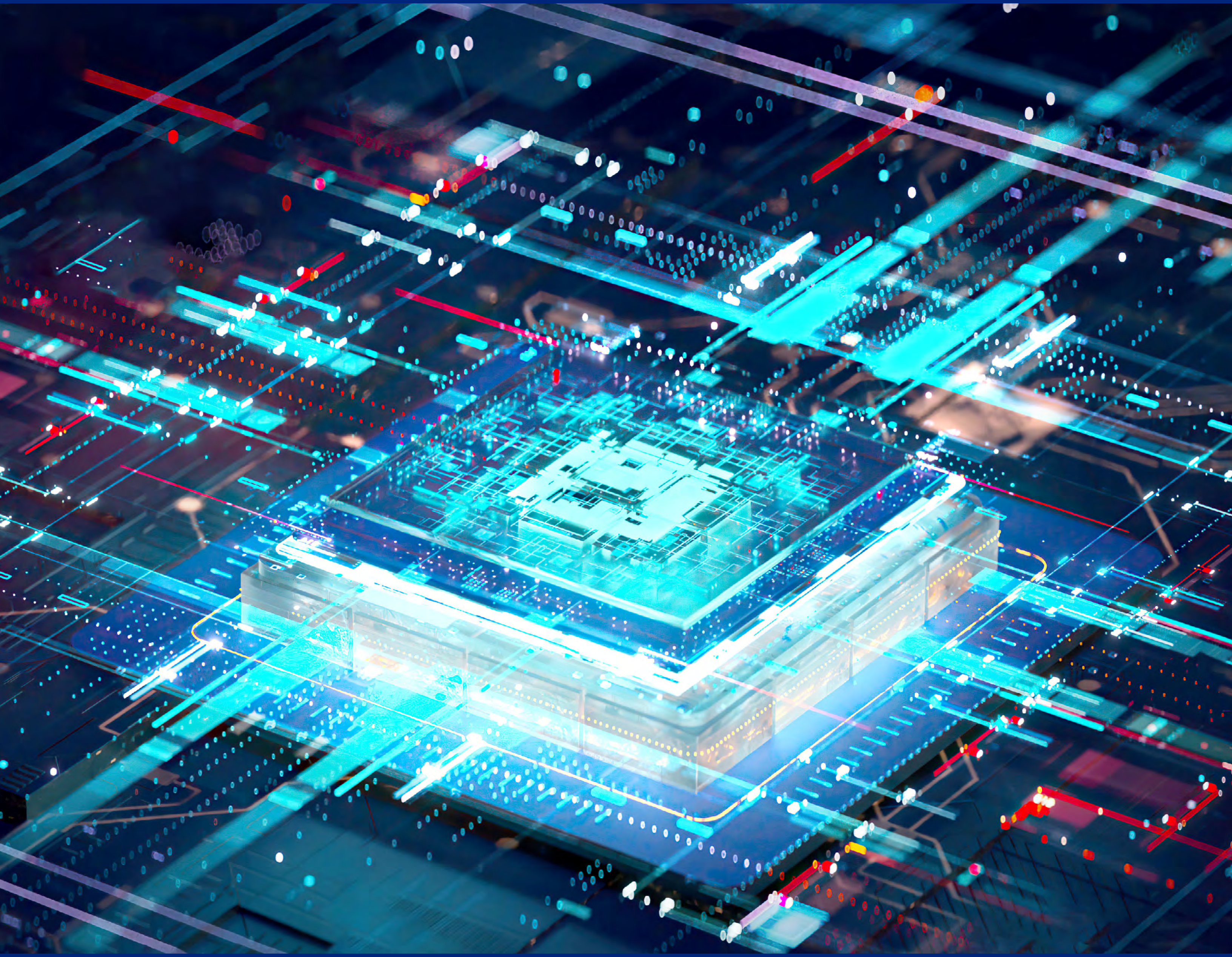
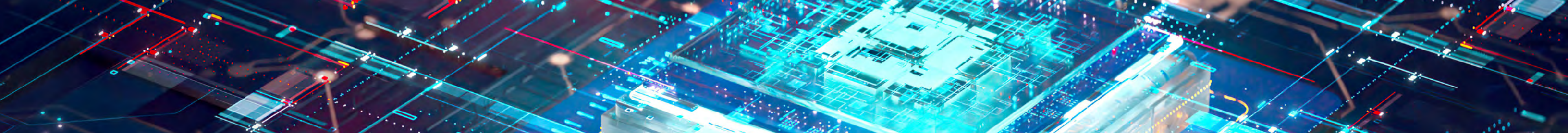
2022 Biennial Performance Report



Accelerating the Next Generation of Technology in Texas



About the 2022 Biennial Performance Report

The Information Resources Management Act, Government Code Chapter 2054, requires the Texas Department of Information Resources (DIR) to prepare and submit to the Governor and the Legislature a biennial performance report on the use of information resources technologies by state government.[1] For purposes of this report, the terms "technology" and "information technology" (IT) include information and communications technology.

DIR compiles this report using state agencies and institutions of higher education (IHE) responses to the 2022 Information Resources Deployment Review (IRDR) that is required by Government Code Section 2054.0965. Most questions in the IRDR are optional for IHEs pursuant to Government Code Section 2054.1211. Since few IHEs respond to these optional questions, the information included in this report is based primarily on responses from approximately 80 state agencies.

All information included in this report is from the IRDR unless otherwise noted.

[1] Government Code Section 2054.055

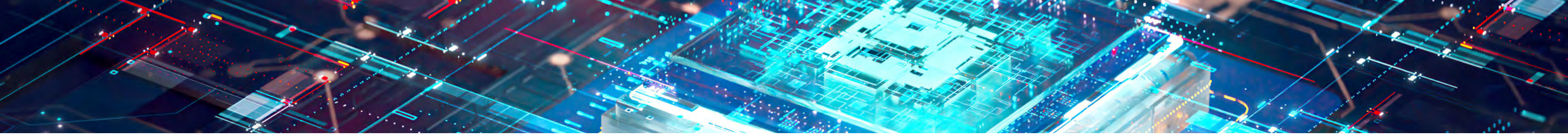
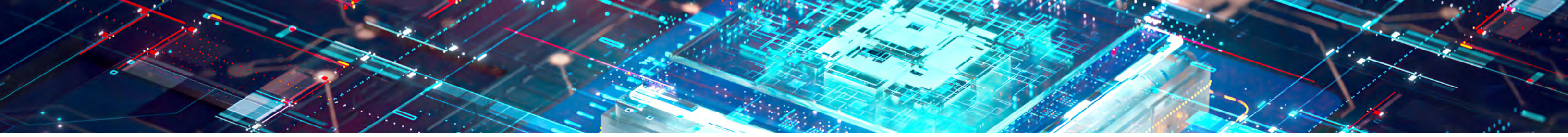


Table of Contents



Letter from the Executive Director

Governor Abbott, Members of the Legislature, and Texas IT Leaders,

In an ever-changing technology landscape, the State of Texas is at the forefront of bringing the next generation of technology to its state agencies and Texas residents. More than ever before, the importance of technology and the people who enable it are critical to the state's mission. State agencies must be prepared to evolve with the changing needs of Texans and proactively plan for and invest in technology that transforms how Texas government serves Texans.

The Texas Department of Information Resources (DIR) is pleased to present the 2022 Biennial Performance Report (BPR) on the use of information resources technologies by state government. DIR produces the BPR to report agencies' progress toward the four strategic technology goals defined in the 2022-2026 State Strategic Plan for Information Resources Management. The report also shares agency success stories, highlighting technology accomplishments that align with these goals.

Goal 1: Secure IT Service Delivery

Goal 2: Advanced Data Management

Goal 3: Strategic Digital Transformation

Goal 4: Proactive Approach to Emerging Technologies

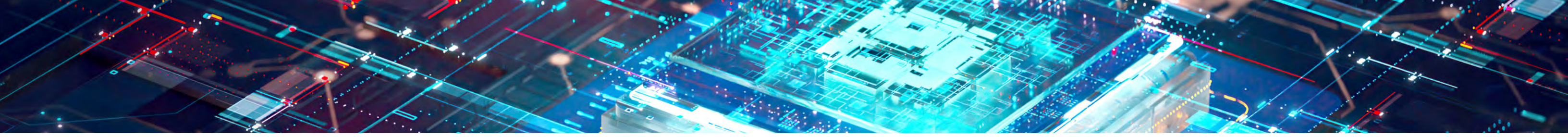
Over the past biennium, Texas government exhibited significant progress in delivering secure, innovative technology that makes government more efficient, effective, transparent, and accountable. Texas agencies are planning for and implementing solutions that modernize Texas government services. To facilitate these efforts, this report includes recommendations for legislative considerations to help state agencies prepare for the next generation of technology in Texas.

Through collaboration with agency technology leaders and with the support of the legislature, the State of Texas will continue to be a national leader in delivering a secure, digital government through well-designed, innovative, and efficient technology solutions.

Sincerely,

Amanda Crawford

Amanda Crawford
Executive Director, Texas Department of Information Resources
Chief Information Officer, State of Texas



Introduction

State agencies are committed to serving Texans by providing high-quality, convenient, and reliable access to government information and services. The COVID-19 pandemic significantly accelerated digital transformation in state government, fundamentally changing the way agencies operate and deliver services to Texans. It is important to understand these changes and to assess the current state of use of information technology resources by government agencies.

This report addresses the progress over fiscal years 2021 and 2022 toward the four technology goals defined in the 2022-2026 State Strategic Plan for Information Resources Management. It highlights state agency technology accomplishments, identifies concerns, and makes recommendations for improving the cost effectiveness and efficiency of the state's use of information resources. The BPR also includes supplemental reports on specific technology issues as required by Government Code Chapter 2054.

Summary of Recommendations

Require local governments and school districts to report cybersecurity incidents to DIR within a minimum reporting timeframe.

Enable private sector peer-to-peer (P2P) payment solutions commonly used by the public to provide additional payment methods for government services.

Require government entities to utilize the standardized ".gov" domain suffix when establishing a new domain name to reduce website spoofing.

Enable broader access to digital government services, streamlined processes, and digitization by expanding the use of digital signatures.

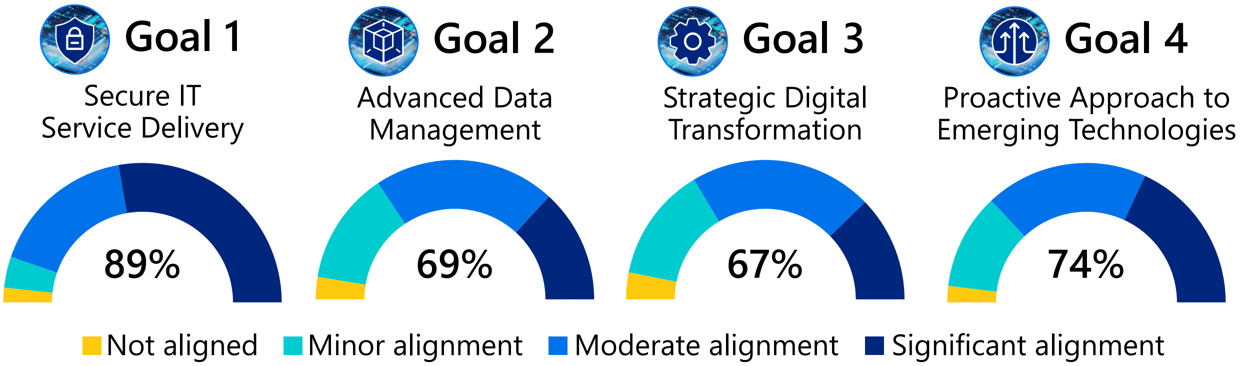
Allow state agencies and institutions of higher education (IHE) to designate a joint information security officer (ISO).

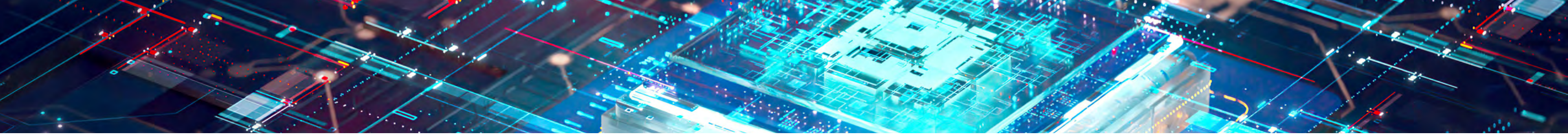
Provide guidance for distributed ledger and blockchain technology best practices.

