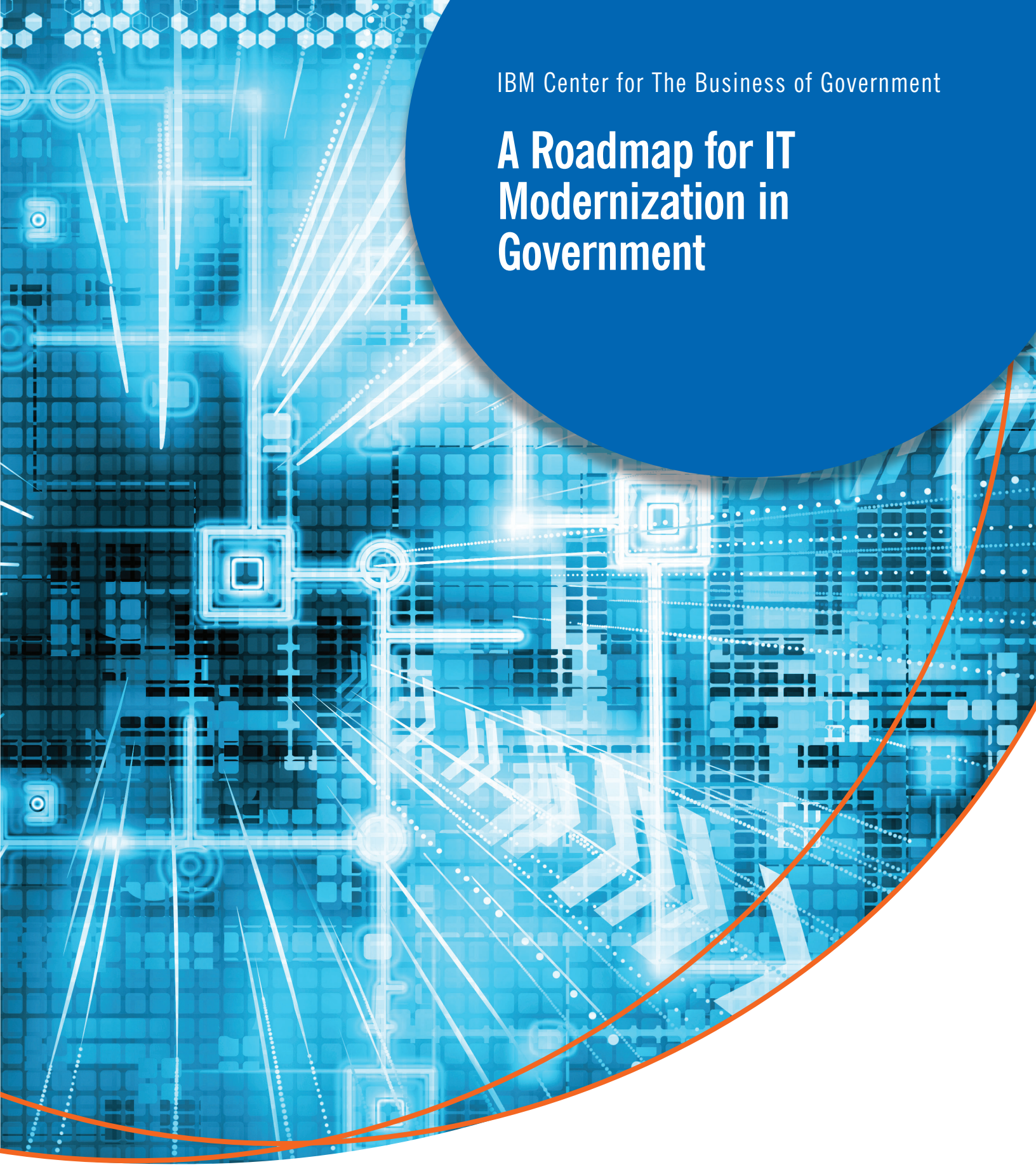


IBM Center for The Business of Government

A Roadmap for IT Modernization in Government

Dr. Gregory S. Dawson
Arizona State University

IBM Center for
The Business of Government
20 years of research for government:
informing today, envisioning tomorrow
1998-2018

A Roadmap for IT Modernization in Government

Dr. Gregory S. Dawson
Arizona State University

IBM Center for
The Business of Government
20 years of research for government:
informing today, envisioning tomorrow

TABLE OF CONTENTS

FOREWORD

On behalf of the IBM Center for The Business of Government, we are pleased to present *A Roadmap for IT Modernization in Government,* by Gregory Dawson, Clinical Associate Professor at Arizona State University.

Professor Dawson's recommended roadmap is based on research into past experiences in IT modernization at the Federal and State level, as well as in industry. He draws lessons from his research and extensive case interviews with Federal and State Chief Information Officers (CIOs). Using these lessons, the author frames impediments to modernization and risks for agencies that do not modernize, including continued cybersecurity weaknesses. The report uses this framing to develop eight key lessons for government leaders at various stages of IT modernization, and concludes by setting out a roadmap for implementation that agencies can adapt to address these key lessons.

DANIEL J. CHENOK

This report comes at a timely moment for government modernization at the Federal level, given the recent enactment of the Modernizing Government Technology Act and its Technology Modernization Fund provisions, as well as the IT Modernization strategy being carried out by agencies and led by the General Services Administration, the Office of Management and Budget, and the Office of American Innovation. Professor Dawson provides a resource for agencies to understand how best to develop a modernization business case, establish and implement a change management strategy, and put in place both a long-term initiative and short-term steps that can help agencies measure real progress.

MICHAEL PREIS

The report builds on several recent studies from our Center about how CIOs and IT leaders can leverage technology to improve mission performance and agency productivity, including:

- Transforming Government Through Technology http://www.businessofgovernment.org/report/transforming-government-through-technology
- A Playbook for CIO-Enabled Innovation in the Federal Government http://www.businessofgovernment.org/report/playbook-cio-enabled-innovation-federal-government
- Creating a Balanced Portfolio of Information Technology Metrics http://www.businessofgovernment.org/report/creating-balanced-portfolio-information-technology-metrics

VLADIMIR SHEBALKIN

We benefited greatly from collaborating with Professor Dawson through the development of this report. Moreover, we hope that the report's lessons and roadmap offer agencies at all levels of government an effective set of experiences and recommendations from which to launch new IT modernization programs or enhance existing efforts.

MIKE CONGER

Daniel J. Chenok
Executive Director
IBM Center for The Business of Government
chenokd@us.ibm.com

Michael Preis
Vice President and Partner
IBM Services
mpreis@us.ibm.com

Vladimir Shebalkin
Offering Lead - Federal Migration Factory Services
IBM Global Business Services - Federal
vladimir.shebalkin@us.ibm.com

Mike Conger
US Federal Team
IBM Global Business Services
mjconger@us.ibm.com

EXECUTIVE SUMMARY

IT modernization in government has substantial and increasing momentum.

Recent U.S. federal legislation and focus at the highest levels of government has fueled activity across agencies, who spend on average 75–80 percent of their IT budget on operations and maintenance (O&M). This activity can significantly improve a public sector environment where new systems development lags behind the private sector, the federal government has excessive costs and significant vulnerability to cyberattacks, and agencies often trail industry in their ability to implement advanced technologies that could dramatically reshape government operations.

This report examines the status of IT modernization in the public sector, and identifies eight key lessons from private industry, state government, and exemplary government agencies:

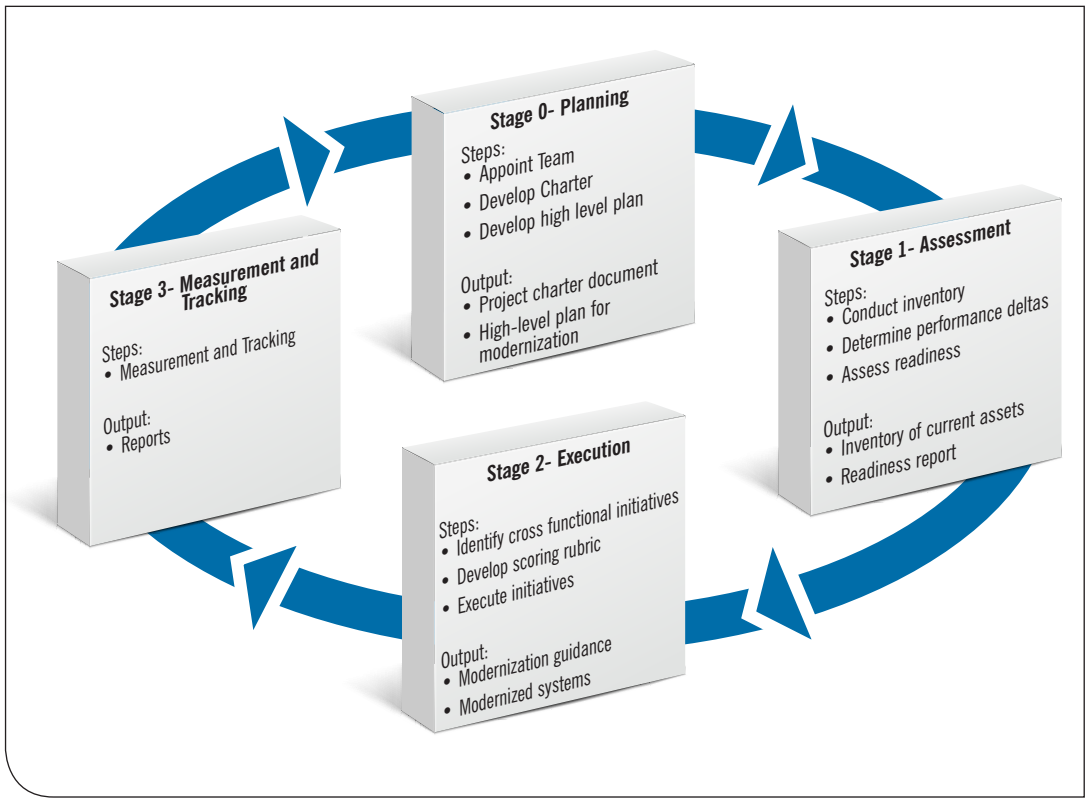
- **Key 1:** Understand the organizational drivers for modernization
- **Key 2:** Plan at the enterprise level
- **Key 3:** Deliver incremental value at the departmental level
- **Key 4:** Communicate value to citizens and shareholders
- **Key 5:** Understand what you have and where you need to go
- **Key 6:** People then processes and only then technology
- **Key 7:** Importance of leadership
- **Key 8:** Look at the "long tail" for modernization

Based on these key lessons, the roadmap below illustrates how successful IT modernization could take place in government, in a manner consistent with the newly released guidance of the Modernizing Government Technology Act (MGT).[1] Major points from the roadmap include:

- Modernization must be an on-going process rather than a single standalone event, to allow for continuous improvement rather than costlier sporadic "catch ups."
- Feedback occurs throughout the process to capture lessons learned and act accordingly.
- Ensure a focus on how technology is supporting mission goals.
- Key and supporting players should be identified for each step, making leadership and operational staff both aware of their requirements and empowering them to act.
- Check-ins with agency leadership, functional leadership, technical leadership, and key users must take place throughout the process.
- Blend a strong acquisition strategy, technical approach and the right team.
- 360-degree communications will foster knowledge and buy-in.
- Measurement identification, and tracking and communication of those measures, should take place both inside and outside the organization.

1. https://policy.cio.gov/modernizing-government-technology/policy/

Figure 1: Roadmap



The federal government has driven a number of modernization successes, even as some significant and high-profile IT system failures have occurred over time. Helpful statutory frameworks can contribute to success, including the Federal IT Acquisition Reform Act (FITARA) and the recently passed Modernizing Government Technology (MGT) Act. Executive Branch policies also play a key role, especially the current administration's IT Modernization Roadmap that builds on prior Administration strategies like "Cloud First."

If the government embraces these lessons, agencies can reduce operating costs, lower the risk of cybersecurity attacks, and position themselves to take advantage of new technologies that improve performance.

INTRODUCTION

The need to improve operational productivity in the public sector is unmistakable: The U.S. federal government faces an annual structural deficit of between $500 billion and $700 billion per year.

By adopting commercially proven best practices in operational productivity, the government could reduce costs by as much as $1 trillion over the next decade.[2] IT modernization—defined as continuously retaining, extending, and modernizing legacy data and technology assets in order to increase value and achieve organizational objectives—is a key component of enhanced productivity. In addition to saving money, modernizing government systems could significantly address the ever-increasing cybersecurity threats and pave the way to implementing high-potential technologies—like analytics, mobile, and artificial intelligence—in the public sector.

Modernization is gaining increasing salience across the federal government. In 2017, the American Technology Council completed its report on the status of modernization of federal information technology (IT).[3] The report focused on the need for modernization in order to improve the "security posture" of federal IT. Additionally, the report highlighted the need for IT modernization to (1) improve citizen-facing services, (2) make better use of mobile technologies, and (3) improve security across the federal government. Three major recommendations were provided:

1. **Modernize and consolidate the federal network by:**
   (a) prioritizing the modernization of high-risk, high-value assets (HVAs),
   (b) modernizing the Trusted Internet Connections (TIC) and National Cybersecurity Protection Systems (NCPS) program in order to support and enable movement to the cloud, and
   (c) consolidate network acquisitions and management.
2. **Move to a shared services model to better enable future network architectures, including:**
   (a) enabling the use of a commercial cloud,
   (b) accelerating the adoption of cloud email and collaboration tools, and
   (c) improving security shared services.
3. **Providing adequate resources for federal network IT modernization,** which will require a realignment of agency-level IT resources using business-focused, data-driven analysis and technical evaluations.

In December 2017, Congress enacted the Modernizing Government Technology Act (MGT) as part of the Fiscal Year 2018 National Defense Authorization Act (NDAA). The MGT established a centralized Technology Modernization Fund (TMF) and associated Technology Modernization Board to address IT modernization needs, and also authorized all CFO Act agencies to establish an IT Working Capital Fund (WCF). In late February 2018, the Office of

2. http://www.techceocouncil.org/news/2010/10/06/press_releases/the_technology_ceo_council_identifies_1_trillion_in_federal_government_savings_according_to_new_report/
3. https://itmodernization.cio.gov/

Management and Budget (OMB) issued initial guidance for federal agencies on how to implement MGT.[4]

These were not the federal government's first attempts at modernization. The E-Government Act of 2002 espoused the need for a modern, well-managed federal IT system and built on previous recommendations from the Clinger-Cohen Act, the Paperwork Reduction Act, OMB Circular A-130, and other laws and policies. The concepts were also incorporated in the Federal Information Security Information Act of 2002, the Federal Information Security Modernization Act of 2014, the Cloud First Initiative, and the Federal Risk and Authorization Management Program (FedRAMP), among other measures.

