities.

Entrenched organizational culture and resistance to change can be stumbling blocks to digital transformation.

Likewise, stakeholders with different expectations and business functions that operate in silos create challenges for digital transformation.

Undocumented processes, outdated business practices, and disparate legacy systems hinder an agency's ability to pursue and execute transformative digital initiatives.

Desired Outcomes

- Digital capability assessments that concentrate on people, processes, and tools.

- Digital transformation strategies focused on improving business outcomes and providing more value to Texans.

- Organizational cultures that embrace digital transformation, cultivate leadership, and establish digital champions, governance, and community.

- Meaningful metrics that measure maturity and drive progress throughout the digital journey.

Objectives

1 Develop a vision and strategic road map that reimagines how Texas government delivers services.

Digital transformation initiatives must be based on an understanding of how the public interacts with state employees, makes payments, finds information, and receives services today, and a vision for how Texans will conduct government business in the future.

Agencies must develop a strategic roadmap for identifying, procuring, and adopting the right technology to improve interactions with their customers, employees, and partners.

By examining new ways to meet customer expectations, agencies can strategically approach adopting digital technologies that improve processes, services, and customer experiences.

2 Conduct a collaborative review of agency goals, business processes, and technology to understand the current level of digital maturity.

Digital transformation starts with understanding the agency's guiding mission, existing processes, and current tools serving the public.

Agencies must establish a digital maturity baseline in order to identify the current state of their digital journey.

Agencies should identify key manual processes that can become digital, legacy IT systems that can be replaced or augmented, and workforce skills that can be leveraged in support of digital transformation.

Conducting a collaborative assessment of functions, processes, and the current IT environment will better position agencies to develop meaningful metrics that drive the digital transformation process.

80% of government organizations have **low to moderate digital maturity.**[1]
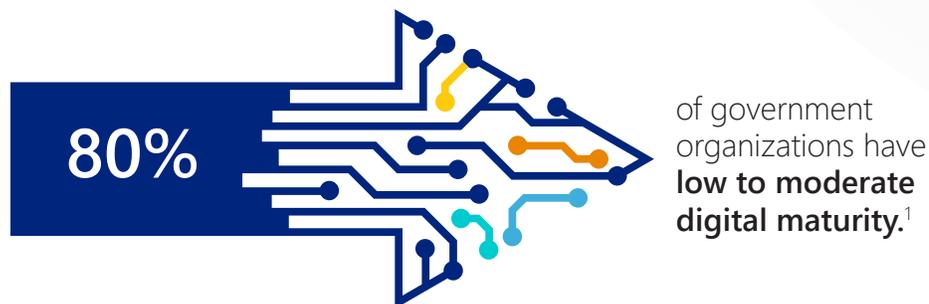
Source: 1) Gartner, April 2020.

Objectives (continued)

3 Understand what Texans need and expect from their government, so that state IT leaders can procure and implement human-centered applications.

In today's digital environment, people are accustomed to using tools that allow remote business transactions.

By considering these expectations, agencies can procure and develop technology that provides user-centric digital government services.

Because Texans were unable to access government services in person during the COVID-19 pandemic, agency website traffic substantially increased across the state.

Agencies must continue to provide technology that enables the public to remotely access government information, make payments for government transactions, and conduct government business that previously required an in-person visit.

As Texans and public sector employees increasingly access government information and services online, it is important to ensure all Texans can access digital government services regardless of their abilities.

Agencies must prioritize accessibility to ensure that websites, applications, and services incorporate features accommodating users of all abilities.

53%

of agency leaders ranked
digital customer experience
as a top initiative for
the coming biennium.[2]

Source: 2) 2021 IT Planning Leadership Survey.

Objectives (continued)

4 Promote mobile-first digital experiences that allow Texans to seamlessly access all government services.

Texans are increasingly using mobile devices to access government services and expect the ability to take care of most government business from their phone.

Providing a modern and secure mobile experience requires responsive web design and well-designed native mobile applications.

Investing in infrastructure such as broadband expansion and next generation cellular technology is essential to ensure continuous connectivity.

Agencies should plan, procure, and implement technology that incorporates mobile-first design allowing Texans to conduct government business from any place, at any time, on any device.

64%

of agency leaders agree that
mobile applications for government
will be moderately to highly relevant
to their organization in the next two years.[2]

Source: 2) 2021 IT Planning Leadership Survey.

