E-BOOK

SOLIX™
Empowering the Data-driven Enterprise

MODERNIZING PUBLIC SECTOR DATA MANAGEMENT:

Building a Data-driven Future with Solix

Executive Summary

Public sector agencies are under increasing pressure to save costs and modernize outdated IT infrastructure and legacy systems while delivering secure, governed, compliant, AI-enabled digital services for a better citizen experience. With newer threat vectors and rising cybersecurity risks, outdated systems and fragmented data present significant risks of data breaches, non-compliant data access, and increased costs. This makes modernization and cloud adoption both a strategic imperative and a regulatory requirement.

Solix enables government agencies to address these challenges through a modern data architecture integrating legacy decommissioning, data unification, federated governance, and AI-readiness. Our platform aligns with federal mandates such as Zero Trust and the 21st Century IDEA Act, helping public agencies transition to secure, interoperable, and future-ready environments. With Solix, government entities can reduce technical debt, optimize infrastructure, and accelerate the responsible adoption of cloud and AI technologies—delivering better outcomes for both agencies and citizens.

The State of Data Management in the Public Sector

Government agencies hold sensitive data like tax and healthcare records, must use it lawfully, and keep it secure. Historically fragmented, this data has limited access, hampered digital initiatives, and reduced transparency. Recent reforms in the US focus on modernization through interoperability, cloud, and AI, exemplified by agencies like DOGE and USDS, which aim to improve efficiency.

Federal and state governments are rapidly adopting AI in their operations and services. According to the U.S. CIO Council, federal agencies have more than doubled their use of AI in 2024 compared to 2023, with agencies publicly reporting over 1,700 ways they utilize Artificial Intelligence (AI) to advance their missions and deliver better experiences to the public. However, with AI, increased data access, oversight, and transparency, privacy concerns emerge, risking misuse and loss of trust. Strong governance, privacy enforcement, and risk assessments are essential to ensure responsible AI use and sustain modernization’s benefits.

What are the Key Drivers of Modernization in the Public Sector?

1. **High Costs of Legacy Databases and Applications:**
Federal and State Agencies continue to operate mission-critical systems that range from 8 years old to over 50 years old. Many are built on obsolete languages (e.g., COBOL) and hardware with known security and compliance vulnerabilities. According to a United States Government Accountability Office (USGAO) report, these legacy systems cost over $300 million annually, diverting precious taxpayer dollars from strategic projects to maintenance initiatives.

2. **The Need for Cloud Migration and Hybrid Cloud Adoption:**
The modernization of FedRAMP aims to speed up secure cloud adoption by standardizing risk assessments, role-based permissions, and access controls. Transitioning from legacy mainframes to commercial cloud and hybrid architectures helps agencies get better IT infrastructure, more cloud options, and improved efficiency, while meeting standards like FISMA, NIST SP-800-53, OMB Circular A-130, and Zero Trust Strategy (M-22-09).

3. **Data Consolidation and Infrastructure Optimization:**
In 2019, the Office of Management and Budget mandated data consolidation and IT modernization to standardize HR, finance, and grants, retire legacy systems, and adopt centralized platforms. This saved over $1 billion in payroll, $2 billion in data center costs, and more than $100 million in agency investments. These efforts reduced technical debt and modernized government services. Despite past cost-saving projects, many agencies still run diverse legacy systems with minimal cloud integration. Data consolidation is crucial for reducing dependencies and costs.

4

To Improve Cybersecurity and Compliance

Maintaining zero-trust environments is essential. OMB Memorandum M-22-09 (“Zero Trust Strategy”) and CISA’s Zero Trust Maturity Model require agencies to meet specific goals for identity, device, network, application, and data security. These mandates aim to reduce attack surfaces, enhance threat detection, and secure access regardless of location, device, or user role. Modernizing legacy IT and fixing security vulnerabilities helps lower threat exposure and maintain a secure, governed data architecture.

