walkme
An SAP company

The future-ready government blueprint

Accelerating success through digital adoption platforms

Learn how digital adoption platforms unlock government modernization success – and return minutes back to mission.

Table of Contents

Introduction

Let's face it – government agencies are up against a pivotal modernization challenge, even as they maintain the highest levels of security and public trust.

With worldwide IT spending projected to reach $5.6 trillion in 2025, every day that your agency struggles with ineffective technology adoption puts a greater strain on your employees, your resources, and the people you serve. The cost isn't just financial – it's measured in diminished service delivery, eroding public trust, and reduced mission effectiveness.

A comprehensive digital adoption strategy is your key to navigating this complex terrain successfully. Let's explore how digital adoption platforms (DAPs) provide the crucial foundation for embracing new technologies securely, effectively, and with maximum return on investment.

$5.6T

in global IT spending projected by 2025

The public sector modernization imperative

Beyond the general push toward modernization, today's public sector organizations operate under unique pressures that private sector organizations rarely face. They must meet efficiency demands while adhering to strict security, compliance, and accessibility requirements.

Mission-critical efficiency needs

> *Public sector organizations face unprecedented demands to operate more efficiently while delivering better service.*

These pressures come from multiple sources:

Rising citizen expectations

People expect the Netflix experience with government services – but public agencies' delivery capabilities are not as responsive or user-friendly.

Budget constraints

Financial limitations can stall modernization efforts or lead to a trade-off between different pressing needs. Training budgets are the first to be cut, putting strain on employees to adopt new technology with minimal support.

Legacy systems

Many organizations grapple with outdated legacy systems that are expensive to maintain and incompatible with newer technologies, which hinders integration and causes bottlenecks.

Federal mandates

The federal government has clearly prioritized AI research and development, and agencies are feeling the pressure to catch up and keep up.

Universal accessibility requirements

Government organizations must meet strict legal mandates around accessibility that go beyond the best practices followed in the private sector. This includes:

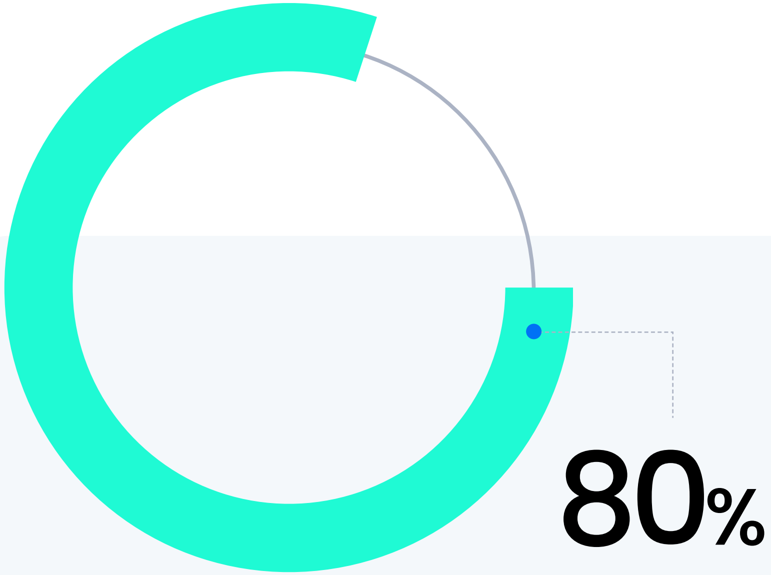
1. Supporting diverse language and communication needs
2. Adapting to varying levels of digital literacy
3. Ensuring consistent service quality across access points

The government workforce itself presents another accessibility challenge – varying degrees of technical dexterity mean solutions must be designed to accommodate users of all skill levels.

Complex security demands

Public sector organizations manage some of the most sensitive information in existence, from national security data to personal healthcare records.

Between ransomware targeting vulnerable legacy systems and advanced phishing campaigns using social engineering, more than [80% of security threats] stem from human decisions. Security-aware user interfaces (UIs) and guidance systems are increasingly important.



80%

of security threats stem from human decisions

Innovation priorities

The public sector's innovation priorities create unique challenges for technology adoption.

Mission-focused

The public sector prioritizes the mission, from ensuring public safety or securing the homeland to providing essential services. Improving service delivery, accessibility, and transparency are at the heart of every decision.

Change management

Agencies must keep pace with rapidly evolving citizen expectations and federal imperatives. This means streamlining legacy processes and adapting them to meet future needs.

