PROVANCE

WHITEPAPER

Modernizing Government IT Services: The Key to Cutting Costs Without Increasing Risk

Practical strategies for government agencies to modernize services while lowering costs, safeguarding trust and minimizing risk.

Authored by John Clark, MBA, ITIL and Solutions Architect Expert, PROSCI Change Practitioner

Introduction

Public sector agencies operate under a unique mandate: deliver essential services at the lowest possible cost while maintaining the highest standards of accountability, traceability, compliance and public trust. Unlike commercial enterprises, profitability is not a goal; service, stability, and risk reduction are. This mission comes with extraordinary pressures: heightened public scrutiny, strict legal mandates, fixed budgets, and the constant need to safeguard employees and constituents alike.

This whitepaper explores the paradox at the heart of public sector IT—how to reduce costs without increasing risk. We reveal why inaction often carries the highest price—hidden risks, mounting technical debt, and operational fragility. Then we outline proven strategies for reducing IT expenditures. Finally, we address the ultimate question: how to achieve cost savings without compromising security, compliance, or operational resilience.

John Clark,
MBA, ITIL &
Solutions Architect Expert,
PROSCI Change Practitioner

John Clark brings over 25 years of experience in enterprise technology strategy, specializing in ITSM, Cloud architecture, AI integration and digital transformation across the public sector—including defense, intelligence and civilian agencies—as well as healthcare, finance and manufacturing.

Over his 13 years at Microsoft, John led modernization programs and cloud adoption initiatives for public sector clients, introducing AI-driven services, strengthening governance models, and delivering multimillion-dollar cost savings. Recognized globally as a subject matter expert in ITSM, Operations and Governance, John is trusted for translating emerging technologies into secure, compliant and business-ready solutions that drive measurable impact and cost-savings. His expertise ensures organizations can adopt innovation with confidence while safeguarding critical operations.

The Public Sector Challenge

Downsized Budgets

Governments worldwide are facing mounting financial strain with global debt exceeding 95.3 trillion (USD).[i] And many organizations are confronting severe funding gaps. In the US, state governments are downsizing amid uncertain revenues,[ii] while in the UK, councils are projected to face an £8 billion funding gap.[iii] Against this backdrop, public sector IT—the backbone of modern service delivery—is under intense pressure to do more with less. A 2025 EY survey shows cost reduction (56%) and cybersecurity (54%) are top priorities for state and local government IT leaders, highlighting the dual challenge of fiscal responsibility and risk mitigation.[iv]

Rising Service Expectations

As commercial services evolve, government services must keep pace with rising expectations for efficiency, transparency, and digital accessibility. Citizens want to interact with government as seamlessly as they do with businesses they interact with daily—through modern tools like chatbots and online portals, anytime and anywhere. They expect intuitive, user-friendly experiences, not the outdated and cumbersome interfaces of legacy systems.

Lack of Skilled IT Professionals

Governments have long struggled to attract highly technical talent. They are often unable to compete with private companies due to (we believe) the misplaced perception that public sector roles are less innovative and are less likely to be career-defining. However, low-code/no-code platforms and AI are transforming these dynamics allowing for more time spent on creative problem-solving and innovation, and economic uncertainty makes stability and purpose more appealing to younger workers.

Lengthy Procurement and Strict Compliance Requirements

Governments have a fundamental duty to serve and protect the public, which drives strict compliance requirements in procurement processes. In democratic nations, procurement must uphold fairness, transparency, and accountability while carefully balancing risk. Unlike commercial enterprises, government officials operate under heightened scrutiny, demanding rigorous safeguards. As a result, procurement cycles are intentionally designed to protect employees and citizens.

Increased Security Threats

Cybersecurity threats such as phishing schemes and ransomware attacks are escalating as criminals increasingly target governments. These attacks exploit two key vulnerabilities: the perception that governments have deep financial, informational and data resources and the continued reliance on legacy systems. Governments hold sensitive information and public concern over breaches is growing, with citizens demanding both security and resilience against cybercrime. Adopting a Zero Trust security posture is essential for government agencies, yet elevating systems to meet this standard remains a significant challenge.