Federal modernization initiatives have yielded some positive outcomes, especially when leveraging Agile development as well as initiatives like cloud modernization, application portfolio optimization, and even artificial intelligence. Three examples follow:[5]

- The Internal Revenue Service (IRS) Modernized E-file System moved all form 1040 processing to a new system in 2012 and decommissioned legacy systems. Underpinning this replacement effort was digitization which required senior leadership commitment and engaging with industry and government partners.
- The Treasury Department Central Accounting and Reporting System eliminated legacy systems, reduced processing between process submissions to account statements from 12 days to the same day, and improved remediation of material weaknesses in audit opinions.
- In the Department of Homeland Security, the Customs and Border Protection Automated Commercial Environment (ACE) provided a faster flow of legitimate trade into the U.S. and a single window for businesses to transmit data.

Additional case studies

In 2013, the Federal Communications Commission (FCC) housed approximately 207 legacy IT systems—some more than 10 years old—and legacy infrastructure spending was consuming more than 85 percent of the Commission's IT budget. Additionally, several paper-based filing systems were still in use and required substantial human effort to capture and understand the data that they contained. Previous upgrades had been attempted in a piecemeal fashion, focused on individual systems and the existing on-premise infrastructure model. This was not surprising, given that the FCC's approach was generally Bureau- or Office-specific, which resulted in an organization that similarly was application-centric and stovepiped. Over time this model led to aging and costly systems that prevented the FCC, as a collective enterprise, from successfully implementing transformational digital projects.

Rather than continuing to invest in on-premise systems, the FCC developed a cloud-based strategy that would enable it to both be more agile to react to consumer demands and also improve the agility and resiliency posture of the Commission. The modernization effort had several goals:

- Improve the agility of the FCC to use IT to alleviate human-intensive activities
- Increase overall resiliency and accelerate data-driven collaborations across the Commission
- Improve the effectiveness and cost efficiencies of the FCC

4. https://policy.cio.gov/modernizing-government-technology/policy/
5. Examples taken from the 2016 report to then Federal CIO Tony Scott from the American Council for Technology-Industry Advisory Council

During Labor Day weekend in 2015, the FCC moved the systems that remained on-premise at its headquarters to a commercial cloud service provider. This move was a massive initiative that required team members working around the clock. Leading up to the initiative, the FCC had moved its email and office functions to a public cloud so that these functions could continue during the big move. The outcomes of the effort were impressive:

- Reduced IT spending on systems maintenance and operations from 85 percent of the budget to 50 percent of the budget.
- Evolved the role of FCC IT from custodians of the physical infrastructure to managers of the cloud-based services and data for the Commission.
- Reduced the time to deliver future solutions to the FCC in 2016 and 2017 to weeks and months versus years.
- Reduced the cost to deliver future IT solutions compared to what the legacy IT model would have cost.
- Allowed the FCC to begin to look across data-sets that spanned the enterprise that had previously been stovepiped in legacy IT systems.

Despite these successes, the public sector has also been home to failed modernization projects. For example, in September 2000, the Federal Bureau of Investigation (FBI) announced its "Trilogy" program, which was designed to upgrade and modernize its information technology infrastructure. The first two parts of Trilogy, purchasing modern computers and implementing high speed telecommunications, were largely seen as successful (despite cost overruns). But the third part, replacing the Bureau's Automated Case Support (ACS) system, was considerably less so. ACS, deployed in 1995, was built on 1970s-era software tools using outdated equipment, and was widely considered to be obsolete even as it was being implemented in 1995.

The original vision of the new system, the Virtual Case File (VCF), was simply a web frontend to the existing ACS data and was projected to be completed in three years. However, with the September 11, 2001 terrorist attacks, the scope of VCF changed into a complete replacement of the ACS system and was simultaneously mandated to be completed in late 2003—almost a year earlier than originally planned—and needed to include much more functionality. Not surprisingly, VCF ran into significant performance problems, and the plug was pulled for the system in April 2005 with criticism that "…[the] software was incomplete, inadequate, and so poorly designed that it would be essentially unusable under real-world conditions". Even in rudimentary tests, the system did not comply with basic requirements: "It did not include network-management or archiving systems—a failing that would put crucial law enforcement and national security data at risk."[6]

Some state projects have suffered the same fate. In 2005, Michigan undertook an effort to replace the Secretary of State's mainframe system used by 131 state offices, only to terminate the project in 2015 because of continued reliance on 1960s-era mainframe systems.[7]

Public-sector technology is often old and upkeep often costly. In 2013, the Government Accountability Office (GAO) analyzed the O&M spending at seven federal agencies and found that, combined, the agencies spent an astounding $7.4 billion on O&M. Several of the systems studied were more than 50 years old and required high-contract costs to maintain. For example, the Defense Department recently used eight-inch floppy drive systems running on

6. http://www.washingtonpost.com/wp-dyn/content/article/2006/08/17/AR2006081701485.html
7. http://www.michigan.gov/sos/0,4670,7-127-1640_61055-365111--,00.html

1970s-era computing systems to coordinate the operational functioning of nuclear forces. The Department of the Treasury used assembly language, popular during the Cold War era, to assess and manage individual and business taxes. The Department of Veteran's Affairs used the COBOL programming language, approximately 50 years old, to track veterans' claims for benefits, eligibility, and death records.

Renee Wynn, CIO of NASA, observes that "modernization is hard to do in the public sector." It is particularly hard since legacy IT represents years or even decades of organizational investment into the people, processes and technologies that underlie the system. It is a challenge to move the embedded organizational knowledge accumulated into the system into a modernized system while maintaining its day-to-day functioning.

Nonetheless, the stakes are significant. A recent IBM Business of Government report summarizing work with the Technology CEO Council noted that "…the government's existing technology infrastructure is widely outdated, expensive to maintain, not secure and incompatible with new innovations."[8] The report estimates that the federal government could achieve $110 billion in cost reduction over 10 years by modernizing IT. Further, once modernized, additional savings of $270 million are achievable from reducing fraud and improper payments (most of which would rely on new technology).

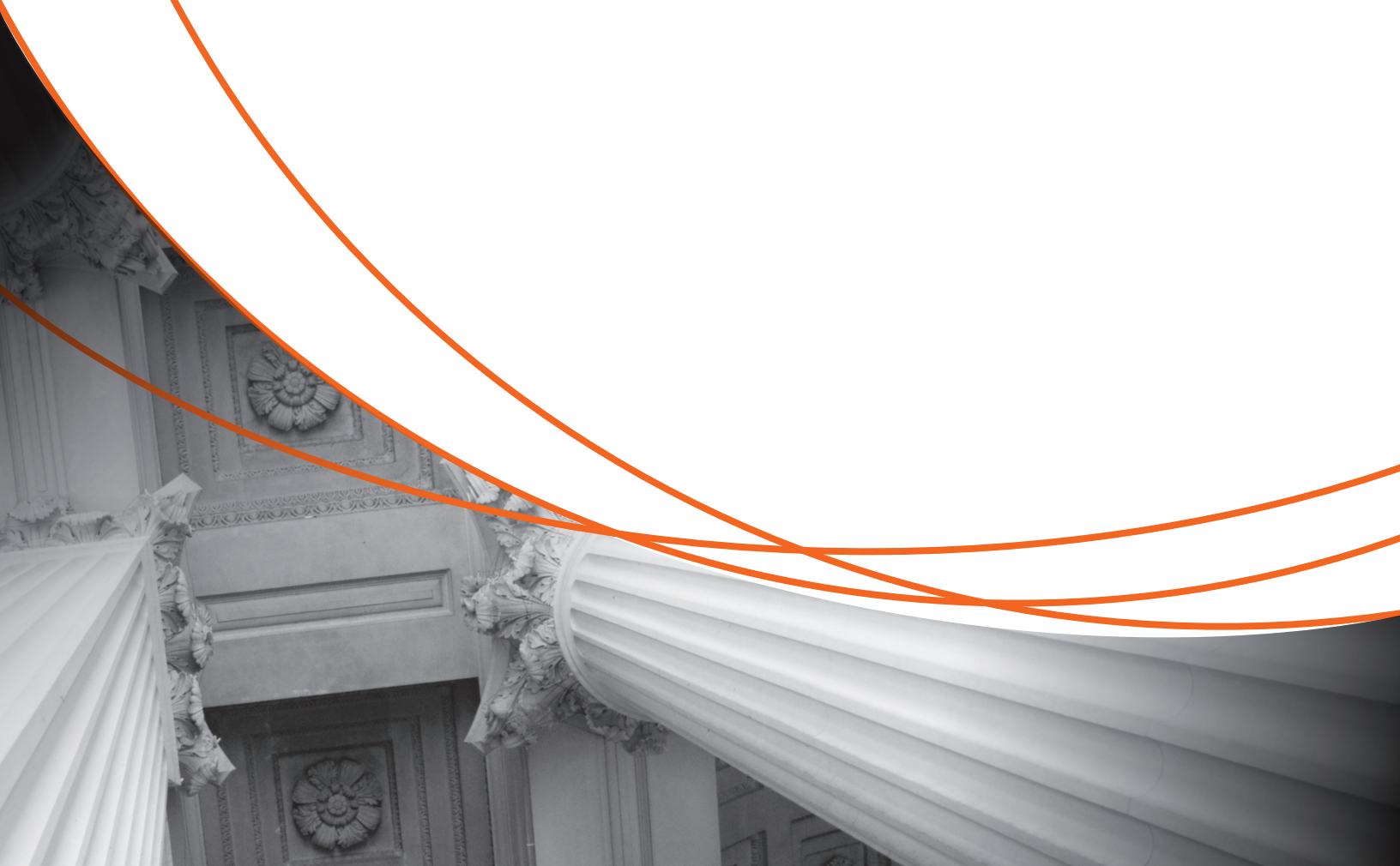
In short, modernizing is worth the effort.

This report is based on the conduct of extensive research on the current status of modernization in the public and private sector, successful and unsuccessful modernizations, and current and upcoming federal programs that will impact modernization. The content was enhanced by reaching out to a number of federal and state government CIOs who have successfully modernized their IT infrastructure— discussing their challenges, what worked, what they would have done differently, and their lessons learned. The complete list of the CIOs interviewed is included at the end of the report.

This research and interviews allowed unpacking the current status of modernization in the private and public sector as well as the challenges within each domain. Major keys to successful modernization in the public sector were isolated, and using those keys enabled the creation of an actionable roadmap for CIOs and other officials to follow to successfully modernize their organizations. Subsequent sections address each of these areas.

8. http://www.businessofgovernment.org/report/transforming-government-through-technology

The Modernization Challenge



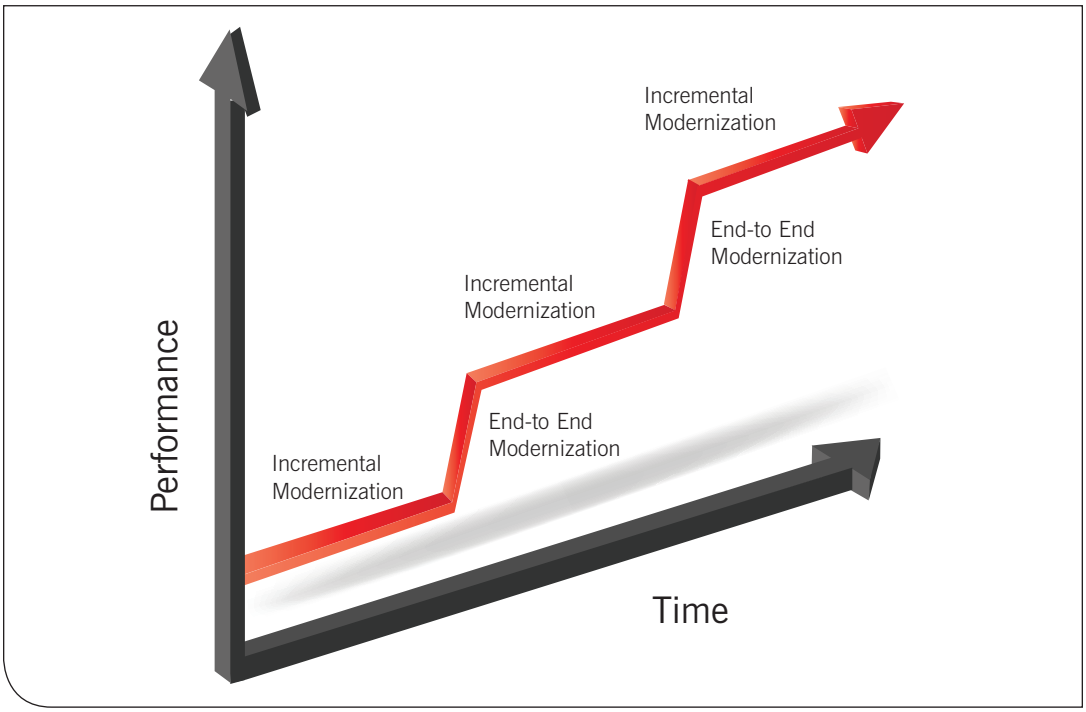
A Brief History of Modernization in the Private Sector

IT modernization is not a new concept in the private sector. As a result of having up-to-date IT, industry can manage technology costs while still taking advantage of new technologies and better protecting itself from cybercrime. Historically, many private-sector organizations have taken an incremental approach to IT modernization, in which they first address immediate points of pain and then, as budgets and time permit, address subsequent issues that arise. This incremental strategy produces short-term improvements and minimizes risk.

However, this incremental strategy constrains the organization to continue operating in its old business model with aging and disparate systems, even as more modern technologies enable new operating models. Over time, this incremental approach can result in increasing complex and redundant systems along with attendant issues with processes and staffing. It is adept at providing a slowly improving "business as usual" approach, but often without the capacity to make profound leaps in technology to capture market share or take advantage of significant technological shifts.[9] In short, this viable short-term strategy yields much less improvement over time and can bring along a host of problems.

