

Digital Modernization for Government

An Implementation Framework



Gregory S. Dawson
Arizona State University

Kevin C. Desouza
Queensland University of Technology

James S. Denford
Royal Military College of Canada

Dr. Marc E. B. Picavet
Queensland University of Technology

Digital Modernization for Government:

An Implementation Framework

Gregory S. Dawson

Arizona State University

James S. Denford

Royal Military College of Canada

Kevin C. Desouza

Queensland University of Technology

Dr. Marc E. B. Picavet

Queensland University of Technology

DECEMBER 2024

Table of Contents

Foreword	5
Executive Summary	6
The Challenge of Modernization	9
Issues in Successful Balancing between Modernization and Transformation	13
Framework	26
Implementing Change	40
Closing Thoughts	44
About the Authors	45
Acknowledgments	48
Recent Reports from the IBM Center for The Business of Government	49

The maturation of next-generation digital technologies, such as large language models and quantum computing . . . promise to revolutionize how public services are delivered, offering unprecedented opportunities for innovation, efficiency and public value creation.



Foreword

On behalf of the IBM Center for The Business of Government, we are pleased to present this new report, *Digital Modernization for Government: An Implementation Framework*, by Gregory Dawson with Arizona State University, James Denford with the Royal Military College of Canada, and Kevin Desouza and Marc Picavet with Queensland University of Technology in Australia.

Governments today increasingly face the challenge of how to integrate transformational digital technologies like artificial intelligence, while maintaining or modernizing legacy infrastructure and applications. This challenge is compounded when officials seek to create value for the public from digital modernization when those technologies have evolved via different strategies, including “waterfall” approaches that often take longer to implement than “agile” approaches.

This report leverages interviews with government leaders, existing case studies, and prior research to create an evidence-based framework for digital modernization. The framework can help government leaders to innovate by harmonizing across multiple computing environments and transformation strategies, increasing effectiveness and efficiency to improve results for the public.

This report builds on multiple prior IBM Center reports by the authors that have helped government leaders to achieve success in technology implementation, including *Artificial Intelligence in the Public Sector: A Maturity Model* and *A Roadmap for IT Modernization in Government*. The report also contributes new research around agile government, adding to the content accessible to government leaders and stakeholders through the *Agile Government Center* (led by the National Academy of Public Administration in collaboration with the IBM Center).

We hope this report helps government leaders to improve their development and implementation of digital government.



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



Adam Jelic
Vice President and Senior Partner
Business Transformation Services
IBM
ajelic@us.ibm.com



Executive Summary

All levels of government are being tasked with taking greater advantage of the boom in technology. However, these efforts are limited both by legacy system debt, and confusion about how to harmonize maintaining legacy systems while still modernizing or transforming other systems. There is also a great deal of confusion about the difference between modernization and transformation.

In this context, digital modernization refers to the necessary incremental evolution of the systems that enable them to continue serving their intended purpose, generally focused on maintaining or improving operational efficiencies. By contrast, digital transformation focuses on redefining how the business of the entity gets done. As such, transformations are far more ambitious and carry a higher risk and reward.

There are several issues associated with successfully modernizing or transforming systems:

Issues	Description
Tension between desires and realities	Often agencies need to realize what they want is secondary to their budget realities. Remaining aware of these budget realities can drive far more realistic goals.
Tensions between modular and monolithic systems	Tradeoffs between modular and monolithic systems is fundamentally a tradeoff between flexibility and simplicity versus integration and control. Choosing smartly is necessary for success.
The cost of newness in government	Government has long been fascinated by new and exciting ideas stemming from private industry, these may introduce new costs.
Solving the agile versus waterfall conundrum	Government has historically been bound to a waterfall approach, but inventive agencies are now better able to merge agile with waterfall to achieve better outcomes.
The challenge of new versus established vendors	Large established vendors have long been the preferred vendors for government agencies, but new entrants can also bring innovation important for transformation.
The need for data management	Securing and governing accurate and up-to-date data is critical for the successful usage of any system.
Accessibility versus security	Agencies need to resolve the struggle between having highly accessible data with the need for appropriate cybersecurity.

Mindful of these issues, this report offers a framework for resolving these issues and enacting effective modernization and transformation.

Solutions	Description
People at the center of all technology decisions	Despite appropriate focus on the latest technology, people should be central to effective modernization and transformation.
Robotic Process Automation (RPA)	RPA is emerging as an elegant and relatively easy solution to solving many of the vexing technology challenges that exist within government.
Generative AI	Much as GenAI is overtaking industry, it has the capability to provide a substantial boost to government but only with adherence to ethical AI standards and principles.
Know what TIME it is	All systems are not created equal and all value is not created equal. Knowing when to Tolerate, Improve, Migrate, or Eliminate (the TIME model) a system is helpful to ensure that funds are being spent most effectively.
Agile/flexible processes versus structure	Government has long relied on highly structured processes and much of that has been driven by procurement regulations. Shifting the mindset to incorporating agile principles into a waterfall design can be helpful while still remaining compliant with procurement rules.
Creative and detailed contracting with vendors and providers	Despite the rigor of government procurement rules, agencies still have a great deal of flexibility in contract operations. Taking advantage of this yields far better outcomes.
Curiosity	Curiosity has long been proven critical to success in many places, being endlessly curious on how to improve things is probably the best starting place for government.

Enacting effective change rests on successfully performing the five steps below, while focusing on the four observations that follow.

Element	Description
Step 1—Ensure the right leadership is in place	Select experienced leaders with technical and change-management skills, align them with the mission, define roles, provide resources, communicate vision, and maintain engagement to drive transformational IT system success.
Step 2—Determine the appropriate implementation approach	Choose waterfall for stable, well-defined projects and agile for evolving, user-focused initiatives. Assess scope, culture, and expertise, or adopt a hybrid model for structured oversight and adaptability.
Step 3—Determine the vendor approach	Learn from established vendors for stability and reliability, and new vendors for innovation and agility. Assess track records and goals or use a mix to balance modernization with minimized risk.
Step 4—Implement a robust data management plan	Create a centralized data governance framework, use automated tools, ensure cybersecurity, and conduct regular audits. Foster accountability and training to maintain data accuracy, security, and adaptability in government technology solutions.
Step 5—Determine which technologies are (and are not) appropriate	Choose technologies aligned with goals, scalable, sustainable, and compliant. Prioritize cost-effectiveness, interoperability, vendor reliability, and future innovation. Engage stakeholders to ensure operational efficiency and public service priorities are met.

Element	Description
Consideration 1—Recognize and resolve the inherent tension between what you would like to do (desires) and what can be done (reality)	Align goals with clear priorities, engage stakeholders early, and use phased implementation. Advocate scalable, cost-effective solutions like open-source software. Promote cross-department collaboration and training to maximize resources and achieve outcomes.
Consideration 2—Resolve the tension between modular and monolithic systems	Choose modular or monolithic systems based on agency needs, scalability, cost, and goals. Modular offers flexibility; monolithic ensures simplicity. Engage stakeholders, assess constraints, and consider hybrids to balance functionality and growth.
Consideration 3—Put people at the center of all technology decisions	Prioritize user-centric design, stakeholder engagement, and inclusivity. Use feedback-driven prototyping, transparent communication, and training to build trust, empower users, and ensure technology enhances public service delivery effectively.
Consideration 4—Remain curious throughout the effort	Stay curious by connecting the project's purpose to your growth, breaking tasks into milestones, learning proactively, collaborating, reflecting on impact, staying organized, and embracing challenges as learning opportunities.

Government depends on successful technology operations, and this report serves as a guide for success to bring digital change that will improve agency operations.



The Challenge of Modernization

In today's rapidly evolving digital landscape, organizations across all industries, including government, are increasingly focused on leveraging technology to remain competitive and agile. However, especially in the case of the public sector, these modernization efforts are not always successful.

For example, in April 2023, the Internal Revenue Service (IRS) described how it was going to use the billions of dollars it received from the Inflation Reduction Act of 2022, and the tens of billions of dollars appropriated to it in August 2022, to transform the administration of the nation's tax system and its underlying services provided to the taxpayers. The technology portion of the plan described how the IRS would retire and replace legacy tax systems, give taxpayers access to their data via online portals, and provide continued security and privacy of tax data.¹ In all, there are 142 separate projects to accomplish these goals. The scope of the planned transformation was incredible.

However, in its audit, the GAO has noted that adequate planning has not taken place and that this planning was necessary to build a go-forward roadmap to implement the strategic portion of the plans. Shortly after, Congress sliced the IRS technology budget by \$20 billion in March of 2024.² While progress is being made on the effort, much work needs to be done.

Two terms frequently used in technology are *digital modernization* and *digital transformation*. Although they are sometimes used interchangeably, these terms refer to different strategies with distinct goals and methodologies. Understanding the differences between them is crucial for organizations aiming to strategically harness technology to drive growth, enhance efficiency, and innovate in an increasingly digital world. As one of our interviewees said, “One of (our) first issues is probably from a strategic perspective [in] making the differentiation in terms of what is a modernization effort and what is a transformation effort.”

-
1. U.S. Government Accountability Office. (2024, March 19). *Information Technology: IRS Needs to Complete Planning and Improve Reporting for Its Modernization Programs*. <https://www.gao.gov/products/gao-24-106566>.
 2. Heckman, J. (2024, March 21). Congress proceeds with \$20B cut to IRS modernization fund in FY 2024 spending deal. *Federal News Network*. <https://federalnewsnetwork.com/budget/2024/03/congress-proceeds-with-20b-cut-to-irs-modernization-fund-in-fy-2024-spending-deal/>.

Digital modernization is information technology (IT) housekeeping—the necessary incremental evolution of systems to ‘keep the lights on’—but it is vital to ensure that systems are fit for purpose and secure. These efforts involve activities such as upgrading and scaling of existing information systems to keep up with internal and external pressures on existing business processes. Modernization efforts are generally focused on operational efficiency and maintaining service quality but without changes to the underlying processes, structures, and people.

The primary goal of modernization is to ensure that existing technology can support the demands of contemporary business environments. For many organizations, outdated technology can become a bottleneck, impeding growth, causing inefficiencies, and driving up maintenance costs. Modernization seeks to remove these roadblocks by making systems more efficient, scalable, and cost-effective. Public policy makers are generally in favor of digital modernization since it is a safer and cheaper investment with fewer downside risks.

Digital transformation is more significant. In transformation, the organization is looking to leverage digital affordances to redefine how the business of government gets accomplished. These efforts often involving building entirely new digital systems which have significant implications of how work is done. Unlike modernization, which focuses on upgrading existing technologies, transformation often introduces new technologies that change business models, organizational processes, and customer interactions. Digital transformation, for example, may involve adopting artificial intelligence, the Internet of Things (IoT) or blockchain technology to create new products, services, and revenue streams. Transformation is more disruptive by nature, requiring shifts in organizational structure, routines, strategy and, often, culture.