Goal 4: Proactive Approach to Emerging Technologies

As agencies face the next phase of modernizing legacy IT systems, they must plan for emerging technologies that are collaborative, scalable, and adaptive to a rapidly changing environment.

While a reliable telecommunications network infrastructure continues to be the foundation for data, video, and voice communications, long-term plans must consider advancements in technologies that fall outside of traditional telecommunication.

Solutions using artificial intelligence (AI), machine learning, robotic process automation (RPA), digital assistants, and low-code or no-code development can help incrementally phase out software, hardware, and services that are no longer supported.

Agencies should take proactive approaches now to increase readiness for the advanced technologies of tomorrow.

Challenges

As pressure grows to replace or augment costly legacy technologies, the constantly evolving IT environment makes it difficult to identify long-term solutions that will withstand the test of time.

Likewise, it is challenging to envision future network innovations that provide next-generation communication services.

Public sector IT investments must follow state procurement requirements to provide accountability and protect taxpayer resources.

It is important to explore ways to streamline processes that allow for timely procurement of emerging technologies.

The workforce challenges for digital government go beyond the need to recruit and retain staff with specialized skills.

Agencies must attract a workforce that embraces emerging technologies if government is to succeed in an automated, AI-driven workplace.

Desired Outcomes

- Well-planned, incremental approaches to legacy modernization that integrate emerging technologies in alignment with the agency's mission and business objectives.

- Strategic initiatives that enable innovative solutions and improve the way agencies procure IT services, plan projects, and deploy new technology.

- Repeatable, flexible methodologies that identify and address legacy system modernization, improve data governance, and modernize contracting practices.

- Streamlined processes, interoperable solutions, improved workflow, reduced risks, and a tech-savvy workforce that can implement advanced technologies providing Texans greater access to government information and services.

Objectives

1 Prioritize investing in platforms and projects that will support emerging technologies and help accelerate legacy modernization.

When planning new technology investments, agencies should consider solutions that enable the integration of emerging technologies.

Whenever possible, the public sector should prioritize cloud-driven "as a service" solutions to lower costs over time and transition away from on-premise models.

Agencies may want to evaluate whether cloud services models can provide the

opportunity to use multiple technologies for the organization to create scalable, interoperable, hyperconnected public services.

Establishing a legacy modernization road map that includes executive sponsorship and governance committees can help agencies define business needs, outline procurement plans, and develop support for emerging technology solutions.

2 Develop flexible and adaptable approaches to procure and implement the innovative technologies needed to meet the modern demands of Texans.

To enable the rapid delivery of quality services in a digital environment, agencies should continue to adopt iterative, collaborative methods of deployment.

IT staff can take agile and DevOps initiatives to the next level by including AI-enabled tools and technologies that facilitate continuous integration, testing, and monitoring for quality assurance.

By implementing modular or microservice-based architectures and cloud technology that allow systems to be replaced over time, government can be better positioned to implement next generation technologies.

Agencies should develop sourcing strategies and agile procurement methods that enable contracting opportunities for a full range of emerging technologies, platforms, and automation tools.

96% of agency leaders agree that **cloud services** will be moderately to highly relevant to their organization in the next two years.[1]

Source: 1) 2021 IT Planning Leadership Survey.

Objectives (continued)

3 Identify opportunities to deploy emerging technologies that will improve the day-to-day delivery of government services.

Agencies should reset the customer experience by identifying projects supported by broadband expansion and next generation cellular technology that transform the way the public interacts with government.

Incorporating technologies that include chatbots, RPA, machine learning, and other low-code or no-code development can help agencies identify solutions that enhance operations and improve customer service.

Consider emerging technologies for core government functions, such as contact management and case management, to meet customer expectations for quick, accurate, and on-demand access to government.

Explore blockchain technology as an option for resolving complex, multi-entity processes.

Although the technology is well-known for its role in digital currencies, it can potentially improve real-time access to critical data and processes that require secure, reliable validation.

15% of governments will use smart contracts **powered by blockchain** to ensure transparent governance of data exchanges by 2025.[2]

Source: 2) International Data Corporation, 2020.

Objectives (continued)

> **4** Develop a resilient workforce that can adapt to emerging technologies and new concepts of public sector work.

AI, RPA, and other emerging technologies could automate a wide range of manual processes, create more efficient workflows, and increase the delivery of mission-critical services.