After too many years of incremental change, many leading private-sector organizations have instead provided a "shock" to the enterprise and adopted an end-to-end, holistic IT modernization strategy. According to McKinsey, this approach can increase productivity by 20–30 percent, reduce operating defects by up to 60 percent, and reduce time to market by 40–60 percent. While unquestionably riskier than an incremental modernization strategy, this broader path also can significantly reduce duplicative work efforts resulting from redundant systems and ensure that the organization has sufficient IT capacity for the long term rather than just for the next several years. Of course, while even end-to-end modernization needs to be planned and executed in increments/phases to be successful, an end-to-end strategy can dramatically reposition IT and its capacity within the organization (see Figure 2).

Figure 2: Comparison of Modernization Strategies



9. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/modernizing-it-for-a-digital-era

End-to-end modernization comes in two different forms: the greenfield model and the two-speed model.[10] Under the greenfield model, the organization undergoes a complete transformation of existing legacy systems; This is generally done only due to a need for significantly new functionality. Implementing a greenfield approach can be costly and risky but, if well-implemented and with suitable advance planning, can also dramatically improve organizational productivity.

Under the two-speed model, an IT organization focuses its efforts on quickly fixing/updating customer facing applications, while taking a slower and more measured approach to updating backend systems. This allows very quick iterations on the frontend without incurring the concurrent cost and risk that goes along with updating supporting systems at the same time. Backend technology is updated in a more moderate pace, which ensures that technology transformation occurs but without putting the organization at substantial risk. This was the approach adopted by Union Bank, in which they first focused on the customer-facing applications and later and more slowly modernized their IT architecture. While the two-speed model can be viewed as a hybrid between the incremental and end-to-end modernization efforts, in reality it is closer to a fully end-to-end effort to replace rather than merely update legacy systems.

Status of Modernization in the Public Sector

This model of incremental improvement followed by end-to-end modernization is not foreign to the public sector.

For example, the state of Oklahoma did incremental modernization of its information technology for a number of years. In 2011, the state found it had 76 separate financial systems, 129 email support servers, and 30 separate data centers (including several that were simply unimproved closets in office buildings). The situation facing Oklahoma was not pretty, given the disparate systems, servers, and data centers. Then, starting in 2011 and facing numerous redundant systems, spiraling O&M costs, and unacceptable vulnerability to cyberattacks, the state launched an end-to-end modernization effort. In addition, the legislature mandated that all of the systems and IT resources for 78 of the state agencies were to be consolidated in the executive branch under the newly formed Office of Management and Enterprise Services (OMES). Another 32 agencies outside of the mandate subsequently joined the consolidation.

The original strategy chosen by the OMES was a regulatory approach and, not surprisingly, agencies pushed back on the consolidation and modernization initiative and successfully stalled it. The initiative had become a political hot potato and new leadership was necessary to change the tone.

In fall of 2013, new state CIO Bo Reese recognized the widely differing missions of the state's agencies. A one-size-fits-all solution would not fit agency customers ranging from transportation to public safety to prisons to tourism. While the CIO had a legislative mandate, success was due to his political deftness and the fact that he was seen as a state government insider who was working with the agencies, rather than using the legislation as a blunt instrument to force compliance.

Oklahoma's end-to-end modernization effort led a consolidation of the state's IT infrastructure into a single data center that absorbed much of the legacy information technology. This tier 3 data center had 93,000 square feet of raised floor with diesel backup generators, internal chillers and berms surrounding the building for wind and debris mitigation.

10. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/two-ways-to-modernize-it-systems-for-the-digital-era

The outcomes of this effort are impressive. State IT spend dropped significantly. and the state reduced its annual IT spend by $112 million. State IT staffing dropped from 1,200 people to 750 people. Additionally, the state achieved $260 million in cost avoidance from IT projects and better contracting. By taking an incremental approach, and then supplementing it with periodic end-to-end modernization, Oklahoma lowered its IT spend and dramatically reduced its vulnerability to cybersecurity threats.

The Federal Experience

Historically, the federal government has largely relied on the incremental approach, due to two major reasons.

First, budget constraints have always been—and are expected to remain—a significant limitation to engaging in end-to-end modernization.

Secondly, agencies have generally had an easier job putting out RFPs for new systems as compared to replacing old ones. This has created a situation in which a generation of systems is not built off those introduced in the previous generation. Moreover, the time to complete system replacement is significant. As a result, what gets approved for funding, versus what is current when the project begins, versus what is available in the market when the project is done—each step can involve several years—can be quite different.

A host of other reasons for incremental change in government also exist, including significant complications with legacy systems and technologies, perceptions of risk and magnitude of risk, complexity of integration across agencies, duplication in programs and systems, and lack of key drivers needed to force efficiencies.

These factors have contributed to a number of problems with public-sector IT, including disconnected systems, non-interoperable hardware, reliance on aging infrastructure and out-of-date business systems and solutions—precisely the problems that much of private industry faced and solved 20 years ago.

In 2016, then-U.S.-federal-CIO Tony Scott estimated that $3 billion worth of federal IT equipment would reach end-of-life status in the next three years. The GAO estimated that over 75 percent of spending on IT in 2016 was allocated to the O&M of legacy systems that are, or are rapidly becoming, obsolete. Such O&M costs are significantly higher than similar costs in the commercial sector (where O&M averages less than 50 percent of IT spending) and forward-thinking state governments (which also average around 50 percent); this legacy O&M allocation further limits federal agencies from modernizing to meet current and evolving needs. This high allocation of IT dollars to O&M is not sustainable for performance in the long term, leaving little room for investment in fixing the underlying problem of obsolete hardware and software. Agencies must carefully allocate spending on IT and make the right investments that can increase efficiency and decrease costs.

Recent legislative action has helped government refocus on the importance of federal agency modernization, most notably the FITARA and the more recent MGT Act. Over time, other federal government initiatives have been suggested to help address modernization, including innovation investment funds, establishment of a digital infrastructure council, set-asides for infrastructure upgrades, and a dedicated capital fund for federal agencies to upgrade their IT systems (now part of the MGT Act). While being in different stages of deployment, all of these initiatives may be helpful for modernization efforts.

Impediments to Modernization in the Federal Government

Impediments to federal IT modernization largely break down into three areas: spending and acquisition, culture, and speed of technology change.

Spending and Acquisition

While the government spends nearly $100 billion annually on IT systems, strategic spending is difficult. Public funds are often tied to particular purposes, making it harder to invest in IT and then directly allocate the spending, savings, and benefit of the investment to the mission—as the private sector does. For example, a private-sector company could identify an IT opportunity that would save money across its brands and thereby reduce overall enterprise costs, while also recognizing the associated return on investment (ROI) over future years. When the financial justification is evident, the company has cause to make the investment.

There are several important differences between public and private-sector ROI calculations. First, in the private sector, there are two levers to push (increased revenue and cost reductions) while the public sector generally only has a single lever (cost reductions). This makes an ROI calculation more challenging.

Second, the public sector is not always allowed to budget in this manner since agencies need to track money within individual accounts. This "bucketing" of costs and benefits into narrowly focused accounts fails to recognize legitimate cross-organizational benefits from spending. As a result, individual departments tend to view themselves as distinct entities rather than as part of a larger enterprise, and they purchase as such. Enterprise approaches are thus challenging, which can lead to multiple purchases of similar software and services that also introduce significant cost and support ramifications.

State governments have not been immune to this kind of thinking. The Oklahoma experience cited above also followed strongly decentralized IT planning, in which individual departments could spend on IT projects with little or no coordination across the state government. As a result of this departmental rather than enterprise-level thinking, Oklahoma wound up with the 76 separate financial systems. It was, in CIO Reese's opinion, a "hot mess."

Another issue with public-sector ROI calculations is that an investment cannot always be adequately valued for outyears as a company can do via a commercial ROI model—using a full cost model where benefits are measured and recognized over a time, and an understanding of the full costs can be identified and applied. For example, if an investment is made in year one and ROI benefits are obtained in year four, government rules generally do not allow budgetary recognition of the outyear benefits and ROI. This is true for the most part, unless a franchise fund (as some agencies have) can provide specific relief for specific purposes. Public-sector

restrictions on the means of recognizing out year ROI as commercial business does thus hinder longer-term public-sector decision making and investments. This, coupled with and supported by the lack of enterprise-level thinking, multiplies the problem.

The newly passed MGT Act[11] has enabled some movement in this direction. It authorizes multi-year funding that addresses ROI recognition over time, providing some movement in multi-year execution with regards to spending. However, it does not solve the cross-accounts problem. Hence, spending rules may still inhibit an enterprise view of technology and force a more myopic (and costly) view.

Culture and measurement

Cultural impediments to changing the status quo also significantly limit modernization. For example, when undertaking innovation within the federal government, numerous federal technologists lament the lack of buy-in from key players in the organization. This lack of buy-in hinders changing from an incremental modernization approach to a more end-to-end enterprise approach. Similarly, few government organizations have the process discipline to undertake major changes in organizational policies and procedures, and this further stymies innovation.

Risk aversion is also an impediment. For example, Pennsylvania CIO John MacMillan believes that the root issue of IT acquisition is deciding how much information can be shared, to be fair to all the vendors and not incur unacceptable procurement risks. MacMillan acknowledges the amount of risk on each side, but also the competing priorities of vendors to maximize profit and the business to minimize cost. MacMillan aptly analogizes this as a "dancing scorpions" problem in which both parties have to embrace each other, but both also recognize that either party can "sting" the other at any time. Other areas of risk aversion also exist, most notably risks involved with making major changes that can potentially introduce major errors into an existing process.

Another cultural problem is the issue of ownership in the public sector. Traditionally, government has focused on ownership of assets—the idea of paying for use in an "as-a-service" model is still taking root. Procurement rules have been equally slow to evolve to this model and this also hinders modernization.

Decentralization is also a cultural issue. Many public-sector programs operate in a highly distributed fashion, where people identify with their local office more than their parent agency. This creates issues when trying to foster agency-wide initiatives, since control and funding often exist at a more granular level, which challenges modernization across the enterprise.

Finally, and perhaps most importantly, most federal agencies fail to systematically implement and track key IT performance metrics. Lacking these metrics, it is difficult to build a sufficient business case to support anything other than incremental modernization. Without hard evidence about the poor performance of the IT systems—which could be readily shown with IT performance metrics—it is much more difficult to build a strong argument for the need for significant modernization. Since few federal agencies diligently track IT performance metrics, building a business case is more challenging. Not surprisingly, metrics play a substantial role in the newly issued guidance on implementing MGT.[12]

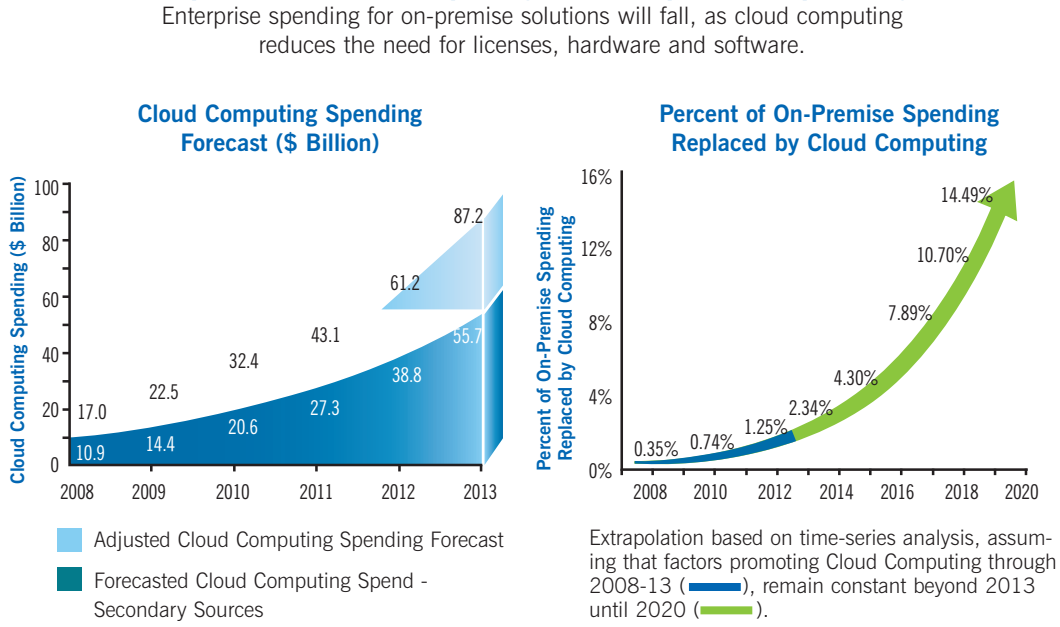
11. http://www.nextgov.com/cio-briefing/2017/09/it-modernization-bill-clears-senate-part-defense-authorization-bill/141109/
12. https://policy.cio.gov/modernizing-government-technology/policy/

Pace of technology change

Without a doubt, the speed of technology change contributes to much of the need for modernization. Futurists such as Ray Kurzweil have dubbed this the "law of accelerating returns," referring to the phenomenon in which the speed that technology changes is not linear but is exponential.

For example, early computers needed to be assembled by hand. Assembly was painstaking and slow. When machines were used to build computers, the pace of assembly sped up -- often dramatically. As industry began to see the value of such an approach, it invested an increasing amount into mechanical assembly technology, further speeding development. The speed of technology change has increased significantly, and all signs point towards this continuing with the advent of technologies such as cloud computing and artificial intelligence (see Figures 3 and 4).