Budget and risk constraints

Limited funds from taxpayers create financial boundaries that agencies must operate within. Public accountability leads to lower risk tolerance, with incremental improvements favored over disruptive innovation.

Extended procurement and implementation timelines

Technology acquisition in the public sector can take up to two years, and implementation another three. These extended timelines significantly impact the ability to remain competitive with private sector counterparts.

The hidden cost of neglecting digital adoption

While modernization is essential for public sector organizations, hasty digital transformation comes with significant risks and hidden costs that span security, compliance, operations, and budgets. These costs are frequently underestimated, leading to project failures and compromised outcomes.

Security and compliance: The foundation of public trust

Every modernization project in the public sector must comply with extensive federal guidelines, including NIST 800-53, FISMA, and FedRAMP. The Federal Information Security Modernization Act (FISMA) requires agencies to provide detailed logs and documentation of compliance activities from project inception. According to the FY 2023 Federal Information Security Modernization Act (FISMA) Metrics, 72% of federal agencies reported challenges in meeting comprehensive security monitoring requirements during digital transformation initiatives.[1]

72%

of federal agencies reported challenges in meeting comprehensive security monitoring requirements

[1] Office of Management and Budget. (2023). "FY 2023 Federal Information Security Modernization Act (FISMA) Metrics." https://www.cisa.gov/federal-information-security-modernization-act

The high cost of security failures

Failure to safeguard data can lead to breaches, impacting not just the public agency and affected individuals, but also potentially compromising national security. Poorly implemented AI systems may result in ethical violations and regulatory intervention, sparking widespread societal debates and significant policy shifts.

Recent breaches across multiple agencies underscore the need to get security right during digital transformation:

1. Department of Health and Human Services (2023): A ransomware attack exposed the personal information of more than 2.8 million individuals.
2. Office of the Inspector General (2023): A phishing attack led to a state-sponsored advanced persistent threat accessing an employee's account.
3. Other instances have recently occurred within the Department of Treasury, Department of Justice, United States Marshals Service, Department of the Interior, and more.

The Government Accountability Office (GAO) reported that federal agencies experienced a 47% increase in cybersecurity incidents during recent digital transformation initiatives.[2] Organizations must budget for comprehensive security planning, implementation, and ongoing monitoring – often underestimated costs in digital initiatives.

[2] Government Accountability Office. (2023). "Information Technology: Federal Agencies Need to Address Ongoing Challenges." GAO-23-105084. https://www.gao.gov/products/gao-23-105084

Budget impact and efficiency considerations

Hidden cost multipliers

Digital transformation costs extend far beyond initial procurement. The Office of Management and Budget (OMB) found that federal IT projects frequently exceed initial budgets by 45% on average, with implementation costs accounting for only 25% of total lifecycle expenses.[3]

License management and resource optimization

Cost duplication is a major concern for public sector organizations. A recent WalkMe Digital Adoption Platform study reveals that organizations underestimate their application portfolios by 1600% – believing they use 37 apps when they actually use 625.[4]

Large agencies risk:

1. Purchasing technology they already own
2. Draining resources into maintaining underutilized licenses
3. Creating redundant systems across departments

[3] Office of Management and Budget. (2023). "Federal Information Technology Acquisition Reform Act (FITARA) Scorecard 15.0." https://oversight.house.gov/release/oversight-committee-releases-fitara-15-0-scorecard/

[4] WalkMe. (2023). "The State of Digital Adoption 2023." https://www.walkme.com/state-of-digital-adoption-report/

The Federal IT Dashboard reports that improper license management costs federal agencies an estimated $3.1 billion annually in unnecessary expenditures.[5] Implementing proper digital adoption strategies can reduce these costs by 30–40%.

1600%

underestimated app usage

Organizations believe they use 37 apps. In reality, they use 625.

$3.1B

wasted annually

$3.1B lost yearly to poor license management.

+30%

in cost savings

Digital strategies cut costs by 30–40%.

[5] Federal IT Dashboard. (2023). "Agency IT Portfolio Analysis." https://itdashboard.gov/

Efficiency gains through proper adoption

When properly implemented, digital transformation can deliver substantial efficiency gains. The U.S. Digital Service documented cases where well-executed modernization efforts reduced processing times by 65% and administrative costs by 40%.[6] However, these benefits are only realized with appropriate planning and execution.