Legacy Systems and Integration Complexity

Securing buy-in for upfront investments is challenging because replacing existing systems is seen as risky, even when new solutions promise lower maintenance costs. Years of multiple functions within governments relying on diverse tools have created fragmented environments with data silos and a patchwork of applications that are hard to consolidate and update, hampering interoperability. Many legacy systems also depend on outdated programming languages, and the shrinking pool of professionals who understand them makes upgrades even more challenging. Cultural resistance further compounds the problem, as concerns about risk and disruption make change harder to achieve.

The Hidden Costs of Doing Nothing

In 2019, the city of Baltimore fell victim to a ransomware attack that crippled municipal services for weeks and cost millions in recovery.[v] More recently, the U.S. Federal Judiciary suffered a cyberattack targeting its decades-old Case Management system. Built in the 1990s and long overdue for modernization, the breach exposed sensitive information and forced courts to revert to paper filings, underscoring the risks of underfunded IT modernization.[vi] In addition, the St. Paul's July 2025 ransomware attack disrupted city services but spared emergency operations, reinforcing the urgency for zero-trust security, tested recovery plans, and strong communication strategies. The incident shows that resilience and pre-arranged data recovery partnerships are essential to limit downtime and protect public trust.[vii]

Keeping legacy systems in place long past their prime compounds technical debt and creates significant operational risks. These outdated platforms demand excessive manual effort, increase service disruptions, and clash with modern technologies. Their lack of integration fosters data silos and inefficiencies, while maintenance costs soar due to obsolete components and scarce specialized skills.

Legacy systems also reduce agility, making it harder to adopt new tools or integrate advanced platforms. They heighten security vulnerabilities, exposing governments to evolving cyber threats and potential data breaches. Developer productivity suffers under complex, hard-to-maintain codebases, slowing innovation and delaying time-to-market—ultimately costing far more than modernization.

In 2025, the US Government Accountability Office reported that the US Federal government spends $100 billion on IT annually—mostly to maintain aging, costly, and vulnerable legacy systems—and urged Congress to require agencies to create modernization plans.[viii] Moreover, it's well known that many of the critical systems have unfixable cybersecurity vulnerabilities and rely on outdated programming languages, making modernization the only viable and cost-effective solution.[ix]

Failing to modernize risks eroding public trust and widening the gap between citizen expectations and government capabilities. Modernization isn't just a technical upgrade, it's a strategic imperative for security, efficiency and resilience.

Strategies to Drive Costs Out of IT

Adopt a Platform-Centric Approach

Public sector agencies can significantly reduce IT costs by moving away from fragmented systems and adopting a platform-centric approach. Platforms provide built-in integrations and access to a wide range of business applications, making implementation faster and less expensive. This consolidation lowers long-term maintenance costs and simplifies upgrades, while reducing the complexity of managing multiple disconnected solutions.

A platform-centric strategy also streamlines workforce requirements. Because platforms share a consistent interface and functionality, agencies can leverage a single skill set across multiple services instead of hiring specialists for each solution. This makes recruiting and training easier, reduces reliance on external vendors, and accelerates innovation, especially if a low-code/no-code or an AI-supported platform is used.

Beyond significant cost savings, platforms enable standardization and interoperability across agencies, eliminating duplication and integration challenges. Shared digital infrastructure supports modular, reusable services, improving security and compliance with built-in governance features. While replacing legacy systems may require upfront investment, the result is a modern, scalable environment that delivers better services to citizens and measurable ROI.

Governments face greater challenges in modernizing than newer organizations because transformation requires more than software upgrades—it demands changes to internal processes and culture. However, agencies that embrace this shift unlock significant benefits: streamlined operations, improved efficiency, and the ability to deliver better services under tighter budgets. By adopting modern platform-centric strategy, agencies can overcome legacy constraints, reduce long-term IT costs and meet rising citizen expectations with agility and accountability.