Establish a statewide Chief Privacy Officer to provide a central point of contact on data privacy matters.

Progress Snapshot

Over half of the state agencies responding to the IRDR reported moderate to significant alignment with the goals identified in the 2022-2026 State Strategic Plan.



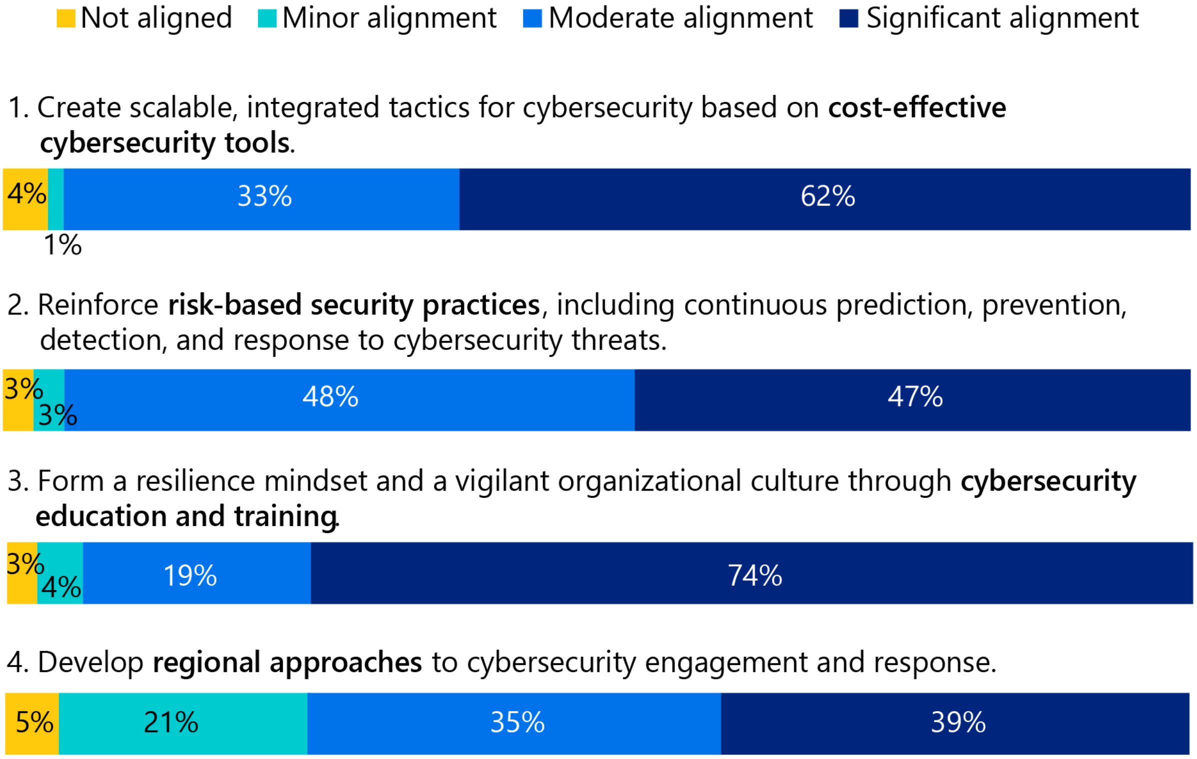


2022-2026 State Strategic Plan
Goal 1: Secure IT Service Delivery

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

The 2022-2026 State Strategic Plan identifies four objectives to help guide state agency efforts to minimize security risks to technology and evolve cybersecurity practices. Desired outcomes for agency alignment with the IT security objectives below include mature, risk-based security programs; cybersecurity-aware organizations; on-going investment in cybersecurity staff; reduced exposure to cyberattacks; and regional approaches to preparedness that build resilience.

Agency Alignment to Secure IT Service Delivery Objectives



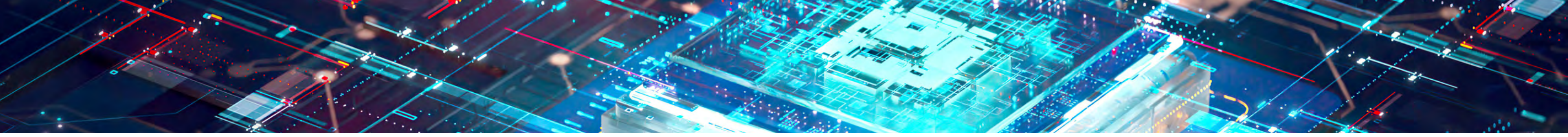
1. Create scalable, integrated tactics for cybersecurity based on **cost-effective cybersecurity tools**.

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

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

4. Develop **regional approaches** to cybersecurity engagement and response.

Source: 2022 IRDR. May not equal 100% due to rounding.

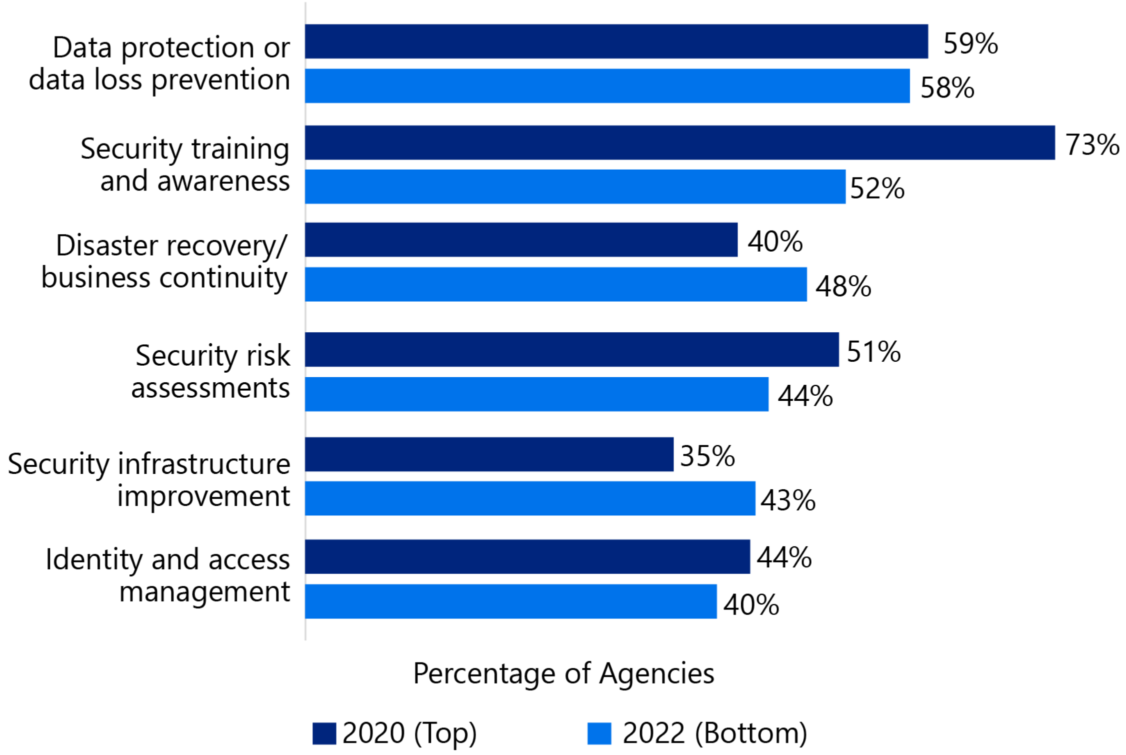


Assessment

The State of Texas has made great strides to address complex cyber threats targeting the public sector. To continue this progress, state agencies must evolve cybersecurity practices and identify security priorities specific to their agencies' missions.

State agencies identified data protection, security training, and disaster recovery among their top security initiatives for the next biennium.

Figure 1: Top Security Initiatives for the Next Biennium



Source: 2022 IRDR.

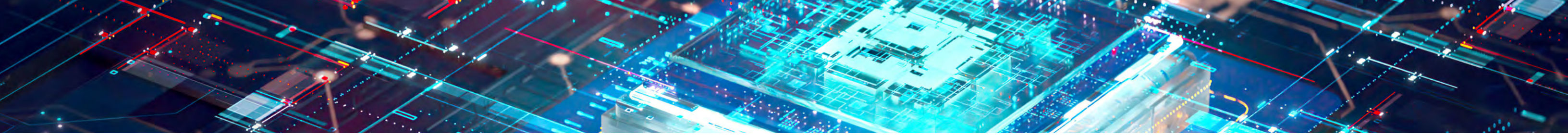
Agencies must have mature, risk-based cybersecurity programs to protect against increasingly sophisticated cyber threats. In 2022, state agencies are showing progress in the following areas.

98% are remediating unsupported software

79% use MFA on all or most systems

58% Executive Director always signs off on security risks

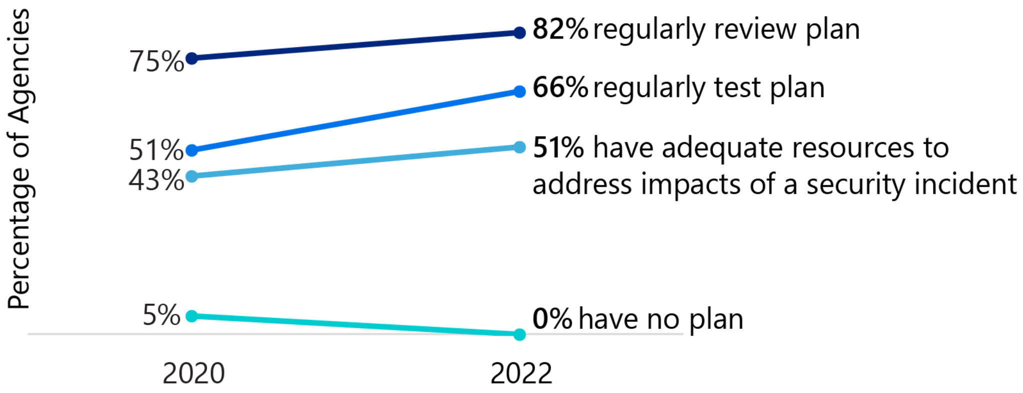
53% integrate security into all third-party contracts



When cybersecurity incidents, natural disasters, pandemics, or other events disrupt IT systems, organizations must respond quickly. Because Texas covers more than 268,000 square miles, regional approaches can help facilitate the rapid restoration of government operations and services.

State agencies reported that they are prepared to respond to and recover from a security incident with 82% of agencies indicating they regularly review or revise their security incident response plans. Furthermore, over half of agencies say they have adequate resources to address the impacts of a security incident. Importantly, all state agencies now have security incident response plans in place; many of these entities are reviewing and testing them regularly – some as often as every six months.