[6] U.S. Digital Service. (2023). "Impact Report." https://www.usds.gov/impact-report

Return on investment metrics

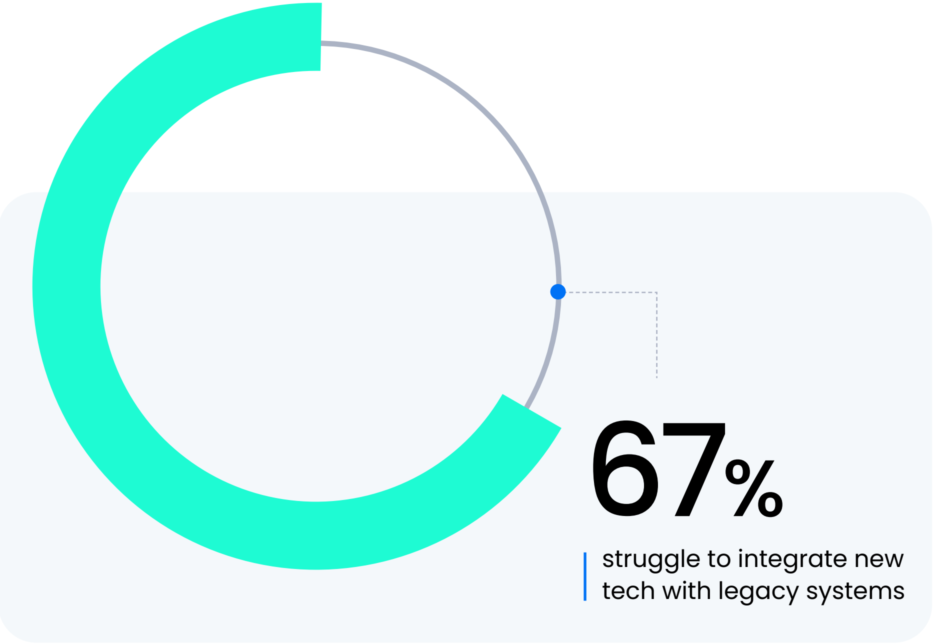
Public sector organizations should establish clear ROI metrics for digital initiatives:

1. **Cost avoidance:** Quantifiable reductions in operational expenses
2. **Time savings:** Reduced processing times and administrative burden
3. **Error reduction:** Fewer costly mistakes requiring remediation
4. **Resource allocation:** More efficient use of human capital

Infrastructure: Building the foundation of successful transformation

System integration across siloed departments

Siloed departments often struggle to solve problems holistically or deliver seamless services. The 21st Century Integrated Digital Experience Act (IDEA) mandates that federal agencies improve digital services through standardization, but implementation requires careful navigation of existing infrastructure constraints.[7] When new technology enters this fragmented landscape, agencies face a delicate balancing act of standardizing solutions while meeting these unique operational demands.



struggle to integrate new tech with legacy systems

Customization requirements

Heavily modified legacy systems require significant adaptation when implementing new technologies. Agencies constantly struggle to balance out-of-box solutions with agency-specific needs; according to a Deloitte study on government digital transformation, 67% of public sector organizations face substantial integration challenges with legacy systems.[8]

Security posture variations

Cross-system security protocols and compliance requirements introduce multiple points of potential data exposure across agency networks.

Different security systems, which require varying levels of protection, create a patchwork of protocols that must work together cohesively. Traditional security measures that were once adequate for simpler systems now strain under the sophisticated demands of modern digital tools.

As agencies navigate this challenging terrain, these infrastructure gaps create hidden costs and risks that extend far beyond their IT budgets.

[7] 21st Century Integrated Digital Experience Act. H.R. 5759, 115th Congress. (2018). https://digital.gov/resources/21st-century-integrated-digital-experience-act/

[8] Deloitte. (2023). "Government Digital Transformation Survey." https://www2.deloitte.com/us/en/pages/public-sector/articles/government-digital-transformation-strategy.html