The implementation approach for modernization versus transformation also varies. Modernization projects tend to be less disruptive, as they usually build on the existing technology stack. The objective is to make improvements while maintaining continuity in operations. It is a way of improving without incurring a great deal of technology debt. As a result, modernization can often be implemented gradually, with systems being upgraded in stages.

In contrast, technology transformation requires a more comprehensive and often riskier approach. It typically involves cross-functional collaboration, redesigning workflows, and upskilling or reskilling the workforce to work with new technologies. Transformation initiatives also tend to be more expensive and time-consuming but can result in deeper, more impactful changes not only to the organization’s technology stack, but also to its underlying processes and competitive positioning. Not surprisingly, the success rate of transformation, by dint of their larger scope, is less than for modernization efforts.

Another important distinction is in the outcomes of each approach. Modernization focuses on efficiency gains, cost reduction, and system reliability. For example, updating an ERP platform may lead to faster processing times, improved data security, and lower maintenance costs. Transformation, on the other hand, aims to create new value propositions and growth opportunities. An agency that undergoes a digital transformation may develop entirely new digital services or reimagine its customer experience in ways that were previously not possible. This aligns with what the IRS was trying to do: fundamentally change how their business operated. While modernization typically provides immediate operational benefits, transformation can open doors to long-term strategic advantages.



Finally, technology modernization and technology transformation serve distinct but complementary purposes in an organization's technology strategy. Modernization focuses on upgrading existing systems to improve efficiency and maintain relevance, while transformation seeks to fundamentally reimagine how technology can be used to create new business models and opportunities. Both approaches are critical to navigating today's rapidly changing technological environment, but understanding their differences is key to deploying the right strategy for a given organizational goal. For most organizations (in or out of the public sector), success in the digital age requires modernization to ensure that systems are up-to-date and secure, and transformation to stay ahead of competitors and meet evolving customer expectations. Balancing these two strategies allows organizations to not only keep pace with change but to lead it.

While digital modernization and transformation are often viewed as two ends of a continuum, most digital projects are more likely to look as falling somewhere in between the extremes, with elements of the two intertwined. A digital project may start as a modernization effort but then the scope grows into a transformation effort. Similarly, a transformation effort may be down-scoped due to a lack of funding or end user support or a change in vision from leadership.

The development of Diia in Ukraine provides a great example of a transformation.³ Starting with the establishment of Ukraine's Ministry of Digital Transformation (MDT) in 2019, the U.S. Agency for International Development (USAID) has been providing technical, financial, and legal assistance in MDT's development of Diia, a mobile application and online portal that

3. USAID. (2023, January 18). USAID Administrator Announces Intent to Provide \$650,000 in Assistance for Digital Transformation. <https://www.usaid.gov/news-information/press-releases/jan-18-2023-us-supported-e-government-app-accelerated-digital-transformation-ukraine-now-ukraine-working-scale-solution-more-countries>.

connects Ukraine's citizen with 120 government services as a one-stop-shop. After Russia's invasion of Ukraine in 2022, Diia has also allowed Ukraine's citizenry to connect to its government's social support services in areas closed by war, and has been used by citizens to access aid and other critical services. Diia is much more than simply putting new technology in place but is rather about fundamentally reexamining how work is done.

Ganesh Selvaraj, who is head of data and AI within a leading public agency, compared his experience of modernization versus transformation as such:



[Modernization] was a big spend. But did it change the way we work? Probably not. Maybe it gave us a bit of a user experience and reduced from frustration. But predominantly we were doing the same job in a new technology and the methodologies were lifted and shifted. We carried the same problem: how we organized our information. We didn't introduce any new taxonomies that's aligned to the business needs. It's the same problem on a new technology. Maybe it was a bit faster and [more] responsive. And maybe it gives some flexibility for people to access things from outside office network and stuff. [Later we did] a proper transformation, not just a modernization. Basically, it was a full-scale replacement of all the technology . . . it was a complete refurbishment. The entire business model and operating model changed with it. From how the customers were dealt with, how the feedback was processed, how they move [service delivery]. I think the whole operating model changed in that journey.



But public sector organizations struggle with differentiating what is a modernization effort and what is a transformation effort and, without this differentiation, it presents a challenge to develop strategies that successfully integrate legacy systems with new digital technologies. In fact, the sheer ubiquity and persistence of embedded legacy systems make their retirement almost impossible and this creates a dynamic where most of the funding and focus of the organization shifts to maintaining current government operations, leaving little budget or focus for either modernization or transformational activities. Even the time and attention that is required to decommission a legacy system is problematic since operational continuity must continue during the decommissioning of the legacy system and the spinning up of the transformational system. As one interviewee told us, *"The retirement of legacy [is] almost impossible in terms of big government engines."*

At the end of the day, making the decision to embark on a modernization or transformation requires unraveling several key issues.



Issues in Successful Balancing between Modernization and Transformation

Through our research, we identified seven issues that need to be resolved in achieving successful modernization or transformation.

Issue 1—Tension between desires and realities

It is easy getting caught up in the buzz words of modernization and transformation and imagine a new world, largely unencumbered by legacy system debt—but this fantasizing has a real cost and level of effort associated with it. As noted earlier, technology modernization is about upgrading and refining, increasing efficiency and preserving functionality value, with a short-to-medium term time horizon. In contrast, transformation aims for a major overhaul of systems and processes, aligning with future opportunities and possibilities due to disruptive innovation. Differences in budget allocation and the willingness to change hinder the balance between these approaches, creating tension and slowing progress.

Budget realities are a central issue, as modernization projects often require less upfront investment than full transformations. Agencies operate within strict budgetary constraints, often driven by election cycles, short-term goals, and public pressure to reduce spending. Because modernization projects typically present lower immediate costs, they are often seen as safer, less financially risky options compared to the extensive investment transformation requires. Yet, choosing modernization over transformation can lead to higher long-term expenses due to the technical debt associated with repeatedly upgrading outdated systems rather than investing in entirely new frameworks. This budget disparity creates tension, as departments must decide whether to pursue short-term gains at the potential expense of longer-term sustainability.

There is no getting around the problem of legacy system technical debt. Bob Osmond, CIO of the Commonwealth of Virginia, estimated that his spending goal is 80 percent devoted to legacy systems and 20 percent available for transformation, but the reality is closer to 90 percent/10 percent and he struggles to avoid having to spend 100 percent of his budget on legacy systems. This is not uncommon and agencies need to grapple with where to spend increasingly tight budgets.

The willingness to change is another significant barrier, influenced by factors such as organizational culture, employee comfort with legacy systems, and the level of perceived risk associated with transformation. Modernization typically involves updating technology with

minimal disruption, appealing to employees and leaders accustomed to legacy systems. Transformation, however, requires a fundamental shift in processes, workflows, and often organizational structure, which can be intimidating for public sector employees who are accustomed to the status quo. Resistance to change within public institutions, particularly among long-tenured staff, reinforces a preference for modernization, even when transformation would offer more lasting improvements.

Additionally, technology transformation requires extensive planning, training, and restructuring efforts, which are often politically unpopular in the public sector. Elected officials may hesitate to support transformation projects that do not show results within their term, as these initiatives often span multiple years. Modernization projects, on the other hand, can theoretically yield faster, more visible improvements that provide political wins in shorter timeframes. This political reality creates pressure to invest in modernization over transformation, perpetuating the cycle of incremental improvements rather than holistic advancements. The lack of bipartisan or long-term support for transformation results in initiatives that are abandoned or underfunded, creating a cycle of dependency on outdated technology.

Ultimately, the tension between technology modernization and transformation in government sectors is rooted in competing priorities: the need for immediate, budget-conscious improvements versus the potential for comprehensive, long-term benefits. While modernization is essential to keep government systems functioning in the short term, relying on it alone can impede innovation and delay the adoption of digital services that meet modern citizen expectations. Addressing this tension head-on requires both cultural shifts within government organizations and political frameworks that support sustained, bipartisan investment in transformational change, allowing governments to build resilient, adaptable technology infrastructures.

The reality is that agencies need to shift from bimodal thinking and to hybrid thinking. Within most transformational programs, there is an element that modernizes the technical stack to allow the new technology, functions and processes to integrate into it. The obverse needs to be true too, in that modernization programs can modify the technology stack in such a way not only to address the immediate business need, but also to set the conditions for full scale transformation in the future. While there is a need to continue to fund legacy systems, not all value is equal and not all capabilities are equal. The challenge is finding a way to keep the legacy system going (short-term requirement) while gradually shifting to modernization and transformation.



Issue 2—Tensions between modular and monolithic systems

Appreciating the paradoxical tension between modularity and monolithic system design requires understanding the inherent trade-offs between flexibility and simplicity. Modular systems are composed of discrete, interchangeable components that can be developed, tested, and maintained independently. This promotes greater flexibility, as modules can be updated or replaced without disrupting the entire system. Modularity fosters innovation by allowing one to experiment in isolated parts of the system. However, this increased flexibility comes with the cost of added complexity. Managing the plug-n-play aspect of modules requires one to think through the overall architecture and interaction protocols between modules upfront that envision future use cases.

On the other hand, monolithic systems are built as a single, unified structure, where all components are tightly integrated and interdependent. Monolithic systems have the advantage of being stable as majority, or even all, possible use cases are envisioned prior to their design and deployment. As such these systems only need regular patches (e.g., for security updates) and minor updates (e.g., to fix functionality issues that are uncovered as features are used). Monolithic systems can often be easier to deploy and maintain in the short term because there is no need to manage multiple moving parts or deal with integration challenges. However, the trade-off is that monolithic designs lack flexibility and often end up silos. Modifying a part of the system often requires significant changes to the entire structure, making it harder to innovate or scale. Over time, as the system grows, this can lead to increased technical debt and reduced agility. As one interviewee told us, *“Our technology aim is to get to a simpler modular world . . . but what we are actually finding is the opposite: the new platforms are just new monoliths.”*

The paradox lies in the inherent tension between the control and coherence of monolithic systems versus the flexibility and adaptability of modular designs. While modularity supports scalability and innovation, it demands careful governance and coordination to avoid system fragmentation. Conversely, while monolithic systems offer short-term simplicity, they can become rigid and difficult to evolve. The challenge for organizations is to navigate this tension by choosing the right design approach based on their goals, scalability needs, and long-term vision. Some may even adopt hybrid models, combining elements of both modular and monolithic architectures to balance flexibility and efficiency. Understanding these tensions allows for more informed decision making, aligning system design with organizational priorities. As Gerald Caron of the International Trade Association of the U.S. Chamber of Commerce noted, *“Even before I got here, they were working on modernizing and they were built since such a way that neither sustainable nor [something] that we could modularly move. How can we make sure that we don’t engineer ourselves into a corner . . . that we can sustain and take on what we want for a longer term . . . that is very important.”*⁴

Unfortunately, agency budgets are rarely amenable to a modular approach and, to get and maintain funding and staffing, the system needs to be treated as a single monolith rather than having modular components. This reality often forces entities to retreat from the optimal modular form to a more monolithic form. If agencies can anticipate this, they can plan a soft landing to a hybrid approach and build in some hooks for future modularity. If not, then they will simply be adding to their field of silos.

