1901 Group
A Leidos Company

Simplifying IT

WHITE PAPER

Accelerating Digital Transformation

How a public sector focused MSP improves security and user experience while reducing IT costs up to 30%

INTRODUCTION
Why a More Efficient IT Service Management (ITSM) Approach is Needed

While the Office of Management and Budget (OMB) Cloud Smart policy continues to drive the move to more secure, lower-cost cloud delivery models, the Government Accountability Office (GAO) estimates agencies still spent upwards of 80% of a $90 billion IT budget in 2019 on the operations and maintenance (O&M) of existing IT investments, including aging legacy systems. [1] As systems age, O&M expenses continue to grow. And while government organizations are making progress on their journeys to digital transformation, Gartner estimates that 80% of them are still only at the initial or developing digital maturity stages of IT modernization.[2]

Continued dependence on traditional IT service delivery is one of the biggest obstacles to digital transformation, as it leverages inefficient labor-based delivery models to monitor and manage IT. From a public sector perspective, this labor and materials model slows IT modernization as it heavily taxes budgets and productivity, limits 24x7 coverage and surge support, and leaves gaps in security, scalability, resiliency, and user experience. Such an outdated IT service delivery model is economically and operationally unsustainable. And with more employees working from home, technology moving faster than ever, a rapidly expanding cyber attack surface, and intense budget scrutiny, a more efficient and secure service delivery model is needed.

TRADITIONAL IT MODEL
Challenges with Traditional IT Service Delivery

The traditional IT service delivery model uses a labor-intensive staff augmentation approach. This augmentation model, used by the systems integrator (SI) community, comes in two flavors. One flavor uses a cost-reimbursable approach to provide and bill for onsite IT services where the primary output is measured in hours worked instead of service outcomes. With this approach, the SI embeds an IT generalist who must continuously multitask to address surge requirements and other IT needs as they arise. But this approach leaves agency customers with gaps in coverage, subject matter expertise, and deep technical skills. The alternative “two-deep” staffing approach, where a technical expert pairs with a practitioner for every job also billed hourly (x2), can handle surges but at a 30% higher labor cost than with the cost-reimbursable approach. Plus, there are additional direct and indirect labor costs related to having to repeatedly clear, badge, onboard, and train new people – if you can find qualified candidates. In addition to staffing, there are inherent challenges with traditional IT service delivery, as outlined below:

- **Limited integration of government-furnished infrastructure monitoring and management tools impedes cross-environment visibility and proactive IT service management (ITSM).** Enterprise monitoring tools are often not well integrated, so data must be manually collected and correlated to be actionable. Getting to the root cause of an issue can also be difficult and time-consuming due to alert noise and potentially unnoticed early warning indicators spread across different dashboards (e.g. ITSM, ITOM, SecOps). Plus, having to maintain so many

disparate tools can easily lead to misconfigurations that cause outages, security vulnerabilities, and poor user experience. The IT Process Institute's Visible Ops Handbook estimates 80% of unplanned outages are due to ill-planned changes made by IT admins, operations staff, or developers.

- Lack of an authoritative, centralized configuration management database (CMDB) that provides an accurate, up-to-date master list of IT assets and configuration items (CIs). To adequately discover and protect assets agency-wide, you need an inventory of all assets and CIs across siloed and networked groups and domains. In a traditional model, such an inventory is impossible to create and keep up to date given the complexity of government IT operations. And if you don't see all the assets and corresponding CIs on your network, you cannot adequately manage security vulnerabilities. These blind spots can result in agencies being out of compliance with the Federal Information Technology Acquisition Reform Act (FITARA) and poor performance on Inspector General (IG) audits. Also, without a centralized CMDB, compliance metrics for vendors enterprise licensing agreements (ELAs) can't be easily tracked and can result in **un-budgeted ELA cost true-ups.**
- Stifled knowledge transfer, innovation, automation, and continuous process improvements. A traditional IT service delivery model can impede modernization as there's no incentive for incumbent SI contractors to train internal IT staff to replace them. Over time, such protectionist behavior creates an operational break-fix mindset that results in higher labor costs and more billable hours rather than a mindset that drives an Agile approach to innovation, security, and process automation.
- Lack of best practices for ITSM leads to lower levels of customer satisfaction. Users expect an automated "Amazon-like" experience where they self-serve via a digital services catalog and shopping cart model. Without this type of service delivery innovation and friendly user experience, employees get frustrated and go rogue downloading and installing unauthorized software to meet their needs – despite security and non-compliance risks and potential costs.

These challenges create unnecessary direct and indirect costs for government agencies that will only continue to balloon over time. Using a managed IT-as-a-Service approach rather than the traditional model improves security and user experience while reducing IT O&M costs up to 30%.