The human element:
Change management essentials

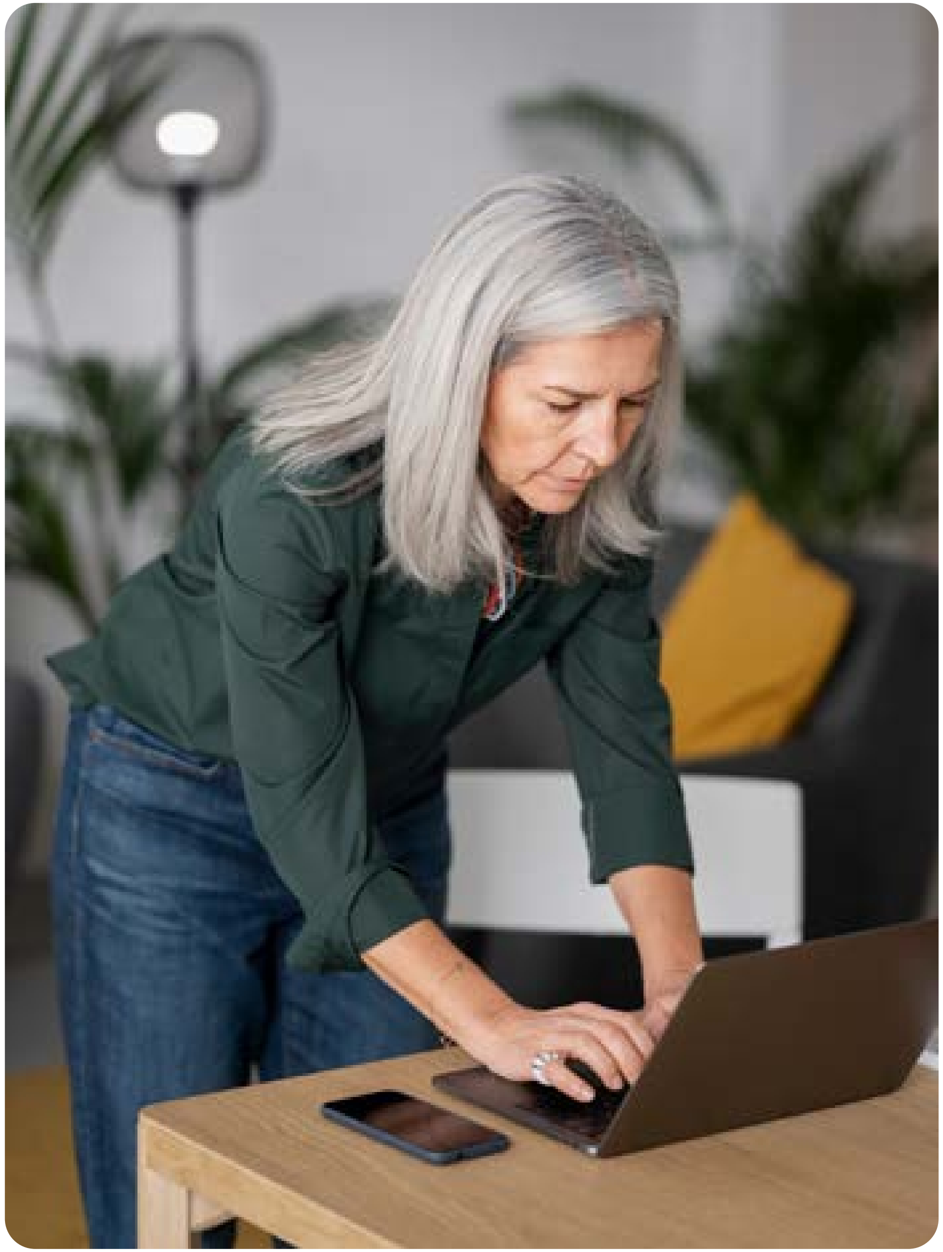
You should not underestimate the human element of digital transformation: Some employees have been using the same tools for the majority of their career and may be resistant to change. This is exacerbated when insufficient training leaves employees on their own. According to OPM Federal Employee Viewpoint Survey data, only 57% of federal employees felt their organization was effectively managing technological change.[9]

Training and support requirements

The "hypercare" period – the three-to-nine month window after deployment – requires intensive support. It's often managed with outdated methods that consume enormous resources but don't meet users where they are. The **Digital.gov Community of Practice** recommends allocating 15-20% of total project budgets to training and change management.[10]

Shadow IT proliferation

When official systems don't meet user needs efficiently, employees often turn to unauthorized tools. The security implications are severe, from bypassed protocols that can lead to exposure of classified or sensitive information to loss of centralized control and visibility.