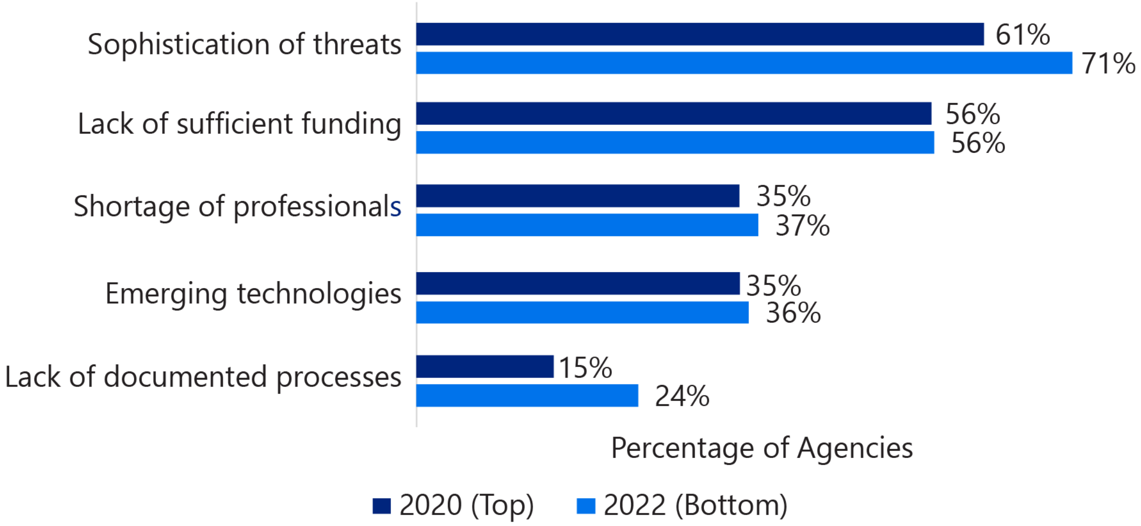
Figure 2: Security Incident Response

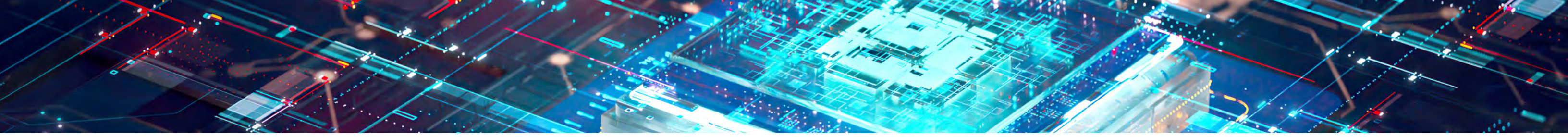


Concerns

Agencies reported the same top five barriers to addressing security issues in 2022 as they did in 2020. The increasing sophistication of threats remains the top issue, with approximately 10% more agencies identifying this as a barrier than in 2020, followed by a lack of sufficient funding and a shortage of cybersecurity professionals. More agencies also reported a lack of documented processes as one of their top barriers.

Figure 3: Top Barriers to Cybersecurity





Recommendations

The Texas Legislature prioritized cybersecurity in the 87th Legislative Session by funding new initiatives and passing forward-thinking legislation to improve the state's cybersecurity posture. The bills passed created regional security operations centers, professional and volunteer cybersecurity incident response teams, the Texas Risk Authorization and Management Program for cloud computing services, and expanded security awareness training.

For the next biennium, DIR recommends that the legislature consider the following actions:

1 Require local governments and school districts to report cybersecurity incidents to DIR within a minimum reporting timeframe.

Sharing information is essential for protecting public sector assets, personal or sensitive information, and critical infrastructure. State agencies and institutions of higher education are required to report certain types of security incidents to DIR within a minimum timeframe, preferably within 24 hours.

Currently, state agencies and institutions of higher education report suspected cybersecurity incidents, including breaches and ransomware attacks, to DIR. School districts report cybersecurity incidents to the Texas Education Agency and county election officials are required to notify the Secretary of State. Also, Texas law does not set a standard timeframe for local governments to report cyberattacks.

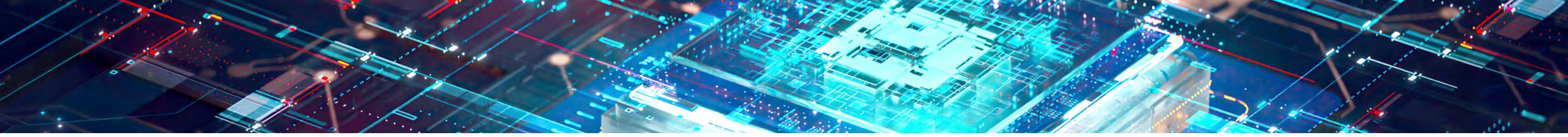
This incongruent reporting of cybersecurity incidents may hinder Texas in tracking trends and understanding the scope and complexity of cyberattacks as well as how they may be related to another cyberattack. By requiring municipalities, school districts, and counties to report cybersecurity incidents to DIR, the state will have a more complete picture of potential threats and may be able to prevent future attacks, avoiding costly response and recovery efforts.

2 Require government entities to utilize the standardized ".gov" domain suffix when establishing a new domain name to reduce website spoofing.

Cybercriminals are known to impersonate legitimate government websites, commonly called spoofing, to disseminate false information; harvest credentials; collect personal information; and spread malware. These activities can lead to system or account compromise and potential financial loss. There have been many examples of this in Texas and nationally.

To stop these malicious actors from setting up websites impersonating government entities, the federal government and security industry experts recommend that government entities use the top-level domain ".gov" to enhance public trust while digitally interacting with their government.

Acquiring a .gov web domain requires that the domain applicant submit evidence to an official government entity confirming they are buying the domain name on behalf of a legitimate local, county, or state government entity.



The .gov domain is only available to US government entities including state agencies, cities, counties, towns, and independent school districts, so visitors to these sites can trust it is the entity it is reporting to be.

Requiring Texas government entities to use the .gov domain for their official websites could decrease the likelihood of Texans falling victim to online attempts to defraud or harm while attempting to digitally interact with their government.

3 Allow state agencies and institutions of higher education (IHE) to designate a joint information security officer.

Information security officers (ISOs) play a vital role in protecting state government assets and information. A nationwide shortage of skilled cybersecurity professionals hinders the public sector's ability to recruit and retain people with the specialized skills and certifications needed for the ISO role. This is particularly challenging for smaller government entities with few full-time equivalent (FTE) positions and limited resources.

Section 2054.136 of the Government Code requires each state agency and IHE to designate an ISO who reports to the agency's executive-level management; has authority over information security for the entire agency; possesses the training and experience required to perform the duties required by department rules; and to the extent feasible, has information security duties as the officer's primary duties. Section 2054.136 does not permit agencies or IHEs to designate a joint ISO as a shared resource.

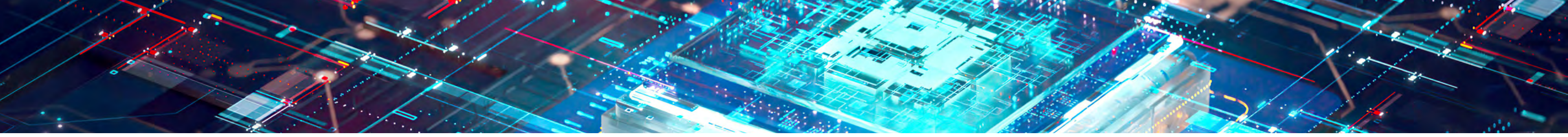
Permitting state agencies and IHEs to designate a joint ISO that is employed by one organization and simultaneously serves as the ISO for two or more designating entities will provide cost-effective, resource sharing that benefits smaller agencies and IHEs. This is also consistent with the provision for joint information resources managers (IRM) under Section 2054.071(b).

Highlights of Agency Accomplishments

The following examples of agency accomplishments demonstrate how implementing a cloud security strategy, a zero-trust environment, and regional approaches to security services and incident response enable the public sector to keep Texans' sensitive information and data secure.

Texas Higher Education Coordinating Board (THECB) – Cloud Security Strategy

The THECB security team established a robust and reliable cloud security strategy to protect the privacy and security of confidential data pertaining to higher education. The strategy consists of three main work streams including developing a roadmap with actionable steps toward zero-trust security, enhancing security modernization by migrating to a secure cloud platform, and adopting a cloud-native security information and event management solution.



Texas Department of Banking (DOB) – Zero-Trust Implementation

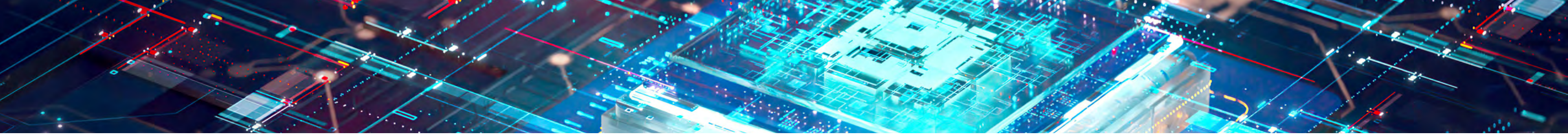
In December of 2020, DOB implemented cloud services in a zero-trust environment for all utility, file, and virtual private network (VPN) services. Zero-trust is a cybersecurity paradigm that focuses on users, data, and assets, rather than a network or perimeter-based approach. Establishing a zero-trust environment has strengthened the agency's security posture and resulted in improved redundancy, increased availability, and performance improvements of public-facing services.

Texas Department of Information Resources (DIR) and Angelo State University – Regional Security Operations Center (RSOC)

In April 2022, DIR selected Angelo State University as the Regional Security Operations Center (RSOC) pilot program to provide security services and incident response to public-sector entities in the region.

The RSOC will offer network security infrastructure that local governments can utilize and give university students hands-on experience to strengthen the cybersecurity workforce of tomorrow. The RSOC may also provide real-time network security monitoring; network security alerts; incident response; and cybersecurity educational services. Eligible customers include counties, local governments, school districts, water districts, hospital districts, and regional state agency offices.

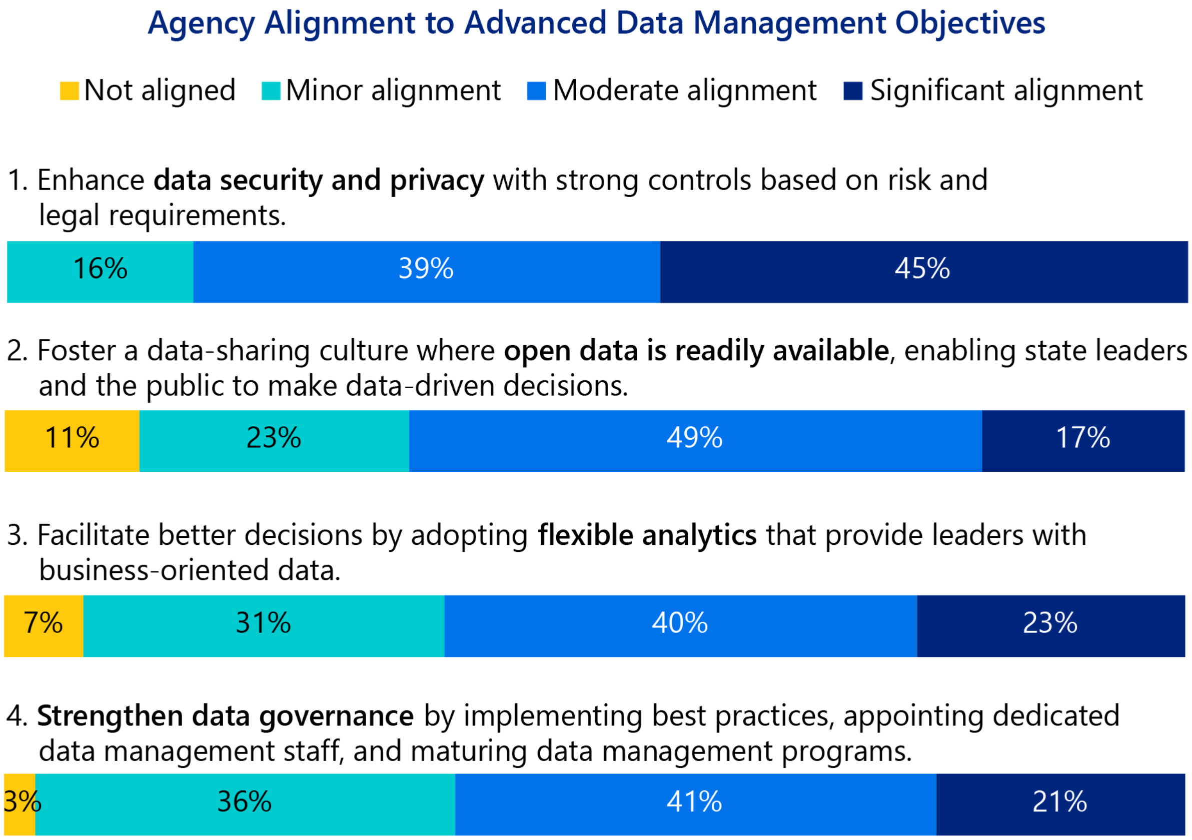
Government Code Section 2059.204 directs DIR to partner with a Texas public institution of higher education to establish this first RSOC as a pilot program. Long-term, it authorizes DIR to partner with additional public universities to establish RSOCs throughout the state to serve local entities and assist in protecting the state from cyber threats.



2022-2026 State Strategic Plan
Goal 2: Advanced Data Management

In the process of providing services to Texans, state agencies collect, create, and manage large amounts of data that must be diligently protected and guarded against misuse.