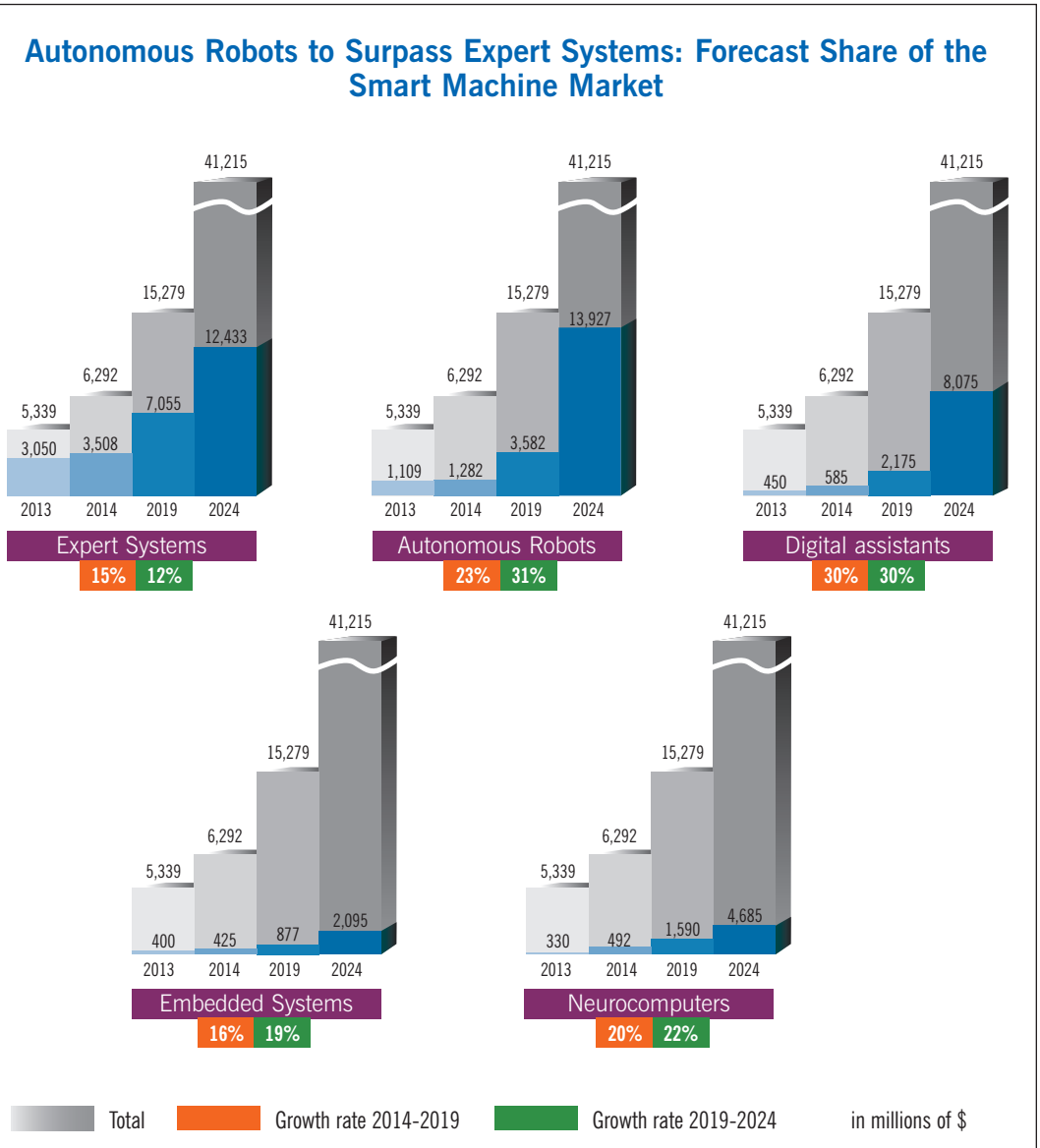
Figure 3: Speed of Cloud Adoption



The cloud computing market is forecast to grow at a rate of 36.6 percent during 2008-13 to $55.2 billion in 2013. It will probably reduce overall technology spending by $30.0-$39.4 billion in 2013, replacing 14.5 percent of global on-premise spending in 2020.

Source: *Research and Innovation Estimates.* *https://softwarestrategiesblog.com/category/federal-cloud-computing/*

Figure 4: Speed of Cognitive Adoption



Source: *BCC Research, Wellesley, Massachusetts, USA. https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/artificial-intelligence-facts-and-forecasts.html*

As the speed of hardware and software change has accelerated, organizational changes have followed suit. For example, technological changes created new organizational operating paradigms, blurring the lines between front-office and back-office processing and incorporating advanced decision making; these organizational changes encouraged greater technical changes. For government today, leveraging this pace of technological change requires time and freedom to experiment with technologies and see how best to employ them. Positive technological changes create a demand for modernization -- a demand that the federal government has been slow to respond to and realize outcomes from.

Impacts from Avoiding Modernization

Failing to modernize can lead to a host of negative impacts. Unless the problem is addressed, these outcomes are likely to increase in severity.

Increasing costs

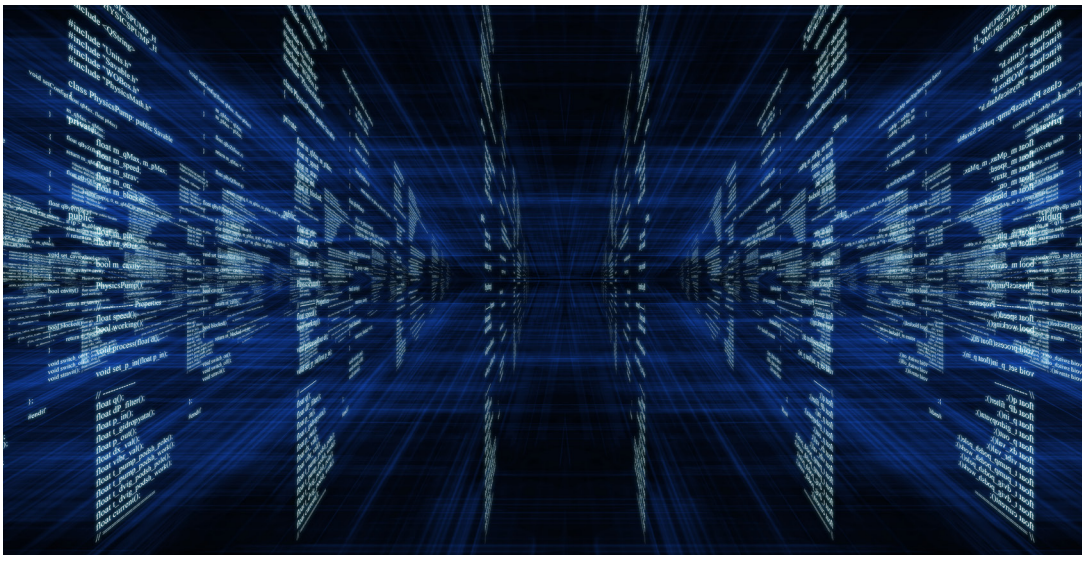
Many agencies continue to rely on aging and obsolete infrastructure, systems, and business applications. Along with high costs due to significant duplication and redundant solutions, agencies face further budgetary and resource constraints due to excessive O&M and technology costs. Older systems will become increasingly difficult to manage and maintain, due to an aging workforce and loss of knowledge, attrition challenges, increasing lack of resources with the requisite skills in legacy technologies, continuing technology obsolescence, and ever-increasing demands to deliver new mission capabilities more rapidly and cost effectively. In short, the public sector faces the same problems that industry faced decades ago.

Dr. David A. Bray, currently Executive Director for the People-Centered Internet coalition and former CIO of the Federal Communications Commission (FCC), echoes this thought. When Bray arrived in late 2013, the FCC was spending 85 percent of its IT budget on legacy systems support and needed to move to the cloud (public or hybrid) in order to reduce operational costs. Bray foresaw a future where these costs would continue to rise and would limit funding available for new initiatives. He also foresaw that the future technology requirements, such as the Internet of Things and machine-learning, would require a more flexible and nimble approach to IT—which cloud-based Software as a Service solutions could provide. In addition, the FCC modernization efforts would allow the Commission to move off vulnerable legacy systems that were difficult to secure or make resilient to modern-day cybersecurity challenges.

The Technology CEO Council report cited above showed how the public sector could reduce overhead expenses to reduce costs by over $300 billion over the next 10 years.[13]

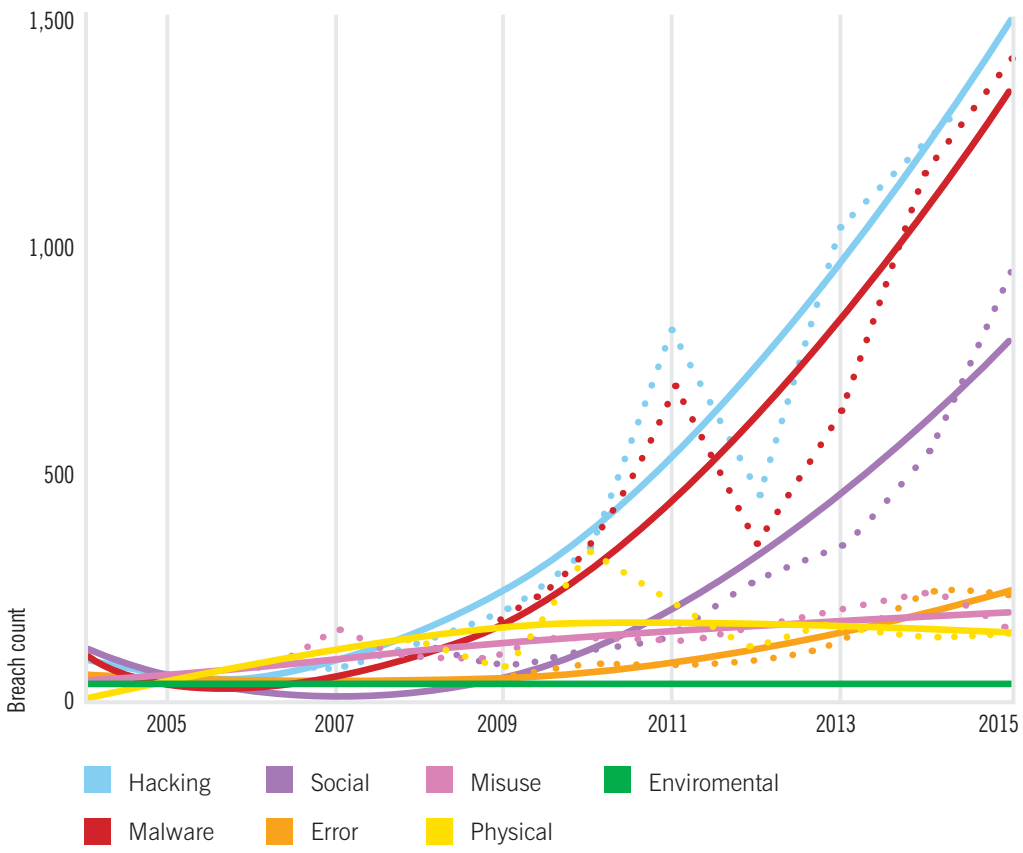
Security and privacy concerns

Cybercrime is one of the most worrying trends in technology, both for the amount of damage that can be done per incident and the number of incidents (see Figure 5).



13. http://www.techceocouncil.org/news/2017/01/12/press_releases/technology_ceo_council_points_trump_team_to_1_trillion_in_savings_for_federal_government_operations/

Figure 5: Rise in Cyberattacks



Source: *InfoSec Resources*

Thus, it is not surprising that government cybersecurity strategies depend upon modernizing legacy information system. As Jeanette Manfra, acting deputy undersecretary for Cybersecurity and Communications for the Department of Homeland Security, said, "It is not always a fact that IT modernization and cybersecurity have to go hand-in-hand, but that is very important and something that this administration recognized immediately: that the lack of modernization is itself a big vulnerability of government." [14]

Unfortunately, the age of public-sector technology and the sheer number of obsolete systems, coupled with inconsistent upgrades and patches, represent a huge vulnerability to the federal government. Oklahoma's CIO Reese experienced this first hand. Prior to modernization (and consolidation), a cyberattack on any one of the systems within the state would be detected by the cybersecurity professionals within the agency. But, once the attack had been detected and fixed, the state had no way to track where the virus went or who else may be infected.

14. https://www.govtechworks.com/why-modernization-is-key-to-national-cyber-strategy/#gs.gJ1eLf4

Further, since the systems were not standardized, a fix in one system would not necessarily work for other systems, even if cybersecurity staff were aware of the need to fix the systems.

Government needs to be proactive in preparing for and preventing cyberattacks, both to protect mission operations and because it makes good financial sense to do so. The State Department's implementation of a modernized and cloud-based infrastructure successfully denied 10 million malicious attacks each month and provided protection against a large distributed denial of service (DDoS) attacks.[15] Using an industry-accepted figure of the cost of a DDoS attack at $40,000 per hour, cost avoidance from good cybersecurity is substantial. Improving security is also one of the key considerations for funding from the MGT Act Technology Modernization Fund (TMF).[16]

NASA STARS MODERNIZATION

To address some of its unique hiring requirements and provide greater transparency in its hiring processes, in 2004 NASA reengineered its staffing and hiring program by implementing its new Staffing and Recruiting System (NASA STARS). Built around an established commercial hiring tool, Resumix, STARS also integrated several custom developed modules that enabled the agency to effectively assess and track large applicant pools that often included highly educated scientists and engineers. When implemented, STARS represented a substantial advance in NASA hiring, and as late as 2011 the system was working well. However, when Resumix announced it was no longer supporting the software and recommended the Agency migrate to a new product, NASA deferred addressing the issue to focus its limited resources on other priorities.

By 2017, NASA decided that the growing cybersecurity threats were sufficiently large to force modernization to occur. While the primary driver for the change was ostensibly the cybersecurity threat, NASA leadership recognized that new government tools and fundamental changes to how agency mission support services were delivered necessitated a significant investment in the agency's hiring program. Thus, the business need and the cybersecurity threat created a "perfect storm" of circumstances for modernization.

The business case for modernization was based around the risk of a cybersecurity event. While the cost of changing the people, processes, and technology was high, the cost of a potential breach event was considerably higher. In addition to addressing the cybersecurity concerns, the investment will support a more effective and efficient hiring and staffing model that will ultimately drive mission success.

Lack of access to advanced technologies

Industry has leveraged advanced technologies quite effectively. For example, companies regularly conduct audits of large-scale transactions in order to uncover fraud, mistakes or shifts in demand. The use of cognitive computing and analytics has been shown to increase fraud detection by 40 percent and is projected to generate an additional $200 billion over 10 years.[17]

15. "How proven technology solutions can save taxpayers more than $1 trillion over a decade while enabling more effective government" by the Technology CEO Council, January 2017
16. https://policy.cio.gov/modernizing-government-technology/policy/
17. "How proven technology solutions can save taxpayers more than $1 trillion over a decade while enabling more effective government" by the Technology CEO Council, January 2017

However, modern hardware and software is required to effectively take advantage of these technologies and access the data to achieve such results.

