Empowering people who serve the public®

tyler technologies

WHITE PAPER

Is Your Legacy Digital Infrastructure Putting You at Risk?

Future-proofing the public sector with strategic investments in technology modernization.

Russell Gainford, Sr. Vice President of Cloud Strategy and Operations, Tyler Technologies

WHITE PAPER

Is Your Legacy Digital Infrastructure Putting You at Risk?

Introduction

As advancements in technology speed up, government agencies face a decision: maintain old legacy systems or invest in modern technology. Agencies face multiple pressures — threats from bad actors, shortages in the workforce, and outdated technologies, among others. The imperative for leaders is not just about keeping pace with technological advancements. It is also about reducing risks by making smart choices that will stand the test of time.

The Trends Accelerating Modernization

In April 2023, Gartner® identified the top 10 government technology trends that could guide public sector leaders in accelerating transformation.[1] Among those trends, Gartner included cloud-based legacy modernization, adaptive security, and AI for decision intelligence.

Eight months later, Government Technology magazine took a look back at the biggest stories of 2023 and made predictions for 2024.[2] Viewing into their crystal ball, Government Technology identified cybersecurity, workforce, and artificial intelligence as the "big three" stories that would make headlines in 2024.

Government Technology highlights a sector midstream in a transformative journey. It is a journey marked by a need to balance the urgency of modernizing legacy systems with the strategic foresight required to future-proof those investments.

Modernization Is Happening in the Cloud

There is a clear shift toward leveraging cloud strategies as the primary approach to modernization. When it comes to cloud-based legacy modernization, Gartner predicts over 75% of governments will operate more than half of workloads using hyperscale cloud service providers by 2025.[1] As part of those efforts, the National Association of State Chief Information Officers (NASCIO) found that 60% of state CIOs have in place a "cloud strategy for moving applications to the cloud (when feasible)." At Tyler Technologies, we have seen nearly 90% of our new city and county clients opting for cloud-based services over on-premises software, up from 50% in 2018.

However, when it comes to the pace of modernization, it seems many governments and agencies are lagging.

1. Gartner Press Release, "Gartner Announces the Top 10 Government Technology Trends for 2023," April 17, 2023. https://www.gartner.com/en/newsroom/press-releases/2023-04-17-gartner-announces-the-top-10-government-technology-trends-for-2023

2. *Government Technology*, "Year in Review 2023: Our Take on the Biggest Stories of the Year," December 2023

NASCIO asked state CIOs what categories of services and functions have been migrated to the cloud (see Table 1). Only a couple of functional migrations to the cloud are nearly complete: email/calendar services (94% done) and collaboration platforms (83% done). Migrations that are largely underway but far from complete include security (84% ongoing, 9% done); data management (77% ongoing, 0% done); and program/business applications (74% ongoing, 4% done). Migrating to the cloud is clearly a work in progress, but as we have seen at Tyler, progress is accelerating.

But waiting to modernize puts agencies at risk.

Table 1: What Categories of Services/Functions Has Your State Migrated to the Cloud?

	Done	Ongoing	Planned	Do Not Know
Email/calendar	94%	6%	0%	0%
Collaboration platforms	83%	17%	0%	0%
Service management	47%	28%	15%	11%
Project and portfolio management	44%	28%	22%	7%
Open data	28%	44%	13%	15%
Mainframe	28%	30%	23%	19%
Identity management	27%	54%	19%	0%
ERP	24%	27%	31%	18%
Human resources/payroll/personnel	24%	38%	27%	11%
Business intelligence/business analytics	22%	63%	8%	6%
Citizen relationship management	22%	47%	24%	7%
Disaster recovery/business continuity	11%	44%	33%	11%
Security	9%	84%	7%	0%
Digital archives	4%	44%	31%	20%
Program/business applications	4%	74%	15%	7%
Data management	0%	77%	16%	7%

Source: NASCIO 2023 State CIO Survey

5 Risks of Delaying Government Technology Modernization

With state and local governments projected to spend more than $144 billion on IT expenses in 2024 according to Government Technology,[3] the stakes are high. Do you risk maintaining outdated systems, or do you embrace change and implement modern technology?

Technical debt, workforce issues, security, workflows and interoperability, and faltering technology support pose risks if you are currently maintaining the status quo. Agencies must confront these challenges head-on to truly see how making changes to technology can protect your operations. We'll explore each risk so you and your organization can take away helpful insights to plan a successful technology transition.

Legacy Technology Risk #1: Technical Debt

In an ideal state, all technology in use would be the latest state-of-the-art available. In reality — due to several factors including budget concerns, change management burden, and lack of political buy-in — agencies often succumb to the idea that their current software is sufficient and decline to invest in an upgrade. However, this mindset contributes to the accumulation of technical debt. Avoiding the short-term costs to update technology often leads to larger, more significant costs later when the software is no longer supported. Older homegrown or legacy systems not only compound this technical debt but also leave organizations bearing the costs of hiring staff trained in outdated technologies, maintaining less efficient tools, facing cybersecurity risks, storing physical papers, and incurring additional upgrade fees. Legacy systems often fall into obsolescence because they are typically on-premises and lack the ability for easy updates.