[9] Office of Personnel Management. (2023). "Federal Employee Viewpoint Survey Results." https://www.opm.gov/fevs/

[10] Digital.gov. (2023). "Change Management Community of Practice." https://digital.gov/communities/change-management/

Emerging technologies: Preparing for the future

AI ethics and governance

> *There's no alternative provider for essential government services, which makes it all the more important that public sector organizations maintain the highest standards of fairness, transparency, and security.*

AI decisions affecting citizens' lives require accountability and appeal processes.

As AI adoption accelerates, organizations face unique ethical considerations:

1. **The risk of embedding systemic inequalities:**
   Without proper oversight, these biases could affect everything from benefit distributions to law enforcement systems.

2. **The challenge of maintaining compliance and protecting citizen privacy:**
   The volume and complexity of data flowing through public sector systems create multiple points of exposure. Security breaches can have far-reaching consequences for national security and citizen welfare.

Each technology brings its own security implications and integration challenges, multiplying the potential points of failure.

Data vulnerability at scale

The sensitivity and sheer volume of data processed by government AI systems create unprecedented vulnerability challenges. As digitization accelerates, agencies must maintain regulatory compliance while protecting vast repositories of citizen data.

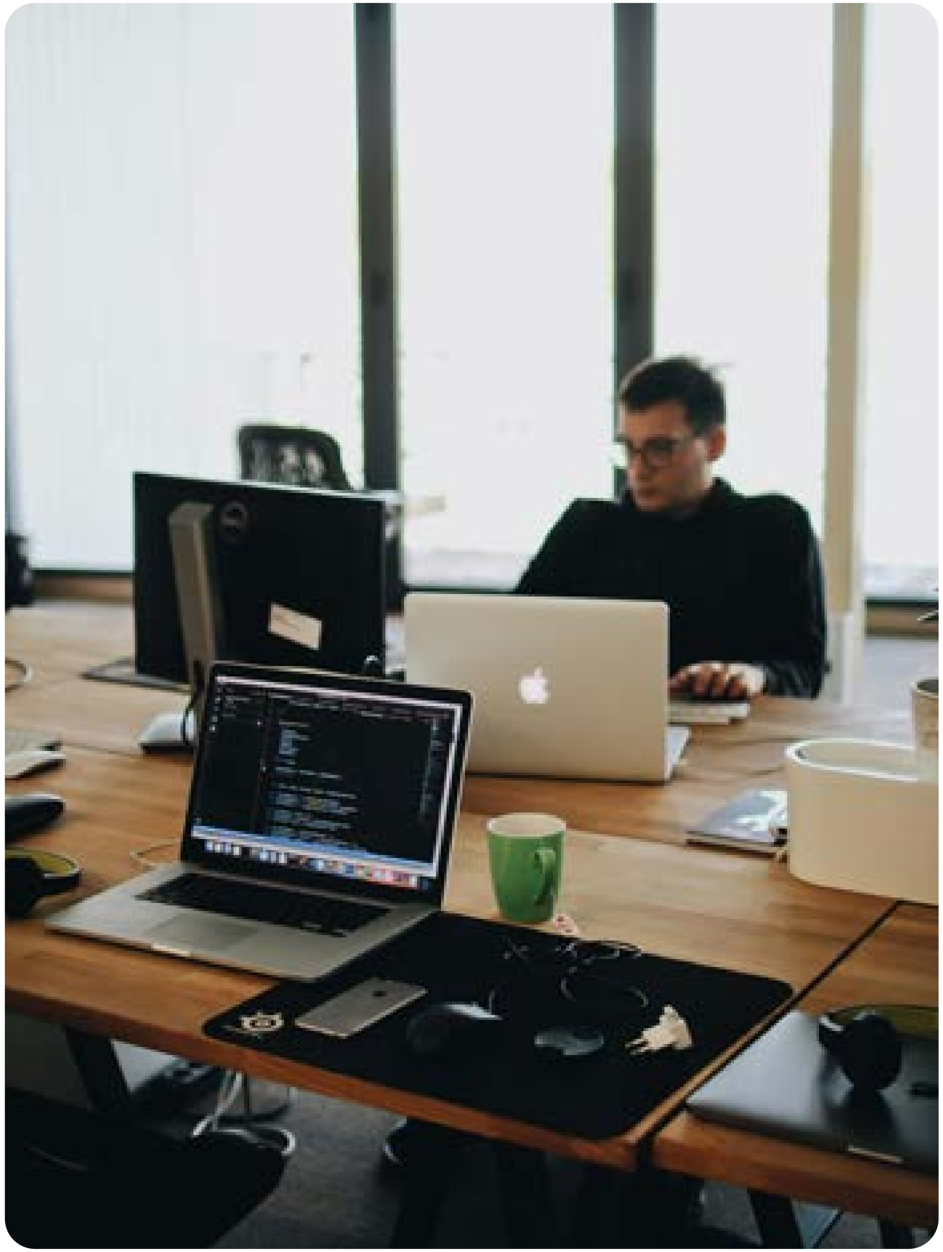
If proper controls aren't established, AI systems can inadvertently expose sensitive information through model outputs.