These technologies can free public servants to focus on work that requires creativity and critical thinking.

Developing the internal knowledge and skills necessary for employees to use AI solutions, procure emerging technologies, and deploy advanced automation is key to success.

Providing employees opportunities for continuous learning, formalized training programs, and upskilling through strong change management practices can help agencies be ready to use emerging technologies that improve government services.

Agencies should develop a roadmap that expands capacity to effectively implement emerging technologies and involves both IT and business unit staff in proof-of-concept projects and Center of Excellence (CoE) activities.

Agencies should explore training opportunities and partnerships with higher education or the private sector to help train staff to fill critical skills gaps.

Offering internships to undergraduate and graduate students with cutting-edge knowledge and skills can build interest in public sector careers and provide vital expertise.
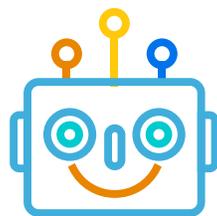
76%
of state CIOs report
introducing chatbots
in response to the
COVID19 pandemic.[2]

Source: 3) 2020 State CIO Survey, NASCIO.

Agency Spotlights

Texas Alcoholic Beverage Commission (TABC)

Comprehensive Technology Transformation

TABC transitioned to more digital capabilities through a comprehensive Technology Transformation Initiative.

First, TABC launched a user-centric redesign of the agency's website that supported a new way for customers to do business with TABC.

This was followed by the implementation of their new cloud-based Enterprise Data Solution infrastructure which includes business analytics and intelligence and a replacement for the existing data mart.

The third component is the Alcohol Industry Management System (AIMS), a new online system for conducting licensing tasks, making payments, and completing reporting requirements.

TABC's Technology Transformation Initiative replaces 18 legacy systems, most of which have not been updated since 2005.

Texas Department of Banking (DOB)

Improved Cybersecurity

DOB has undertaken a full migration of systems to cloud services to improve availability, resiliency, and the agency's security posture.

As part of an overall technology modernization strategy, the DOB determined that the agency would reduce the cost to maintain servers with an equal or lower cost of operations as the agency transitioned away from on-premises modernization efforts.

This strategy allows them to maintain control of internal and external networks while mitigating cybersecurity risks including ransomware and supply chain compromise.

This incremental approach to modernization will help the agency to adopt and maintain appropriate technologies to support efficient, effective, and secure operations.

Agency Spotlights (continued)

Texas Department of Transportation (TxDOT)

Project Coordination and Data Sharing with TxDOTCONNECT

TxDOT delivered an award-winning, web-based application called TxDOTCONNECT to transform the way the agency plans and manages the state's transportation programs and projects.

TxDOTCONNECT replaces approximately 40 disparate legacy systems, including mainframes and interfaces to the agency's data lake and geospatial warehouse to streamline data sharing.

The system is available to 3,500 TxDOT employees and almost 1,000 external partners such as consultants, contractors, vendors, metropolitan planning organizations, local governments, and the Federal Highway Administration (FHWA).

This modern, user-friendly system not only reduced the number of systems and costs, but also provides new functions and reporting capabilities, and improves communication and collaboration among TxDOT teams and external partners.

Texas State Board of Architectural Examiners and Texas State Board of Public Accountancy

Collaborative Approach to Modernization

When the Texas State Board of Architectural Examiners and Texas State Board of Public Accountancy were required to relocate from a state-owned building to a private building, they saw an opportunity for a collaborative approach.

They decided to assess co-location options for their network and servers and established a cooperative agreement.

The process involved coordinating logistics, vendor selection, project management, and establishing the cabling, fiber, and circuit infrastructure needed for secure connectivity and redundancy.

Each agency purchased and relocated more modern servers, assessed data, and inventoried physical assets to better align their information resources with their respective missions.

Together they were able to overcome the challenges of a relocation and modernization effort during a pandemic.

The results were improvements in data management, increased security, and reduced risk.

Texas State University (TXST)

Cloud Migration Enhances Application Performance

TXST moved its Student Information System (SIS), which had been hosted on-premise, to a managed cloud-based hosting environment.

By moving to the cloud, it allowed the university to reduce licensing costs and the need for legacy database administration.

While still in the early stages of being in production in the new environment, TXST is seeing application performance improvement in the cloud environment, less downtime of the system, and less use of in-house resources in maintaining patches and versions of the system.