The 2022-2026 State Strategic Plan identifies four objectives to guide state agencies in developing a strong data governance program that balances privacy and security with information sharing and data analytics. Desired outcomes for agency alignment with the data management objectives below include data that is readily available for decision-making; high-value, publicly available data assets; strong data privacy practices and controls; mature data governance; broad data literacy; and meaningful data metrics to measure progress.



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

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

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

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

Source: 2022 IRDR. May not equal 100% due to rounding.

Assessment

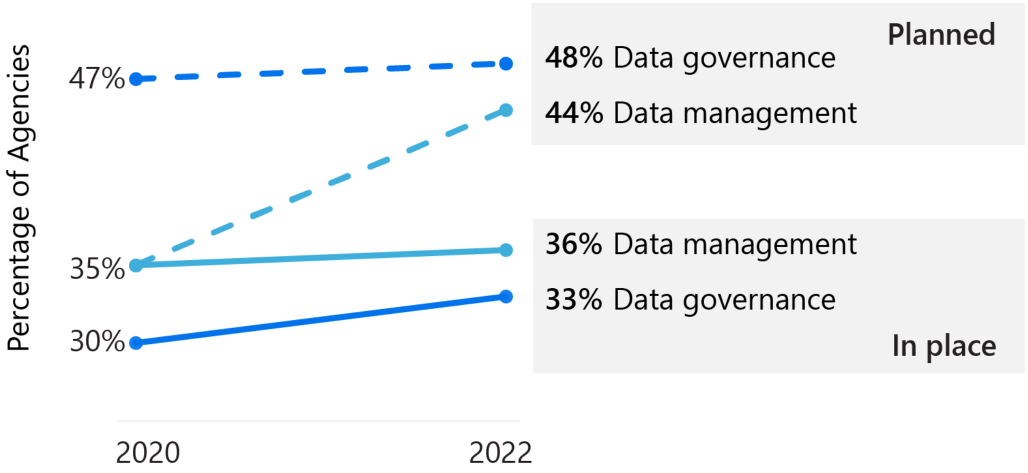
The 87th Legislature acknowledged the need to accelerate data security, sharing, and transparency by passing legislation that established a data management advisory committee and requires state agencies with 150 or more full-time employees to designate a data management officer.

Agency data management officers are responsible for establishing a data governance program for their agency, coordinating with the state's Chief Data Officer and key agency personnel, and posting at least three high-value data sets on the Texas Open Data Portal. As of July 15, 2022, DIR's Office of the Chief Data Officer reports that 59% of the 107 state agencies required to appoint a data management officer have done so.

Data distributed over many departments can make implementing strong data governance and best practices challenging. Yet strong data governance is vital for helping state agency employees understand how to use, share, manage, and dispose of data properly.

Most agencies reported they have or are planning to have a data governance structure and a data management program that oversees the data life cycle including the collection, classification, use, and disposal of agency data.

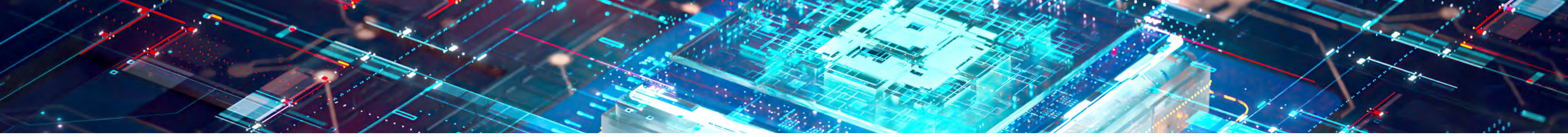
Figure 4: Data Management and Governance



Open data in government is important for public access, oversight, and trust. It can reduce fraud, waste, and abuse while increasing transparency. Open data also gives Texans access to public information without needing to formally request information from a governmental body[3] under the Texas Public Information Act.

State agencies can foster a data-sharing culture by making open data easy to find and access on their website or through the Texas Open Data Portal at www.data.texas.gov.

[3] Government Code Section 552.003(1)



675

As of July 31, 2022, 26 agencies self-reported they have published 675 high-value data sets on the Texas Open Data Portal, a 35% increase from September 1, 2021.

$3.1 million

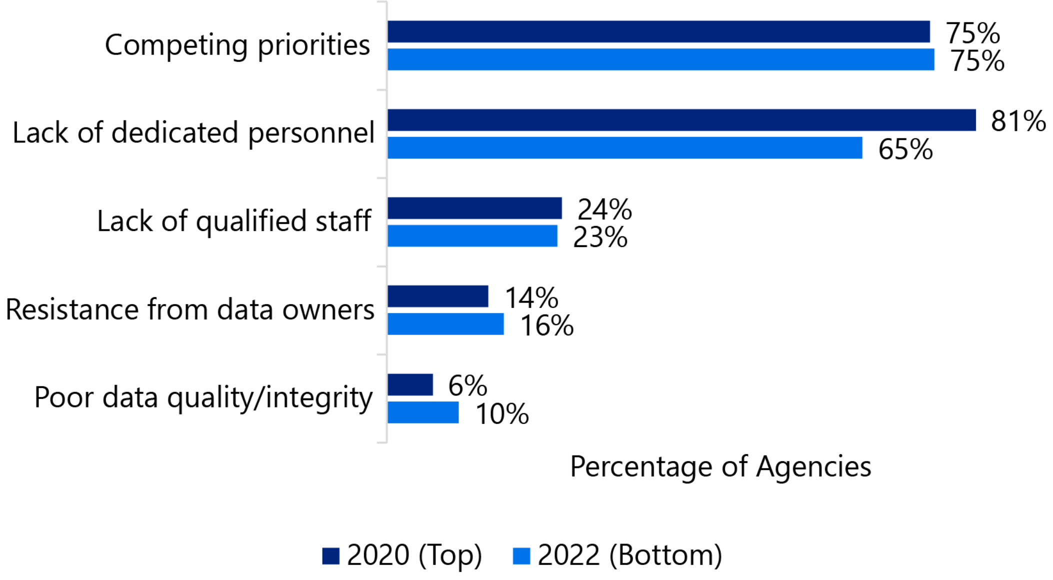
The Texas Chief Data Officer estimates this provides an estimated $3.1 million in opportunity cost savings through public information request reductions.[4]

A strong data analytics program can transform how an agency does business by providing insight for agency decision-makers into processes and operations. Agencies responding to the IRDR indicated that they are making progress, with 58% of agencies reporting they have business intelligence or analytics capabilities in 2022. This is up slightly from 56% in 2020.

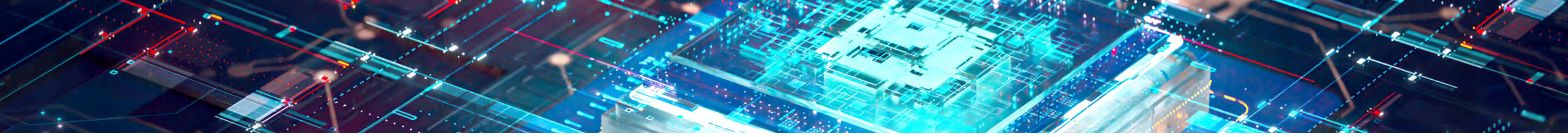
Concerns

State agencies understand the value and importance of strong data governance. Yet, agencies reported that competing priorities and a lack of dedicated or qualified personnel continue as significant barriers in implementing a data management and governance program.

Figure 5: Top Barriers to Data Management and Governance

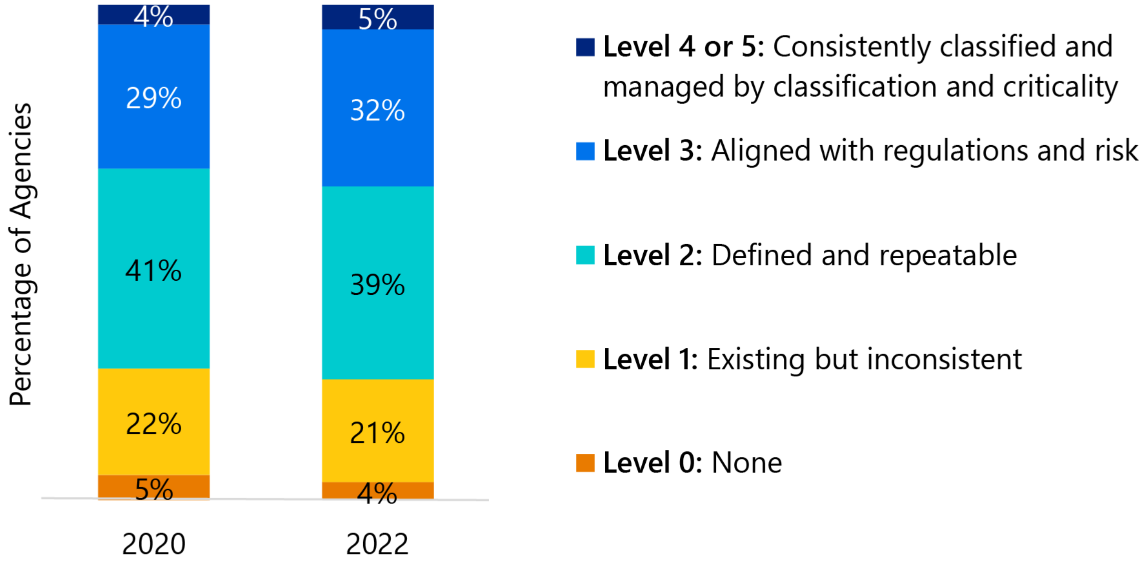


[4] Estimate is based on the assumption that 30% of the total data views and downloads were a result of a public information request redirect to the OPD for the 26 agencies currently publishing on the Texas Open Data Portal.



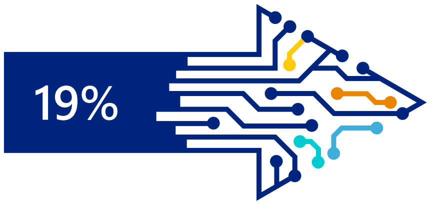
Agencies need a data-literate workforce that manages data throughout its entire lifecycle to identify and protect confidential and sensitive data. Data classification is essential to applying the proper controls. In Texas, state agencies are required to establish an information classification policy. This policy must follow the minimum standards established by federal and state law. Agencies reported little progress in data classification maturity since 2020 with only five percent of agencies indicating they consistently classified and managed data by classification and criticality.

Figure 6: Data Classification Maturity



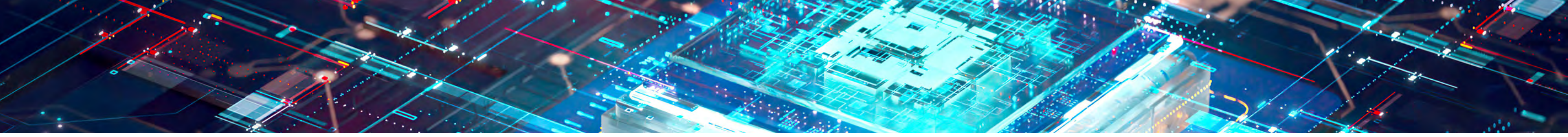
Understanding the maturity of data governance helps agencies move toward data-driven policy goals. Of the agencies responding to the IRDR:

reported they have not assessed their agency's data governance maturity



reported they have established data-driven policy goals

Over the next biennium, there will likely be improvements as state agencies implement Senate Bill 475 and designate a data management officer that oversees the agency's data governance and management.



Recommendations

The 87th Legislature supported advanced data management efforts by passing comprehensive data security and management legislation that strengthens the state’s standards on agencies’ data management practices.

For the next biennium, DIR recommends the following actions to further advance data management practices at Texas state agencies.

1 Establish a statewide Chief Privacy Officer to provide a central point of contact on data privacy matters.

To provide government information and services, the State of Texas collects, uses, and manages vast amounts of personal, financial, and health information from residents. Like every other state in the nation, Texas has a top cybersecurity official focused on identifying, preventing, detecting, and responding to information security and cyber threats. Now more than twenty states also have a statewide role to ensure the privacy of residents’ personal information is protected as well.

Establishing a state chief privacy officer role will provide a central point of contact for state agencies on legal and policy matters involving data privacy. The duties may include a biennial privacy review and resources for implementing best practices throughout Texas government.