5

To Enhance Citizen Experience and Digital Service Delivery

According to analytics.usa.gov, about 2 billion visits occur monthly on federal websites, totaling over 80 billion hours of public interaction, with more than 50% on mobile devices. This shows citizens prefer digital interactions with public agencies. A strong digital infrastructure is vital to support this shift. Under the 21st Century Integrated Digital Experience Act and OMB Memo M-23-22, agencies must standardize and adopt shared services. Modernizing legacy systems and adopting new architectures is key to providing the intuitive, secure, and accessible digital services that citizens expect.

Aging Infrastructure Still Dominates: According to a Gartner survey, nearly one in three CIOs in government agencies reported that their oldest core application is over a decade old, highlighting the urgent need for modernization.

Barriers to Modernization: Why It’s Not Happening Fast Enough

Cost Justification and Executive Buy-In
A significant chunk of federal IT budgets is dedicated to sustaining critical legacy systems, leaving limited funds for optimization projects. Agencies compete modernization proposals against mission-critical services and struggle to secure multi-year appropriations without a standardized ROI model.

Procurement and RFP Complexity
The Federal Acquisition Regulation’s fixed-scope lasts 12-18 months, often mismatching the agile cloud and DevOps lifecycle. Modular contracting tools like Indefinite Delivery/Indefinite Quantity (IDIQ) contracts allow agencies to pre-approve vendors after selection, then place orders as needed instead of issuing new RFPs for each requirement. However, with uneven adoption, the “time-to-award” contracts often extend beyond vendor development timelines, which hampers innovation.

Skill Gap in the IT Workforce
Federal agencies today are facing several challenges in attracting quality IT workforce. Public sector pay caps, outdated hiring processes, and protracted security clearances leave roles vacant for several months if not years. This persistent shortage of skilled workforce–cloud architects, analysts, and AI specialists seriously impedes modernization efforts. The US Government Accountability Office flags these skill deficits as serious national security risks.

Fragmented Data with Governance Inconsistencies
Data stored in silos often lack uniform metadata standards, which affects its overall understandability. For IT modernization and unification, poor data understandability can lead to limited insights, increased bias, system integration failures, and a reduced ability to leverage AI for decision-making. With inconsistent metadata and unreliable governance frameworks, IT modernization timelines typically face delays, scope creep, and higher costs due to repeated data discovery efforts and integration issues.

Building Blocks to a Modern Data Architecture

As data operations grow more complex, successful large-scale modernization efforts require more than just isolated solutions. They begin with a comprehensive data management strategy and a clear, end-to-end architecture that enables organizations to manage data effectively from creation to deletion, insights, and AI.

Modernizing data architecture for the public sector and other enterprises heavily dependent on legacy systems starts with retiring databases and applications into a secure, searchable, scalable, and compliant archive. Structured decommissioning helps organizations reduce technical debt and maintenance costs while freeing up talent and infrastructure for more strategic initiatives.

Here are five things to keep in perspective while modernizing public sector data architectures:

1. **Interoperable Data Formats and Storage Flexibility**

   The foundation of a modern data platform begins with a flexible and scalable storage layer, a system that combines the essential functions of a data warehouse and data lakes in one platform. Open table formats like Hudi, Iceberg, and Delta Lake are key enablers of these architectures. These formats encourage standardization, allowing multiple tools to access the same datasets without creating dependencies.

   - Facilitates better system interoperability while reducing data duplication and siloed storage
   - Enables scalable analytics, staging curated data, and even cross-departmental collaboration
   - Supports version control and ACID compliance