4. IBM Center for The Business of Government. (2024, May 6). *Enhancing Information Technology at the International Trade Administration (ITA): A Conversation with Gerald Caron, CIO at ITA*. <https://www.businessofgovernment.org/interviews/5346>.

The paradox of modularity and monoliths contributes to the reality that most public sector efforts are generally more focused on incremental modernization rather than true digital transformation. Resolving this issue allows for more transformational activities to emerge.

Issue 3—The cost of newness in government

Government's infatuation with recruiting technology experts to come in and address challenging innovation issues is well-known and organizations, such as 18F, have been largely successful in supporting technology change.⁵ The success of 18F is due, in large measure, by recruiting external industry experts to serve a short stint as a full-time government employee in order to more easily transfer the lessons and successes of the private sector into the public sector. 18F successes include such things as analytics.usa.gov, College Scorecard, and websites for various government agencies.^{6,7}

However, the recruiting of outsiders as government CIOs as a practice is much less successful. In a report for the Brookings Institution, we examined the phenomenon of hiring “rockstar CIOs,” who are recruits lured from the private sector into the public sector with a mandate to spark innovation.⁸ In this report, we found that, rockstar CIOs were significantly outperformed by career CIOs who have experience working in government.

Career vs Rockstar CIOs—Who Performs Best?

In a 2014 study that compared the effectiveness of state-level CIOs, the authors compared “rockstar CIOs” (those CIOs that had little or not government experience prior to becoming a state-level CIO) with those career CIOs (those CIOs with a long career in government technology before becoming a CIO). The authors found that, almost without exception, career CIOs outperformed rockstar CIOs. Several reasons were offered:

Career CIOs know the rules of government and, while they may not always like them, they understand that they need to be followed. Rockstar CIOs generally do not understand these rules and regularly have run afoul of them.

Government employees, aware of the historically short tenure of an incoming rockstar CIO, often realize that they can simply wait out the newly arriving rockstar. By the time the rockstar CIO realizes this, they are already looking for an off-ramp to go back to industry.

Agency directors (or mayors or legislatures) are often unwilling to risk implementing a major initiative simply based on the star power of the new rockstar CIO. Major initiatives are politically risk and trust is necessary for them to be successful and these business leaders simply do not have that trust in a new and untested CIO.

5. The Verge. (2014, March 22). The government now has a fast-moving IT office modeled after a startup. <https://www.theverge.com/2014/3/21/5533892/the-government-now-has-a-fast-moving-it-office-modeled-after-a-startup>.
6. Brown, M. (2015, March 19). Several U.S. government websites now offer real-time analytics. Geekwire. <https://www.geekwire.com/2015/several-u-s-government-websites-now-offer-real-time-analytics/>.
7. The White House. (2015, September 12). Fact Sheet: Empowering Students to Choose the College that is Right for Them. <https://obamawhitehouse.archives.gov/the-press-office/2015/09/12/fact-sheet-empowering-students-choose-college-right-them>.
8. Denford, J. S., Dawson, G. S., & Desouza, K. C. (2014, September 30). Are Rock Star CIOs the Secret to Public Innovation? Brookings. <https://www.brookings.edu/articles/are-rock-star-cios-the-secret-to-public-innovation/>.

One of our interviewees put it this way: *“There are many necessary processes and constraints in the government. Outsiders can get themselves in jail if they do not understand those [things]. You have to work with the budget people, cybersecurity, privacy, acquisitions, legal, etc., [and make sure] they are focused on protecting the agency and public. That is where the private sector types can get into trouble.”* She went on to add, *“It takes time to trust. You build your track record in different agencies and then move into the CIO role. You need to be a good government citizen first.”*

Robert Osmond of Virginia supports this belief and says, *“Generally, I get a lot of support. I came out of industry into VDOT so it brought a tremendous amount of credibility. Agencies see me as an advocate. It was different coming from VDOT [into the CIO role] since I knew the legal and regulatory framework and had established trusted relationships with the agency CIOs that I serve. Since I came from an agency, I was able to hit the state level running. Otherwise, I would have had to spend the first two years learning government, navigating the budget, preparing and reviewing legislative decision packets, and involving oversight boards. . . . It is just very hard for someone to come in to the state CIO role without state experience.”*

JR Sloan of Arizona added to this, saying, *“I’ve seen the influx of people from the outside: those that come in here with [an attitude] of ‘I’m here to tear things up and fix them.’ If you come in thinking that all [the government people] are idiots, be prepared to fail. My experience in government is that there are a lot of good people who are smart and who want to do good things and, yes, they have to work within the constraints that they have. But the reason my colleagues are successful is that they have been in government for a while, know its challenges and processes and how it works.”*

At the end, agencies need to find a way to harness the new technology ideas emerging from private industry but to also realize that successful implementation of this new ideas is largely dependent on experienced government CIOs.

Issue 4—Solving the agile versus waterfall conundrum

Public sector technology projects often present unique challenges, from strict regulatory requirements to large, complex systems with long lifecycles. When choosing between agile and waterfall methodologies, both offer advantages and disadvantages that can significantly impact project outcomes. Blending the two approaches—which one of our interviewees described as *“wagile, [meaning] agile principles in a waterfall approach”*—can help public sector projects benefit from the strengths of each while minimizing their respective drawbacks. As Osmond of Virginia put it, *“Agile project management is more of a mindset than a methodology,”* and government simply cannot afford to remain in the theoretical realm of pure agile rather than being more pragmatic with its application.

Agile offers significant benefits in the context of government technology projects, particularly in terms of flexibility and adaptability. Given the fast pace of technological advancement, the ability to pivot quickly and adjust to evolving requirements is crucial. Agile allows for iterative development, enabling government teams to continuously improve software, incorporate stakeholder feedback, and deliver functional increments over time. This is particularly useful for complex projects where it’s difficult to foresee every requirement at the outset. Additionally, agile promotes collaboration and transparency, with regular communication between developers, users, and government stakeholders. This helps align the project more closely with the end-users’ needs and expectations.



Despite its advantages, agile can also pose challenges in government settings, particularly due to the lack of rigid structure and documentation. Government projects need to adhere to strict procurement processes, regulatory frameworks, and audit requirements, which demand clear documentation, timelines, and deliverables—something agile can deprioritize in favor of flexibility. Furthermore, agile requires active engagement from stakeholders, which can be difficult in large government agencies where decision making is hierarchical, complex and slow. The iterative nature of agile can also lead to challenges in budget control, as the flexible scope may cause costs to increase unpredictably. As one of our interviewees noted, *“We cannot do agile as it was intended but are doing it as best as possible within government processes.”*

Waterfall, with its structured, linear approach, aligns well with the regulatory and compliance needs of government projects and has been long been the choice within government for these very reasons. Each phase—requirements gathering, design, implementation, testing, and maintenance—is completed sequentially, providing clear documentation and measurable progress along the way. This is valuable in government environments where audits, accountability, and long-term maintenance are crucial in an environment where staff turnover is high and political oversight changes every two to four years. Waterfall’s predictability makes it easier to manage timelines, budgets, and risk, as the detailed planning phase allows for clear expectations and deliverables within a high personnel churn environment where projects outlast most if not all of their contributors. This methodology works well in projects with clearly defined objectives and requirements that are unlikely to change over time.

One of the primary drawbacks of waterfall in government technology projects is its inflexibility. Since waterfall relies on the assumption that all requirements are known upfront, it can be ill-suited for projects where technological or policy changes emerge mid-way. Government projects, especially large-scale transformational or monolithic initiatives, often face changing political priorities, evolving citizen needs, or emerging cybersecurity threats. The inability to adjust the project scope after the design phase in waterfall can lead to delays, cost overruns, or solutions that fail to meet current needs. Additionally, stakeholder feedback is typically delayed until the testing or implementation phase, which can result in a project that doesn’t fully address user requirements.

Given the distinct advantages and disadvantages of both agile and waterfall, many government agencies are moving toward hybrid models that blend elements of both methodologies. This approach can deliver the rigidity and structure needed for regulatory compliance while allowing for flexibility and iteration in development. For example, a project might begin with a waterfall-like phase for initial planning, procurement, and establishing high-level requirements. Once these are in place, the development phase can switch to agile, enabling the team to work iteratively while incorporating user feedback and adjusting to new requirements until the system is considered fully ‘in-service.’

This hybrid approach allows agencies to mitigate the risks of scope changes while still benefiting from agile's adaptability. It also ensures that there is enough documentation and oversight for regulatory and compliance needs, making it easier to track progress and ensure accountability. By blending the two, government projects can achieve the best of both worlds: the predictability and governance of waterfall, combined with the innovation and responsiveness of agile. As one of interviewees described it, *"We are held back from pure agile by agency processes. It is not pure . . . and we cannot do agile as it was intended. But we are doing it as best as possible within government processes."*

Issue 5—The challenge of new versus established vendors

Public agencies today are increasingly challenged to find the right balance between working with established vendors and engaging with nontraditional digital solution providers. Established vendors offer familiarity, proven track records, and a deep understanding of government procurement processes, which can reduce risk and ensure compliance with regulations. Their solutions are often reliable and have been tested in similar contexts, providing agencies with a sense of security. Further, there is often a flow of staff between the agency and the established vendor leading to a rich and complex web of interrelationships and trust. However, working exclusively with these known vendors can limit innovation and the adoption of cutting-edge technologies, as these providers may be slower to innovate due to bureaucratic constraints or legacy systems.

On the other hand, nontraditional digital solution providers, such as start-ups and tech disruptors, offer innovative and agile solutions that can address complex problems in new ways and this is important for both modernizations and transformations. These firms tend to be more nimble, capable of deploying novel technologies quickly. Engaging with them can inject fresh ideas and capabilities into public services. However, there are risks involved, including lack of experience with large-scale government projects and unfamiliarity with regulatory requirements. This creates tension, as public agencies must balance the promise of innovation with the potential for increased operational risk. As one of our interviewees observed, smaller sup-



pliers are often incapable of supporting the large-scale efforts required for digital transformation, despite their potential for innovation. Further, as another interviewee said, *“Another issue we started was like, we hire a [smaller] contractor [and] they do some work. Maybe they don’t get it all done in that contract and now we’re bringing in another [smaller] contractor and we start again from scratch.”*

Ganesh Selvaraj reflected on another challenge with technology vendors:



If I think of a technology vendor, they want to sell more technology beyond what we need. Some are good, but the majority wanted to sell suites of applications that we may not use for a long, long period of time, but it all depends on our maturity. It’s very rare that they hop on this maturity journey to come with the organization to sell things at the appropriate time. The organization is not using the investment optimally. Nothing is used optimally. It just feels like we are over invested. So things get complicated.



Clearly the existing contracting model is substandard, and agencies need to find creative ways to balance the tensions that come with working with known vendors and engaging with non-traditional digital solution providers. This will require agencies to rethink how they assess vendor performance and stimulate more innovation within the broader ecosystems. The current contracting process makes it challenging, though not impossible, for new entrants to work with the public sector (especially on large-scale efforts). While the traditional players have the advantage of history on digital initiatives and scale (to handle large-scale efforts), the track record of successful delivery on digital efforts is mixed.