Public sector organizations must approach digital transformation with comprehensive planning that accounts for security, costs, infrastructure, human factors, and emerging technologies. By addressing these areas proactively, agencies can realize the full benefits of modernization while mitigating hidden costs and risks.

Beyond AI: The expanding technology landscape

While AI dominates the public eye, don’t overlook the explosion of other new technologies on the horizon:

- Blockchain for secure transactions
- IoT devices for smart city initiatives
- Cloud computing for remote services
- Quantum computing



The DAP advantage

With all these challenges, it may feel overwhelming for agencies to successfully serve the public while embracing innovation. But it can be done – and done well.

How? With a comprehensive digital adoption strategy. A digital adoption platform (DAP) is a key element for any organization.

What is a digital adoption platform?

> *DAPs function as a marriage between a public organization's standard operating procedure and its technology.*

The DAP sits on top of the technology and facilitates a seamless experience through interactive, just-in-time guidance.

Structured digital implementation

> *DAPs function as a contact lens, making UI improvements without modifying underlying systems.*

This allows agencies to modernize their user experience without the risks and costs of changing core functionality. Users can adapt to new systems gradually and with minimal disruption, while implementation is accelerated exponentially.

Employee enablement: Meeting users where they are

The DAP sits on top of the technology and facilitates a seamless experience through interactive, just-in-time guidance.

Extensive toolkit of contextual solutions

The on-demand nature of DAP guidance enables employees to get support in their moment of need – whether that's during their first week on the job or months later when performing an infrequent task. The traditional "pull model" training is replaced with contextual learning that delivers guidance precisely when needed – no more digging through manuals or SharePoint sites.

Get assistance when needed:

1. During onboarding with new systems
2. When encountering infrequently used features
3. After system updates or policy changes
4. During complex multi-step processes
5. When transitioning between related systems

This approach eliminates the "forgetting curve" problem of traditional training.

Hypersegmentation

DAPs offer customizable solutions that can be tailored to specific roles, responsibilities, and locations to ensure that WalkMe solutions directly apply to each employee's day-to-day tasks.

DAPs deliver hypersegmented experiences tailored to:

1. Employee roles and responsibilities
2. Geographic location and jurisdiction
3. Experience level and digital proficiency
4. Language preferences and accessibility needs

Accommodations

Diverse workforces are supported with multilingual content and accessibility features that comply with government standards. To ensure users can learn comfortably, DAPs deliver guidance:

- Visually
- Interactively
- Textually

Compliance by design

Compliance enforcement can be tailored according to need, from gentle reminders to strict procedural guardrails that prevent policy violations. Rather than treating compliance as a separate training topic, DAPs embed directly into workflows:

1. Real-time policy guidance that prevents violations
2. Automated data validation that catches errors before submission
3. Interactive reminders about security protocols
4. Documentation of completion for audit purposes

AI integration

In a world that threatens to leave the public sector behind on innovation, DAPs are here to partner with organizations as they embrace digital transformation.

Serving as the foundation for public sector digital transformation, DAPs enable organizations to meet security demands while keeping pace with an evolving technology landscape that increasingly requires AI.

Government agencies exploring AI face a dual challenge:

1. Ensuring employees can effectively use powerful AI tools.
2. Maintaining strict control over how they're deployed.

Solutions to both challenges can be found within a DAP.

DAPs bridge the critical human readiness gap and reduces employee resistance by providing:

Contextual learning

Embedded AI guidance directly into employee workflows, rather than separate training sessions.

Personalized support

Adapted guidance based on role, experience level, and prior interaction history meet users where they are.