University of Texas at Austin

Blockchain Improves Identity and Access Management

UT at Austin's Dell Medical School worked with experts from UT-Austin's Information Technology Services (ITS), the Cockrell School of Engineering, and University of Arizona College of Medicine to find a way for patients to securely share their health data.

Using blockchain technology, the group created a decentralized identity management prototype called MediLinker, which provides patients with the ability to share their information from their own blockchain wallet with trusted healthcare providers of their choice on the blockchain.

Next, UT-Austin ITS parlayed this blockchain knowledge to create the Self-Sovereign Identity (SSI) proof of concept, demonstrating authentication to a website using a verifiable credential held in an identity wallet.

This project represents a forward-looking vision for university identity and access management for defining and managing roles and access privileges, and the circumstances in which users are granted (or denied) those privileges.

For users, SSI brings personal autonomy to the internet in a safe and trustworthy system of identity management.

DIR Program Support

DIR's mission 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.

DIR can support and assist agencies to meet the goals outlined in this state strategic plan. This section highlights just a few of the enterprise services DIR provides to promote efficiency and service in state government.

For more information, search for these topics on www.dir.texas.gov or call 1-855-ASK-DIR1.

Bulk Purchase

Desktops, Laptops, Tablets, Software, and Other IT Equipment

DIR leverages the state's purchasing power to negotiate competitive discounts for government entities on information and communications technology products and services.

Bulk purchasing occurs when multiple government entities come together and buy large quantities of technology products.

Bulk purchase initiatives simplify the state agencies' procurement process because purchases made under a DIR bulk purchase agreement are exempted from certain spending limits and thresholds.

Centers of Excellence (CoE)

Texas Cloud Tiger Team, Artificial Intelligence

In 2019, DIR established the Texas Cloud Adoption CoE, also known as the Cloud Tiger Team, to accelerate cloud adoption and acceptance throughout state government.

Through a public-private partnership, the CoE trains agency employees on cloud solutions using real-life use cases.

In 2020, DIR created the award-winning AI-CoE to promote emerging AI technologies that deliver secure, efficient government services to Texans.

The AI-CoE demonstrates how using chatbots, RPA, machine learning, and other advanced technologies can improve government services for the taxpayers of Texas.

Cloud Services

Infrastructure, Platform, Software, Broker, and Assessment Services

For agencies considering cloud services, DIR offers resources to help decision makers evaluate available cloud-smart strategies and proceed with cloud adoption.

When agencies have developed a cloud strategy and are ready to move forward, DIR has several offerings available through DIR's cooperative contracts and shared technology services.

These services include the Texas private cloud with two redundant, resilient, consolidated data centers, and three public cloud service providers as well as other cloud services.

Communications Technology Services and Contracts

VoIP, Internet, Data Plans, Wireless Devices

Texas agencies have access to a portfolio of telecommunication, voice, data, video, wireless, and Internet services at highly competitive prices through DIR enterprise contracts.

The Texas Agency Network (TEX-AN) program provides voice services, data services, internet services, and telecommunications infrastructure for state and local government and institutions of higher education.

DIR provides network security monitoring, alerting, and analysis services to help internet customers protect critical information resources. Network Intrusion Prevention Services (IPS) proactively identifies and blocks known threats to network security.

These services initiate automatically when an agency utilizes DIR-provided internet services.

Data Coordination

Texas Data Program, Texas Open Data Portal, Texas Data Management Framework

The Texas Data Program provides leadership, services, and resources to help agencies develop individual agency data management programs.

The program's primary goals are to improve data governance, provide opportunities for data sharing, and work with agencies to collaboratively establish policies, standards, and best practices.

The Texas Open Data Portal (data.texas.gov) is the state's official repository for open data and promotes government transparency, citizen self-service data participation, and the efficient use of public resources.

The Texas Data Management Framework (TDMF), based on the core principles of the Data Management Association (DAMA) Data Management Body of Knowledge (DMBOK), provides a governance framework for Texas government.

Innovative Procurement Lab (IPL)

Improving Information Technology Procurement and Contracting

DIR established the Innovative Procurement Lab (IPL) to help agencies collaboratively explore different ways to achieve successful contract engagements in compliance with state laws.

This initiative aims to streamline IT procurement processes, increase market engagement, abbreviate upfront requirements, and uncover other innovations for the procurement and contracting process.