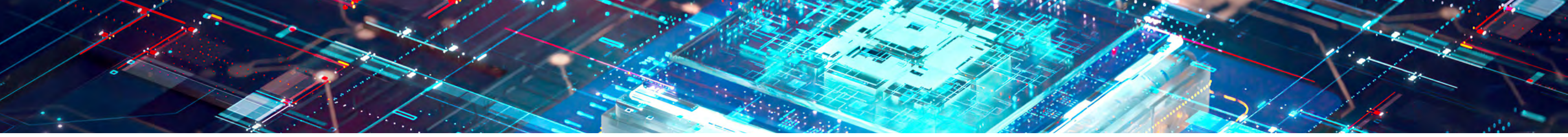
Establishing a state privacy officer would help government employees improve practices for the collection, use, and storage of personal, sensitive, or regulated data. The role would also educate Texas consumers about the use of their personal information on mobile and digital networks and steps they can take to help protect this information.

Highlights of Agency Accomplishments

Texas government entities are making progress toward data management goals and objectives. The following examples of agency accomplishments demonstrate how hyperconverged infrastructures, modern data management platforms, and utilizing the Texas Open Data Portal are helping state agencies to excel in providing innovative delivery of government services.

The University of Texas at San Antonio (UTSA) – Hyperconverged Infrastructure Implementation

UTSA’s University's Technology Solutions delivered a hyperconverged infrastructure for research to transform and empower the university’s research community and innovation ecosystem. This platform provides scientific gateways to researchers, educators, and students, and arises from the new comprehensive cybersecurity data management plan that serves as the foundation for all research produced at UTSA. This comprehensive, resilient, flexible, and efficient IT infrastructure platform meets or exceeds standards set by federal agencies and serves one main goal: to reduce the time it takes to conduct and present research.

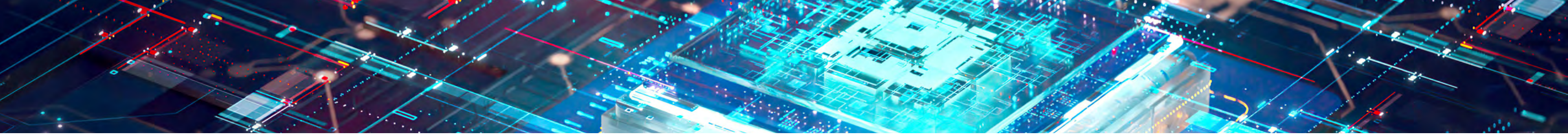


Texas Department of State Health Services (DSHS) – State Health and Analytical Reporting System

DSHS established the State Health Analytics and Reporting Platform (SHARP), a single unified enterprise platform for DSHS public health analytics, reporting, data management, data exchange, and data sharing. The improved capabilities provided by the SHARP platform include infrastructure capacity capable of scaling to address long-term analytical and reporting; the ability to securely share COVID-19 data with local health entities; significantly improved performance of statistical analysis; and a way to monitor and secure the movement of sensitive data within and outside the platform. Additionally, the SHARP platform provides enough capacity to address the known near-term and long-term data management and data processing needs of the agency. It provides standards-based data exchange capability that enables real-time data exchange between various point-of-care facilities and DSHS.

Texas Department of Agriculture (TDA) – Use of the Open Data Portal

TDA joined multiple state and local governments in adding their most requested data to the Texas Open Data Portal (ODP). These datasets are accessible to the public on the data.texas.gov home page and exportable to Excel-compatible files. Groups participating in federally funded nutrition assistance programs provide TDA with required information using the Texas Unified Nutrition Program System. TDA provides a dashboard that displays the number of meals and snacks approved for reimbursement for the current program year for school nutrition programs, child and adult care food programs, and summer meal programs. The dashboard is updated daily and based on meal reimbursement datasets published on the ODP.

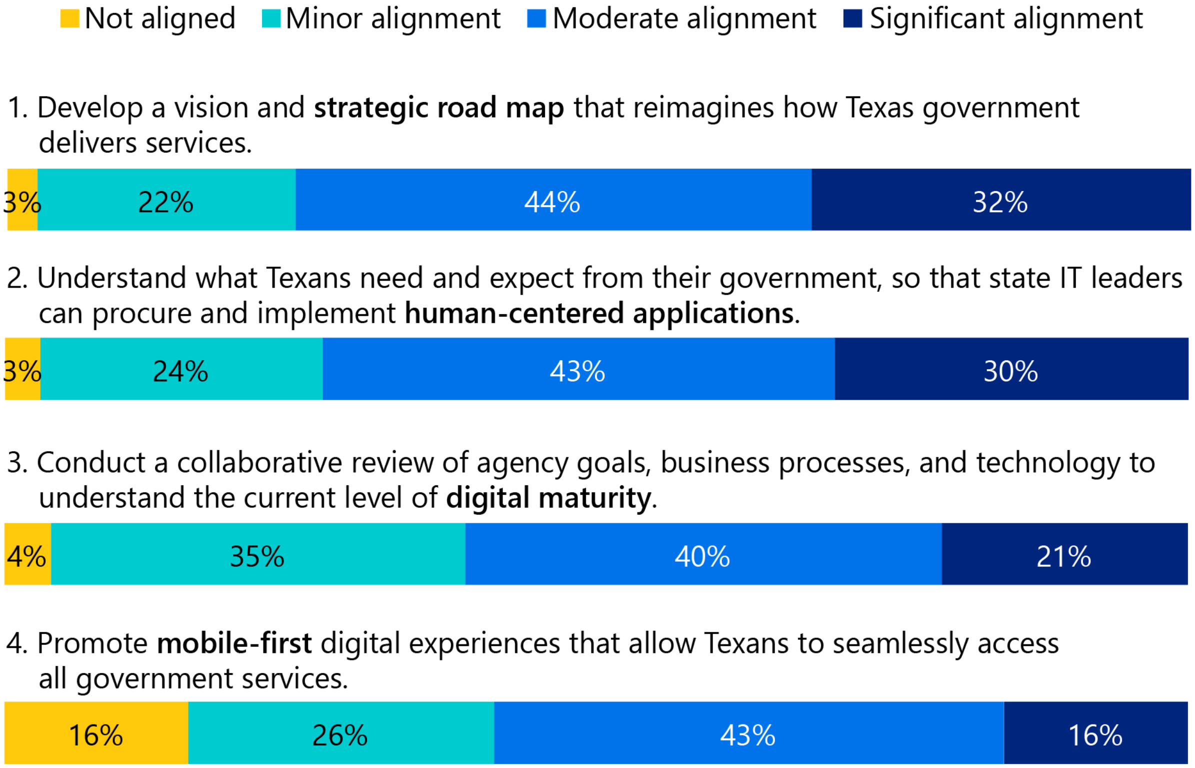


2022-2026 State Strategic Plan
Goal 3: Strategic Digital Transformation

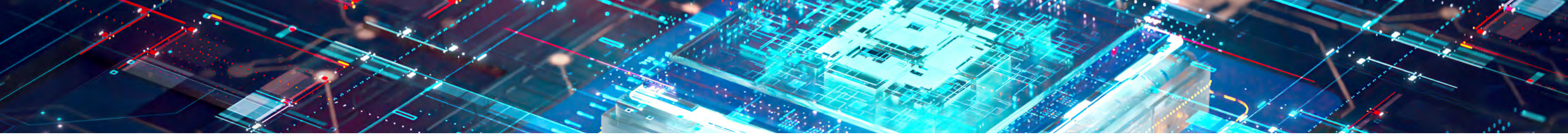
Most Texans are accustomed to shopping, banking, and paying bills online and expect the same streamlined experience from government agencies. State agencies must take a strategic approach to digitally transform how Texas government delivers value to Texans.

The 2022-2026 State Strategic Plan identifies four objectives to help guide state agency efforts toward a strategic approach for the adoption of digital technologies. Desired outcomes for agency alignment with the digital transformation objectives below include increased digital capabilities; digital strategies focused on improving business outcomes; organizational cultures that embrace digital transformation; and meaningful metrics that measure maturity and drive progress throughout the digital journey.

Agency Alignment to Strategic Digital Transformation Objectives



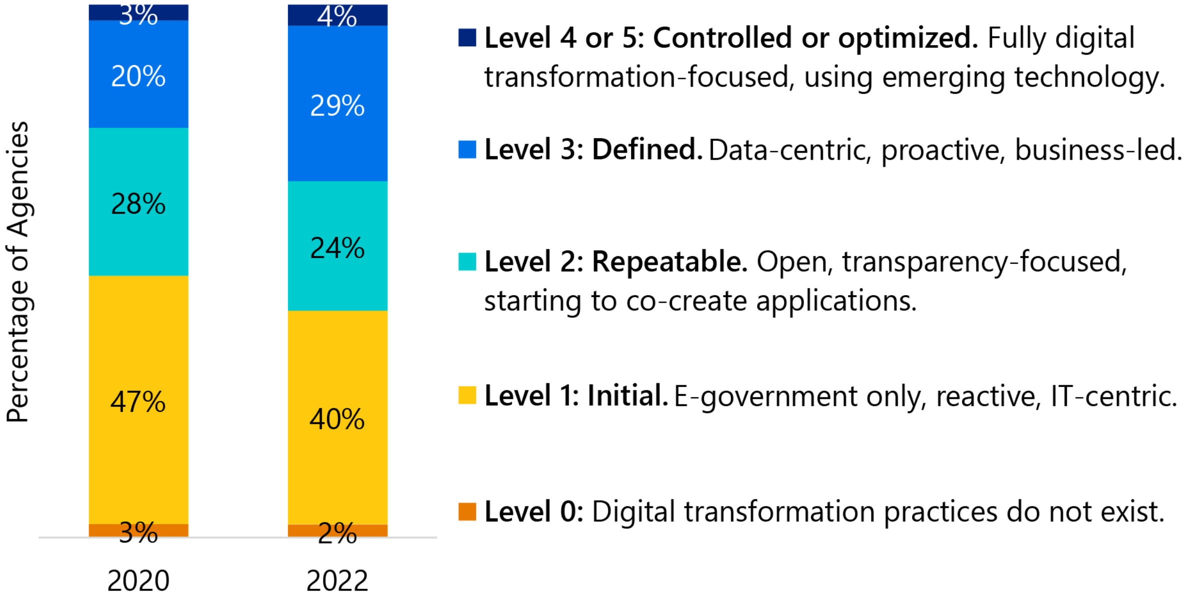
Source: 2022 IRDR. May not equal 100% due to rounding.



Assessment

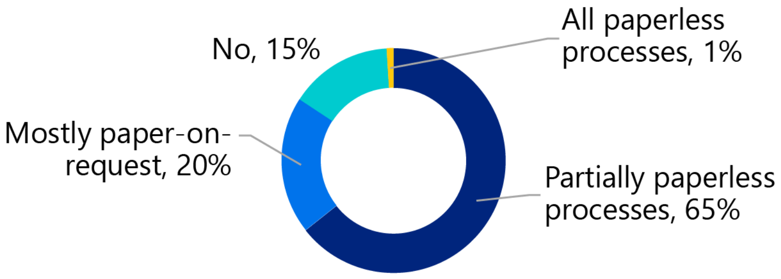
Lasting transformation requires the integration of the right technology with people, processes, and tools to fundamentally change how the public sector operates. In recent years, Texans have had access to more digital government services. State agencies responding to the IRDR reported increased digital maturity, with 57% reporting their 2022 digital transformation status as repeatable, defined, or controlled and optimized, up from 51% in 2020.

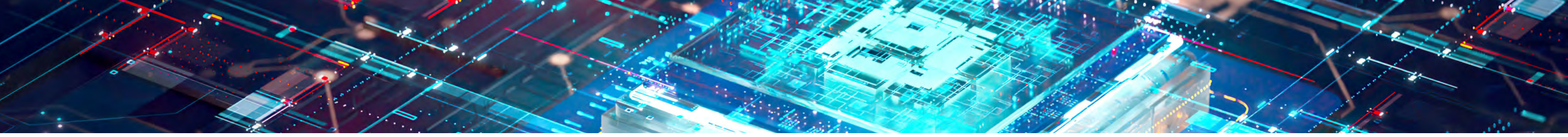
Figure 7: Digital Transformation Maturity



The initial stages of digital transformation maturity may be reactive, IT-centric, and government-focused. The initial stages represent foundational elements of a state agency's effort toward government efficiency and include activities like providing paperless or paper-on-request processes. At this point, most Texas agencies are partially paperless.