Performance support

Just-in-time assistance at the exact moment of need

AI governance

Beyond adoption, DAPs establish the essential governance structure that responsible AI deployment demands:

Usage visibility

Comprehensive dashboards showing which AI tools are being used, by whom, and how

Compliance monitoring

Real-time enforcement of ethical guidelines and security protocols

Pattern detection

Early identification of potential bias issues before they impact citizens

Access control

Granular permissions that limit AI tool access based on role, training, and authorization

As large language models and other AI tools continue evolving at unprecedented speed, DAPs maintain continuous oversight while enforcing organizations' ethics standards and supporting zero trust architecture implementation.

Zero Trust Architecture:
A security model that requires strict identity verification for every person and device trying to access resources, regardless of whether they are inside or outside the network perimeter.

The result is a balanced approach that empowers employees while maintaining control. By promoting transparency in automated decisions and ensuring fair citizen access, DAPs transform AI from a potential risk into a powerful, responsibly managed asset that enhances rather than compromises an organization's mission.

Continuous improvement and adaptation

DAPs enable agencies to shift from traditional waterfall implementation approaches to more agile, continuous improvement models. IT departments can monitor the efficiencies and inefficiencies, with DAPs serving as the foundation for transformation.

With DAPs, agencies deliver ongoing improvements through continuous monitoring and data-driven adjustments.

Measuring success

The financial impact of improved efficiency is substantial when viewed across the entire federal workforce:

The average cost of a single federal employee is 85 cents a minute, $51 an hour, $408 a day, and over $106,000 annually. Just 10 minutes of improved efficiency each day saves $2,200 per employee, per year. Across the federal workforce, that's $6.6 billion in potential savings.

Average Federal Employee Cost

$106K+	per year
$408	per day
$51	per hour
85¢	per minute

10 minutes saved =

$2.2k

Each employee saves $2,200 annually with just 10 minutes of daily efficiency gains.

Potential savings

$6.6B

Saving 10 minutes per day across the federal workforce adds up to $6.6B each year.

Resource optimization

Eliminating unnecessary steps in digital processes – those that add no value but consume time – provides a concrete measurement of efficiency improvements. Tracking the reduction in these "empty clicks" demonstrates tangible workflow optimization.

Mission-focused improvements

DAP success metrics capture how technology implementations free up employee time for mission-critical activities rather than administrative tasks. This efficiency gain means more time to spend on valuable, human-centric work.

WalkMe for the public sector

As the pioneer of the digital adoption category and the only cloud-based FedRAMP-Ready DAP in the marketplace, WalkMe stands alone in its ability to meet the rigorous demands of government agencies. It has already transformed how many federal, state, and local agencies deliver citizen services, enhance employee productivity, and maximize technology investments.

Unmatched government credentials

WalkMe's unique position in the government technology space gives agencies the confidence to modernize with security and compliance built-in.

WalkMe's comprehensive data protection controls include critical capabilities for maintaining security in government environments:

1. field-level visibility restrictions that limit access to sensitive information
2. censorship settings that can mask confidential data
3. robust prevention measures against unauthorized data exposure

WalkMe's FedRAMP-Ready status means you can deploy modern cloud solutions that meet even the most stringent security requirements without compromise. For agencies requiring complete isolation, WalkMe's flexible architecture allows for on-premise deployment within fully siloed environments. Security is ensured regardless of your infrastructure needs.

The enterprise-grade advantage

As the most mature DAP vendor in the market with more than 40% market share, WalkMe has built an enterprise-grade platform specifically designed for a strong and expanding base of public sector clients. From the Department of Defense and federal civilian agencies to state organizations and higher education institutions, WalkMe delivers solutions tailored to the public sector's unique needs.

Data-driven methodology helps you measure impact and ROI through enterprise-level dashboards. Quantified results cater to senior executives who have a goal-based approach. Measurable outcomes ensure your agency can demonstrate the value of its technology investments.

WalkMe prioritizes self-sufficiency through a low-code platform, making it easy to onboard non-technical users. Pre-built solutions based on industry best practices accelerate implementation, while proprietary Element Recognition technology – protected by 16 granted patents – detects changes in underlying applications, ensuring end-user journeys remain unaffected even as systems evolve.

Designed for mission speed and scale

WalkMe is the only solution that can identify changes in underlying applications and offer bulk replacement mechanisms that address problems quickly to maintain continuity in mission-essential functions. The unified DAP experience extends beyond web applications to desktop and mobile, providing consistent support across all digital touchpoints.

More than just a platform, WalkMe leads the DAP market with an extensive partner ecosystem, community resources, and comprehensive training and certifications.