Additionally, public agencies need to look for ways to build ecosystems of collaboration rather than seeing these vendors as competing forces. Initiatives such as open data platforms, sandbox environments, and innovation labs can foster a space where traditional and nontraditional vendors can work together to co-develop solutions that meet the needs of government more holistically. By facilitating partnerships across the spectrum of vendors, public agencies can tap into the innovation of start-ups while benefiting from the stability of established vendors. This strategic synergy not only enhances the agility and effectiveness of public services but also ensures that agencies are better equipped to handle the fast-paced changes in the digital landscape.

Public agencies should be more active in shaping the digital innovation ecosystem. They can take greater responsibility for scaling solutions. The agency must identify key scaling issues upfront and have a plan to address them, including a clear exit strategy if scaling encounters unforeseen problems.

Evolution of a Federal AI Ecosystem

In a study comparing U.S. federal AI spending from 2017—2022⁹ and 2023—2024,¹⁰ several key trends emerged:

- Total of funds obligated grew from \$216 million > \$675 million
- Potential award value grew from \$355 million > \$4.56 billion
- NAICS 54 code (reflecting professional, scientific and technical services) potential award value grew from \$311 million > \$1.932 billion
- NAICS 51 code (reflecting information and cultural industries) potential award value grew from \$5 million > \$2.195 billion
- Number of federal agencies with AI contracts grew from 17 > 23
- Department of Defense contracts grew from \$269 million > \$4.323 billion
- Number of vendors with over \$10 million in contract value grew from 4 > 205

The 2017—2022 ecosystem of AI vendors was mostly comprised of small contractors, often headquartered close to a military installation. Given that the Department of Defense is, by far, the largest and most active agency in the federal AI marketplace, it makes sense for an AI vendor to be located close to their primary client.

The 2023—2024 ecosystem still has a large number of small vendors whose main source of revenue is often a single contract with a nearby federal client but the market is now seeing larger vendors moving in. Similarly, there is a large increase in number of contracts but particularly in the value of the individual contract. This makes sense as the market is maturing and is shifting from a study orientation to a live systems implementation.

Contractual challenges loom large in this and there are challenges rigid contractual terms with suppliers that limit flexibility and transformation. As one of our interviewees noted, *“With a fixed price contract, which is often the case, the systems integrator has to deliver by a certain date. Because of that, they are not going to be flexible [and] are not going to support your organization’s [goal] to transformation. With a more open contract, the SI will support greater [flexibility] and how much transformation you could potentially get.”*

Balancing between known vendors and new suppliers requires trust. As one of our interviewees said, *“Trust is foundational for digital transformation.”* Without trust, transformational efforts are unlikely to occur as parties will likely face significant organizational resistance in trying to work through governmental siloes. When asked what trust means in this context, the respondent noted it is a function of switching costs. The greater the switching costs, due to the established vendor’s integration within the digital ecosystem, the higher the perceived

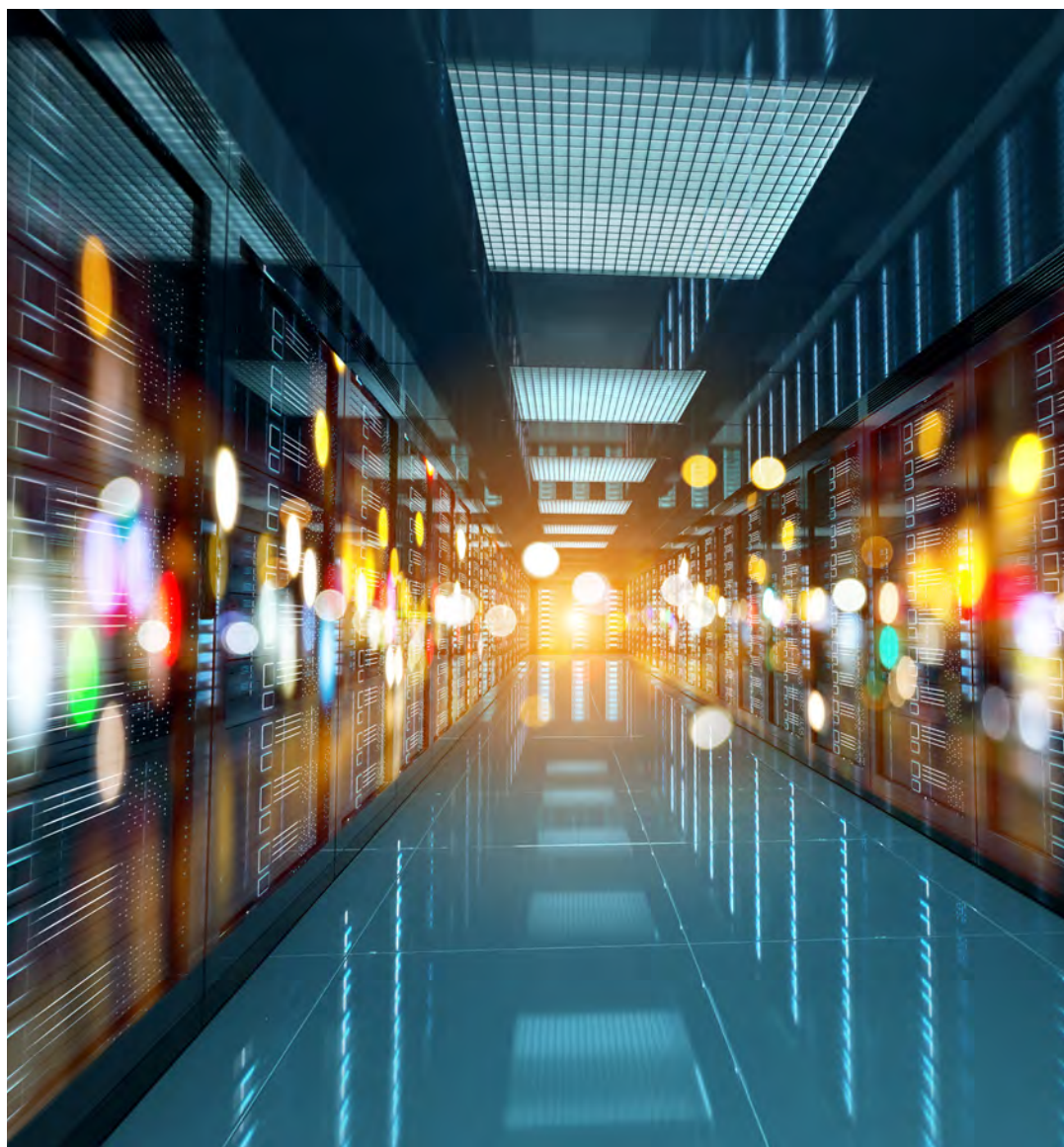
9. Dawson, G. S., Desouza, K. C., & Denford, J. S. (2022). Understanding artificial intelligence spending by the U.S. federal government. Brookings. <https://www.brookings.edu/articles/understanding-artificial-intelligence-spending-by-the-u-s-federal-government/>.

10. Larson, J., Denford, J. S., Dawson, G. S., & Desouza, K. C. (2024). The evolution of artificial intelligence (AI) spending by the U.S. government. Brookings. <https://www.brookings.edu/articles/the-evolution-of-artificial-intelligence-ai-spending-by-the-u-s-government/>.

trust. Established vendors also benefit from organizational slack, which enhances perceived reliability. Their solutions are comprehensive and refined over time, thus presenting lower risk. The established players are large-scale system integrators, which acts as a significant barrier to entry for smaller (and new) entrants into the digital innovation space.

Issue 6—The need for data management

It is hard to overstate the importance of data in creating digital modernization or transformation. Accurate and up-to-date data is essential to the successful operations of public sector organizations because it forms the foundation for effective decision making and policy implementation. Governments and public institutions rely on data to allocate resources, assess the needs of communities, and track the progress of public initiatives. When data is accurate and current, these organizations can make informed decisions that reflect real-world conditions, ensuring that public services are responsive and targeted. Without reliable data, public sector organizations risk making decisions based on outdated or incomplete information, leading to inefficiencies and potential misallocation of resources.



Centralized vs. Decentralized Data Governance

In their article entitled “Learning from IT Centralization: How to Decide Who Owns the Data,” the authors compared centralized versus decentralized data governance using data from the U.S. states.¹¹ Their major findings were that centralized data governance outperformed decentralized data governance in seven key ways:

- **Major finding 1—Better IT departmental performance:** Full centralization or mostly centralized governance consistently linked to higher IT departmental performance and the dominant factor for IT performance was the ability to control the IT purse strings for the organization.
- **Major finding 2—Higher levels of innovation:** Full centralization or mostly centralized governance was linked to higher innovation. While overall high centralization was linked, the dominant factor for innovation was the ability to successfully implement centralized project management.
- **Major finding 3—Equal split of organizations on centralization:** Despite strong evidence that centralization is superior for both IT departmental outcomes and amount of innovation, organizations were approximately equally divided between fully centralized, fully decentralized, and federated (mixed), with those in the latter two groups showing lower performance and innovation than the first. This suggested to us that organizations struggled to know where to rest on the centralization/decentralization debate.
- **Major finding 4—Greater ease of implementing advanced technologies:** Centralized governance facilitates the movement to advanced technologies including cognitive computing systems, analytics, and artificial intelligence since these technologies are heavily dependent upon data being available and in a common format to fuel the advanced technologies. While decentralized data governance can work, it adds a substantial level of difficulty to the implementation of advanced technologies since different formats, owners, and philosophies of data are likely to exist.
- **Major finding 5—Fewer cybersecurity issues:** Centralization is likely to reduce cybersecurity issues since the organization can apply a common data security framework to protect data versus a multitude of frameworks with varying levels of effectiveness.
- **Major finding 6—Facilitates modernization:** Modernization is frequently needed to allow an organization to evolve its systems to being able to handle more complex processing required for such things as analytics. While decentralization does not preclude modernization, centralizing can allow a more focused attention than the more diffuse attention that can occur with decentralization.
- **Major finding 7—Lower coordination hurdles:** The level of coordination necessary to enact change is likely to be easier if it is single project rather than multiple projects with differing standards, stakeholders, and operating philosophies.

With that said, government still struggles with data. As a senior executive of a public agency noted, “*There are little data bits all over the place. And, for the last two years, I haven’t seen any clear data strategy. . . . I think we have got a lot of work to do from a data perspective.*” Echoing that, Sloan of Arizona told us, “*Data is what we [government employees] are stewards of, but projects tend to fail on data. Without good data management and governance, even the most advanced technologies struggle to deliver the desired results.*”

11. Denford, J. S., Desouza, K. C., & Dawson, G. S. (2018, October 3). *Learning from IT Centralization: Who Should Own the Data?* Cutter. https://www.cutter.com/article/learning-it-centralization-who-should-own-data-500911?check_logged_in=1.