To ensure an investment in technology is future-proof, it's crucial to opt for systems designed within modern cloud environments. Such systems leverage the cloud's inherent scalability which allows for automatic and seamless updates, enhancements, and maintenance. This approach not only minimizes technical debt by keeping the system current but also leads to improved functionality, efficiency, and service quality. Moreover, the subscription fee models of most cloud solutions make IT budgeting predictable from year to year.

Legacy Technology Risk #2: Workforce Retirements

At the state level, 37% of IT budget dollars go toward IT staffing according to data from Government Technology.[4] With that significant investment in people, the impact of an aging workforce in the public sector poses a serious risk. In the federal workforce for instance, IT workers aged 60+ have doubled since 2007 while those under 30 have declined.[5] This means many workers will retire within the next few years, leaving a shrinking pool of younger workers to fill the gaps. Simply put, younger workers are not attracted to working with antiquated technology and processes. Not only is it tough to train a new employee on outdated processes and old programming languages, but it is also extremely hard to recruit for the skill set required to maintain these older technologies.

Now imagine equipping your workforce with cloud solutions that reduce staff effort and free them for higher-level work. Advanced systems can improve efficiency and attract a new generation of tech-savvy employees. Those aged 20-29, primarily Gen Z, are eager to engage with cutting-edge technology. Attracting Gen Z to the public sector not only bridges the gap left by an outflux of retiring staff but also positions the organization as a forward-thinking employer.

Legacy Technology Risk #3: Security

Agencies still running on older technology should be concerned about security vulnerabilities in their operations. Globally, ransomware attacks in state and local government organizations continue to rise, with some surveys showing that the number of affected organizations doubled between 2021 and 2023. It's not a matter of *if* you will face a security concern but *when* — and how prepared you are.

3. *Government Technology*, "Projected State & Local IT Spend, 2022-2028," July 18, 2022

4. *Government Technology*, "2020 State IT Spending Breakdown," January 15, 2021

5. The White House, "Chapter 13. Strengthening the Federal Workforce," 2023

Let's also not forget that on-premises software systems are more vulnerable to disruptions from natural or man-made disasters.

The advantage of cloud-based solutions lies in their ability to receive automatic updates, which eliminates manual interventions to install the latest security patches. This ensures that systems are always up-to-date and less vulnerable to cyberthreats. With cloud services, governments and agencies can customize their security settings, tailoring data access and sharing capabilities to the needs of specific offices and roles. Look for a strong cloud-based identity and access management system for data security, compliance, and protection.

Legacy Technology Risk #4: Workflows and Interoperability

One of the biggest challenges in legacy systems is the inability to streamline workflows and connect data between systems. While existing systems might seem adequate, when most organizations truly inspect their operations, they typically find time-consuming processes, siloed functions, and much room for improvement. Employees are simply not as efficient on older systems. They must navigate multiple programs, manipulate information manually, handle paperwork, and compile data from disparate sources.

On the other hand, cloud-based systems are driven by intuitive workflows, shared data, automation, and increasingly, machine learning and artificial intelligence. With automation and AI-driven insights, tasks that once took extensive manual effort between departments or field staff can be streamlined or eliminated entirely. For example, timesheet and payroll processing that used to take multiple days of manual effort to complete, can now be completed in a single morning. Imagine having automated processes that turn your organization into a seamlessly connected, productive machine.

Legacy Technology Risk #5: Faltering Technology Support

When it comes to support, it's important to differentiate between a mere software vendor and a dedicated technology partner. Government agencies often grapple with constraints imposed by traditional software vendors. For instance, a vendor may be acquired and the new parent company may end product enhancements or support. Or they may fail to keep pace with technological advancements. Or they may simply go out of business, rendering their software obsolete.

Alternatively, a dedicated cloud technology partner will continually invest in system enhancements and long-term support. This partner will update systems behind the scenes without the need for onerous on-site upgrades or downtime. A dedicated technology partner will also ensure that the most critical asset — your agency's data — is not only preserved but also optimized for current and future needs. The decision to modernize can be frictionless with the right technology partner.

Table 2 offers a side-by-side look at the risks of staying with your legacy solution compared to the benefits of migrating to the cloud.