The original innovation leader

As the creator of the digital adoption category, WalkMe brings unmatched experience and expertise to government deployments. WalkMe customers benefit from an expansive knowledge base of best practices, implementation strategies, and proven methodologies in the industry.

WalkMe doesn't just help you adopt technology – it transforms how your agency serves citizens in the digital age.

Proven success

The numbers speak for themselves: WalkMe delivers a three-year 494% ROI over three years. This isn't theoretical value – it's validated performance across thousands of implementations, including numerous government agencies.

City of Chandler: A case study

After deploying WalkMe to improve employee experience and simplify change management for its diverse workforce, the City of Chandler saw:

25–30m

Time saved on expense reports

50%+

Enrollment in system alerts

1,800+

Employees supported in real time

> *"The breadth and depth of WalkMe's capabilities help us create impactful experiences for our team members and organization – and we're excited to continue developing how we use WalkMe moving forward."*
>
> Traci Tenkely, IT Project Manager at the City of Chandler

Sector-specific applications

DAPs can be tailored to the unique needs of different government sectors:

Defense and intelligence agencies

Take advantage of classified information protection, multi-level security clearance management, secure deployment in classified environments, and supply chain modernization support.

Civilian agencies

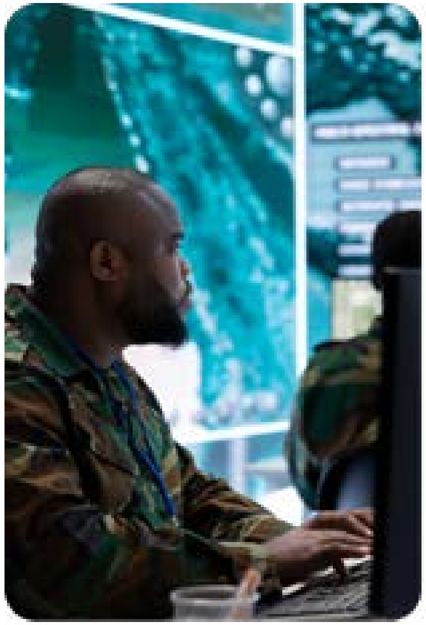
Benefit from citizen service delivery optimization, privacy-compliant automation, transparent processes, and improved access to benefits.

Government healthcare providers

Leverage DAPs for HIPAA compliance support and patient data protection strategies.

Educational institutions

Use DAPs to secure student information, simplify administrative processes, and easily guide students and educators through new learning platforms.



Conclusion

Government agencies already embracing digital adoption platforms are gaining decisive advantages – serving citizens faster, operating more efficiently, and attracting innovative talent eager to work with modern tools.

What separates these forward-thinking organizations from those falling behind isn't budget size or technical sophistication – it's their commitment to a comprehensive digital adoption strategy. They've recognized that DAPs are the critical bridge connecting ambitious modernization goals to actual mission success.

Your path forward begins with three concrete steps:

1. Assess your current digital adoption maturity. Identify where your employees struggle with existing systems and which upcoming technology initiatives would benefit most from structured adoption support. This baseline understanding will help you prioritize your implementation strategy.
2. Explore how a FedRAMP-Ready DAP like WalkMe can integrate with your specific security requirements and technical environment. Request a demonstration focused on your highest-priority use cases to see firsthand how the platform works within your context.
3. Develop a phased implementation plan that begins with quick wins to build momentum. Start with a high-visibility process where improved efficiency would immediately benefit both employees and citizens. Use the success metrics from this initial deployment to make the case for broader implementation.

Agencies that take these steps now will define public sector excellence for the next decade. Those that hesitate will face an increasingly difficult path to digital relevance, widening the gap with each passing month.

Your agency stands at a pivotal moment. Will you lead the transformation that citizens increasingly expect, or will you struggle to catch up as the digital landscape continues to evolve? The choice – and the opportunity – is yours.

About WalkMe

WalkMe is a global leader in digital adoption, helping organizations across industries navigate the complexities of digital transformation. Our digital adoption platform provides the tools needed to ensure that new technologies are fully embraced by employees and customers alike.

With WalkMe, organizations gain access to in-app guidance, automated workflows, and real-time analytics, all designed to enhance the user experience and improve technology adoption. Our platform is trusted by government agencies worldwide to drive change, streamline processes, and achieve their mission objectives in a fast-evolving digital landscape.

Request a demo