2 Federated Data Governance

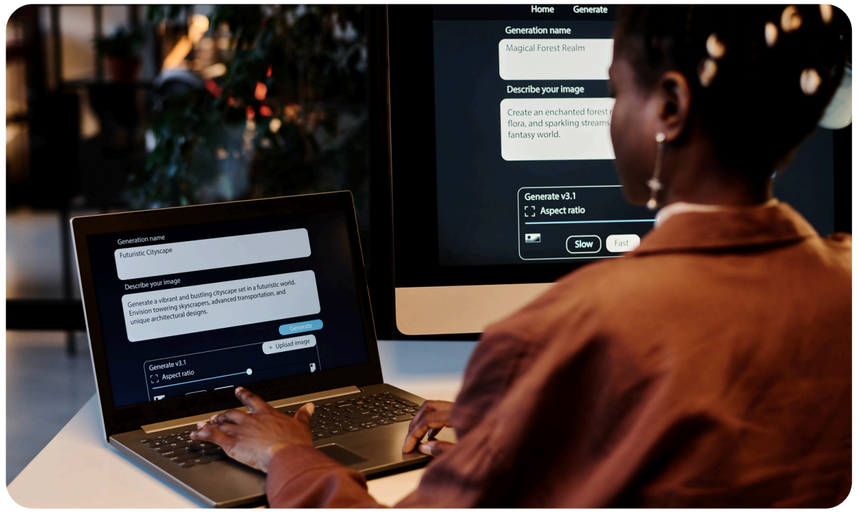
Having the right data governance frameworks helps organizations ensure responsible use. Federated data governance for the enterprise allows individuals across departments to manage their data while aligning with a shared data governance policy framework. This decentralized model preserves autonomy while ensuring consistency, compliance, and collaboration.

- Promotes local data stewardship, with enterprise-level insights
- Ensures department-level adherence to compliance and regulatory standards
- Facilitates better inter-departmental collaboration and boosts joint initiatives

3 Data Security and Privacy-by-design

Public sector agencies handle vast volumes of highly sensitive data, requiring controls to be directly embedded into the infrastructure, processes, and interfaces right from the start. A zero-trust, privacy-by-design approach to data management ensures that robust access controls, encryption, and audit mechanisms strictly govern all data assets.

- Reduces breach risk while maintaining operational agility
- Ensures governance principles are adequately enforced
- Improves traceability and accountability through detailed audit logs



4 Semantic Layer Powered By AI

The value of enterprise data hinges on how well professionals understand their data. Large companies often decommission outdated applications and databases to streamline infrastructure, but existing data platforms usually can't identify “dark” legacy data. An AI-powered semantic layer can automatically uncover dark data, enrich metadata, and improve data visibility.

- Democratize and enable self-serve data access for non-technical professionals within data workflows.
- Enable “Prompt-to-SQL” querying to simplify the way data is accessed
- Improve data discoverability and institutional knowledge sharing

5 Real-time Data Access & Analytics

Modern data architectures require real-time data processing from a wide range of sources. This is essential for time-sensitive tasks such as monitoring, resource management, incident detection, and live reporting. Instant insights enable quicker decisions, minimizing delays between data collection and action.

- Enables continuous monitoring, transformation, and enrichment of data as it gets generated
- Helps improve situational awareness with live dashboards and operational analytics
- Support immediate alerting and anomaly detection through automatic threat detection

The Role of Partners and Ecosystems in Modernizing the Public Sector

Choosing secure and compliant solutions is crucial. However, what truly drives project success for modernization today is scalable solutions that are also flexible enough to adapt as needed. Proven technologies must seamlessly integrate with existing data infrastructure while enhancing capabilities to include AI and support enterprise AI initiatives. Modernization isn’t just about replacing systems; it's about creating real synergy and interoperability between legacy systems and next-generation tools.

Agencies increasingly rely on systems integrators, cloud service providers, and AI technology experts to manage complexity across hybrid and multi-cloud environments. By selecting the right vendor, public sector agencies can accelerate modernization, streamline operations, and reduce overall risk. With the right data ecosystem, agencies can deploy modern data and AI capabilities more quickly, with improved governance and security aligned with their long-term goals.

Solix for Government: Enabling an AI-driven Public-Sector

Solix empowers agencies in the public sector to modernize their IT infrastructure, enforce data governance, ensure regulatory compliance, and enable AI. Our solutions span four pillars:

- Decommissioning Legacy Information Systems, Modernizing IT Infrastructure and ILM
- Unifying Data from Diverse Sources
- Data Governance, Compliance & Security
- Enabling AI

SOLIX™ Empowering the Data-driven Enterprise Product Landscape to Modernize Government IT Infrastructure

Legacy IT Decommissioning and Modernization

Application Retirement

Retire legacy, redundant applications into safe, compliant, cost-effective data storage

Database Archiving

Move inactive, historical data from production databases into low-cost archival storage

Email Archiving

Securely store and preserve email, their metadata, and attachments in a centralized, searchable archive

File Archiving

Move inactive unstructured datasets like documents, spreadsheets, PDFs, images, and multimedia to low-cost, long-term storage

Unifying Data from Disparate Sources

Data Lake Plus

Integrate data from legacy systems, active applications, cloud sources, and enterprise repositories.