Table 2: Legacy Technology Risks Versus Modern Infrastructure Benefits

	Legacy Technology Risks	Modern Infrastructure Benefits
Overview	• On-premises, manual updates • Unconnected, siloed systems • Spotty vendor support	• Modern cloud environment • Connected, shared workflows • Secure, always up to date
Technical Debt	• Budget dollars contribute to maintaining dated systems • Unpredictable future costs • Higher total cost of ownership throughout the life of the software • Limited return on investment as technical debt grows	• Budget dollars contribute to an always up-to-date system • Predictable subscription costs • Lower total cost of ownership throughout the duration of the subscription • Large return on investment without technical debt
Workforce Issues	• Difficult-to-recruit skill sets to support outdated technology • More staff means higher overhead and employment costs • Limited opportunities for mobile work	• With proper training, the system is operable by anyone • Fewer workers means lower overhead and employment costs • Mobile technology options enable hybrid work schedules
Security	• Old, failure-prone software • Limited security controls • Vulnerabilities in data-sharing and information access • Cybersecurity vulnerabilities in software programs due to lack of updates	• Up-to-date, resilient software • Role-based access controls • Secure, compliant data-sharing methods and information architecture • Added security layers against ransomware and other cyberthreats
Workflows and Interoperability	• Siloed, limited on-premises software functionality • More steps to access data and compile information • More steps to manipulate content so it "fits" • More keystrokes, manual effort, paper involved	• Extremely capable, efficient, integrated systems • Fewer steps to access data and compile information • Data, reports, etc. are agile and customizable • More automation and intuition, less paperwork
Support	• Lack of support from software vendor • Stagnant technology capabilities rarely updated • Smaller vendors are often privately held, limiting viability in financial security	• Ongoing support from dedicated technology partner • Technology capabilities always up to date • The right technology partner will be future-thinking, with a history of success and stability

Conclusion

Operating with old tools and software is challenging and frustrating. Don't leave your organization at risk trying to maintain homegrown or legacy systems. Modern cloud systems await. While the initial short-term investment might be more costly than keeping an outdated system running, the long-term benefits — avoiding the accumulation of technical debt and not having to worry about an old system's performance — are too important to overlook.

Whether you are ready to migrate to the cloud or not, find a technology partner with a history of longevity and industry experience, and engage them in an operational assessment. A simple review of your technology and processes can go a long way in determining a modernization plan for your organization.

Additional Resources

For additional insights for government leaders, visit Tyler's Resource Center. If you would like more information about Tyler solutions, contact us at info@tylertech.com or visit tylertech.com.

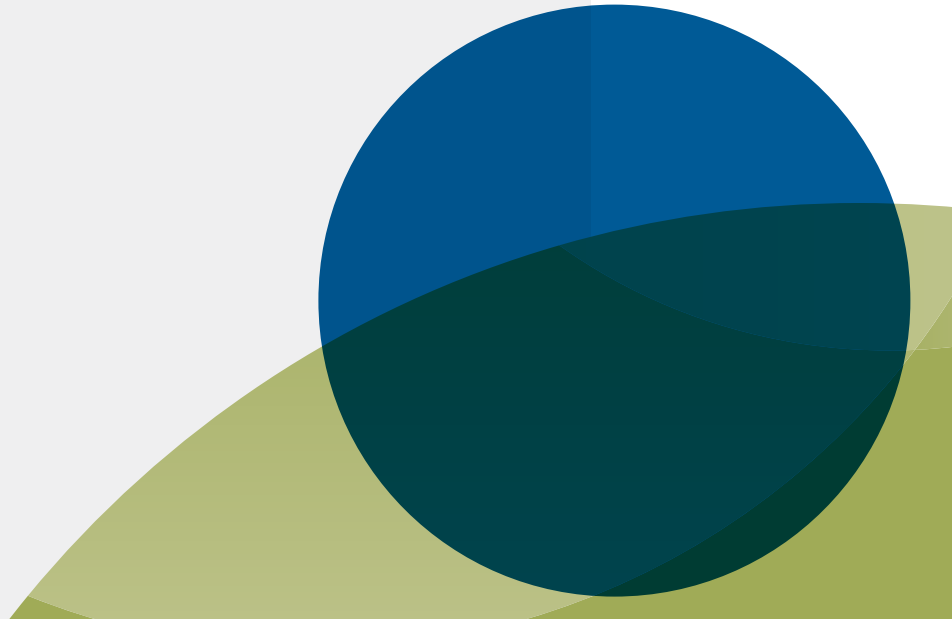
About the Author

Russell Gainford is the senior vice president of Cloud Strategy and Operations for Tyler Technologies. Russell defines best practices for cloud development, operations, and deployment to achieve the full value of Tyler's cloud-first approach for both Tyler and its clients.

ABOUT TYLER TECHNOLOGIES, INC.

Tyler Technologies (NYSE: TYL) is a leading provider of integrated software and technology services for the public sector. Tyler's end-to-end solutions empower local, state, and federal government entities to operate efficiently and transparently with residents and each other. By connecting data and processes across disparate systems, Tyler's solutions transform how clients turn actionable insights into opportunities and solutions for their communities. Tyler has more than 44,000 successful installations across 13,000 locations, with clients in all 50 states, Canada, the Caribbean, Australia, and other international locations. Tyler has been recognized numerous times for growth and innovation, including on Government Technology's GovTech 100 list. More information about Tyler Technologies, an S&P 500 company headquartered in Plano, Texas, can be found at **tylertech.com**.

tylertech.com | 833.895.3783 | info@tylertech.com



CM-DIRISK-WP-34020-0324