Leverage Automation and AI

The benefits of automation are well known—eliminating repetitive manual tasks, streamlining operations and improving resource utilization.[x] It can also accelerate service delivery and boost productivity without requiring proportional increases in staffing or infrastructure. These efficiencies free employees to focus on higher-value initiatives, reducing labor costs and improving overall performance.

AI builds on these benefits by introducing learning, predictive analytics and optimization capabilities. Implementing both automation and AI can enable organizations to identify inefficiencies and redesign processes for cost savings. Studies show the financial impact can be significant. Microsoft and IDC found that for every $1 invested in generative AI, organizations are seeing an average return of $3.70.[xi] Similarly, process automation can cut time spent on routine tasks like scheduling by more than 50%, driving measurable savings.[xii]

Public sector agencies are increasingly prioritizing AI and automation as core modernization strategies. Gartner predicts that by 2029 60% of Government agencies globally will automate over half of citizen transactional interactions using AI agents, up from less than 10% in 2025.[xiii] The cost of automation and AI is falling, while the cost of doing nothing is increasing, making modernization an undeniable imperative. These technologies empower governments to do more with less, reducing technical debt and future-proofing IT investments. In short, automation and AI are no longer optional—they're essential for driving efficiency, cutting costs and delivering better services under tight budgets.

Standardize and Streamline IT Service Delivery with ITSM

IT Service Management (ITSM) is a structured approach to designing, delivering, managing, and improving IT services throughout their lifecycle. Leveraging ITSM best practices and standardizing and streamlining IT service delivery are proven strategies for reducing complexity and driving down IT costs. Public sector agencies should focus on meeting citizen needs efficiently, not be constrained by the outdated, disparate IT systems that have grown like weeds over time. When agencies standardize IT service delivery economies of scale emerge, duplication disappears and the cost of delivering services drops significantly. Moreover, centralized data and standardized workflows will further amplify these savings by creating a single source of truth. This improves visibility, accelerates decision-making and reduces errors that lead to costly downtime.

Streamlined service delivery fosters collaboration and optimizes resource utilization. Integrated workflows allow teams to share tasks seamlessly, improving efficiency, and enhancing staff and citizen satisfaction without increasing overhead. In short, standardization and centralization aren't just operational improvement—they are essential strategies for reducing IT costs and enabling agencies to deliver consistent, high-quality services under tight budgets.

Optimize Asset Management

Leveraging cloud for IT resources makes sense, but there are still assets that need to be managed by the IT organization. A modern, proactive IT Asset Management (ITAM) strategy significantly reduces costs for government IT by improving visibility, traceability, and control. Optimized ITAM provides a clear view of total cost of ownership (TCO), factoring in performance history, incident trends, and vendor ratings. This prevents agencies from overspending on assets that seem inexpensive upfront but carry high maintenance costs later. Accurate tracking of hardware and software also eliminates redundant purchases, enables license reclamation, and supports better vendor negotiations. Integrating ITAM with procurement systems ensures timely renewals, avoids penalties, and leverages vendor performance data for smarter purchasing decisions—critical for agencies operating under tight budgets.

Beyond cost savings, ITAM enhances operational efficiency and service delivery. Detailed asset data—such as warranty coverage, support contracts, leasing agreements, and lifecycle status—empowers IT teams to resolve incidents quickly and cost-effectively. For example, knowing a device is under warranty prevents unnecessary replacement expenses. Automation and real-time dashboards further reduce administrative overhead, allowing agencies to shift from reactive to proactive management. This improves resource allocation and elevates the quality of services provided to citizens.

Finally, ITAM strengthens compliance and security, essential for government organizations handling sensitive data. Centralized tracking of assets and licenses minimizes audit risks and ensures regulatory adherence. ITAM done right becomes a strategic enabler—supporting transparency, accountability, and data-driven decision-making for resource planning and crisis management. In short, optimized ITAM transforms IT from a cost center and into a driver of efficiency and governance excellence.