BEST PRACTICE
Transition to a Public Sector Focused Managed Services Provider (MSP)

A public sector-focused managed service provider offers customers a more efficient IT-as-a-Service delivery model, an efficient alternative to the traditional IT staff augmentation model. Managed services transition customers from a labor-hour, staff augmentation approach to a proactive outcome-based service approach for managing IT infrastructure and services. Transitioning to a managed services approach not only improves service delivery, quality and performance, but promotes operational efficiencies and leverages a repeatable factory-like approach to technology automation to accelerate digital transformation. Also, IT workforce management in a managed services model leverages talent available in rural areas, rather than in major cities where labor rates can be higher.

Having IT job and training opportunities in rural areas expands the applicant pool available and offers lower cost of living, access to talent, and high quality of life. It also emphasizes employee retention and has a certification-based culture where individuals learn continuously to maintain their technical edge.

A public sector-focused MSP can deliver IT and digital business services in a FedRAMP-authorized environment where tasks are completed and optimized using standardized, battle-tested, factory-like playbooks and automated workflows powered by a high-performance, intelligent service delivery platform. Leading MSPs can help agencies substantially reduce IT O&M costs if they have these characteristics:

- A proven and repeatable factory-like approach to efficiently integrate and migrate legacy systems, tools, and data to more secure, efficient cloud platforms (e.g. AWS, Azure, Google, etc.)
- A unified, scalable, and resilient automation platform that can proactively monitor, manage, and optimize IT spanning multi-cloud, hybrid IT, and traditional data centers
- Best practice processes, playbooks, and runbook automation for workflow, compliance, and business process automation (e.g., ITIL, CMMC, ISO, CMMI, etc.)
- State of the art 24x7 Enterprise IT Operations Centers organized around a DevSecOps culture and Centers of Excellence (CoE) with certified technical experts in a DoD cleared facility who support a function, not a single customer
- Flexible managed IT-as-a-Service with hybrid pricing models and outcomes-based service level agreements (SLAs)
- Access to a broader-based talent pool in rural areas adjacent to colleges and universities that may have lower labor costs for specialized and skilled IT professionals

From a contract and pricing perspective, managed services are typically purchased in a per unit, firm-fixed-price (FFP) delivery model, not on a cost-reimbursable or time and materials basis. The per-unit price can include any number of variables including but not limited to people, facilities, tools, compute, storage, software, security, etc. It can include best practice automation playbooks; highly trained technical practitioners and subject matter experts leveraged across customers; cleared facilities; advanced integrated IT tools; state of the art security; 24x7 O&M; and ensuring services meet SLAs.

Agency CIOs are embracing managed services in place of the government's existing IT service time and materials delivery model to gain up to a 30% reduction in IT O&M costs. With managed services, end users can more securely consume digital services without a heavy lift from the IT team. With public-sector focused managed services, there is lower risk of vendor or cloud "lock-in", no high hourly labor costs, substantially fewer integration headaches, and options for streamlined procurements.

CHALLENGES

Start by Reviewing Your Current IT Landscape & Future Needs

Agency CIOs who want to leverage a managed services model to accelerate digital transformation should first conduct a thorough review of their current IT landscape, paying attention to the following:

- Software licensing costs tied to outdated service delivery models and contracts
- Hourly contract rates and the number of labor hours billed for the manual performance of O&M tasks
- Manual IT processes and tasks that impede innovation and productivity and are prone to errors, production delays, and security incidents
- Legacy IT operations (ITOM) and ITSM tools that aren't integrated and provide little visibility across or control over complex on-premise, hybrid IT, and cloud environments
- End of life and end of support hardware

Gartner suggests agencies should also consider how to address these IT modernization trends in the next 12-18 months.

- *Anything as a Service (XaaS)* — a new service delivery model for a full range of cloud and IT services via usage-based subscription models that shift CapEx to OpEx
- *Adaptive Security* — automatically detects and mitigates continuously evolving cyber threats
- *Citizen Digital Identity* — services to securely manage access to government services Citizen
- *Digital Engagement* — across mobile, chatbot, and augmented reality channels
- *Agile by Design* — principles, and practices to move agencies toward desired target states faster
- *Shared Services 2.0* — high-value business capabilities such as enterprise-wide managed IT services, cloud platforms, and services, or AI/ML-driven analytics
- *Analytics Everywhere* — predictive, autonomous capabilities that enhance decision making

CONCLUSION

Managed Services Accelerate Digital Transformation & Prepare You for Future Challenges

By replacing the government's traditional IT service delivery model with a managed services model for a firm-fixed-price, customers can reduce IT O&M costs up to 30% and have performant service delivery around the clock, adequate and adaptable security, and more satisfied users. Managed services leverage factory-like process automation to deliver, monitor, and manage IT systems, applications, and tools across on-premise, hybrid IT, and multi-cloud environments.

A managed services delivery model can also easily accommodate new technologies such as microservices, blockchain, high-performance computing, Internet of Things (IoT), and technologies yet to be invented and deployed to solve future challenges.

> "We've built substantial cloud migration, modernization, security, and operations capacity all in a managed services model!"
>
> **Sonu Singh**
> CEO 1901 Group

[1]GAO Report – June 2019
[2]Gartner Research, Digital Maturity in Government – April 2020