Currently, many public-sector agencies lack the ability to leverage their own data to support decision making. Today, organizations must deal with vast amounts of information, often obtained from numerous sources and distributed across multiple non-integrated platforms and repositories. The information is not currently accessible in an integrated fashion that would enable informed decision-making needs. Furthermore, the information (structured and unstructured) is often not consistent in a way that allows agencies to identify trends, predictive analysis, data visualization, statistical analysis, or patterns and correlations. Large volumes of data also require automated mechanisms for preparation, transformation, refinement, and management. Thus, effectively implementing technical innovations such as analytics and AI at scale are simply still out of reach across much of the government.

However, the benefit from implementing advanced technologies is huge, and some parts of the public sector have achieved remarkable outcomes. For example:

- The State of New York used advanced analytics in order to quickly evaluate tax refund requests before the funds are disbursed. Using this strategy, New York has been able to deny $1.2 billion in improper refund requests over the last six years, even after challenges have been settled.[18]
- In Alameda County, CA, the Social Services agency implemented a consolidated client benefits and activities database and applied analytics to successfully save $11 million a year in taxpayer spending. The use of analytics allowed rapid fraud detection (in minutes rather than months), eliminated redundant work, and gave the agency the ability to spot service issues before they occur.[19]
- The Social Security Administration (SSA) has worked to develop a model for determining continuing disability benefits. The model can process disability applications in less than a second, projected to save $1 billion over five years while helping the SSA achieve its goal of paying benefits to disabled applicants within 20 days.[20]

18. "How proven technology solutions can save taxpayers more than $1 trillion over a decade while enabling more effective government" by the Technology CEO Council, January 2017
19. https://www.scribd.com/document/71353877/TCCOneTrillionReasons
20. "How proven technology solutions can save taxpayers more than $1 trillion over a decade while enabling more effective government" by the Technology CEO Council, January 2017

A LESSON FROM INDUSTRY: UNION BANK MODERNIZATION

Banking has undergone a renaissance recently. Originally put in a defensive IT posture due to the financial meltdown of the last decade, banks are now shifting to the offensive and Union Bank is leading the charge. Union Bank of San Francisco, with its $105 billion in assets, has been quietly executing a IT modernization effort to better serve customers while grappling with security concerns and cost management. This multi-year effort is less about technology and more about customer collaboration and insights. As Jane Clabby of Clabby Analytics puts it, "In banking, it's all about innovation—there's a push to become more consumer oriented."[21]

With a strong reputation for quality, Union Bank is one of the top banks in terms of customer service and customer experience—and is also well-known for its financial performance, approach to governance, and leadership. Thus, while modernization needed to occur, it was essential to ensure that the integrity of the customer experience was maintained.

Union Bank undertook a two-speed modernization effort in which they focused on customer-facing applications (e.g., an increased focus on mobile computing) while taking a slower approach to updating the architecture. As Chief Technology Officer Dana Edwards pointed out, they were not in a position where they could do a greenfield modernization --the bank was simply too large to do so.[22]

At present, Union Bank is close to completing its three-year modernization effort.

21. https://chernigiv-online.com/i/t/union-bank-smart-enterprise-exchange-banking-modernization/2684601
22. https://chernigiv-online.com/i/t/union-bank-smart-enterprise-exchange-banking-modernization/2684601

Keys to Successful Modernizations

Several key lessons emerge from this report's analysis of successful modernization initiatives:

- **Key 1:** Understand the organizational drivers for modernization
- **Key 2:** Plan at the enterprise level
- **Key 3:** Deliver incremental value at the departmental level
- **Key 4:** Communicate value to citizens and shareholders
- **Key 5:** Understand what you have and where you need to go
- **Key 6:** People then processes and only then technology
- **Key 7:** Importance of leadership
- **Key 8:** Look at the "long tail" for modernization

Each key lesson is described in more detail below.

Key 1: Understand the Drivers for Modernization

The previous section discussed potential impacts if modernization is not addressed in the federal space, including cost, security and privacy concerns, and lack of access to new technologies. Numerous other drivers may exist within any organization. For example, older technology may make the need for skilled staff either inside or outside the agency the most pressing issue.

Regardless, CIOs should understand the drivers for modernization within the organization and then tailor a strategy to fit those drivers. All modernization is not equal, and some aspects or strategies better suit some drivers than others. By taking the time to understand the drivers, a more cogent modernization strategy can be developed. For example, the modernization driver for Union Bank was the need to more innovatively address consumer demands. Similarly, at Lufthansa, the driver was to be able to utilize analytics to gain a competitive advantage.

LUFTHANSA MODERNIZATION

Lufthansa's motivation for an IT modernization was a desire to be more innovative in the areas of customer experience, handling irregular situations, predicting aircraft delays, and predicting preventative aircraft maintenance. These four items became touchstones that guided the modernization and set the order and pace of change. This required Lufthansa to shift their data analytics from just structured internal data to truly using big data to provide insights.

Lufthansa identified several critical success factors:[23]

- Employing a formal, top-down value discovery process as the basis to make decisions, rather than relying on "gut-level" decisions
- Involving the CEO to set the strategy and communicate the value of strategic IT to the organization
- Adopting service-centric guidelines to guide deployment
- Using business-case-driven decision making, and creatively deploying modernization to maximize value
- Building an IT architectural foundation to promote growth and future innovation
- Using outsourcing and effective vendor management to address the complexity of the effort
- Engaging in meticulous data governance and talent planning

As a result of this modernization, Lufthansa incorporated new unstructured data into future decision making rather than solely relying upon internal existing data. Lufthansa could also leverage its IT modernization to utilize analytics for competitive advantage.

As Wynn, CIO of NASA, points out, "The federal government is so widely varied in the services that each agency provides that numerous use cases for modernization exist. The key to successful modernization is being appreciative of these differences and not [glossing] over them." Moreover, as the newly issued guidance on the implementation of the MGT Act points out, the TMF is expected to focus funding on projects that address cybersecurity issues, financial and other organizational priority and risk areas. Additionally, it appears that greater weight will be given to projects that have "a demonstrable and visible impact to the public, in alignment with the agency's mission…and clearly showcases how expected outcomes will enhance the delivery of services that reduces burden, improves performance, or has the potential to produce positive long term benefits."[24] Thus it is important that the agency mission linkage is made clear.

Key 2: Plan at the Enterprise Level

One of the outcomes of decentralization within the public sector has been a change in thinking from an organizational perspective to a program perspective. This makes sense: most people hired into an organization develop programmatic expertise and affiliation. Given the size and

23. http://www.misqe.org/ojs2/execsummaries/MISQE_V16I1_Chenetal_Web.pdf
24. https://policy.cio.gov/modernizing-government-technology/policy/

expanse of federal agencies, identification with programs is a natural consequence. Yet enterprise-level thinking opens up doors that simply are not possible at the program level. For example, the use of shared services is a natural solution that follows a shift to an enterprise view.

This orientation requires the organization to take advantage of centralized approaches. Texas, as noted by CIO Todd Kimbriel, has been able to switch from departmental thinking to enterprise-level thinking by creating an "office supply store" mentality. The state centralized technology purchasing, leveraging state-wide demand volumes and thus driving down costs for all customers. Similarly, through centralized shared services, Texas was able to drive efficiencies, increase agility, and reduce costs and risks. However, the shared services program required customers to relinquish control over those elements, which spawned a natural customer resistance to change. To address this, the state adopted a strategy that requires customers to be involved with every major decision. According to Kimbriel, the state accomplished this governance with three groups: a solutions group (focused on technology), an IT council leadership group (focused on strategic technology conversations), and a business executive leadership group (focused on high-level business issues).

STATE OF TEXAS SERVER MODERNIZATION

When Texas elected officials looked at the state's technology infrastructure, they knew that it needed to be consolidated, modernized, and offered as a shared service to the state. Servers were present in literally in every corner of the state, and IT staff were managing the servers quite differently from each other. This led to substantial challenges for the state, from the standpoint of cost, legacy systems, and cybersecurity.

The first task that confronted Texas was convincing the staff of the decentralized agencies to participate in the centralized data center program and leave their legacy data centers behind. To both absorb the servers and to assure the customers that they would never have to return to the previous legacy environments, the program promised them that 20 percent of the servers would be refreshed every year.

Although it took a long time, the centralized data center program was able to consolidate the target goal of 75 percent of the servers into a shared data center model and provide templated reference architectures for consistent application of technology across participating agencies. The program did not require agencies to settle on a single architecture, but instead offered a series of architectures that would all be able to meet their processing demands. While the program was willing to do customized server builds, it turned out to be only minimally necessary as the standard architectures were generally found to be sufficient.

Once the servers were consolidated, the program incorporated a hybrid cloud model (to augment the existing private cloud model) and enabled a self-service capability for customers to directly control operations with their selected cloud or on-premise provider. This infrastructure as a service approach allowed Texas customers to reduce the time to implement a new server from 14 months in 2010 (physical private cloud) to 2 hours in 2017 (virtualized hybrid cloud).

Oklahoma CIO Reese had a different strategy to promote thinking on an enterprise organizational level: a legislative mandate. As noted above, the mandate, directed Reese to consolidate all systems and resources for 78 state agencies under the newly authorized Office of Management and Enterprise Services. Once announced, 32 additional agencies voluntarily joined the consolidation and Reese was able to advance thinking on an organizational level.

This key is also seen in the newly issued guidance for implementing the MGT Act, in which the development of common solutions is considered to be a relevant consideration for TMF funding. Such common solutions may involve commercial products and services, and also apply throughout the enterprise.

Key 3: Deliver Incremental Improvement at the Department Level

While planning benefits at an enterprise level, delivery of benefits occurs most tangibly at the departmental level. The fastest way to lose momentum is to try to implement a "big bang" at the enterprise organizational level. Implementation progress is much easier at the departmental level, and focusing attention on delivering incremental improvements can pave the way for greater cooperation at the organizational level.

Delivery of benefits that shows value to individual efforts can build support for organization-wide transformation. This is the strategy that CIO Bray of the FCC employed. His first major modernization initiative was relatively simple: shift the consumer help desk to a cloud-based solution and, by doing so, reduce the cost by approximately half. Bray had a fortunate set of circumstances that allowed him to move forward on the help desk and built momentum for further modernizations. This allowed him to both show small wins at the local level and take advantage of low-hanging fruit for modernization at the organizational level.

With planning is at the enterprise level, small modernization efforts can build momentum and confidence for larger projects.

Key 4: Communicate Value to Stakeholders

Even the best-planned and managed modernization effort can drain major stakeholders—and "modernization fatigue" is a real danger. Communicating the value of the modernization to stakeholders can minimize the risk.

Dickie Howze, CIO for the state of Louisiana, described the need to communicate both up and down within the organization. In his case, a new administration was elected partway through a modernization effort in October of 2015, and Howze was approached by agency staff who argued that the consolidation was not working and needed to stop. By that time, however, Howze had been able to develop a strong business case for the modernization that highlighted the savings from consolidating. Because of this data, the modernization continued and brought substantial additional benefits to the state.

To be most persuasive, the value communicated to stakeholders needs to address more than just IT benefits or cost savings, but should also tie to larger mission objectives. This is consistent with the goals of the MGT.

Key 5: Understand What You Have and Where You Need to Go

Modernization is not a one-size-fits-all strategy, and an early step in modernization requires a thorough inventory of an organization's assets. This has proven surprisingly difficult to do in government, and often the results shock even the most experienced CIO. John MacMillan, CIO for the state of Pennsylvania, sent out a survey to ask agencies about the types of database software that they used to underpin their applications. According to MacMillan, the most common answer was "I don't know" or "I'm not sure," making it a challenge to build the path forward.

But without spending the time to assess the current inventory, agencies can fail to leverage existing technologies or can be unaware of more pressing issues. Either result is suboptimal, whereas assessing the current inventory facilicates taking action to reduce redundant and duplicate systems and applications.

Key 6: People First and Then Processes and Then Technology

Every CIO interviewed had the same advice: start with people and evolve processes prior to addressing technology shortfalls. Two cases illustrate this point:

- As NASA's Wynn points out, agencies need to focus on the bell curve of human behaviors—some embrace change, some resist change, and those in the middle wait to see where they should follow—and recognize where people stand, to develop an effective change strategy. Wynn focuses on the top of the bell curve (the fence sitters) based on a belief that innovators will always be in favor of modernization and laggards never will. According to Wynn, the fence sitters should be the focus of persuasion.
- Howze of Louisiana used the same philosophy of starting with the people before discussing any technology changes. In his case, he moved 1,100 IT people from agencies into the newly created Division of Administration that housed the budget, management, and IT functions for the State's executive agencies. Howze faced considerable pushback from both the individuals as well as their former agencies—staff worried about losing their jobs or taking salary cuts. In Howze's case, technology progress needed to follow resolving the people issue.

Once people are identified and suitably empowered to help drive change, agencies need to look at applicable processes. As Wynn of NASA pointed out, while there are numerous advantages of moving to the cloud, simply moving the technology ("lift-and-shift") will likely "kick the can" down the road. While some immediate short-term modernization occurs, without identifying the underlying people and process issues, a lift-and-shift will shortly encounter similar modernization challenges in the future. By solving the current and future people and process issues along with the technology issues, modernization problems can be solved rather than delayed. Further, a lift-and-shift often does not involve a major technology refresh or a significant modernization of the current system, and thus rarely solves underlying problems.

CIO observations of the need to address process include:

- Ed Toner, CIO for the state of Nebraska, echoes this point and suggest that, "if the processes and procedures are bad, the technology will die." Toner describes Nebraska as being "tool agnostic" and suggests that all tools can be either good or bad, but the people and processes have to be right regardless of the tools.

- Bray of the FCC discussed this topic at some length and noted the difficulty of organizational change, particularly for those people doing their best in the face of challenges but who have not received training to update their skills. Bray suggests investing considerable time to solicit perspectives on organizational problems, through a Socratic method of asking questions and actively listening to team members, and also asking what they think can help resolve these problems. This approach empowers all team members to be creative problem solvers. It also shifts an organization's culture, from being reluctant to identify problems or solutions to actively working problem-solving into every team member's job description.

There is simple pragmatism behind this: failing to solve the people and then the process issues is akin to what one CIO called "paving the cow path," in which inefficient approaches were simply speeded up but the underlying problems remained the same.