Leverage Enterprise Service Management and Multi-Discipline ITSM

One of the most effective ways to reduce IT costs is to extend the proven principles and practices of ITSM throughout all IT departments and across the organization. Multi-discipline ITSM[xiv] and Enterprise Service Management (ESM)[xv] spread cost savings by standardizing processes, centralizing data, and enabling self-service across the organization. ESM extends proven service management practices beyond IT, reducing duplication and manual work, while multi-discipline ITSM unifies workflows and communications within IT. Together, these approaches minimize operational overhead, accelerate service delivery, and foster collaboration—allowing teams to identify and eliminate wasteful practices and leverage automation for routine tasks, which significantly lowers labor and administrative costs.

Both ESM and Multi-discipline ITSM enhance accountability and transparency, ensuring resources are allocated effectively and services are delivered consistently. Integrated workflows and centralized data help organizations avoid siloed operations that often lead to redundant spending and inefficiencies. These improvements not only reduce direct IT costs but also optimize the performance of other business units, amplifying the overall return on investment.

Ultimately, ESM and Multi-discipline ITSM transform service delivery into a unified, streamlined experience that benefits employees and customers alike. By leveraging AI, automation, analytics, and shared solutions, organizations achieve higher productivity and better outcomes without increasing costs—making the implementation of these disciplines strategic tools for cost control and operational excellence.

Plan for Value Realization

Public sector agencies succeed when IT strategies align with organizational goals. To achieve this, agencies should develop a roadmap that captures and tracks the benefits outlined in the business case. While it's difficult to prove that a negative outcome was avoided, defining measurable success metrics—such as cost savings, efficiency gains, and improved service delivery—makes value tangible. Tracking these metrics post-implementation ensures accountability and transparency. Leveraging ITSM to standardize processes and governance helps technology drive efficiency rather than add complexity. Planning for value realization means every dollar invested delivers measurable organizational benefits or reduces risk.

Strategies to Reduce Risk

If you haven't already adopted the Power Platform and Azure

Technology can serve as a transformative enabler. Adopting Microsoft Power Platform and Azure enables agencies to modernize operations and achieve substantial cost savings without increasing risks. By leveraging a low-code, AI-enabled platform solution, agencies can streamline workflows, reduce manual effort, and minimize the need for highly technical skills and custom development. A recent Forrester Total Economic Impact study found that organizations deploying Power Platform realized a 224% ROI over three years and an $81.7 million net present value, with up to 25% savings per impacted employee.[xvi] These savings come from improved operational visibility, direct IT cost reductions and enhanced customer engagement, while, incidentally, reducing shadow IT and fostering a culture of digital innovation.

Standardizing on Microsoft's ecosystem allows agencies to retire redundant systems, eliminate overlapping licenses and reduce support costs. The Power Platforms' AI, automation and low-code/no-code capabilities, further reduce reliance on costly external contractors and IT teams, while modern and user-friendly capabilities such as portals and chatbots can empower citizens and improve satisfaction. Microsoft's ongoing commitment to innovation—over $30 billion in R&D in 2025 alone[xvii]—ensures governments will benefit from the latest advancements.

Security and compliance are paramount, and Azure provides a robust, compliant foundation for Power Platform, protecting sensitive data and meeting regulatory requirements. Trusted by over 95 percent of Fortune 500 companies[xviii] and many public sector organizations worldwide, Azure is recognized as one of the most secure cloud platforms available. Microsoft invests over $1 billion in cybersecurity research and development per year,[xix] employing more than 3,500 security experts to protect customer data and infrastructure. Microsoft's Zero Trust strategy[xx] combined with Azure's multi-factor authentication, encryption (including double encryption) and proactive monitoring, help government agencies minimize vulnerabilities and respond swiftly to threats, while maintaining authorizations like FedRamp High, DoD IL5, CJIS, HIPAA, GDPR and other compliance certifications.[xxi]

By choosing Power Platform and Azure, agencies unlock a foundation of resilience and public trust. This unified approach delivers measurable costs savings and robust security, while empowering agencies to adapt quickly, integrate seamlessly with a diverse ecosystem of business applications, and deliver citizen services that are modern, efficient and secure.