The IPL helps customers and the vendor community work together better to improve procurement and contracting for IT solutions across the state.

IT Commodities and Services

Hardware, Software, Seat Management, and Staffing Services

Through the Cooperative Contracts program, DIR leverages the purchasing power of the state by negotiating and administering over 900 contracts with IT providers for products and services.

The Cooperative Contracts program offers computers, software, security offerings, networking and telecommunications equipment, IT staffing services, deliverables-based services, artificial intelligence, technology-based training, and more.

DIR's technology contracts are used as a benchmark across the country for aggressive discounts and exceptional service levels.

IT Education and Guidance

Strategic Planning, Project Management, Digital Accessibility, IRM Continuing Education

DIR facilitates and guides the management of statewide technology through technology strategic planning, policies, standards, guidelines, and procedures.

DIR provides consultation and training on the Project Delivery Framework, best practices, and tips for minimizing risk in IT projects. DIR also assists state agencies to comply with state and federal accessibility requirements.

In addition, DIR provides education, guidance, training, and technical assistance to help agency information resources managers (IRM) navigate state technology laws and meet continuing education requirements.

Online Payment Services

Licenses and Registrations, Permits, and Records

Texas.gov provides payment processing for state agencies and eligible local government organizations that conduct online business with constituents.

The Texas.gov payment solution is a secure, Payment Card Industry (PCI) compliant product that allows customers to process online and over-the-counter payments for services such as licenses and registrations; property taxes and records; permits; and vital records.

Security Services

Leadership, Education, SPECTRIM, Managed Security Services,
Information Security Services, Cybersecurity Framework, TDIS

DIR offers information security products through cooperative contracts and provides targeted information security services.

DIR chairs the Texas Cybersecurity Council, offers a statewide Cybersecurity Framework, and SPECTRIM (Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management) for governance, risk, and compliance management.

Managed Security Services (MMS) include security monitoring, device management, incident response services, threat analysis, and more.

Texas Digital Identity Solution (TDIS) offers streamlined identity verification, risk-based multi-factor authentication, and single-sign on access, allowing Texas government employees to access authorized agency systems easily and securely.

DIR fosters cybersecurity information sharing and certifies cybersecurity awareness training.

Shared Technology Services

Data Center Services, Texas.gov, Managed Application Services,
Managed Security Services, Open Data Portal

DIR's Shared Technology Services (STS) are a set of managed IT services that DIR customers can use to accelerate their service delivery in a reliable, modern, and secure manner.

The program offers a combination of services that can be consumed incrementally to meet individual agency needs.

These services include highly secure public and private cloud solutions, application development and maintenance, managed security services, Texas.gov digital commerce, and more.

STS allows DIR customers to treat IT as a service instead of an internal project.

Strategic Digital Services

Digital Transformation, Digital Maturity, TxT

DIR's Strategic Digital Services program assists agencies with the adoption of digital technology.

The program guides state government to transform manual processes into digital processes, modernize technology, and shift a task-based workforce to a knowledge-based workforce.

It features a digital transformation guide to help agencies understand guiding principles and digital maturity.

In addition, it helps agencies find resources for digital transformation such as Texas by Texas (TxT), a mobile-first digital assistant offering secure digital government services with a single user account and stored payment information.

DIR State Strageic Plan Process Recap

Issued by DIR, the State Strategic Plan (SSP) provides direction to state agencies and institutions of higher education for the use of information technology. The SSP is a five-year rolling plan developed every two years with insights from the technology industry and state, local, and federal government.

The strategic goals outlined in the SSP provide a roadmap for agencies to follow when developing the IT components of their agency strategic plans. Collaboration is a key factor in helping determine the Statewide Technology Strategic Goals.

DIR is required to appoint an advisory committee that consists of representatives from state agencies, institutions of higher education, the public, local government, industry, and the federal government. Through a collaborative, facilitated discussion, the appointed advisory committee discusses the technology trends affecting agencies now and in the next two to five years, the ideal technology environment, and strategies to address those technology trends as the state moves toward the ideal environment.

DIR surveys chief executive officers (CEOs), chief information officers (CIOs), and information resource managers (IRMs) in state agencies and institutions of higher education and consults with multiple stakeholders and subject-matter experts to help narrow the focus areas of the SSP.

In addition, DIR conducts in-depth research and analysis of top technology trends and priorities impacting both government and the private sector around the country to determine the final statewide technology strategic goals to address in the SSP.