Finally, Andrea Fletcher of CMS said, *“Oh man, we have a mountain of data. I wish I could say that we are really good at using data all the time. There are a lot of challenges with data access to data in the government. It is very much locked down in many places for good reason. But it’s not like we just have, you know, some big, big data. Everybody wishes we had a big data lake where you could just like go query whatever you want and answer all your questions. That’s not the way it works, right? Data is often very siloed.”*¹²

Clearly data and the management of data negatively effective modernization and transformation and agencies need to get this right in order to effect the modernization or transformation that they desire.

Issue 7—Accessibility versus security

Cybersecurity plays a critical role in technology modernization and transformation within the public sector, ensuring that as organizations adopt new digital tools and platforms, they remain resilient against ever-evolving cyber threats. As Alexis Bonnell of the U.S. Air Force Research Lab recently said, *“We need to think about [security] in a catalytic way, meaning, that it is as dangerous for us to cut people off from critical data as it is to let that information get into the wrong hands . . . that is going to have to be the critical balance of our cybersecurity future.”*¹³

Public sector entities, with their large volume of sensitive information, including citizen data, financial records, and critical infrastructure details, are prime targets for cyberattacks. As governments embrace technology-driven solutions such as cloud computing, IoT, and artificial intelligence, their digital footprint expands, making cybersecurity a top priority. Modernization or transformation without robust cybersecurity measures could expose vulnerabilities, leading to breaches that can erode public trust, disrupt essential services, and result in significant financial losses. As Bonnell of the Air Force Research Lab said, *“Cybersecurity is absolutely critical, right? . . . We have to approach cyber to both protect our informational advantage but not disadvantage ourselves by making it too hard to find the right information.”*¹⁴

The increasing complexity of cyber threats requires public sector organizations to implement advanced cybersecurity solutions as part of their digital transformation efforts. Traditional perimeter-based security models are no longer sufficient to protect against sophisticated attacks like ransomware, phishing, and nation-state cyber espionage. Modern cybersecurity solutions, such as zero-trust architectures, encryption, multi-factor authentication, and AI-powered threat detection systems, are necessary to secure both the internal networks and the cloud-based services used by government agencies. Incorporating these technologies into modernization initiatives allows public sector organizations to proactively defend against cyber risks while ensuring the seamless operation of their digital platforms.

One of the key aspects of successful cybersecurity integration in public sector technology modernization is workforce readiness. With cyber threats growing in sophistication, governments need skilled cybersecurity professionals capable of managing advanced security tools and

12. IBM Center for The Business of Government. (2024, August 19). *Executing the Digital Strategy for the Centers for Medicare and Medicaid Services (CMS): A Conversation with Andrea Fletcher, Chief Digital Strategy Officer at CMS.* <https://www.businessofgovernment.org/interviews/5352>.

13. IBM Center for The Business of Government. (2024, October 28). *Exploring the IT Strategy at the U.S. Air Force Research Laboratory: A Conversation with Alexis Bonnell, CIO & Director Digital Capabilities Directorate, AFRL.* <https://www.businessofgovernment.org/node/5393>.

14. IBM Center for The Business of Government. (2024, October 28). *Exploring the IT Strategy at the U.S. Air Force Research Laboratory: A Conversation with Alexis Bonnell, CIO & Director Digital Capabilities Directorate, AFRL.* <https://www.businessofgovernment.org/node/5393>.

responding to potential breaches. Training and upskilling public sector employees in cybersecurity best practices are crucial, as human error remains one of the most significant factors in cyber incidents. As part of their modernization strategies, public sector organizations must invest in both technology and talent, creating a cybersecurity-aware workforce that can adapt to the evolving threat landscape.

Additionally, cybersecurity is essential for ensuring the resilience of critical infrastructure and public services during the digital transformation process. As public sector organizations digitize services such as healthcare, transportation, energy, and defense, they become more dependent on interconnected systems that, if compromised, could lead to widespread disruptions. Cybersecurity strategies must be designed to protect these essential services from attacks that could have national security implications or threaten public safety. By embedding cybersecurity into the core of their technology modernization initiatives, governments can safeguard critical infrastructure and maintain the continuity of operations in the face of cyber threats.

Lastly, effective cybersecurity in public sector technology transformations also supports public trust and compliance with regulatory standards. Citizens expect their governments to protect personal data and maintain the integrity of public services. Any security breach can severely damage public confidence and hinder the success of digital initiatives. Additionally, public sector organizations must comply with data protection regulations, such as the General Data Protection Regulation (GDPR) or the National Institute of Standards and Technology (NIST) frameworks, which mandate stringent cybersecurity practices. By incorporating cybersecurity into modernization efforts, governments can not only protect against breaches but also ensure that they meet regulatory requirements, fostering greater public trust in their digital transformation journey.

But issues remain. For example, as Fletcher of CMS recently said, *“About 80-90 percent of code that’s written nowadays . . . is all open source and . . . there are security vulnerabilities with that. And, people don’t always update to the most [recent] version.”*¹⁵ Managing this tension is critical for information security.

15. IBM Center for The Business of Government. (2024, August 19). *Executing the Digital Strategy for the Centers for Medicare and Medicaid Services (CMS): A Conversation with Andrea Fletcher, Chief Digital Strategy Officer at CMS*. <https://www.businessofgovernment.org/interviews/5352>.



Framework

Mindful of the issues facing government executives, we offer a framework for resolving those issues and enacting effective modernization and transformation.

Component 1—People at the center of all technology decisions

People are at the heart of government technology modernization and transformation because these initiatives are performed by people (government employees) to serve people (citizens) within a governance structure under people (politicians). Successful technology transformations are not just about adopting new tools or systems; they require aligning with the needs of the people developing, using, or are being impacted by these technologies. As Bonnell of the Air Force said, “I [came to realize] that driving innovation and change was more about people and identity, and how we stick together, than it was the particular technology.”¹⁶ Without strong communication and a focus on people, even the most advanced technologies can fail to deliver their intended benefits.

Metz of the Department of the Defense emphasized this, saying, “What was missing, I believe, is the fact that we needed to focus on the people doing the transforming—how they receive, think about, and use technology, and equating (that understanding) to business outcomes. Most people aren’t technologists. If we talk about buzzwords like zero trust and cloud, that doesn’t really resonate with a controller or logistician or human resources. But if you talk about how the technology leads to a business outcome that relates to them, now we’re having a conversation. Now we’re able to solicit what they need and ensure that the technology we’re delivering is meeting that need.”¹⁷

16. IBM Center for The Business of Government. (2024, October 28). *Exploring the IT Strategy at the U.S. Air Force Research Laboratory: A Conversation with Alexis Bonnell, CIO & Director Digital Capabilities Directorate, AFRL*. <https://www.businessofgovernment.org/node/5393>.

17. IBM Center for The Business of Government. (2024, March 11). *Delivering World-Class IT: A Conversation with Danielle Metz, Director, Information Management & Technology Director and CIO, Office of the Secretary of Defense*. <https://www.businessofgovernment.org/interviews/5195>.

A Rare Consensus: Cloud Migration

The campaign to move to the cloud from on-prem solutions is touted as a wildly successful change management effort.¹⁸ The campaign, jointly led by Reps. Darrell Issa (R-Cali.) and Gerald Connolly (D-Va.), was designed to spur government to accelerate the move to the cloud. Connolly said at the time, *“We agree on nothing. We don’t agree on the IRS issue. We don’t agree on Benghazi. We don’t agree on [Operation] Fast and Furious. We don’t agree about the Obama administration. We don’t agree on the role of federal regulation in our lives. We don’t agree on the direction of the economy. We don’t agree on whether it’s sunny out or dark and cloudy. With one exception . . . We came together on the issue of technology—the whole issue of how the federal government manages IT reform.”*

The approach taken was to communicate the expectations in a clear and straightforward, but not patronizing, manner. The mantra “don’t be a box hugger” and its associated humorous graphic was used to signify that cloud migration was a positive thing and holding on to physical infrastructure was an outdated concept. This was an effective way to avoid the use of buzzwords around cloud computing. In the end, the communication strategy conveyed the desired end-state while respecting the target audience by not “dumbing-down” the issue.



Not surprisingly, the effort was supported by major cloud vendors. But the group was broadly seen as a nonpartisan effort that drew support from both sides of the aisle.

Clear and effective communication is critical throughout the entire modernization process, from initial planning to implementation and beyond. It ensures that all stakeholders—public employees, decision makers, citizens, and vendors—are aligned on objectives, requirements, and timelines. Open communication helps bridge the gap between technical experts and non-technical personnel, ensuring that everyone understands the purpose and benefits of the new technology. As Bonnell of the Air Force said, *“We see this time and time again, where a leader will come in and say, we’re going to do this differently now, myself included. People start doing that and we assume success and it’s going to stick. But if you don’t change how people think and feel and help them understand why they’re doing things differently, it’s not going to stick.”*¹⁹

Focusing on people means prioritizing the needs, concerns, and abilities of those who will be using the technology. Technology is merely a tool to empower individuals to work more efficiently, make better decisions, and serve the public more effectively. As Bonnell said,

18. CIO. (2014, January 16). Is the Federal Government Ready to Embrace the Cloud? <https://www.cio.com/article/288422/government-use-of-it-is-the-federal-government-ready-to-embrace-the-cloud.html>.

19. IBM Center for The Business of Government. (2024, October 28). *Exploring the IT Strategy at the U.S. Air Force Research Laboratory: A Conversation with Alexis Bonnell, CIO & Director Digital Capabilities Directorate, AFRL*. <https://www.businessofgovernment.org/node/5393>.

“Technology is frankly nothing without people and their understanding of what we’re trying to do differently.”²⁰ Without considering how technology fits into existing workflows or how it might affect day-to-day tasks, modernization efforts can lead to frustration and inefficiency. Communication helps identify these needs early on, allowing agencies to design or select technology solutions that are user-centric and tailored to the actual demands of public service work. Engaging employees in the process through workshops, surveys, and feedback loops is essential for creating technology that people want to use and can easily adopt.

Moreover, technology alone cannot solve the complexities of government transformation. The adaptability and mindset of the workforce are far more important. Successful technology transformations require a workforce that is open to learning new skills and adjusting to new processes. Communication plays a key role in cultivating this adaptability, as it provides the necessary guidance, support, and training that employees need to feel comfortable with the changes. Leaders must communicate not only the technical aspects of the transformation but also the broader vision of how the changes will benefit both public servants and citizens.