If you have already adopted the Power Platform and Azure

If your agency has already embraced the Power Platform and Azure, you've built a strong foundation for cost savings, risk reduction, and operational efficiency. These platforms are designed for seamless interoperability, making it easy to connect data and processes across Microsoft 365, Dynamics 365, Azure, and hundreds of third-party solutions. By eliminating data silos and creating a single source of truth for citizen information, you're already reaping the benefits of a unified, secure, and flexible digital environment. Azure's support for a wide range of programming languages, frameworks, and systems—both Microsoft and non-Microsoft—means your agency can build, deploy, and manage applications in whatever way best fits your needs.

Now is the perfect time to build on that success by extending these capabilities to additional business applications such as ServiceTeam ITSM and ITAM. By deploying solutions on top of your existing platform investment, you can further streamline service delivery, automate routine tasks, and apply best practices across departments. These purpose-built applications are designed to maximize the value of your Power Platform and Azure investment, helping you achieve even greater cost savings, reduce manual workload, and maintain the highest standards of security and compliance. Most importantly, they empower your agency to keep innovating and adapting to the evolving needs of the public you serve.

Implement ServiceTeam for ITSM and ITAM

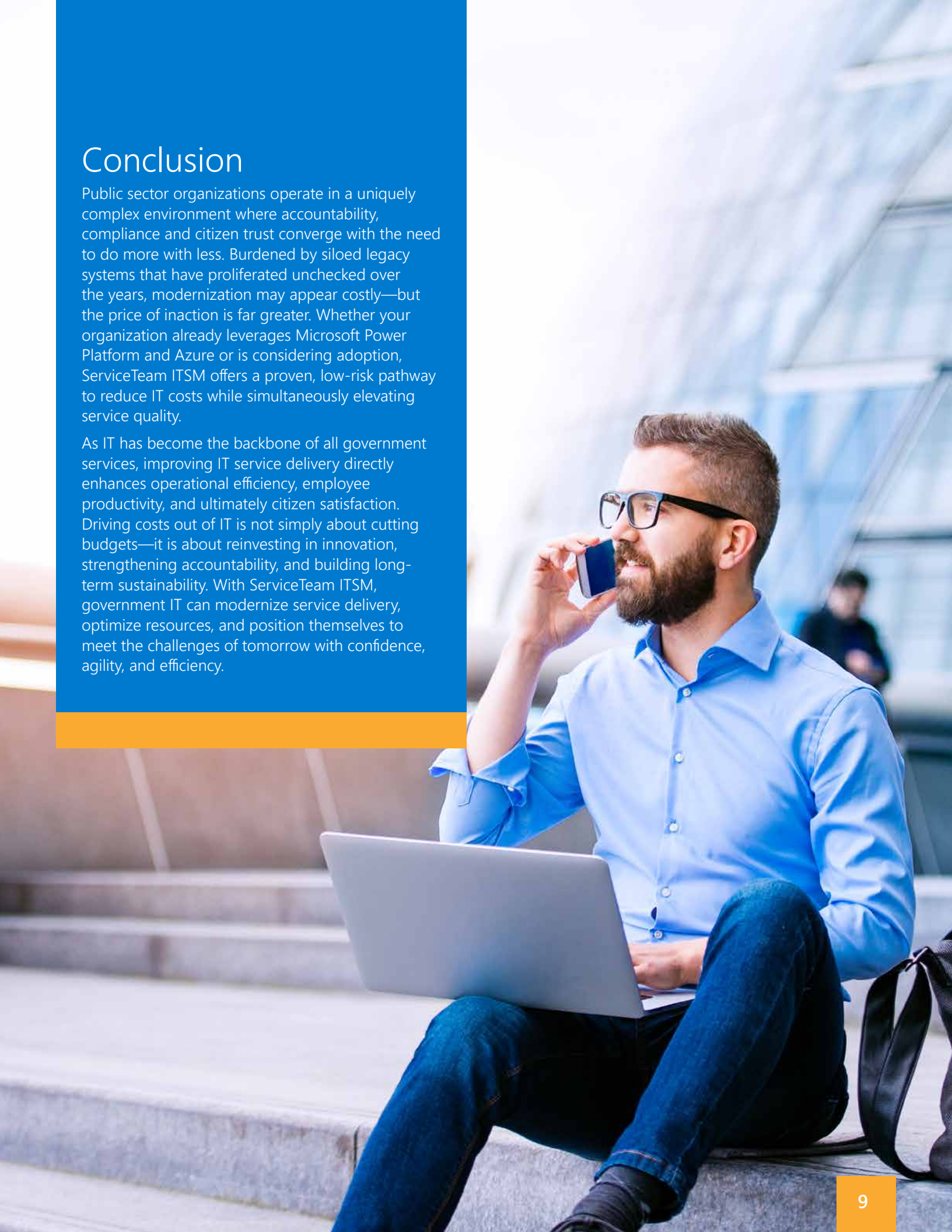
ServiceTeam ITSM and ServiceTeam ITAM stand out as cost-effective business applications that fit seamlessly into the Microsoft ecosystem, making them an ideal choice for public sector agencies seeking to drive down IT costs without increasing risk. During many of my years at Microsoft, I worked alongside Provance and I've seen firsthand how ServiceTeam delivers real value—not just in theory, but in practice as demonstrated by successful deployments in organizations like the City of London and the City of London police and Carver County.