Once the plan is finalized, it is sent for review and approval by DIR's Board of Directors. The SSP must be delivered to state leadership by November 1.

Acknowledgements

DIR appreciates the valuable input provided by agency information resources managers, practitioners, and executives in the development of this plan.

DIR also thanks its program staff for their support and expertise.

The 2022-2026 State Strategic Plan for Information Resources Management Advisory Committee was appointed by DIR's governing board on January 28, 2021.

DIR wishes to thank the committee for their leadership, time, and commitment to this project.

Glossary of Terms

Agile. A method of project management used especially for software development, that is characterized by the division of tasks into short phases of work and frequent reassessment and adaptation of plans.

Agile Procurement. An iterative approach that leads to best value awards in shorter periods by developing the solicitation in a series of sprints to have vendor demonstrations and discussions throughout the procurement phase.

Anything as a Service (XaaS). Array of cloud-based services or applications that are accessed on demand or on a subscription basis.

Artificial Intelligence (AI). The use of computers to emulate human (natural) intelligence such as knowledge representation, planning, learning, problem solving, reasoning, natural language processing, and observation. AI maybe used to assist with forecasting, decision making, automation, and translation in order to optimize tasking traditionally performed by humans and increased productivity and efficiency. AI is an umbrella term that encompasses a wide variety of technologies, methods, and platforms to accomplish these tasks.

Autonomics/Autonomous and Semi-Autonomous Things. Self-managing technologies that operate independently or with limited human oversight to perform activities within a complex system including drones, smart-machine technologies, mobile robots, and autonomous or semi-autonomous vehicles.

Blockchain. Transactional records shared by participants in a network that are cryptographically signed with irrevocable exchanges of value including virtual currency, digital assets, and smart contracts.

Business Continuity Plan (BCP). A process resulting in a document that identifies an organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization.

Case Management as a Service. A modular and interoperable approach to the design and development of cloud-based case management solutions as digital products.

Center of Excellence (CoE). A team of skilled knowledge workers whose mission is to provide the organization they work for with best practices around a particular area of interest. The concept of creating special-interest groups for thought leadership originated in lean manufacturing.

Chatbot. A form of Artificial Intelligence software that is used to conduct an on-line chat conversation via text or text-to-speech, in lieu of providing direct contact with a live human agent.

Cloud. On-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.

Cloud Services. Storing, managing, and accessing data over a public or private network.

Collaboration Tools. Software that enables collaboration through a shared network or online solutions including workstream and content collaboration tools with channels, chat features, audio/video calls, and shared documents.

Connectivity. Ability to interconnect platforms and systems including enterprise networking, broadband, 5G services, and enhanced internet services.

Continuity Plans. Plans, procedures, training, and exercises that ensure a government organization can continue to perform its essential functions during the disruption of normal operations.

Customer Experience (CX). Strategies that consider a customer's perceptions and feelings toward an organization based on the sum of all digital experiences that the organization provides.

Cybersecurity. Securing and protecting government and citizen information.

Data Analytics. Using data to inform planning, provide business intelligence, and enhance decision-making including predictive, prescriptive, and operationalized analytics.

Data Governance. Practices and processes to ensure the formal management of data assets within an organization including the establishment of roles such as data officers.

Data Management Tools. Technologies for data management strategies that put organizations in control of their business data, including the practice of classifying, storing, and terminating data.

DevOps. An enterprise software development phrase, short for Development and Operations, used to mean a type of agile relationship between development and IT operations. The goal of DevOps is to change and improve the relationship by advocating better communication and collaboration between these two business units.

Digital Accessibility. Digital services providing electronic information and services through multiple ways so that communication is not contingent on a single sense or ability.

Digital Transformation. The adoption of digital technologies to create new or improve existing processes, services, and customer experiences.

Edge Computing. A computing environment in which information processing, content collection, and delivery are placed closer to the sources and repositories of this information.

High-Value Dataset. Information that can be used to increase state agency accountability and responsiveness, improve public knowledge of the agency and its operations, further the core mission of the agency, create economic opportunity, or respond to need and demand as identified through public consultation. The term does not include information that is confidential or protected from disclosure under state or federal law.

Hyper-automation. Combination of tools such as AI, machine learning, and robotics process automation that the public sector can use to support enterprise initiatives for seamless access to public services.