As Metz of the Department of the Defense explained, the effort requires much more than lip service from those in charge, but also requires them to walk the walk:



It was really important to us to talk to the user. We conducted individual listening sessions with principal staff assistants. We were able to hear their concerns, frustrations, what was going right, what was going wrong. I was able to ask one question that we elicited a consistent theme. The question was, how do you use technology to execute your mission? The resounding response was, we don’t. This creates a culture of collaboration, where people are encouraged to embrace innovation rather than resist it.²¹



As Osmond of Virginia put it, *“When you frame [a technology decision] about what it is going to do for them, 95 percent come along. Those unwilling to be a part of new process or organization eventually find different opportunities. Look, people generally want to do interesting things and add value. People want to play for the winning team. The more winning you do, the more winning they want to do.”*

In the end, people are the ones who make technology work and people are the ones who can make sure it does not work if it is not communicated, trained and supported properly. In fact, there is a considerable body of academic research to point out the fact that when humans are faced with a system that they do not support but in a function for which they care deeply about the outcomes, they will actively work around the system rather than using it correctly in order to get their job done effectively. Technology itself is neutral and cannot achieve anything without the human effort, creativity, and problem-solving needed to implement and maintain it.

20. IBM Center for The Business of Government. (2024, October 28). *Exploring the IT Strategy at the U.S. Air Force Research Laboratory: A Conversation with Alexis Bonnell, CIO & Director Digital Capabilities Directorate, AFRL*. <https://www.businessofgovernment.org/node/5393>.

21. IBM Center for The Business of Government. (2024, March 11). *Delivering World-Class IT: A Conversation with Danielle Metz, Director, Information Management & Technology Director and CIO, Office of the Secretary of Defense*. <https://www.businessofgovernment.org/interviews/5195>.



The DoD's Metz described how she incorporated this change management into her project, saying:



The biggest challenge is change and change management. There are some organizations and individuals who were doing well with the status quo. They were able to identify value in what they were providing and doing for their respective organization. If there's going to be a change to that status quo, there's going to be tension and frustration and feeling that their value is going to be taken away. We had to come at it more people oriented, right? Because if you can't engage with the people, then you're not going to impact the mission. We try to build trust and prove our value—as an office, and as to why we were doing this. The point of our office was to democratize access to technology.²²



While technology is an enabler, it is people who determine how it will be applied, improved, and integrated into daily operations. Good communication ensures that this human element remains central to any modernization effort, making it clear that transformation is about more than just the tools—it's about empowering the people who use them to better serve society. Thus, placing people and communication at the core ensures that technology truly enhances government operations and delivers public value.

Component 2—Robotic Process Automation (RPA)

RPA is an elegant solution to several technology and human capital issues that are omnipresent in government. By shifting human work to RPA, the work can be arranged once and done multiple times.²³ Melinda Rogers, of the Department of Justice, described why her agency used RPA: *“We have been leveraging the benefits of RPA for some time now. We use it in automating business processes, especially when dealing with integrating processes and data between disparate legacy systems. Whether that's compiling cybersecurity, monitoring data from sources or optimizing complex workflows, robotic process automation has allowed justice to move forward with automation for critical business functions without having to invest in a whole system or platform efforts.”²⁴*

-
22. IBM Center for The Business of Government. (2024, March 11). *Delivering World-Class IT: A Conversation with Danielle Metz, Director, Information Management & Technology Director and CIO, Office of the Secretary of Defense*. <https://www.businessofgovernment.org/interviews/5195>.
23. O'Leary, K. (2021, February 17). *RPA in Federal Financial Management Organizations*. IBM Center for The Business of Government. <https://www.businessofgovernment.org/blog/rpa-federal-financial-management-organizations>.
24. IBM Center for The Business of Government. (2024, September 23). *On the Information Technology Strategy at the U.S. Department of Justice: A Conversation with Melinda Rogers, Chief Information Officer at DOJ*. <https://www.businessofgovernment.org/interviews/5422>.

Findings on RPA Usage

A 2021 study on RPA usage in federal CFO organizations examined 14 financial management organizations and found that most of the organizations had five or more bots in production at the time.²⁵ The study found that:

- Identifying a “simple, well-documented” business process as a proof of concept was the favored strategy.
- Strong organizational change management was necessary to alleviate staff fears about job losses
- Good working relationships with the CIO’s office was critical to success.
- The development of a thorough business case was necessary to persuade agency leaders and this was often done with using a standard intake form to capture specifics about the process under consideration.
- Many organizations under-estimated the amount of work necessary to build the bots.
- Security challenges were higher with unattended bots but still existed for attended bots.

RPA offers significant value for government agencies by streamlining routine tasks and improving overall operational efficiency. Many government processes, such as handling applications, processing data, and managing records, involve repetitive, rule-based actions that RPA can automate. By doing so, agencies can reduce the time spent on mundane tasks, freeing up staff to focus on more complex, high-value work. This shift not only improves service delivery but also allows governments to function more efficiently, meeting increasing demands with existing resources.²⁶

RPA can also enhance accuracy and compliance in government operations. Manual data entry and processing are prone to human error, which can lead to costly mistakes, delays, or compliance issues. By implementing RPA, agencies can improve the accuracy of their data handling, ensuring that critical information is processed correctly and consistently. This reduces the risk of errors and enhances compliance with regulations, which is particularly important for agencies handling sensitive or regulated data.

Finally, RPA contributes to improved public services and citizen satisfaction. Automating processes such as application submissions, payments, or inquiries can significantly reduce processing times and improve the responsiveness of government services. Faster turnaround times lead to a better experience for citizens, who benefit from quicker access to the services they need. Moreover, by optimizing workflows, government agencies can be more agile and adaptive to the evolving needs of the public.

As a result of all of these benefits, RPA is close to a “must have” for modernization or transformation initiatives. Similar to the TIME model for systems, agencies should follow what we are calling the RCCE model for assessing RPA candidates. The RCCE model looks at various processes and assess them for their **Repeatability** (frequency that the process is repeated in a

25. O’Leary, K. (2021, February 17). *RPA in Federal Financial Management Organizations*. IBM Center for The Business of Government. <https://www.businessofgovernment.org/blog/rpa-federal-financial-management-organizations>.

26. O’Leary, K. (2021, February 17). *RPA in Federal Financial Management Organizations*. IBM Center for The Business of Government. <https://www.businessofgovernment.org/blog/rpa-federal-financial-management-organizations>.

given time period), **Consistency** (amount that the process changes over time), **Criticality** (importance of getting the process correct) and **Ease** (ease of creating the RPA). Any process that scores high under all four dimensions is an excellent candidate for incorporating RPA.

Component 3: Generative AI

Generative AI has the potential to play a key role in government technology modernization and transformation, offering innovative solutions that improve efficiency, decision making, and service delivery. However, to leverage generative AI effectively, governments must ensure its use adheres to ethical AI principles and complies with regulatory frameworks. By focusing on transparency, accountability, bias mitigation, and data security, generative AI can help solve critical challenges while upholding ethical standards and government regulations. As Bonnell of the Air Force pointed out, *“My guess would be that we probably have about 6 percent of our knowledge structured. It’s a bit ironic that we take a lot of confidence from that structured information, but it only represents 6 percent of our knowledge. The surprise and excitement for me—as I look at this job now and in the coming years—is the ability to put all of our knowledge on the table, to be able to use generative AI.”*²⁷

One significant way generative AI can assist in government modernization is through mindful and responsible automating and streamlining administrative processes. As Bonnell of the Air Force said, *“People [in large part] are turning to generative AI tools, including GPT, to reduce toil—to take things that might have taken them four hours before and get them done in four minutes. To be clear, AI isn’t about giving us the answers. It’s helping us curate and have options at speed and scale.”*²⁸

Another area where generative AI can drive transformation is in citizen engagement and service delivery. AI-driven chatbots and virtual assistants powered by generative models can offer more personalized and responsive services, answering questions, helping citizens navigate complex systems, or assisting with applications. These systems can handle large volumes of requests and provide 24/7 support. However, to meet government regulations on data privacy and security, these AI solutions must be designed with robust data protection measures, ensuring that sensitive personal information is kept secure and that AI models are trained on compliant datasets free from biases or discriminatory patterns.

Generative AI can also support decision making and scenario planning by generating multiple models or simulations to predict outcomes of policy changes or new initiatives. Governments can use AI-generated insights to explore the potential impacts of various strategies, helping them make more informed choices. In this context, ethical AI principles must be applied to ensure that AI-driven recommendations are fair, unbiased, and based on reliable data. This involves rigorous auditing and validation of AI models to avoid perpetuating systemic biases, ensuring that policy decisions based on AI insights are equitable and just.

Ethical considerations are especially important when using generative AI to assist with data processing and integration. Governments often manage vast amounts of data, some of which are sensitive or regulated. Generative AI can help transform this data into actionable insights, but agencies must ensure that AI tools comply with data governance policies and avoid creat-

27. IBM Center for The Business of Government. (2024, October 28). *Exploring the IT Strategy at the U.S. Air Force Research Laboratory: A Conversation with Alexis Bonnell, CIO & Director Digital Capabilities Directorate, AFRL*. <https://www.businessofgovernment.org/node/5393>.

28. IBM Center for The Business of Government. (2024, October 28). *Exploring the IT Strategy at the U.S. Air Force Research Laboratory: A Conversation with Alexis Bonnell, CIO & Director Digital Capabilities Directorate, AFRL*. <https://www.businessofgovernment.org/node/5393>.

ing outputs that could lead to biased or unfair treatment. To align with ethical AI guidelines, these models should undergo regular assessments for bias and fairness, and there should be clear oversight mechanisms in place to ensure accountability for AI-generated decisions.

Finally, to fully harness the potential of generative AI while staying within ethical boundaries, government agencies must focus on transparency and accountability in AI deployment. This means clearly communicating how AI is being used, the logic behind its decisions, and providing opportunities for human oversight. AI models should be designed to produce explainable outcomes, ensuring that public sector workers can interpret and validate the AI's recommendations. Ethical AI frameworks can be adopted, such as maintaining human-in-the-loop processes for critical decisions and having fail-safe mechanisms in place to correct or override AI-generated outputs when necessary.

Recommendations for Implementing AI

In the IBM Business of Government's *Pathways to Trusted Progress*, the report outlines critical recommendations for implementing AI in government.²⁹ These included:

- **Recommendation 1—Promote AI-human collaboration when appropriate.** Different kinds of AI call for different levels of human involvement, and citizens are generally more comfortable with a human being involved in providing direct services.
- **Recommendation 2—Focus on justifiability.** Justifiability can be thought of as an outwards-facing business case, and with citizens as a primary audience. The government needs to articulate why an AI system needs to be developed, the amount of human involvement, and execution strategies.
- **Recommendation 3—Insist on explainability.** Government must be able to explain why the AI came to a proposed decision, including the data that was used for the decision. This becomes increasingly important with decision making for high-stakes outcomes.
- **Recommendation 4—Build in contestability.** Just as citizens can appeal to a person in government about the fairness of a decision, they also need to be able to contest the decisions made with AI. This feedback loop helps ensure that decisions are reasonable and not prone to bias.
- **Recommendation 5—Build in safety.** While AI is deployed, risks can arise that make a safety feedback loop important. Government needs to either create or join an incidents tracking database to capture and act upon feedback.
- **Recommendation 6—Ensure stability.** The machine learning function in AI means that supporting algorithms will be constantly tweaked in response to new information. Not only does the AI system need auditing prior to implementation; regular examinations will ensure that AI provides stable results.