Financially, simply addressing the technology issue provides short-term gains that are minimal and transitory. The better strategy first involves the people necessary to support change—and develop and rationalize the processes—before addressing technology. This is not to suggest that the CIO should be blind to innovative technologies (as we discuss in Key 8), but rather should put people and process solutions in place before technology solutions. And those who are undertaking modernization need to be prepared for a long process, as highlighted by the experience of the state of Ohio.

STATE OF OHIO MODERNIZATION

The scope of the modernization that the CIO of Ohio faced in updating the State of Ohio Computing Center (SOCC) was enormous. The state's IT setup was fragmented and inefficient, with 32 data centers in 26 cabinet agencies and comprising 9,000 servers and 19 different email systems. Ohio was spending approximately 70 percent of its technology budget on its aging infrastructure rather than on citizen facing application.

Given the size and scope, the CIO likened his approach to the "it takes a village" perspective and involved all the key stakeholders. He created eight different workgroups and asked 12 of the state's CIOs to focus on smaller topics, such as enterprise architecture, security, business rate construction, network, storage and servers. By creating the smaller groups and staffing them with top talent in each area, the CIO fostered manageable understanding of the problems to be solved.

Their findings were surprising. For example, the business rate discussion work group was under the initial impression that total annual IT spending was $700 million, but once they reconciled (with the help of agency CFOs) the vast and conflicting number of IT spending account codes, they uncovered approximately $950 million in annual IT spending. Similar surprises were seen in other work groups.

For Ohio, it took two years to initiate a dialog and plan a modernization strategy with his agency customers. Once the strategy was designed, it took an additional year to remediate the SOCC and then an additional two years for server migrations and deepening the partnership. The timing was worth it, though, and Ohio was able to reduce its spending on legacy systems from 80 percent of its budget to 45 percent of its budget. Davis believes that it was necessary to spend this time and repeatedly talked about "planning the work and working the plan."

Key 7: Importance of Leadership

Each IT modernization needs key executives who can drive change. NASA's CIO Wynn emphasizes the need for an effective project/program manager to be involved and empowered. Wynn stresses that the project manager needs to support the proposed change and have the flexibility and empowerment to undertake the modernization. Finally, she emphasizes the need for all levels of leadership to support the project manager in enacting necessary changes.

CIO Reese of Oklahoma has a different set of challenges resulting from their consolidated status. When state IT was not yet consolidated, each agency would develop its systems and protocols to address the various audit demands of its federal partners. For example, by mid-2017 Oklahoma had already been audited separately by the FBI, IRS, Social Security, and HHS. As CIO, Reese had developed the state's technology profile to meet the most stringent demands of all the various auditing agencies, but found that the federal auditors tend to view the state as a series of silos and rarely share information with other auditors. In Reese's words, this created a "hairball of a mess" to be addressed—it becomes a challenge for the state to be in compliance without a single set of compliance regulations, when newer versions of software are deemed compliant for some audits while only older versions are compliant for others. As CIO for the consolidated enterprise, Reese works with federal agencies to encourage the development of a single (or at least non-contradictory) set of regulations for audits.

Other leadership perspectives can drive modernization as well. CIO Toner of Nebraska was formerly an IT leader at TD Ameritrade and FirstData, and was specifically brought on by the governor (a former leader at TD Ameritrade) for his private-sector modernization and innovation experience. As Toner describes it, the governor tasked him to "leverage technology in innovative ways [so we] can open up government and help it work for the people of Nebraska." Toner recalls a note that he received from an agency director at the end of the modernization effort: "Ed, I gave you a hard time, gave your people a hard time, and I was totally against this. But, I was totally wrong."

This was also one of the key success factors for Lufthansa's successful modernization described above. In their case, the CEO set the strategy for the modernization and then spent time communicating its value to the rest of the organization. Because of this, it was easy to see that senior leadership was behind the modernization and, facilitating engagement with the rest of the organization.

The CIO should not take on all of the modernization burden personally. Cross-functional teams can involve multiple leaders in planning and assist with inevitable change management related issues. The guidance on implementing MGT makes this clear, and having executive level support for the proposed modernization is a key part of the Initial Project Proposal Template.[25]

Key 8: Look at the "Long Tail" for Modernization

Modernization requires the commitment of resources to achieve both near-term and long-term benefits. However, as noted earlier, the public sector has difficulty addressing out-year budgeting needs. In the short term, immediate efficiency gains and cost reductions can occur while additional substantial benefits can accrue in the out-years.

This is referred to as the "tail" for efforts, and a long-tailed effort is one that continues to achieve benefits in the future.

For example, consider the following possible long-tail benefits of modernization:

- Cloud Transformation: Modernization can facilitate the movement of data and applications to the cloud. The use of cloud architectures and standard cloud services increases portability across cloud solution providers (CSPs), thereby providing increased flexibility and cost control. This can positively affect cost and support cybersecurity preparedness (see below). Finally, scalability within the cloud environment enables computational workloads not imaginable today.
- Improved Cybersecurity: Given cybersecurity threats that face commercial and government organizations today, agencies need more rapid identification of emerging threats and automated capabilities to detect, analyze, and respond accordingly. Emerging standards, like those in the Federal Risk and Authorization Management Program (FedRAMP), open cloud solutions to new workloads and reduce the risk of inadvertent disclosure of data. New threats that emerge quickly and proliferate rapidly can be addressed using intelligent and automated security threat detection capabilities. Augmented intelligence technology can support cognitive security operations centers (SOCs) with modern approaches to support human decisions, helping security analysts parse thousands of reports that have never before been accessible to modern security tools.
- Cognitive Computing: Artificial intelligence and machine learning can provide people with insight to make better business decisions through analytics, strengthening decision-making capabilities. These cognitive computing technologies process natural language information to enable systems to seamlessly interact with citizens and deliver customized services. For example, for Student Loan Borrowers, cognitive solutions could develop a system to predict borrowers at a higher risk for default and reach out to these borrowers to reduce their payment or find other innovative ways to avoid default.
- Agile Capabilities improvement: The organization of the future will not blindly follow a strategic plan that was developed years ago and now sits on an office shelf. Successful organizations should apply Agile iterative principles across the enterprise—whether in strategic planning, during the execution of change programs, developing new products and solutions, or managing day-to-day business operations. They will continually learn, refresh, and improve. Digital and Agile capabilities enable organizations to rapidly adapt to changing environments—quickly setting up new teams, prototyping rapidly, developing strategies and plans in real-time with actionable, traceable results, and delivering new solutions to meet evolving mission needs.

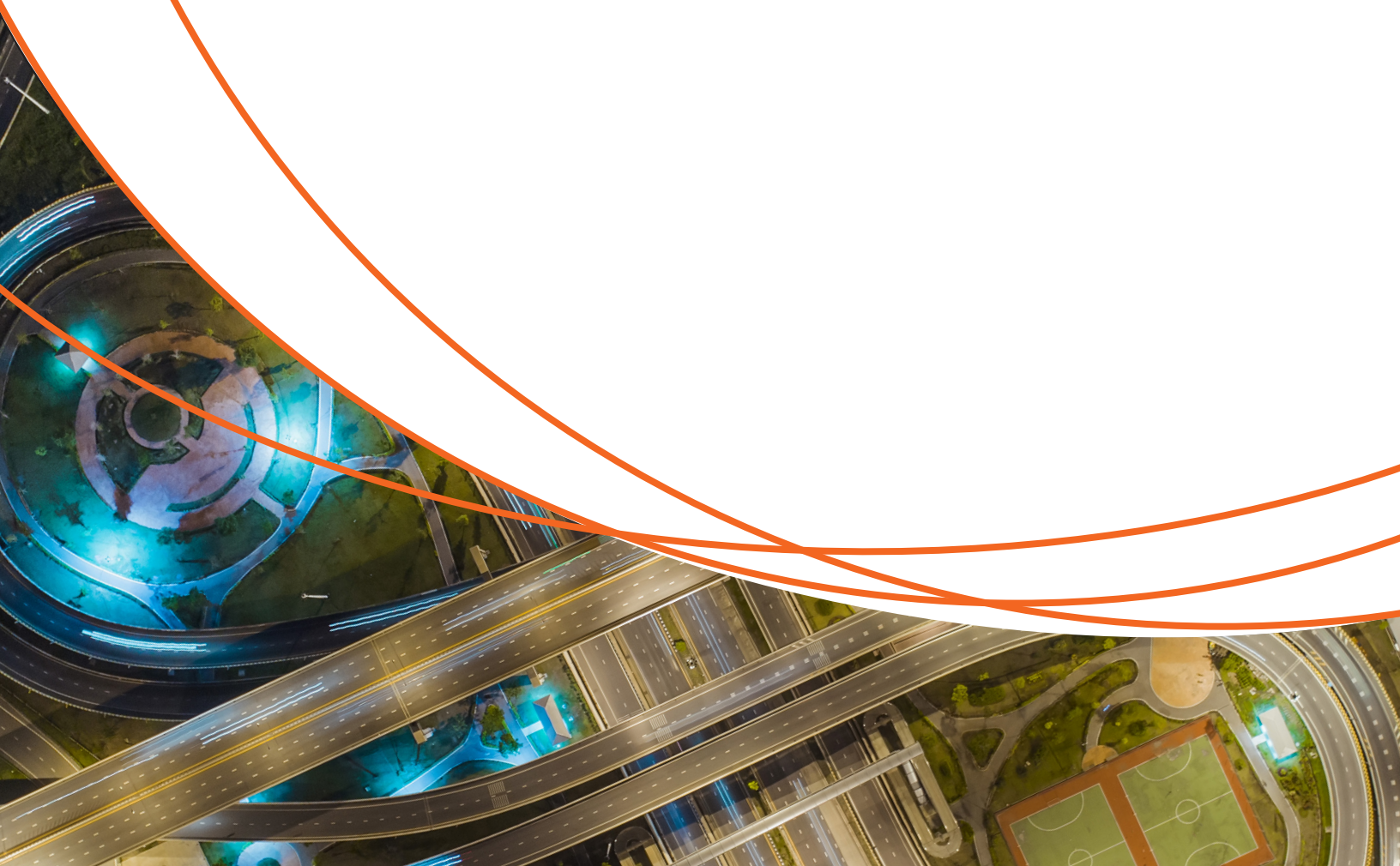
25. https://policy.cio.gov/modernizing-government-technology/policy/

- Mobile adoption: In state and local government, approximately one percent of citizen and business interactions are fully mobile enabled. Government and Industry are working together to aggressively mobile-enable all efforts across states, and the percentage of interactions that are mobile enabled is expected to increase to 45 percent by the end of 2017 and to 80 percent by the end of 2019.[26] Enhanced apps and capabilities can be used to reach out to citizens and provide just-in-time services; for example, FEMA can notify citizens of an approaching storm, while the State Department can proactively notify citizens of expiring passports. Integration of cognitive technologies into mobile platforms can provide higher levels of automation for customer service interactions through intelligent agents, interacting with citizens through the channel of their choice (text, voice, email), and giving a consistent user experience across these platforms.

Some of these future benefits are difficult to quantify at present, but are consistent with the private sector progress. Modernization is a necessary first step to achieve long-term returns.

26. Ericssson Mobility Report, November 2017

Recommended Roadmap

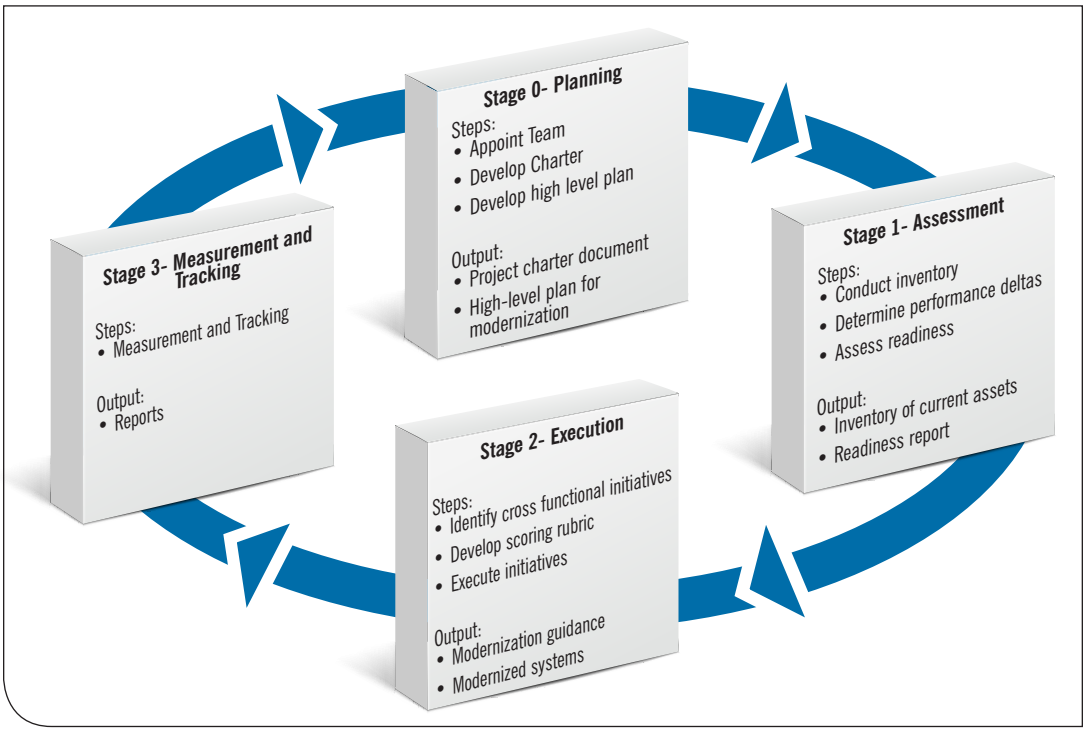


Implicit in modernization are several core principles, which in many ways are present in any innovative approach to solving existing problems:

- **Principle 1:** Most organizations are good at generating modernization ideas (e.g., cloud or SaaS) but weaker at bringing the ideas to fruition. As a result, modernization advocates often get frustrated by organizational inertia to enact change, and quickly give up.
- **Principle 2:** Modernization ideas both big and small emerge from every part of the organization and all may have merit. It is important not to rely solely on a single individual (e.g., the CIO) or even a small group of individuals to generate all valid modernization ideas.
- **Principle 3:** Modernization is a process and not an event. So, while tempting to focus on the short term, modernization must remain a strategic focus of the organization. Doing otherwise merely solves an immediate problem while setting up the organization for an unending future of crisis-centric approaches.
- **Principle 4:** All modernizations are not created equal. Some modernizations involve quick-hit technology-centric solutions, while other modernizations are longer-term efforts that require substantial personnel and process-centric changes.
- **Principle 5:** Modernization is a complex undertaking and requires dedicated resources with specialized knowledge and skill for successful program execution. If sufficient and appropriate resources are not available in-house, outside support may be required.
- **Principle 6:** Industry can provide valuable insight in adapting private-sector practices into the public sector. However, this process needs to be very carefully managed and deployed.