Identity and Access Management (IAM). A broad administrative area that establishes a unique identity for individuals and associates their established identity with user rights and privileges. It is an enterprise business strategy that governs the definition, storage, use, and management of identities.

Incident Response. The mitigation of violations of security policies and recommended practices.

Integration. Making independently designed applications and data work well together.

Internet of Things (IoT). Network-connected objects that can send and receive data.

Glossary of Terms (continued)

IT-as-a Service (ITAAS). An operational model where the information technology (IT) service provider delivers an IT service to a business. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for limited user-specific application configuration settings.

Legacy Systems. A computer system or application program that is operated with obsolete or inefficient hardware or software technology.

Low-code Development. Development platform that provides a development environment used to create application software through a graphical user interface instead of traditional hand-coded computer programming.

Machine Learning (ML). Machine learning is the study of computer algorithms that improve automatically through experience. It is seen as a subset of artificial intelligence.

Mobile Applications. Computer programs or software applications designed to run on a mobile device such as a phone, tablet, or watch.

Multi-factor Authentication (MFA). A security enhancement in which a technology user must provide two or more pieces of evidence to log into an account or access a system including factors such as a password, a device assigned to the user, or biometrics.

Next-Generation Application Development. The development of scalable, reliant applications that meet broad business objectives using tools and techniques like low-code development platforms, containerization, and microservices.

No-code Development. Development platform that allows programmers and non-programmers to create application software through graphical user interfaces and configuration instead of traditional computer programming.

Open Data. Providing public access to data in standardized and easily usable formats.

Open Data Portal (ODP). In Texas, the official central repository of publicly accessible electronic data for the State of Texas for data that can be freely used, re-used, and redistributed by anyone.

Open Source Software. Software with its source code made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose.

Predictive Analytics. An approach to data mining with an emphasis on: predication, rapid analysis, business relevance, and ease of use.

Privacy (Digital/Data). The practice of identifying, securing, and managing personal data in digital and online mediums in a manner that aligns with customer expectations for security and confidentiality.

Project Management. A system of procedures, practices, and technologies that provides the planning, organizing, staffing, directing, and controlling necessary to successfully manage a project.

Remote Work. An alternative workplace arrangement in which employees do not commute or travel to a centralized place of work, such as an office building, warehouse, or store.

Responsive Design. A graphic user interface design approach that adjusts smoothly to various screen sizes such as a computer monitor screen or mobile device.

Robotic Process Automation (RPA). A digital enablement technology that predominantly leverages a combination of user interface and surface-level features to create scripts that automate routine, predicable data transcription work. In other words, it is a rules-based technology that uses software to automate repetitive tasks normally performed by humans to improve processes and gain efficiencies.

Security Enhancement Tools. Automated technology installed on endpoints to prevent and detect malicious actions, including user or entity behavioral analytics, multi-factor authentication, endpoint detection and response, and host intrusion prevention or protection systems.

Security Operations Centers (SOC). A centralized function for an organization or enterprise employing people, process, and technology to continuously monitor, prevent, detect, analyze, and respond to cybersecurity incidents.

Shared Technology Services. Technology provided through a shared, collaborative governance model. Statewide shared services available through DIR's Shared Technology Services include data center, managed security, managed applications, and Texas.gov e-commerce portal.

Software-defined Solutions. Technology solutions delivered as software, such as software-defined storage and networking, and infrastructure as a service; includes the ability to use virtualized compute, storage, networking and cloud management for data centers, local area networks, wide area networks, and more.

Texas by Texas (TxT). A secure, centralized, mobile-first application to conduct business with multiple Texas government entities that provides users with the ability to create an account, verify their identity once, and establish a profile with their name, address, and payment information.

User-Centric Design. An iterative design process using a mixture of investigative and generative methods to understand users' needs.

Virtual Reality/Augmented Reality. Virtual reality is a computer-generated simulation or recreation of a real-life environment or situation. Augmented reality is computer generated enhancements to existing reality with ability to interact with it.

Workforce Management Tools. A collection of technologies that bring together core human resources capabilities of evaluation and improvement; time management; metrics and recognition; assistance and task management; and recruiting and onboarding.

Zero-Trust. Term for an evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources.

DIR

Texas Department of Information Resources

300 West 15th St., Suite 300, Austin, TX 78701
1-855-ASK-DIR1 | dir.texas.gov | @TexasDIR | #DIRisIT