29. Desouza, K. C., & Dawson, G. S. (2023). Pathways to trusted progress with artificial intelligence. IBM Center for The Business of Government. <https://businessofgovernment.org/sites/default/files/Pathways%20to%20Trusted%20Progress%20with%20AI.pdf>.

By incorporating these principles and focusing on transparency, fairness, and security, generative AI can significantly advance government technology modernization efforts without violating ethical standards or regulatory requirements. This approach fosters trust in AI systems and ensures they serve the public interest responsibly.

Component 4: Know what TIME it is

Osmond of Virginia uses the TIME (Tolerate, Improve, Migrate and Eliminate) model to understand each of his systems. The TIME model is a strategic framework applied in government agencies to evaluate and enhance system components, enabling agencies to allocate resources effectively, streamline operations, and ensure policy objectives are met efficiently. This model assists in the categorization and decision-making processes by breaking down the assessment of systems into four key actions. Government agencies can use this structured approach to make informed choices about which components to maintain, upgrade, replace, or discard, ultimately fostering better service delivery and responsiveness to public needs.

- **Tolerate** refers to system components that may not meet ideal performance standards but still function adequately enough to retain in the short term. This might include legacy systems or established protocols that, while outdated, do not critically hinder operations. These components are maintained to avoid unnecessary disruptions and excessive costs. By tolerating specific systems, agencies can allocate resources to more urgent areas while planning for gradual improvements or future replacements. Tolerating allows for a more flexible approach, prioritizing stability and continuity.
- **Improve** focuses on system components that have significant potential but require enhancement to reach optimal performance. For government agencies, this could mean updating technologies, enhancing workforce skills, or refining existing policies to better align with agency goals. The “Improve” phase supports modernizations that refine processes without requiring a full system overhaul. For example, updating data security protocols or training staff in new software can yield efficiency gains without the extensive time and budget required for full system replacements. Improvements not only increase operational efficiency but also help government agencies to gradually modernize.
- **Migrate** applies to system components that, while valuable, would function more effectively within a new framework or platform. Migration can involve transferring data to a more advanced database, swapping out legacy components of the technology stack, adopting cloud-based solutions, or transitioning to a new policy approach to address shifting public needs. In government, migration might mean moving from paper-based records to digital systems or adopting interagency platforms that allow for real-time information sharing. Migrating systems can be complex and resource-intensive, but it ultimately enables government agencies to improve scalability, accessibility, and responsiveness to the public. In short, these are excellent systems for transformation.
- **Eliminate** targets components that are no longer relevant or are inefficient, redundant, or outdated, leading to unnecessary costs and complexity. Government agencies often face constraints in budget and resources, and eliminating nonessential or redundant processes can streamline workflows and reduce costs. By systematically identifying components that no longer serve their purpose, agencies can simplify their systems, reduce technical debt, and reallocate resources to higher-priority areas. Systems and processes can also be eliminated as a part of a successfully realized modernization or transformation initiative and, in fact, this may be one of their strategic objectives. Eliminating outdated policies or programs also helps agencies focus on innovation and modernize their operations to serve the public more effectively.

Successfully using the TIME approach allows the agency to consciously decide their approach to each existing system, thus enabling a more informed spend.

An aspect of assessing TIME is the data view. As Sloan of Arizona put it, *“If data is water, then IT is the plumber. Can IT help provide access to the data, yes, but data quality is not an IT problem; it’s a business problem. We have done data maturity assessments for several agencies. Now they can focus on data being a key asset—with every employee understanding that they are the steward for their data. Employees need to understand the impact of their decisions and their role in data management—a latent investment that we are overdue in needing to make in some agencies.”*

As such, once the TIME analysis is done, a thoughtful dive needs to be taken into the data and what to do with it.

Component 5: Agile/flexible processes versus structure

In technology modernization and transformation projects, there is often tension between adopting an agile, flexible process and the necessity for structure and control. Agile methodologies offer the ability to quickly adapt to evolving requirements, enabling teams to deliver incremental changes and pivot in response to new insights. This flexibility is essential in fast-paced technological environments, where rapid changes in tools, frameworks, and customer needs often demand continuous iteration. However, the same characteristics that make agile appealing can also lead to challenges in maintaining focus on long-term goals.

Conversely, large-scale technology transformation projects often require a high degree of structure and governance to ensure all moving parts are aligned. Modernization efforts—like migrating legacy systems, overhauling infrastructure, or implementing enterprisewide platforms—often involve many stakeholders, complex dependencies, and significant investments. In such cases, structured processes ensure that timelines are met, resources are managed effectively, and risk is minimized. Well-defined processes, thorough documentation, and robust oversight help prevent scope creep, ensure compliance with regulatory standards, and provide accountability across teams and departments. As Metz, of the DoD, said, *“We do need to have rigor and structure, but they need to be adaptable and in line with the current reality that we live in and with technology, because it’s so dynamic. That means you constantly need to be refreshing your business processes so that they’re not becoming a hindrance to your ability to deliver technology.”*³⁰

The tension arises when the need for flexibility conflicts with the necessity for structure. In technology, adhering too strictly to structured plans can lead to inefficiencies. Teams may find themselves stuck in rigid processes that don’t account for the rapid pace of change in the tech landscape. Conversely, too much agility without proper guardrails can result in chaos—projects may drift, objectives can become unclear, and critical deadlines might be missed. Striking the right balance between these two approaches is critical, as both offer unique advantages in the context of transformation initiatives.

One potential resolution to this tension is the concept of hybrid frameworks—a blend of agile and structured methodologies. For example, scaled agile frameworks (SAFe) allow for agile processes at the team level while maintaining a structured approach to portfolio management,

30. IBM Center for The Business of Government. (2024, March 11). *Delivering World-Class IT: A Conversation with Danielle Metz, Director, Information Management & Technology Director and CIO, Office of the Secretary of Defense*. <https://www.businessofgovernment.org/interviews/5195>.

budget allocation, and risk mitigation at higher organizational levels. This allows organizations to be nimble in execution while ensuring that strategic objectives remain clear. The right blend depends on the project's scale, the industry, and the organizational culture, but hybrid models can provide the flexibility to adapt while keeping essential governance in place.

Ultimately, the choice between flexibility and structure in technology modernization hinges on contextual factors. For innovation-driven transformations, flexibility may take priority, whereas for high-stakes projects with critical infrastructure, structured processes are often nonnegotiable. For example, the COVID response required great flexibility while statutory changes to Medicare require a much more structured approach. The key to success lies in tailoring the approach to fit the specific needs of the project while recognizing that modern transformations are rarely a one-size-fits-all endeavor. A thoughtful combination of both agility and structure ensures that modernization efforts are responsive, sustainable, and scalable.

18F Agile Recommendations

To facilitate the evolution to agile, 18F has published an agile contract format document which slims down the solicitation document to around a dozen pages but still follows all of the applicable procurement rules and keeps it under the contracting officer's control.³¹ They recommend including several key elements:

- **A Statement of Objectives versus a Statement of Work**—They suggest that, since the agency does not know exactly what needs to be done, it is impossible to define it up front. The Statement of Objectives focuses on the collaborative effort between the developers and the product owners to define what needs to be done on a sprint-by-sprint basis.
- **A labor-hour contract versus a firm fixed price**—18F suggests that the agency is not buying a finished product but is instead buying the developer's time but with rigid guardrails to ensure that the output is consistently and rigorously measured to ensure it is meeting expectations. This allows for both more flexible spending but also easier contract escape clauses for poor performance.
- **A short base of performance**—The argument is that the agencies is hiring a developer to perform a defined set of objectives and then leave. A longer contracting period muddies the water.
- **A nominal appendix of the backlog of user stories**—This provides an insight into the type of stories that may be necessary in terms of complexity or length. Because the agency is buying a labor hour (rather than a finished product), it is not necessary to fully and completely inventory or specify each possible story.
- **Quality assurance and surveillance plan**—This specifies how "good" is going to be measured and secured.
- **Specification of the lead developer and the Project Manager**—In doing a labor hour contract, the people performing the work is critical and so the agency must know who they are getting in order to judge the quality of the firm.

31. Jaquith, W., Hart, R., Hopson, M., & McFadden, V. (2019, August 20). An Agile Software Development Solicitation Guide. 18F. <https://18f.gsa.gov/2019/08/20/an-agile-software-development-solicitation-guide/>.



Component 6—Creative and detailed contracting with vendors and providers

Governmental procurement rules are intentional. However, how an agency complies with these procurement rules allows room for agencies to be creative. The heart of that is working with vendors as peers rather than adversaries and jointly coming up with solutions. The ability to create innovative processes for working with vendors, while still fully complying with applicable rules and regulations, is a critical skill in performing a modernization or transformation.

Creative contracting solutions can significantly enhance collaboration between government agencies and vendors on technology modernization and transformation projects, enabling both parties to work more effectively while staying compliant with government contracting rules. Traditional procurement processes often prioritize rigid requirements, timelines, and cost structures, which can be a barrier to innovation and flexibility. Creative contracting approaches, such as modular contracting, performance-based contracts, and the use of innovation funds, offer more agile frameworks. These frameworks allow both vendors and agencies to adapt to evolving needs, integrate emerging technologies, and iteratively develop solutions, all while staying within regulatory bounds.

Metz of the Department of the Defense described how her agency used creative contracting by saying:



If we can come up with a strategy where there's enough commonality . . . then we can go after those [funding] resources together, instead of sniping at each other. Based on that, we can come up with agreed upon performance metrics, what we think the service level agreements is, and [do it] in partnership with the service provider. As the service provider implements our plan of action, the governance structure allows us to be able to have that community, to continue to foster that rapport, that openness, that safe space to exchange ideas and to have real conversations that are data driven, because we are using the same performance metrics.³²



32. IBM Center for The Business of Government. (2024, March 11). *Delivering World-Class IT: A Conversation with Danielle Metz, Director, Information Management & Technology Director and CIO, Office of the Secretary of Defense*. <https://www.businessofgovernment.org/interviews/5195>.

One such solution is modular contracting, which breaks down large, complex technology projects into smaller, manageable phases or modules. This approach allows government agencies to procure services in incremental steps, providing flexibility to adjust requirements as the project progresses. For vendors, this means they can deliver parts of the solution in stages, responding to feedback and refining the next phase based on lessons learned from the previous one. This structure reduces risk for both parties, as agencies can course-correct more easily without being locked into long-term contracts with static terms. Modular contracting also ensures compliance with procurement rules by adhering to project oversight and performance evaluations at each phase. Further, this allows the agency to follow a modular approach to contracting rather than having to approach it as a monolith.

Performance-based contracting is another solution that aligns the interests of both agencies and vendors by focusing on outcomes rather than prescriptive tasks. Instead of specifying exactly how a vendor should achieve results, agencies outline desired outcomes and allow vendors the flexibility to determine the best approach. This incentivizes innovation, as vendors can propose new technologies and methodologies that are better suited to achieving the desired outcomes. Performance-based contracts help agencies access cutting-edge solutions while still meeting government procurement regulations, which often focus on measurable results and accountability. Candidly, this can be a challenge as many stakeholders are often vested in how a project is accomplished and significant change management may be necessary.