Any successful modernization effort addresses the people, processes, and technologies currently in place and develops a plan to reduce risk, promote adoption, and realize benefits. This report distills the essence of numerous modernization strategies and experiences into the roadmap approach recommended in Figure 6, and is consistent with the guidance on implementing MGT.

Figure 6: Roadmap



This roadmap is not a waterfall model, but rather a circular model. This is because modernization is not a single event, but rather an ongoing process requiring continuous attention. By treating modernization as a process, organizations can better manage technology investments and continue to stay on pace with change, rather than having to engage in a costlier "catch up" situation.

Finally, a feedback loop from each stage to the prior stage reflects the fact that modernization solutions need to be continuously assessed and considered. With the feedback loop, important insights can be gathered and made actionable. The next section details elements of the roadmap.

Stage 0: Planning

Objective: To form and charter the core modernization team and establish their overarching goals

Steps:

0.1: Appoint team lead and cross-functional core team members. Primary responsibility: Agency Director (or designate)

0.2: Develop/approve project charter, establish governance protocols and codify goals for the modernization effort. Primary responsibility: Core team leader

0.3: Develop/socialize high-level plan for modernization. Primary responsibility: Core team

Major outputs:

- Project charter document
- High-level plan for modernization

In this stage, modernization starts to move from concept to action.

In the first step (0.1), the agency director, likely in concert with the entire organizational leadership structure, formalizes IT modernization as a key agency goal and forms the core modernization team that will guide the modernization effort. The core team should act as an executive steering committee for the project, and team members should have sufficient stature within the organization to command respect and be able to cajole or, if necessary, force actions. The CIO can act in the role of core team leader, consistent with the role of the CIO under FITARA. In this context, the CIO is more of a "first among equals" who leads by persuasion. This will ensure that the project has required executive support, key to successful implementation and called for under the MGT Act.

In the second step (0.2), the core team, under the facilitation of the core team leader, develops a project charter document to guide the interaction between team members, clearly establishes a governance structure for the organization, and codifies overall goals for modernization. As previously discussed, core team members should stratify numerous modernization goals into levels of importance, consistent with overall federal guidance. Additionally, the project charter should include the guiding principles of a communication plan to inform and educate agency staff, including mission leaders and cross-functional personnel.

To prevent modernization from being an "IT thing," the communications plan should frame the activity as involving business issues that happen to have an IT component. Similarly, the plan should address people and process in addition to the technology. By framing the plan around business problems, modernization is far more likely to be accepted by senior management and cross-functional staff. This keeps the focus on business issues and agency mission issues that MGT supports.

Once developed, the project charter should be reviewed and approved by the Agency Director and then distributed as appropriate under the communications plan.

After the project charter has been approved, work on a high-level plan for modernization (step 0.3) can begin. The plan will have numerous tracks to be developed and rationalized, and these tracks should generally align to the people-process-technology triad needed for long-term modernization. In addition, tracks should be cross-functional rather than system-centric. For example, procurement related issues across systems can be treated together in the process track, shifting the modernization dialog from a system-by-system approach to an enterprise view.

The high-level plan should not fall victim to "paralysis by analysis" and should focus on the broad brush strokes necessary to get modernization moving. Said differently, the high-level plan should create a scaffolding by which each modernization initiative can hang and evolve, rather than being fully comprehensive.

Once the high-level plan is developed, each core team member needs to socialize the plan with key internal and external stakeholders—not for approval, but rather to gain beneficial insights and support for the plan.

Finally, these plans could be submitted to a central authority – for example, OMB at the Federal level -- to track implementation progress. This creates a momentum for moving forward on modernization since successes and lessons learned will be highlighted. Second, it offers an avenue for cooperation and sharing best practices among agencies.

Stage 1: Assess Current Environment and Establish Performance Deltas

Objective: Capture the organization's as-is state in order to have a baseline of organizational assets and to define relevant performance deltas

Steps:

1.1: Plan and conduct an inventory of current assets. Primary responsibility: Core team and work groups

1.2: Determine performance deltas. Primary responsibility: Core team

1.3: Assess modernization readiness. Primary responsibility: Work groups

Major outputs:

- Inventory of current assets
- Readiness report

In this stage, the organization begins to understand what it has and how far it needs to go to accomplish its modernization goals, consistent with the template for TMF funding.

In the first step (1.1), the organization, led initially by the core team, plans and conducts an inventory of all of the relevant systems, including technology, people, and processes. Initially, each core team member should lead work groups to capture the major systems that are part of their department. As one federal CIO said, "if you don't get a handle on what you have, it could be nearly impossible to define a roadmap, identify duplication of applications draining resources, or make a business case for new IT investments and projects."[27]

27. https://www2.deloitte.com/us/en/pages/public-sector/articles/ten-it-modernization-tips.html

CIO Howze of Louisiana followed this strategy as well. His goal was to "leave the lights on" while they learned what they had inherited, to understand and document the "as-is." Once they understood the current environment, they were able to make informed decisions on what to consolidate, what to standardize on, who would help, and what the processes would be.

This effort is not a walk in the park. As noted earlier, when MacMillan of Pennsylvania asked state IT offices which programming languages their applications were built with, the most frequent answer was "I don't know" or "I am not sure." Considerable digging may be required to get the correct answer.

The core team should develop a data capture strategy that will ensure that all of the relevant data is captured for each system. At a minimum, the document should capture:

- Technology (including hardware, software, and telecommunications infrastructure)
    - Type of technology (brand, manufacturer, etc.)
    - Age (initial purchase date and any major upgrades since then)
    - Estimated useful life
    - Usage (number of users, concurrent, named, etc.)
- People
    - Number/type of people performing all tasks associated with the system
    - Experience of people
    - FTEs assigned
- Internal business processes and functions, and external contracts
    - Internal business processes and functions
    - Hardware contracts, maintenance, duration
    - Software contracts, maintenance costs, duration
    - Services contracts, costs, number of people

Once this document has been developed, work teams for the various offices can begin the inventory. Generally speaking, most of the inventory work can be done via email and on-line forms, but each function can devise its own data-capture strategy. The output of this step is a complete, enterprise-wide inventory.

It is important to also capture people and process data in addition to the systems data. Simply put, people use technology to solve business problems and use processes to implement and manage technology. As Reese of Oklahoma noted, technology can come and go but people hold the institutional knowledge of how the business works. Without this focus, as people move on the institutional knowledge will be lost and services will suffer. This will also help ensure that knowledgeable staff can make reasonable estimates to meet repayment requirements, like those in the TMF.

In the next step (1.2), performance deltas for each system can be determined. There are numerous ways to do this.

At NASA, Wynn divides assets into three categories: keep, decommission, and modernize. "Keep" assets are satellites that generally have a 7–10-year life cycle (although some have been functioning since the 1970s). NASA does what it can to upgrade these assets, but the

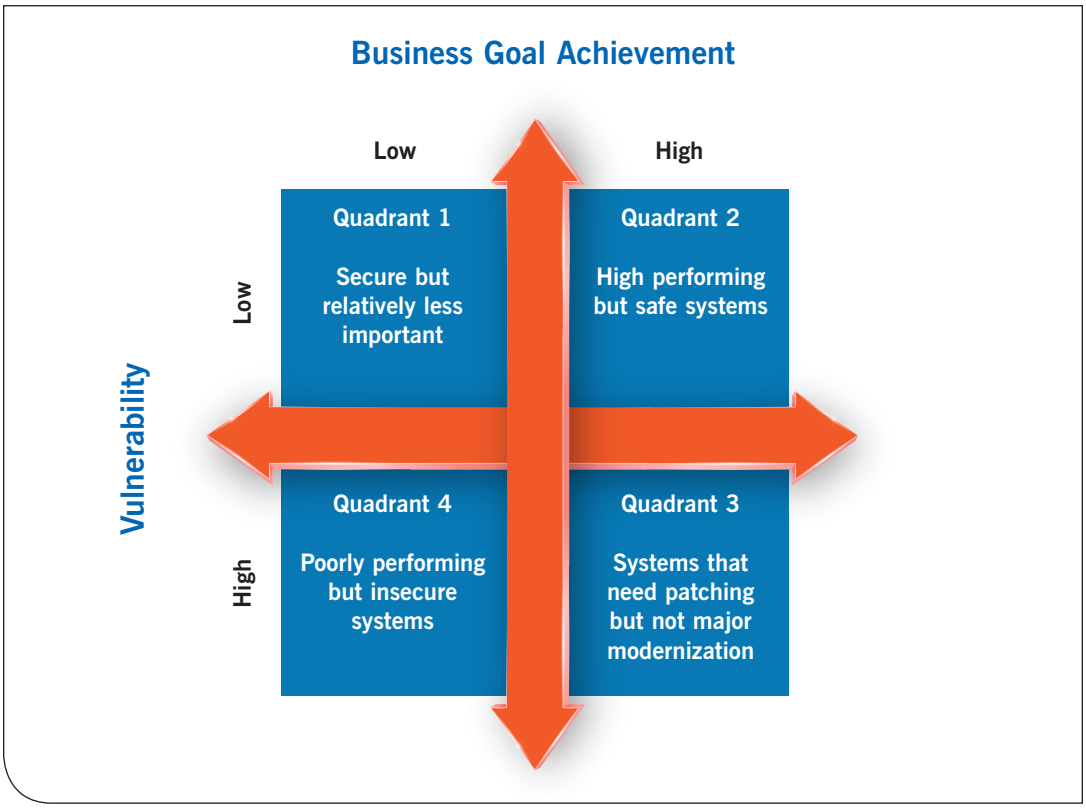
primary focus is on managing them from a cybersecurity position. Wynn describes "decommission" assets as looking at future business needs and tracking backwards to current processing needs, to see what the future requires from a technology, people, and process standpoint. If no future business need exists, the system is decommissioned. If a future need exists, the system (people, process, and technology) are "modernized" (or upgraded). This approach focuses on the future needs of the organization rather than just the status quo.

Michael Hermus, U.S. Department of Homeland Security Chief Technology Officer, recommends that CIOs "take legacy systems that are the most expensive to operate and divide them into two categories: those that get a lot of attention and support core business needs, and those that aren't part of the core business. Then, take the ones that aren't part of the core business and decommission them."[28]

This report recommends the use of performance deltas as follows. The first piece, business goals, focuses on how well the system meets its primary business purpose, addressing multiple relevant questions: Is the system fully compliant with its core mission? Are critical dates generally met? Are users generally satisfied with performance? Are there any upcoming mandates that would require a major overhaul (e.g. analytics)? Have any performance issues been noted either internally or externally to the agency?

The second piece focuses on systems vulnerability, defined broadly as including cybersecurity obsolescence, staffing, and other factors. Putting the two pieces together allows for stratifying systems as shown in Figure 6.

Figure 6: Typology of Systems[29]



28. https://www.govtechworks.com/why-modernization-is-key-to-national-cyber-strategy/#gs.obMcydY
29. A number of different typologies are available for usage, including IBM's Application Portfolio Analysis (APA). We are not trying to suggest that this is the only typology that is available and, as needs dictate, another similar typology can be used.

From the chart, systems can be placed in one of the four quadrants in order to develop an initial stratification. Systems in Quadrant 4, low business goal achievement and high vulnerability, would naturally rise to the top of modernization efforts, while those with high business goal achievement and low vulnerability (Quadrant 2) would be less pressing.[30] A similar prioritization is part of the TMF funding criteria.

In the final step (1.3), work teams would develop a readiness profile for each system. The readiness profile should focus on readiness for cross-functional goals, including analytics and shared services, and address technology, people, and process readiness. In this step, systems will begin to cluster together in terms of stratification and readiness. Systems in the low-business-goal and high-vulnerability quadrant that is more ready for cross-functional goal achievement would rise to the top.

All of the readiness information, along with the supporting documentation, should be prepared by the work groups and then reviewed and validated by the core team. This ensures that the core team takes a cross-agency perspective and can readily understand better targets.

Stage 2: Modernization Execution

Objective: To identify and begin to execute the modernization strategy

Steps:

2.1: Identify cross-functional initiatives. Primary responsibility: Core team

2.2: Develop and apply the modernization scoring rubric to select initial modernization targets. Primary responsibility: Core team

2.3: Execute modernization initiatives. Primary responsibility: Work teams

Outputs:

- Modernization guidance
- Initial modernized systems

In this stage, the focus is on identifying and executing the modernization strategy with key insights gained from prior steps.

In the first step (2.1), the core team needs to identify and formalize cross-functional initiatives. These initiatives, many of which are part of "long tail" discussion, can be leveraged across the enterprise and include such things as moving to the cloud, implementing cognitive computing, and shared services models of usage. The entire enterprise can benefit, but the costs should not be placed on any single system or program. By focusing on cross-functional initiatives, the core team can also align progress with individual initiatives.[31]

It makes sense that cloud computing initiatives are among the first to be implemented, since they are the most mature of modernization initiatives and offer the quickest potential savings. The U.S. is the leader in cloud adoption—but the public sector is considerably behind, despite the federal "cloud first" policy commenced in 2011. The Professional Services Council's (PSC) 2016 Federal CIO Survey found that only 5 percent of federal IT leaders felt that sufficient effort had been made to move strongly into the cloud.[32] Migrating to the cloud can be a win for the federal government, since adequate knowledge of how to do it and a strong base of service providers exist. It fits the "do once, use many times" approach.