ServiceTeam ITSM is built natively within the Power Platform, allowing it to fully capitalize on the platform's low-code/no-code, standardization, automation and AI capabilities. This means that agencies can benefit with ServiceTeam ITSM from simplified configuration, powerful analytics and intelligent service delivery, all while following proven ITSM and ITAM best practices.[xxii] Agencies end up with the best of both worlds. Because ServiceTeam operates within the Azure ecosystem, Azure capabilities and benefits "flow-through" to Serviceteam, bestowing enhanced security, greater flexibility, scalability and reliable backup and disaster recovery to name a few.[xxiii] Deploying ServiceTeam ITSM and ITAM as part of a platform-centric strategy ensures agencies can modernize IT service delivery, reduce operational overhead, and maintain compliance—all while minimizing risk and maximizing value.

Conclusion

Public sector organizations operate in a uniquely complex environment where accountability, compliance and citizen trust converge with the need to do more with less. Burdened by siloed legacy systems that have proliferated unchecked over the years, modernization may appear costly—but the price of inaction is far greater. Whether your organization already leverages Microsoft Power Platform and Azure or is considering adoption, ServiceTeam ITSM offers a proven, low-risk pathway to reduce IT costs while simultaneously elevating service quality.

As IT has become the backbone of all government services, improving IT service delivery directly enhances operational efficiency, employee productivity, and ultimately citizen satisfaction. Driving costs out of IT is not simply about cutting budgets—it is about reinvesting in innovation, strengthening accountability, and building long-term sustainability. With ServiceTeam ITSM, government IT can modernize service delivery, optimize resources, and position themselves to meet the challenges of tomorrow with confidence, agility, and efficiency.