Figure 8: Agencies with Paperless or Paper-on-Request Processes in Place

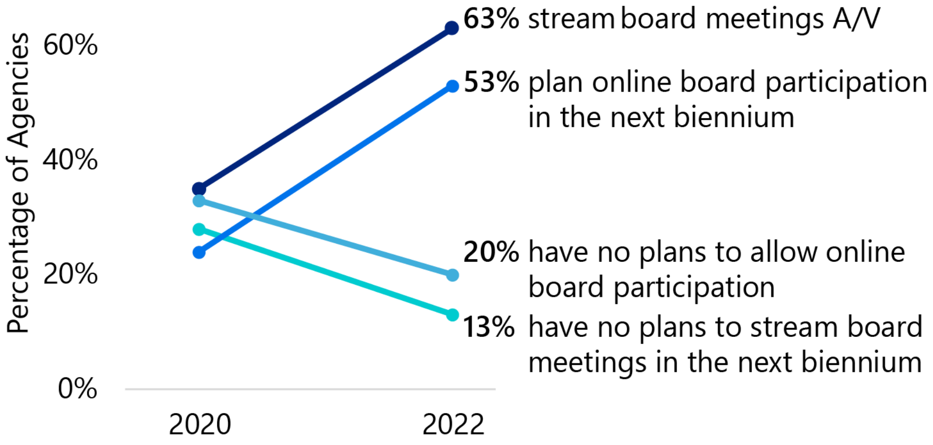




More state agencies responding to the IRDR reported they stream audio or video of board meetings on the internet than ever before. Also, more than half of these agencies indicate they plan to allow board members to participate virtually in board meetings during the next biennium.

This not only allows for broader geographic representation by potential board members, but also saves taxpayer money by reducing travel costs for current board members.

Figure 9: Online Board Meetings



Moreover, state agencies reported significant progress on several fronts including using PC-based conferencing tools, accepting online forms and payments, and incorporating responsive design that provides improved customer experience on mobile devices.

94%

prefer to use PC-based applications like Zoom or Microsoft Teams for video conferencing.

75%

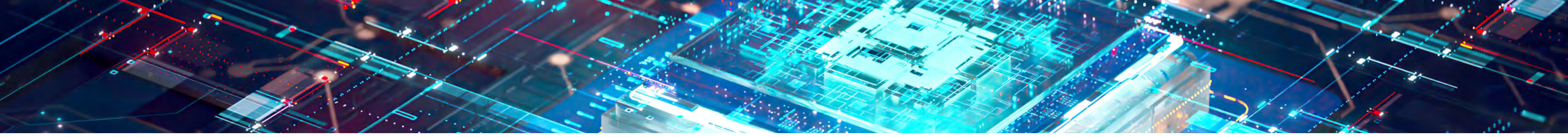
collect payments online or are interested; 56% use Texas.gov for online transactions.

91%

provide online submission of applications or forms, an increase from 85% in 2020.

73%

use responsive design to optimize mobile device functionality for some or all of their public-facing applications.

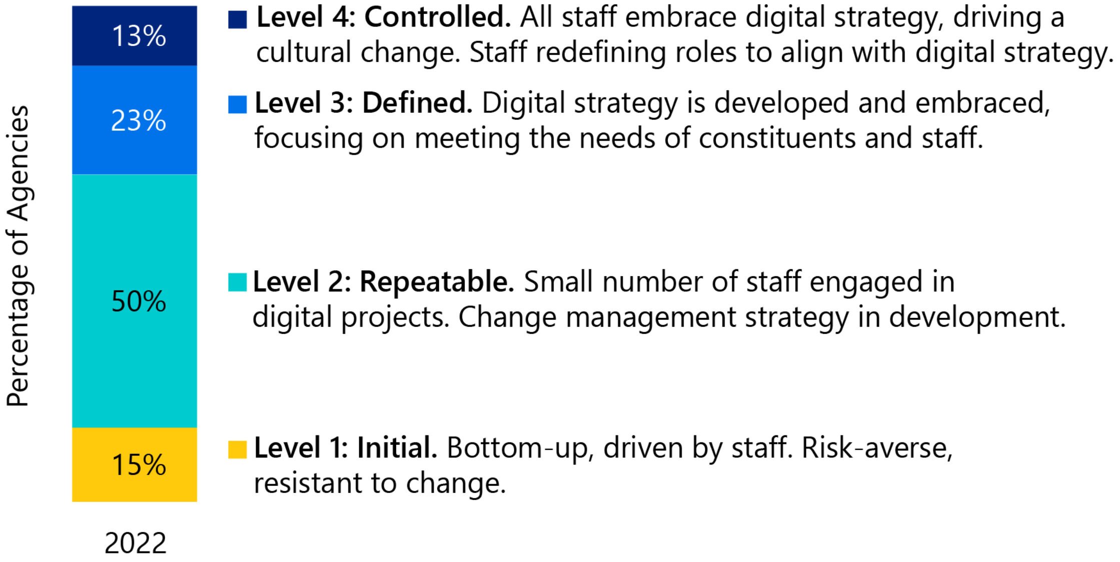


Concerns

Demonstrating that new digital capabilities are worth the investment can be challenging, especially when contrasted with competing priorities. Entrenched organizational culture and resistance to change can be stumbling blocks to digital transition. Likewise, stakeholders with different expectations and business functions that operate in silos pose challenges to creating high-quality digital government. Overcoming these obstacles requires a keen understanding of organizational readiness and willingness to embrace change.

When asked to characterize their organization's ability to embrace digital transformation, most state agencies responded that they are in the early stages of development.

Figure 10: Agencies' Ability to Embrace Digital Transformation



A digital transformation strategy must consider the impact change has on customers, employees, partners, and other stakeholders. When managed properly, employees may perceive it as an enhancement to their contributions, rather than a replacement. It is essential that a change management plan includes employees' perspectives and provides accurate information about transition in a positive way.

It is critical that the public sector provide access to government services and transactions through well-designed native mobile applications similar to those made available by private companies. State agencies should also consider investing in broadband expansion and next generation cellular technology (5G).

Although agencies are much more familiar with native mobile application development than they were two years ago, 71% reported that they are not planning any native mobile application development at this time.

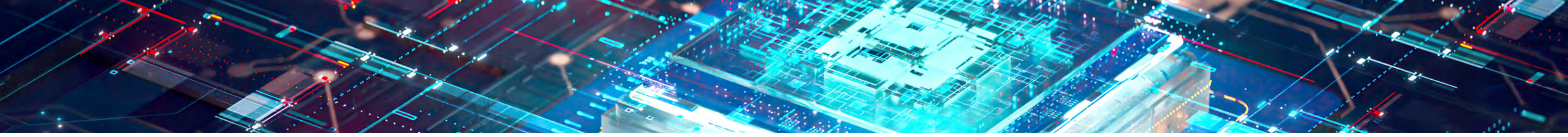
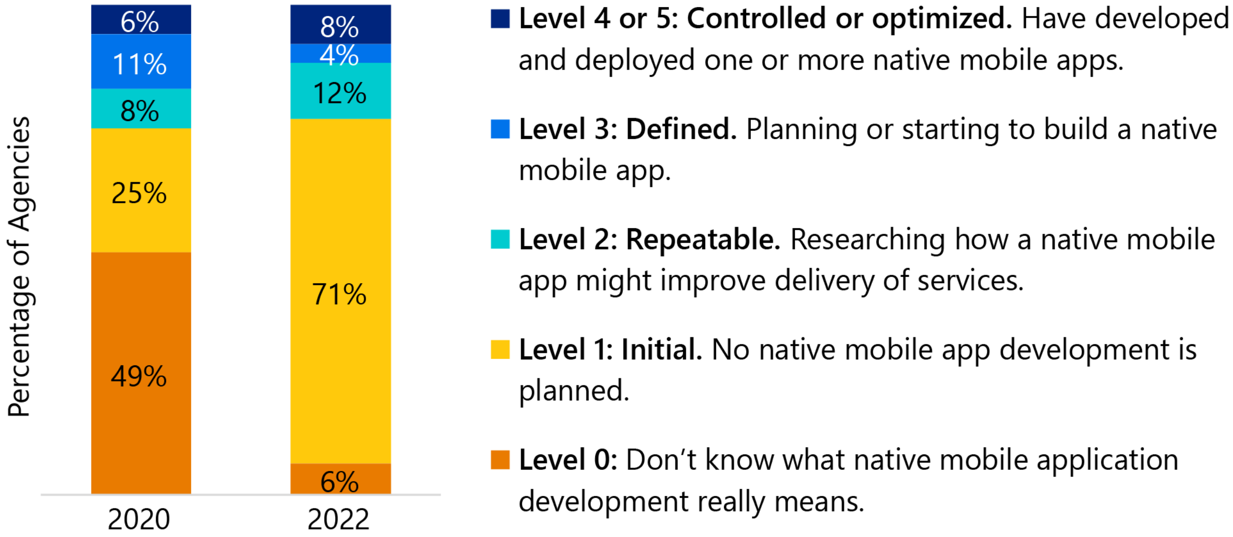


Figure 11: Native Mobile Applications Capability



■ **Level 4 or 5: Controlled or optimized.** Have developed and deployed one or more native mobile apps.

■ **Level 3: Defined.** Planning or starting to build a native mobile app.

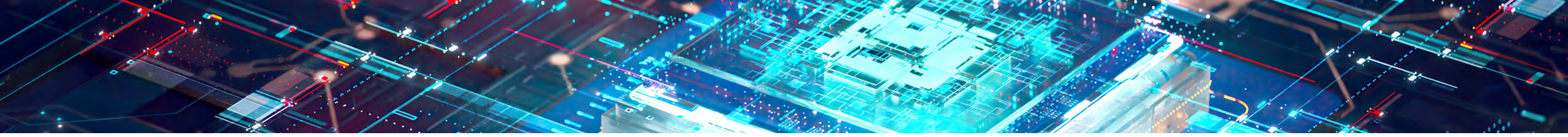
■ **Level 2: Repeatable.** Researching how a native mobile app might improve delivery of services.

■ **Level 1: Initial.** No native mobile app development is planned.

■ **Level 0:** Don't know what native mobile application development really means.

As the technology agency for the state, DIR has worked over the last biennium to develop a native mobile application that allows the public to access key government services. In 2022, DIR, in collaboration with other agencies, launched Texas by Texas (TxT), a native mobile application available through both the Apple and Google Play stores. Through TxT, Texans may create a single and secure online account that allows them to manage many of their government licenses and registrations issued by different agencies, receive proactive reminders for renewal or registration, and complete other government transactions quickly and securely.

T★T Texas x Texas



Recommendations

The 87th Legislature advanced efforts to transform and streamline Texans' experience with government by passing legislation to ensure that future native mobile applications did not duplicate efforts already made through Texas.gov. This avoids inefficiencies and ensures a unified, uniform, secure customer experience by prohibiting state agencies from developing agency-specific native mobile applications that duplicate a functionality of Texas.gov, including TxT, unless DIR grants an exemption.

For the next biennium, DIR recommends the following actions to help state agencies advance digital transformation efforts throughout the state.

1 Enable private sector peer-to-peer (P2P) payment solutions commonly used by the public to provide additional payment methods for government services.

In 2020, the use of P2P payments escalated as consumers turned to digital solutions for making payments and receiving money. P2P payments are non-credit card systems for transferring cash from one party to another. Funds are debited from the user's bank account and credited to the recipient's account. Examples are Google Wallet, PayPal, Snapcash, and Venmo.

Currently, Texas government agencies can use Texas.gov's payment services solution to allow their constituents to pay for government services via credit card, debit card, and eCheck (ACH) transactions online, at the point-of-sale, through a mobile device, interactive voice response (IVR), and on a recurring basis. The Texas.gov solution provides extensive financial reporting and integrates state government payments with the Texas Comptroller of Public Accounts' (CPA) accounting system. At this time, P2P payments are not accepted by Texas.gov.