Unify structured, semi-structured, and unstructured data into a scalable, metadata-driven architecture for accelerated decision-making and AI readiness.

Enable a single source of truth for analytics, AI, and compliance workloads.

End-to-end governed, ACID Compliant and Secure Repository

Create and stage data products for internal and external consumption and insight generation

Data Governance, Compliance & Security

Sensitive Data Discovery

Automatically discover sensitive data fields across different data fields and data formats

Data Masking

Mask, anonymize, and obfuscate sensitive data fields, to prevent unauthorized data access

Consumer Data Privacy

Manage, protect, and comply with global consumer privacy regulations like GDPR, CCPA, LGPD, NYDFS, HIPAA, and PCI with ease

Federated Data Governance

Enforce governance principles, discover sensitive data, and mask it in-place, without having to move data

Enabling AI

Enterprise AI

Stage curated datasets to be used across AI and advanced analytics use cases

Intelligent Data Classification

Discover dark data automatically as you ingest data, and enrich metadata fields, classify based on file type, and sensitivity

Solix GPT

Enable prompt-to-SQL queries in natural language to democratize data access, and improve time-to-insights with a chatbot-like interface

References

- *Cybersecurity Workforce: Departments Need to Fully Implement Key Practices.* (2025, January 16). GAO. https://www.gao.gov/products/gao-25-106795

- Domeyer, A., Hieronimus, S., Klier, J., Weber, T., & McKinsey & Company. (2021, September 20). *Government data management for the digital age*. Government data management for the digital age | McKinsey. https://www.mckinsey.com/industries/public-sector/our-insights/government-data-management-for-the-digital-age

- Martorana, C., & U.S. CIO Council. (2025, January 15). AI in Action: *5 Essential Findings from the 2024 Federal AI Use Case Inventory*. CIO Council. https://www.cio.gov/ai-in-action/

- Pascal, A., Stranger, A., Schneier, B., Zalesne, K., Pyati, N., Hubbard, S., Graubard, V., & Harvard Kennedy School Ash Center for Democratic Governance and Innovation. (2025, March 31). *Understanding DOGE and Your Data*. Understanding DOGE and Your Data – Ash Center. https://ash.harvard.edu/resources/understanding-doge-and-your-data/

- *Requirements for delivering a digital-first public experience.* (n.d.). Digital.gov. Retrieved June 26, 2025, from https://digital.gov/resources/delivering-digital-first-public-experience

- Walsh, K., & United States Government Accountability Office. (2023, May 10). *Agencies Need to Continue Addressing Critical Legacy Systems* [Testimony Before the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, Committee on Oversight and Accountability, House of Representatives]. United States Government Accountability Office. https://www.gao.gov/assets/gao-23-106821.pdf

- The White House. (2025, January 20). *Establishing And Implementing The President's "Department Of Government Efficiency*". The White House. Retrieved June 16, 2025, from https://www.whitehouse.gov/presidential-actions/2025/01/establishing-and-implementing-the-presidents-department-of-government-efficiency/

- Young, S. D. (2023, September 22). whitehouse.gov. https://www.whitehouse.gov/wp-content/uploads/2023/09/M-23-22-Delivering-a-Digital-First-Public-Experience.pdf

- Young, S. D. (2024, July 25). *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)* [Memorandum for the Heads of Executive Departments and Agencies]. fedramp.gov. https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf

- Young, S. D. (Ed.). (2025, January 15). *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements* [Memorandum for Heads of Executive Departments and Agencies]. whitehouse.gov. https://whitehouse.gov/wp-content/uploads/2025/01/M-25-04-Fiscal-Year-2025-Guidance-on-Federal-Information-Security-and-Privacy-Management-Requirements.pdf

SOLIX™
Empowering the Data-driven Enterprise

Stay Connected

www.solix.com

info@solix.com

+1.888.467.6549