Endnotes

i Deloite (2025). 2025 Government Trends:
https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/government-trends.html#delivering-on-lower-cost

[ii] Pew Research Center (2024). State Budgets are Downsizing:
https://www.pew.org/en/research-and-analysis/articles/2024/07/15/state-budgets-are-downsizing

[iii] Deloite (2025). 2025 Government Trends:
https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/government-trends.html#delivering-on-lower-cost

[iv] EY (2025). Government State and Local 2025 Survey Findings:
https://www.ey.com/en_us/insights/government-public-sector/ey-government-state-and-local-2025-survey-findings

[v] Wikipedia (2025). 2019 Baltimore Ransomware Attack:
https://en.wikipedia.org/wiki/2019_Baltimore_ransomware_attack

[vi] Reuters (2021). US Federal Court Filing System Breached in Sweeping Hack:
https://www.reuters.com/world/us/us-federal-court-filing-system-breached-sweeping-hack-politico-reports-2025-08-07/

[vii] Builtin (2025). Lessons From a Major Cyber Attack on a City Government: Z
https://builtin.com/articles/lessons-cyber-attack-city-government

[viii] US Government Accountability Office (2025). Information Technology: Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems: https://www.gao.gov/products/gao-25-107795

[ix] ExecutiveGov (2025). GAO Report Finds 11 Critical Gov't Tech in Need of Update.
https://www.executivegov.com/articles/gao-report-it-modernization-legacy-systems-federal-agencies-vulnerabilities

[x] Provance (2025) What's the Difference Between Automation and AI:
https://www.provance.com/blog/whats-the-difference-between-automation-and-ai/

[xi] Microsoft (2023) What Can Copilot's Earliest Users Teach Us About AI at Work?
https://www.microsoft.com/en-us/worklab/work-trend-index/copilots-earliest-users-teach-us-about-generative-ai-at-work

[xii] Microsoft (2025). Transforming Government Efficiency and Mission Delivery Whitepaper:
https://techcommunity.microsoft.com/blog/publicsectorblog/unlocking-opportunities-for-government-efficiency/4372684

[xiii] Gartner (2025). Gartner Reveals Top Technologies Shaping Government AI Adoption:
https://www.gartner.com/en/newsroom/press-releases/2025-09-09-gartner-reveals-top-technologies-shaping-government-ai-adoption

[xiv] Provance (2025) Drive Efficiency, Performance and Innovation: Strategic Value of ITSM Across Corporate IT Whitepaper:
https://www.provance.com/resource/strategic-value-of-itsm-across-corporate-it-whitepaper/

[xv] Provance (2025). Beyond IT: 10 Ways ServiceTeam ITSM Powers ESM: https://www.provance.com/blog/enterprise-service-management/

[xvi] Forrester (2024). The Total Economic Impact™ of Microsoft Power Platform:
https://tei.forrester.com/go/Microsoft/PowerPlatform2024/?lang=en-us

[xvii] Statistica (2025). Microsoft Corporation: R&D Expenditure.
https://www.statista.com/statistics/267806/expenditure-on-research-and-development-by-the-microsoft-corporation/

[xviii] Microsoft (2025). What is Azure?: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure/

[xix] Microsoft (2025). Trust Your Cloud: https://azure.microsoft.com/en-us/explore/trusted-cloud/

[xx] Microsoft (2025). Protect and Modernize Your Organization with a Zero Trust Strategy:
https://www.microsoft.com/en-us/security/business/zero-trust

[xxi] Microsoft (2025). Azure Government: Azure, Dynamics 365, Microsoft 365 and Power Platform Services Compliance Scope:
https://learn.microsoft.com/en-us/azure/azure-government/compliance/azure-services-in-fedramp-auditscope

[xxii] Provance (2024). Not Just a Simple Power App: How ServiceTeam Leverages the Microsoft Power Platform for Comprehensive ITSM and ITAM: https://www.provance.com/blog/serviceteam-microsoft-power-platform-itsm-itam/

[xxiii] Provance (2024). More Than Just an App on Microsoft Azure: How Azure Capabilities Flow Through ServiceTeam Power Apps to Benefit our Customers. https://www.provance.com/blog/azure-flow-through-serviceteam-benefit-customers/