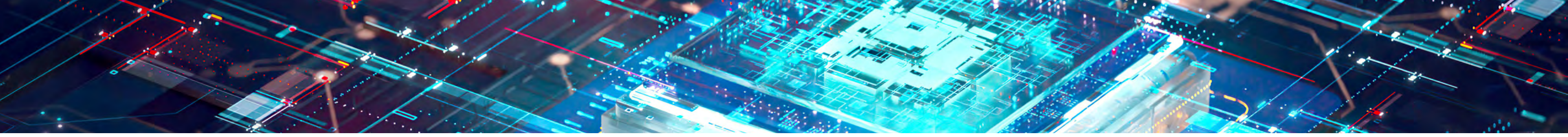
Expanding the sources of payments accepted by Texas.gov and other portals beyond credit cards or debit cards will enable Texans to make payments and complete government transaction in the user-friendly manner they are accustomed to in the private sector.

2 Enable broader access to digital government services, streamlined processes, and digitization by expanding the use of digital signatures.

Currently, a digital signature can be used to authenticate a written electronic communication sent by an individual to a state agency or local government if the signature complies with DIR's rules as well as rules adopted by the state agency or local government.

Government Code Section 2054.060 details how a digital signature may be used for written electronic communications to state agencies and local government. DIR further defines requirements for the use of digital signatures by state agencies and institutions of higher education in 1 Texas Administrative Code Chapter 203 as authorized by DIR's general rulemaking authority found at Government Code Section 2054.052(a).

Allowing more digital signatures in lieu of handwritten signatures, without additional rulemaking, could lead to improved administrative efficiency and reduced costs.



Highlights of Agency Accomplishments

Texas government is making progress toward the goals and objectives for strategic digital transformation. The following examples of agency accomplishments demonstrate how state agencies can improve the customer experience and reduce costs by understanding customer needs and expectations at the beginning of the transformation journey.

Texas Department of Motor Vehicles (TxDMV) – Registration Renewal in Texas by Texas (TxT)

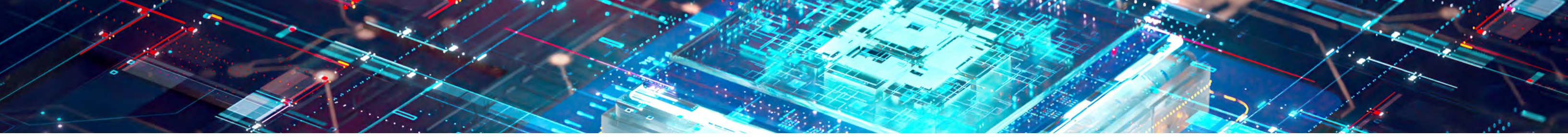
TxDMV recently partnered with DIR to implement vehicle registration renewal services in the TxT application. TxDMV has a presence in both the TxT web and mobile applications and offers Texans the ability to renew their vehicle registration from the convenience of a mobile-friendly web application or mobile app. Since November 2021, over 1.3 million Texans have linked their vehicle to their TxT account and approximately 950,000 of those linked vehicles have been registered using the TxT application.

Texas Commission on Law Enforcement (TCOLE) – Secure Share Application Implementation

The 87th Legislature tasked TCOLE with developing and implementing an electronic process for agencies to share licensed peace officers' employment files for background investigation purposes. In response to Senate Bill 24, the agency launched the TCOLE Secure Share application on March 1, 2022. The application facilitates the secure electronic file sharing of personnel files and records to inform law enforcement agencies across the state in hiring decisions.

Texas Department of Transportation (TxDOT) – Geospatial Portal Implementation

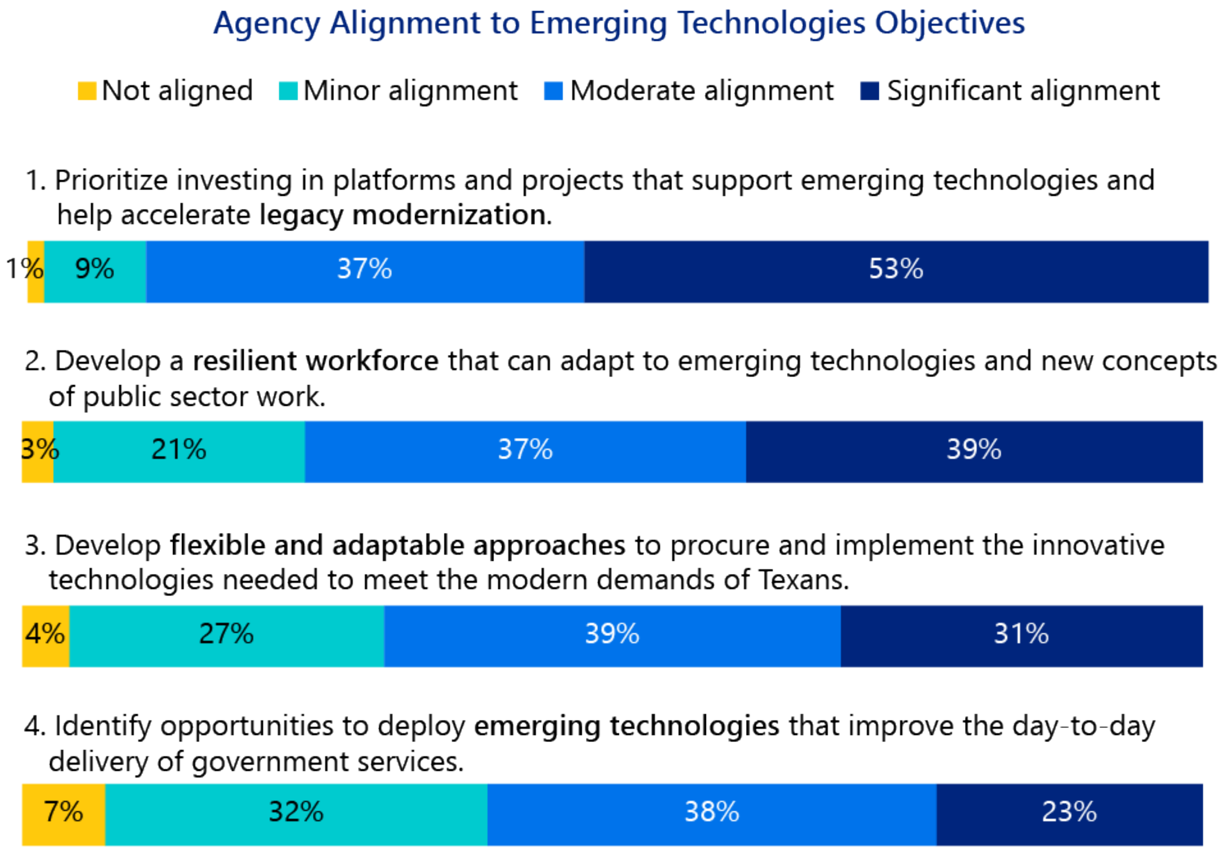
The TxDOT geospatial portal reduces outdated data capture and entry processes. Because applications were driven by the user community, users who were expected to utilize the applications in their day-to-day workflows approved the functionality. The vision for the functionality was motivated and adjusted by the users along every step of the development path, promoting long-term buy-in and achieving improved safety, increased efficiency in data collection, higher data quality, and built-in quality controls.



2022-2026 State Strategic Plan
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 technology environment.

The 2022-2026 State Strategic Plan identifies four objectives to increase state agencies' ability to prepare for the advanced technologies of tomorrow. Desired outcomes for agency alignment with the emerging technology objectives below include approaches that integrate emerging technologies at the appropriate time; strategies that improve the way agencies plan, procure, and deploy IT services and new technologies; methodologies that identify and address legacy system modernization; and hiring and retaining a workforce capable of implementing advanced technologies that provide Texans greater access to government information and services.



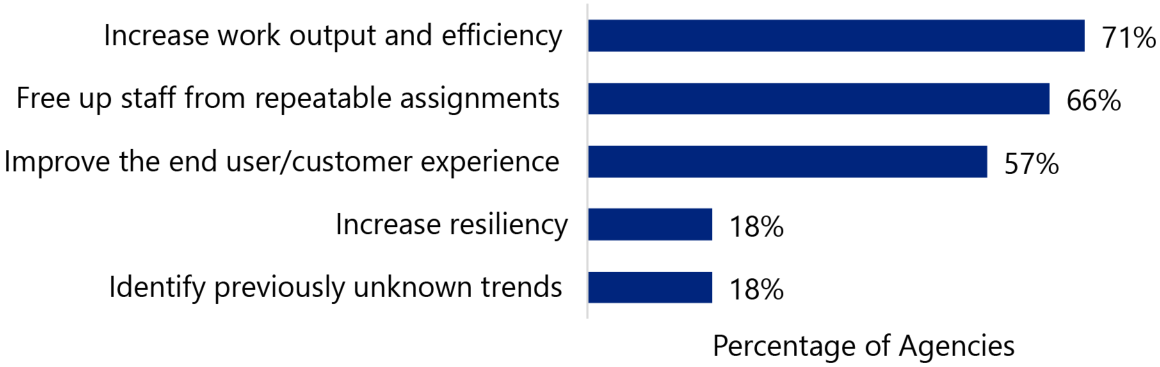
Source: 2022 IRDR. May not equal 100% due to rounding.

Assessment

Agencies reported that they are making progress on modernizing legacy systems and applications with 22% of agencies considering themselves fully modernized; 75% of agencies said at least half of their application portfolios are modernized. Issues associated with legacy applications include unavailable software maintenance upgrades, the inability to adapt or enhance software, limited expertise, and insufficient technical support and documentation.

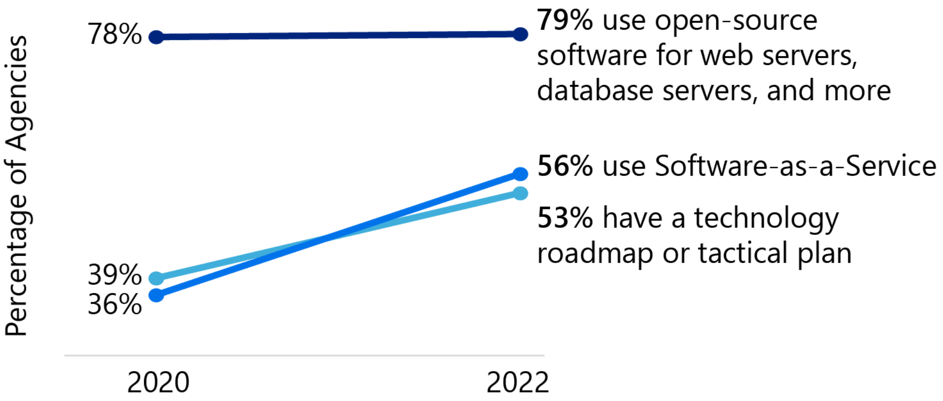
Agencies not only understand the urgency of modernizing but are also poised to take advantage of the benefits of artificial intelligence (AI). Over a third of state agencies report they have already deployed some form of intelligent automated solutions. Top AI priorities include increasing worker output and efficiency, freeing up staff work hours from repeatable tasks, and improving the customer experience.

Figure 12: Top AI Priorities



In addition, state agencies completing the IRDR reported progress in areas that make them well-positioned for modernization including using open-source and Software-as-a-Service as well as having a technology roadmap.