30. This is similar to the concept of High-Risk, High-Value Assets (HVA) program that was started in 2015.
31. Although these are presented as cross-functional initiatives, they can also easily be applied to cross agency initiatives.
32. https://www.pscouncil.org/News2/NewsReleases/2016/PSC_Releases_26th_Annual_Federal_CIO_Survey.aspx

This is not to suggest that everything should be moved to the cloud. Certain data has a much higher requirement for protection, and analysis needs to be undertaken to ensure that a cloud provider can provide equal or better security under federal guidance. Applications that are not appropriate (either technically or programmatically) for the cloud should still be considered targets for in-place modernization.

The other cross-functional initiative that should be on the forefront is an expansion of the shared, reusable enterprise services that span government agencies, reducing duplication of major business systems (e.g., Financial Management, HR, payroll, and benefits). These shared services can be commercially owned, or government owned and commercially supported. Several agencies have already ventured into the shared services model (among others, these include the Federal Aviation Administration at DOT, the Financial Management Services at Treasury, the Department of Commerce, the Department of Veterans' Affairs, and the General Services Administration), and are seeing some success. Shared services could span across agencies or expand fully within an agency. The General Services Administration's Unified Shared Services Management Office is leading significant activity in this space, working with OMB and both customer and provider agencies. This is also consistent with the MGT and similar precepts that encourage use of commercial products and services.[33]

Both moving to the cloud and implementing shared enterprise systems requires significant transition work, including planning for necessary downtime. Clearly, business demands will drive how quickly this can happen and in what order.

Running in parallel with this step is the task of updating old and cumbersome procurement processes. Previously, most modernizations were associated with purchasing new hardware and software, and the procurement vehicles fit that model. However, a significant percentage of upcoming modernizations will be based on acquiring a service rather than a product. Procurement rules need to be updated as the cross-functional initiatives are being developed, to ensure that they work together. The PSC has listed necessary procurement changes as good starting points, including:

- adopting performance-based contracting
- supporting consumption-based purchasing for cloud computing
- taking advantage of current flexibility in the Federal Acquisition Regulation (FAR) to speed introduction of new technologies
- discouraging the use of lowest-price technically-acceptable (LPTA) evaluations for complex technology procurements

In the second step (2.2), the agency needs to develop a scoring system[34] to guide modernization progress based on the drivers for the modernization developed in the project charter discussed in Table 1, consistent with guidance provided under MGT. Once defined, a scoring system can help with selecting modernization candidates in a host of ways.

Various State and Federal experiences demonstrate different approaches to prioritization:

- Toner of Nebraska suggests that the easiest place to start modernization is at the heart of the organization—its network. Once Toner created a single network from the "mess" of

33. https://policy.cio.gov/modernizing-government-technology/policy/

34. A number of scoring systems exist, and they generally consider how much the modernization will (1) contribute to organizational strategy, (2) provide cost savings, (3) be required to achieve payback, (4) require substantial human resources, (5) availability of resources and (6) place substantial risk on the organization. This mixture of hard and soft scores is appropriate since not all factors are easily quantified (e.g. amount of risk).

numerous networks, modernization targets became much easier to identify and implement. For example, after Toner fixed the network "mess," he could build a business case to create a private cloud for the state. Rather than using a commercial cloud provider, the CIO's office drives private cloud activity and passes savings along to user agencies.

- MacMillan of Pennsylvania takes a risk-based approach to identifying and selecting modernization initiatives. He looks at the supportability and sustainability of the current environment relative to the needs of the business, assessing both technology and labor market support issues. The CIO then takes a portfolio approach to decide what initiatives to undertake and when. MacMillan carefully selects high and low-risk initiatives to be done together, to stretch the organization but without introducing undue risk. Cloud technology is a good example of the need for planning. According to MacMillan, while cloud technology can be a great solution to modernization and relieve internal network pressures, organizations need to avoid the "siren's song" of the cloud and ensure that the systems are "right placed" to improve performance and reduce risk.
- Davis of Ohio made an interesting discovery while working with agencies to modernize and migrate their IT infrastructure. He found that the agencies with strong IT processes and discipline often vied to be first in modernizing, while many reluctant agencies did not have formalized processes. Davis attributes this to the incredible scrutiny that modernization puts on the agency. Generally speaking, a well-performing IT organization will be comfortable with scrutiny, while under-performing IT organizations will be uncomfortable.
- Bray suggests looking for quick wins in order to build momentum for larger initiatives. In Bray's case, selecting the first initiative was easy. The Chairman of the FCC in 2014 was at a function at the Commission's Gettysburg offices when he noticed that consumers were all filling out hardcopy forms. He encouraged Bray to identify a better solution. This led the CIO team to modernize the consumer helpdesk as a quick win with the backing of the Chairman.

At this point, the organization needs to decide whether to use a two-step or a greenfield model; each could be of value. In cases where full functionality needs replacement, the greenfield model may be preferable. In cases where customer-facing functionality needs immediate replacement but the backend functionality is relatively stable, a two-step approach may be preferable.

A new and final consideration for modernization targets will be the newly issued rules surrounding the IT modernization funds authorized under the MGT Act. While the operational processes for this fund are just now being shared, the criteria for project funding will be an important determinant for project selection.

Once modernization targets have been selected and initial planning has taken place, performance metrics for each initiative should be developed and the planning documents and performance targets should be developed for tracking, publication, and central coordination (by OMB in the federal environment).

In the final step (2.3), modernization execution begins. There are myriad ways to modernize, but the most compelling involves Agile development methods. As evidenced by the FBI VCF's troubled implementation, stakeholders often pile on requirements that may not directly relate to the targeted modernization effort. To resolve problems like this, Agile approaches can be a valuable strategy to address these issues.[35] An Agile strategy will enable the agency to plan and execute a phased approach that achieves quick wins to increase momentum while reduc-

35. http://www.businessofgovernment.org/report/guide-critical-success-factors-agile-delivery

ing resistance. This is a pragmatic means of dealing with the considerable planning and effort associated with a large-scale modernization effort, since sufficient evidence from the private and public sectors shows that larger projects more frequently fail than smaller projects. Agile also lowers risk and allows for mid-course corrections as required.

In the FCC case, since the overall goal was to shift away from 207 legacy systems that were "on-premise" in agency-operated servers and move them to the cloud in an extremely short period of time, the risk of migration issues was real. As a result, the FCC approached this complex effort in phases, with the first demonstration phase (replacing the customer help center) accomplished in six months and for about $450,000—vs. what had been quoted for a legacy, on-premise approach of 12-16 months and $3.2 million. The FCC CIO team showed that modernization was possible, and the team could then start to address more complicated legacy issues with greater momentum.

In concept, agencies may wish to halt legacy system funding as modernization initiatives unfold, but this may not be practical to support continued mission support and delivery. As pointed out by the PSC report, delaying or canceling such contracts could put the government at an unacceptable level of risk.

Stage 3: Measure and Track Initiatives

Objective: To track and measure the success of initiatives

Step:

3.1–3: Capture and report metrics.

Output:

- Reports

The final step is to track successes, failures, and lessons learned from each modernization initiative, using performance metrics discussed in step 2.3. Once these metrics have been agreed upon and the scoring has been accepted, the appropriate government coordinating office (OMB at the federal level) should track the achievement of metrics as well as adjustments necessary to improve performance, also consistent with the MGT Act guidance. There may also be advantages to implement performance incentives at this point, such as gain sharing or share-in-savings approaches. While the federal government does not have a great deal of experience in implementing such models, data from the private sector and the States show that this may be of value for multi-year modernizations.

Finally, the metrics will indicate when additional modernization efforts are necessary, which completes the loop back to Stage 0. Additional modernizations are inevitable and need to be anticipated.

CONCLUSION

The high allocation of public-sector O&M costs, in relation to the commercial sector, is not sustainable and only treats short-term symptoms instead of modernizing IT to correct systemic problems.

Federal agencies must consider their spending on IT and how to make the right investments that can increase efficiency and decrease costs. IT modernization initiatives can transform an organization's infrastructure, technologies, applications and services to greatly reduce costs, improve performance and meet evolving mission needs and priorities. Key advantages afforded by IT modernization initiatives include:

- Ability to utilize modern, industry-leading technologies to meet future needs
- More rapid delivery of solutions due to increased automation
- Improved business process and operational performance
- Deeper insights and operational visibility via big data and analytics
- Improved decision making via analytics and cognitive solutions
- Expanded use of government-wide enterprise services and compatibility across government platforms, systems and databases
- Reduced redundancies via the consolidation of application portfolio and services
- Ability to leverage cloud computing solutions
- Ability to utilize commercially available solutions for cloud, mobile, data and social
- Improved application portability and use of standardized managed services

However, significant issues will remain if the problem is left unaddressed, including:

- Unsustainable and escalating costs
- Challenges with an aging workforce and a shortage of people with skills to support increasingly obsolete technology
- Inability to meet rising security threats

The government should make key investments in IT modernization and identify and prioritize the necessary initiatives for maximum effectiveness. Priority investments should be integrated into the budget planning cycle, and appropriate measures must be taken to provide a foundation for continuous innovation and improvement. With recent statutory and agency progress, the federal government is well-positioned to set an example in implementing modernization frameworks, like those outlined in this report, and moving forward with effective IT modernizations that improve mission performance.

ACKNOWLEDGEMENTS

List of Those Interviewed for This Project.

Bo Reese, Chief Information Officer, Office of Management and Enterprise Services, State of Oklahoma

David Bray, Currently Executive Director for the People-Centered Internet coalition and former Chief Information Officer of the FCC

Dickie Howze, Chief Information Officer, State of Louisiana

Ed Toner, Chief Information Officer, State of Nebraska

John MacMillan, Chief Information Officer, Commonwealth of Pennsylvania

Renee Wynn, Chief Information Officer, NASA

Stu Davis, Chief Information Officer and Assistant Director of Administrative Services, State of Ohio

Todd Kimbriel, Chief Information Officer and Deputy Executive Director, Texas Department of Information Resources, State of Texas

ABOUT THE AUTHOR

Dr. Gregory S. Dawson is a Clinical Associate Professor at the Center for Organization Research and Design (CORD) within the College of Public Programs at Arizona State University and is also an Assistant Professor in the W. P. Carey School of Business.

DR. GREGORY S. DAWSON

Dr. Dawson was awarded his PhD in Information Systems from the Terry College of Business at the University of Georgia.

Prior to becoming an academic, Dr. Dawson was a Partner in the Government Consulting Practice at PricewaterhouseCoopers, joining PwC (formerly Coopers & Lybrand) in the Washington, D.C., office and later relocating to Sacramento, California. Dr. Dawson was a leader in the field of public sector outsourcing as well as information systems implementation. He has worked extensively with the federal government (including Central Intelligence Agency, Department of Defense (Army, Navy, Air Force and Marines), the Federal Deposit Insurance Corporation (FDIC), and the Bureau of the Census, among others) and with a variety of state governments (including Virginia, North Carolina, Pennsylvania, New York, and California). After leaving PwC, Dr. Dawson was a Director at Gartner, working in the state and local government practice.

Dr. Dawson is also the President of the Association for Information Systems Special Interest Group on IS Leadership and co-leads a track on IS leadership at a major IS conference. His research is primarily focused on information systems leadership and innovation in the public sector. His work has been published in a variety of top academic and practitioner journals. His research has been published in Journal of the Association for Information Systems, Decision Support Systems, Organization Science, *Journal of Management Information Systems, ACM Transactions on Management Information Systems, Communications of the Association for Information Systems, InformationWeek* and numerous Brookings Institution reports.

KEY CONTACT INFORMATION

To contact the author:

Dr. Gregory S. Dawson

Clinical Associate Professor
Center for Organization Research and Design

Arizona State University

300 E Lemon St.

Tempe, AZ 85287

Phone: (602) 908-1915

GregorySDawson@gmail.com

REPORTS FROM THE IBM CENTER FOR THE BUSINESS OF GOVERNMENT

For a full listing of our publications, visit www.businessofgovernment.org

Recent reports available on the website include:

Acquisition

Ten Actions to Improve Inventory Management in Government: Lessons From VA Hospitals by Gilbert N. Nyaga, Gary J. Young, and George (Russ) Moran

Beyond Business as Usual: Improving Defense Acquisition through Better Buying Power by Zachary S. Huitink and David M. Van Slyke

Collaborating Across Boundaries

Cross-Agency Collaboration: A Case Study of Cross-Agency Priority Goals by John M. Kamensky

Interagency Performance Targets: A Case Study of New Zealand's Results Programme by Dr. Rodney Scott and Ross Boyd

Improving Performance

Seven Drivers Transforming Government by Dan Chenok, Haynes A. Cooney, John M. Kamensky, Michael J. Keegan, and Darcie Piechowski

Five Actions to Improve Military Hospital Performance by John Whitley

Maximizing the Value of Quadrennial Strategic Planning by Jordan Tama

Leadership, Change, and Public-Private Partnerships: A Case Study of NASA and the Transition from Space Shuttle to Commercial Space Flight by W. Henry Lambright

Innovation

Tiered Evidence Grants - An Assessment of the Education Innovation and Research Program by Patrick Lester

A Playbook for CIO-Enabled Innovation in the Federal Government by Gregory S. Dawson and James S. Denford

Making Open Innovation Ecosystems Work: Case Studies in Healthcare by Donald E. Wynn, Jr., Renée M. E. Pratt, and Randy V. Bradley

Leadership

Best Practices for Succession Planning in Federal Government STEMM Positions by Gina Scott Ligon, JoDee Friedly, and Victoria Kennel

Risk

Risk Management and Reducing Improper Payments: A Case Study of the U.S. Department of Labor by Dr. Robert Greer and Justin B. Bullock

Ten Recommendations for Managing Organizational Integrity Risks by Anthony D. Molina

Using Technology

Delivering Artificial Intelligence in Government: Challenges and Opportunities by Kevin C. Desouza

Using Artificial Intelligence to Transform Government by The IBM Center for The Business of Government and the Partnership for Public Service

Digital Service Teams: Challenges and Recommendations for Government by Professor Dr. Ines Mergel

Ten Actions to Implement Big Data Initiatives: A Study of 65 Cities by Alfred T. Ho and Bo McCall

The Social Intranet: Insights on Managing and Sharing Knowledge Internally by Dr. Ines Mergel

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, DC 20005
202-551-9342

website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

Stay connected with the IBM Center on:

or, send us your name and e-mail to receive our newsletters.

IBM Center for
The Business of Government

20 years of research for government:
informing today, envisioning tomorrow

1998-2018