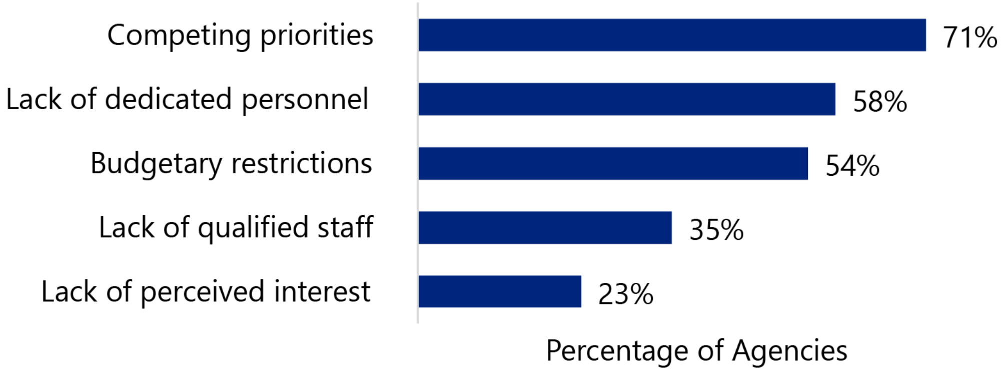
Figure 13: Progress on Emerging Technologies



Concerns

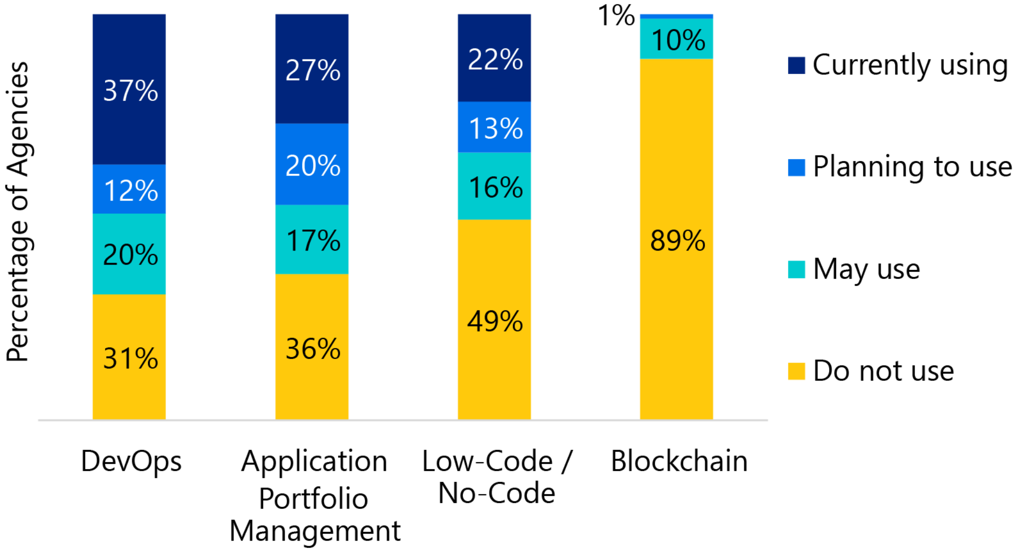
When asked to define the agency's maturity with intelligent automated solutions, 85% of state agencies said they are in the initial stages. This means they lack repeatable and defined processes for implementing AI. Barriers to deploying AI include competing priorities, lack of dedicated personnel, and budgetary restrictions.

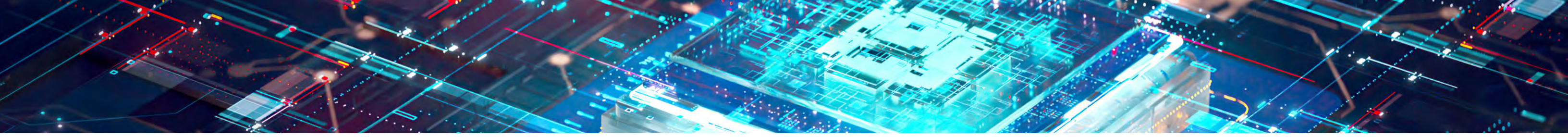
Figure 14: Top Barriers to Deploying AI Solutions



Agencies have made more progress toward some emerging technologies than others. Over a quarter of agencies are using DevOps and Application Portfolio Management while 22% have adopted low-code/no-code development; however, blockchain technology is seeing no active use and only 1% of agencies are currently planning to implement it.

Figure 15: Agencies' Use of Emerging Technologies and Tools





Recommendations

The 87th Legislature demonstrated its commitment to technology modernization by passing two bills establishing committees and working groups to ensure that modernization projects are overseen and funded. The first of these was House Bill 4018, which established a legislative oversight committee on agency technology modernization projects and a dedicated fund for those projects. This legislation requires state agencies to identify legacy IT infrastructure risks and be proactive in planning for and deploying modern solutions that enable the integration of emerging technologies. The second of these bills, House Bill 1576, established a work group to develop a master plan for the blockchain industry's expansion in Texas and to recommend policies and state investments in connection with blockchain technology.

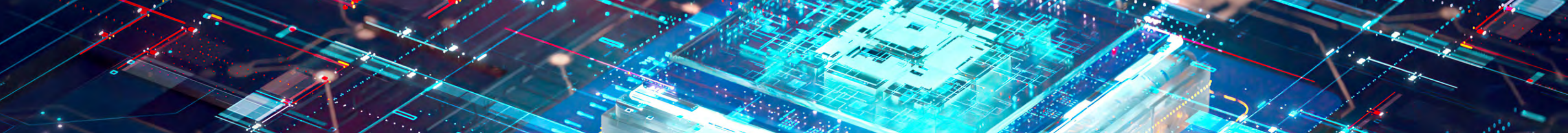
For the next biennium, DIR recommends the following actions to encourage state-agency adoption of emerging technologies.

1 Provide guidance for distributed ledger and blockchain technology best practices.

The term distributed ledger technology is an umbrella term used to refer to a variety of software implementations that keep a verifiable ledger of transactions. A blockchain protocol is a subset of distributed ledgers that uses a specific data structure. Using this specialized data structure, a blockchain protocol tracks transactions in a way that can be simultaneously used and shared within a large decentralized, publicly accessible network.

It is important for public-sector organizations to receive guidance on best practices and gain an understanding of the technology before considering its use and implementation.

The work group established under House Bill 1576 shall issue policy recommendations in connection with blockchain technology. Following best practices that align with the work group's guidance for distributed ledger technology infrastructure will help public-sector organizations better understand how and when to leverage the technology. Best practices could include, but are not limited to, defining blockchain benefits, use cases, contractual language, development of a blockchain innovation/center of excellence, and education or curriculum development.



Highlights of Agency Accomplishments

The following examples of agency accomplishments demonstrate how applying rapid application development, using an automated virtual assistant, and investing in upskilling the next generation of workers is helping state agencies fulfill their mission.

Texas Education Agency (TEA) – Utilization of Rapid Application Development

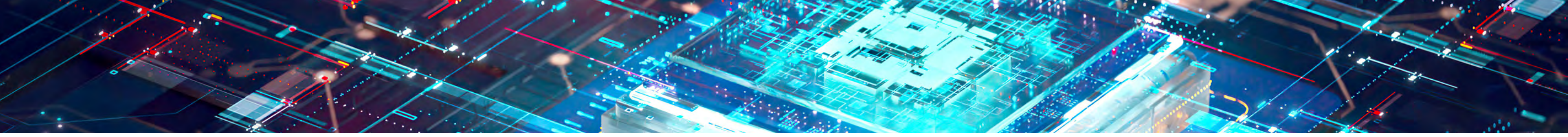
To make it easier for families to complete Supplemental Special Education Services (SSES) application forms, TEA built and deployed a new application system using rapid application development, an adaptive software development approach. The system processes SSES applications using Public Education Information Management Systems (PEIMS) codes and Free or Reduced Lunch (FRL) status to determine a family's eligibility and economic status to ensure low socioeconomic families receive prioritization. This system has resulted in a cost savings of $3.8 million and a 381% increase in the number of applications received.

Texas Health and Human Services Commission (HHSC) – Maya Chatbot

In November 2021, HHSC began using an automated virtual assistant, Maya the chatbot, to communicate with Spanish-speaking Texans about the federal Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) services available to new mothers and families with young children. Spanish is the primary language in more than 35% of Texas households receiving WIC services. Chatbot translation is one of the latest efforts to improve the experience of people seeking information about Texas WIC services.

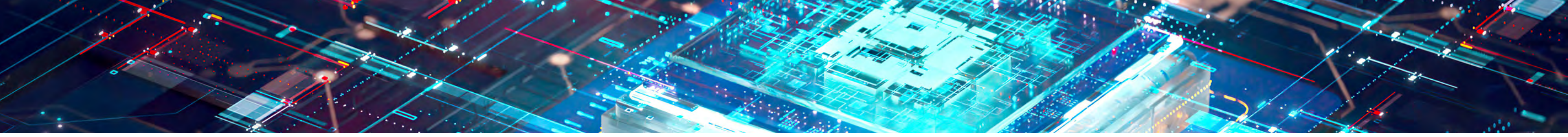
Texas Workforce Commission (TWC) – IT Software Engineer Apprenticeship Program

TWC developed a registered IT software engineer apprenticeship program to build skills for the workforce of the future. Using funding already allocated for these positions, TWC was able to pilot a state agency apprenticeship program using ten vacant programmer positions at no additional cost. The two-year program, approved by the Department of Labor (DOL), allowed TWC to attract staff with a passion for coding who may not have the necessary experience. During the two years, apprentices will receive 144 hours of training and have 2,000 hours of work assignments each year under the supervision of an assigned coach. TWC was able to swiftly fill ten vacancies using this approach, and the new apprentices are excited to earn while they learn. Now that TWC is a DOL-approved apprenticeship employer, the agency can quickly add new job classifications for apprentices in areas such as infrastructure, cloud technologies, project management, and more. More information about this apprenticeship program is available by contacting cio@twc.texas.gov.



Conclusion

Texas government has made notable advances in providing secure IT service delivery, protecting and managing data, moving toward digital services, and taking proactive approaches to emerging technologies. Over the next four years, DIR will promote the goals and objectives in the 2022-2026 State Strategic Plan and assist state agencies in further developing reliable, secure digital services and advocating for IT modernization across the State of Texas. Setting goals and monitoring progress are critical in helping state IT leaders prepare for and take full advantage of inevitable changes and innovation in technology.



Glossary of Terms

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 may be used to assist with forecasting, decision-making, automation, and translation to optimize tasks traditionally performed by humans and increase productivity and efficiency. AI is an umbrella term that encompasses a wide variety of technologies, methods, and platforms used to accomplish these tasks.

Application Portfolio Management. A framework for managing enterprise IT software applications and software-based services. DIR has implemented Application Portfolio Management software as a service available to state agencies.

Blockchain. A digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network.

Chatbot. A form of AI software that is used to conduct an online chat conversation via text or text-to-speech. A chatbot is often used in lieu of providing direct contact with a live human agent or as a precursor to 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.

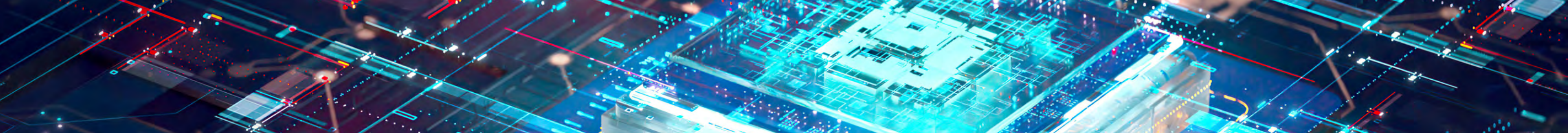
Customer Experience. Strategies that consider a customer's perceptions and feelings toward an organization based on the sum of all digital experiences that the organization provides.

Cybersecurity. Cybersecurity is the practice of instituting and monitoring controls to protect networks, devices, and data from unauthorized access or criminal use to insure the confidentiality, integrity, and availability of 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.

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

Digital Transformation Maturity. A maturity model that characterizes an organization's ability to embrace digital transformation.

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.

Hyperconverged Infrastructure. A software-defined, unified system that combines all the elements of a traditional data center including storage, computing, networking, and management.

Identity and Access Management. 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.

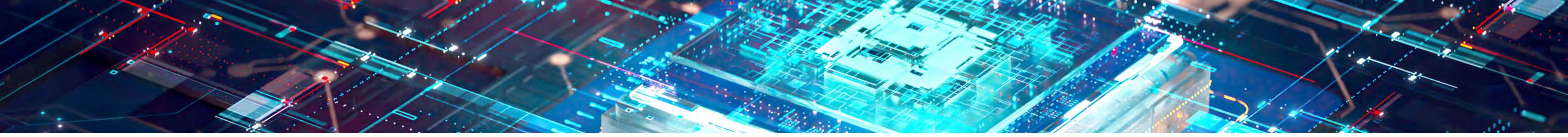
Integration. Making independently designed applications and data work well together.

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

Low-code/No-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.

Maturity Model. A tool used to assess an organization's people, processes, and capabilities.

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



Multifactor 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.

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 and distributed 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 prediction, 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 statutory requirements and 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.

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

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

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.

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.

Texas Department of Information Resources

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