Collaborative contracting mechanisms such as “Other Transaction Authorities” (OTAs) or “Challenge-Based Acquisitions” also foster better partnerships between government agencies and vendors. OTAs, for example, offer a more flexible procurement process for research and development, allowing agencies to work with nontraditional contractors, startups, and technology innovators who might not typically engage in government contracting. By using these innovative contracting authorities, agencies can bypass some of the bureaucratic hurdles that slow down traditional procurement while still adhering to the oversight and reporting requirements essential in government contracts. This approach encourages vendors to bring new ideas to the table, fostering a more dynamic and innovative problem-solving environment.

Finally, partnership-based contracting solutions such as joint ventures, consortia, and public-private partnerships enable agencies to pool resources and expertise with vendors while remaining compliant with contracting rules. These approaches allow for greater collaboration on complex modernization projects, where multiple stakeholders might be involved. By leveraging the diverse skills and knowledge of different vendors and public entities, agencies can create more comprehensive solutions to modernization challenges. Structured under the right legal frameworks, these partnerships balance the need for innovation with the rigor of government oversight, ensuring that all parties adhere to contractual obligations while working toward a common goal.


One thing that underlies the success of all of these alternative contracting approaches is how the role of the vendor staff is seen relative to the internal government staff. An adversarial relationship is unlikely to yield positive outcomes.

Osmond of Virginia describes how he deals with contractors, saying, *“I view them as an extension of my team and rely on them to bring in expertise and run the infrastructure. We have 300 core employees but around a thousand contractors . . . we follow the contractual processes and requirements, but once they are awarded the contract, then they are a part of the team.”*

Metz, of the DoD, described how she viewed contractors, saying:



That's a lot to ask of a service provider. It goes well beyond what they were stood up to do. You can see that we've set them up for failure. I think that's what we were trying to go after. There's a smarter way about doing this where we're able to offload the unnecessary things that we put on the service provider and smarten up the customer base so that we can hold ourselves to account. We can treat each other as peers instead of adversaries, because we're all going after the same precious resources.³³



Through these creative contracting solutions and maintenance of positive vendor relationships, government agencies can maintain the flexibility needed to adapt to evolving technological landscapes, improve vendor relations, and ensure successful modernization and transformation projects. At the same time, the regulatory integrity of government contracting processes is preserved, safeguarding accountability, transparency, and fair competition.

Solution 7—Curiosity

Curiosity is a critical driver for solving government technology modernization and transformation problems, as it fosters a mindset of exploration and continuous learning. In the rapidly changing landscape of technology, government agencies are often tasked with updating legacy systems, adopting new technologies, and meeting evolving citizen expectations. Curiosity encourages agencies and their leaders to ask “what if” and “why not” questions, prompting deeper investigation into existing problems and alternative solutions. This exploratory approach is essential in uncovering innovative ways to modernize systems and adopt cutting-edge technologies that can transform government services.

Moreover, curiosity leads to a better understanding of emerging technologies and their potential applications. When government officials and technologists maintain a curious mindset, they are more likely to stay informed about advancements in artificial intelligence, cloud computing, data analytics, and cybersecurity. This awareness enables them to anticipate how these technologies can be leveraged to improve operations, enhance efficiency, and address security concerns. For instance, by exploring the potential of automation or blockchain technology, curious leaders can identify novel solutions for improving transparency and service delivery. As Bonnell of the U.S. Air Force said, “*Curiosity is a key survival trait. It's our job to know what's out there . . . and to know or invent as what we need to do.*”³⁴

33. IBM Center for The Business of Government. (2024, March 11). *Delivering World-Class IT: A Conversation with Danielle Metz, Director, Information Management & Technology Director and CIO, Office of the Secretary of Defense*. <https://www.businessofgovernment.org/interviews/5195>.

34. IBM Center for The Business of Government. (2024, October 28). *Exploring the IT Strategy at the U.S. Air Force Research Laboratory: A Conversation with Alexis Bonnell, CIO & Director Digital Capabilities Directorate, AFRL*. <https://www.businessofgovernment.org/node/5393>.



Curiosity also encourages collaboration and knowledge sharing, which are essential in solving complex modernization challenges. Government technology projects often involve multiple stakeholders, including internal teams, external vendors, and partner organizations. A curious approach invites open communication, brainstorming, and the sharing of diverse perspectives, which can lead to more holistic and creative problem-solving. Through curiosity-driven inquiry, teams can break down silos and better understand how different systems and processes can work together, ultimately leading to more effective modernization efforts.

Finally, curiosity helps overcome resistance to change, a common barrier in government technology transformation. People naturally resist new systems and processes that disrupt their routines, but curious individuals are more inclined to embrace change as an opportunity to learn and improve. By fostering a culture of curiosity, government leaders can encourage their teams to approach modernization challenges with a positive, open mindset. This helps build a more adaptable workforce that is ready to experiment with new tools, processes, and methodologies, which is critical for navigating the complexities of technology transformation. As Bonnell of the U.S. Air Force puts it, *“Those who excel in government . . . are those people who use those curiosity muscles . . . to curate their knowledge sources and they are just going to move at light speed.”*³⁵

35. IBM Center for The Business of Government. (2024, October 28). *Exploring the IT Strategy at the U.S. Air Force Research Laboratory: A Conversation with Alexis Bonnell, CIO & Director Digital Capabilities Directorate, AFRL*. <https://www.businessofgovernment.org/node/5393>.



Implementing Change

Enacting the harmonization of traditional and emerging technologies for digital modernization and transformation involves performing five distinct steps while keeping in mind four overarching considerations.

Step 1—Ensure the right leadership is in place

- Ensuring the right leadership for a transformational implementation effort requires identifying leaders who possess both technical understanding and the ability to drive organizational change.
- Prioritize selecting individuals with experience in managing large-scale IT projects, preferably within the public sector, and aligning them with the agency's mission and goals.
- Clearly communicate the vision and benefits of the transformation to build commitment and establish accountability by defining roles and expectations early.
- Foster a supportive culture by providing leaders with the resources and authority needed to address challenges effectively.
- Regularly engage leadership through updates, collaborative problem-solving, and celebrating milestones to maintain enthusiasm and alignment throughout the implementation process.

Step 2—Determine the appropriate implementation approach

- To determine the appropriate implementation approach—waterfall or agile—for a transformational government technology project, evaluate the project's scope, complexity, and flexibility requirements.
- Waterfall is ideal for well-defined projects with stable requirements, such as compliance-driven initiatives, where a linear, sequential approach ensures thorough planning and documentation.
- Agile, on the other hand, suits projects with evolving requirements, high stakeholder engagement, or a need for iterative development, such as innovative or user-focused solutions.
- Assess the agency's culture, technical expertise, and capacity to adopt agile methodologies effectively. Consider hybrid models if aspects of the project require the structured oversight of waterfall alongside agile's adaptability to changing needs.

Step 3—Determine the vendor approach

- To determine whether to use new or established vendors for large transformational government projects, consider the project's complexity, risk tolerance, and need for innovation.
- Established vendors often bring proven expertise, reliability, and familiarity with government processes, making them a safer choice for projects requiring stability and predictable outcomes.
- Conversely, new vendors may offer innovative solutions, competitive pricing, and agility, which can be advantageous for projects emphasizing modernization or unconventional approaches.
- Evaluate vendor track records, capacity to scale, and alignment with the project's goals.
- Additionally, consider a balanced approach by leveraging a mix of established and new vendors, fostering innovation while minimizing risk.

Step 4—Implement a robust data management plan

- To implement a robust data management plan for a large government technology solution, focus on integrating data accuracy, currency, and security through a multi-layered approach.
- Establish a centralized data governance framework with clear policies for data collection, validation, and updating processes to ensure information accuracy and timeliness.
- Employ automated tools for real-time data synchronization and integrity checks to prevent errors and inconsistencies.
- Implement robust cybersecurity measures, including encryption, access control, and continuous monitoring, to safeguard sensitive information.
- Regularly audit and update the plan to address emerging threats, ensure compliance with regulations, and adapt to evolving data needs.
- Foster a culture of accountability and training among personnel to uphold these standards.

Step 5—Determine which technologies are (and are not) appropriate

- To determine appropriate technologies for a large government technology transformation, assess alignment with strategic goals, scalability, and long-term sustainability.
- Evaluate the technology's compliance with regulatory and security requirements, ensuring it meets government standards.
- Consider cost-effectiveness, interoperability with existing systems, and ease of integration to minimize disruptions.
- Analyze vendor reliability and support for the technology's lifecycle, along with its potential for future innovation.
- Finally, engage stakeholders to understand needs and concerns, ensuring that the chosen technologies address both operational efficiency and public service priorities.



The considerations are:

Consideration 1—Recognize and resolve the inherent tension between what you would like to do (desires) and what can be done (reality)

- To address the tension between goals for new system and their embedded constraints of budgets and staffing, begin by aligning the vision with clear, measurable priorities that reflect the organization’s most critical needs.
- Engage stakeholders early to ensure buy-in and realistic expectations, and explore phased implementation strategies that deliver incremental value while adapting to resource limitations.
- Advocate for scalable, cost-effective solutions such as open-source software or modular designs that can evolve over time.
- Finally, foster collaboration across departments to pool expertise and encourage training initiatives that empower personnel to maximize existing resources, bridging the gap between aspirations and achievable outcomes.

Consideration 2—Resolve the tension between modular and monolithic system

- To resolve the tension between modular and monolithic systems, focus on aligning the choice with the agency’s specific needs, resources, and long-term goals rather than striving for an ideal yet unattainable solution.
- Evaluate factors such as scalability, cost, interoperability, and implementation timelines.
- Modular systems can offer flexibility and adaptability, making them suitable for dynamic or rapidly evolving requirements, while monolithic systems provide cohesion and simplicity, often better suited for agencies with stable, uniform processes.

- Prioritize stakeholder input, assess potential constraints (e.g., budget, technical capacity), and consider hybrid approaches to balance immediate functionality with future growth, ensuring the decision supports the agency's mission effectively.

Consideration 3—Put people at the center of all technology decisions

- Placing people at the center of transformational technology decisions in the public sector involves prioritizing user-centric design and inclusive engagement throughout the development lifecycle.
- Begin by conducting comprehensive stakeholder consultations to understand the needs, expectations, and challenges of both end-users and system administrators.
- Employ human-centered design principles, focusing on accessibility, usability, and inclusivity to create systems that serve diverse populations equitably.
- Continuously solicit feedback through iterative prototyping and testing to refine solutions based on real-world usage.
- Prioritize transparency and effective communication to build trust and ensure alignment with public values.
- Invest in training and support to empower users, fostering a sense of ownership and confidence in the system.
- By focusing on people first, technology becomes an effective tool to enhance public service delivery effectively.

Consideration 4—Remain curious throughout the effort

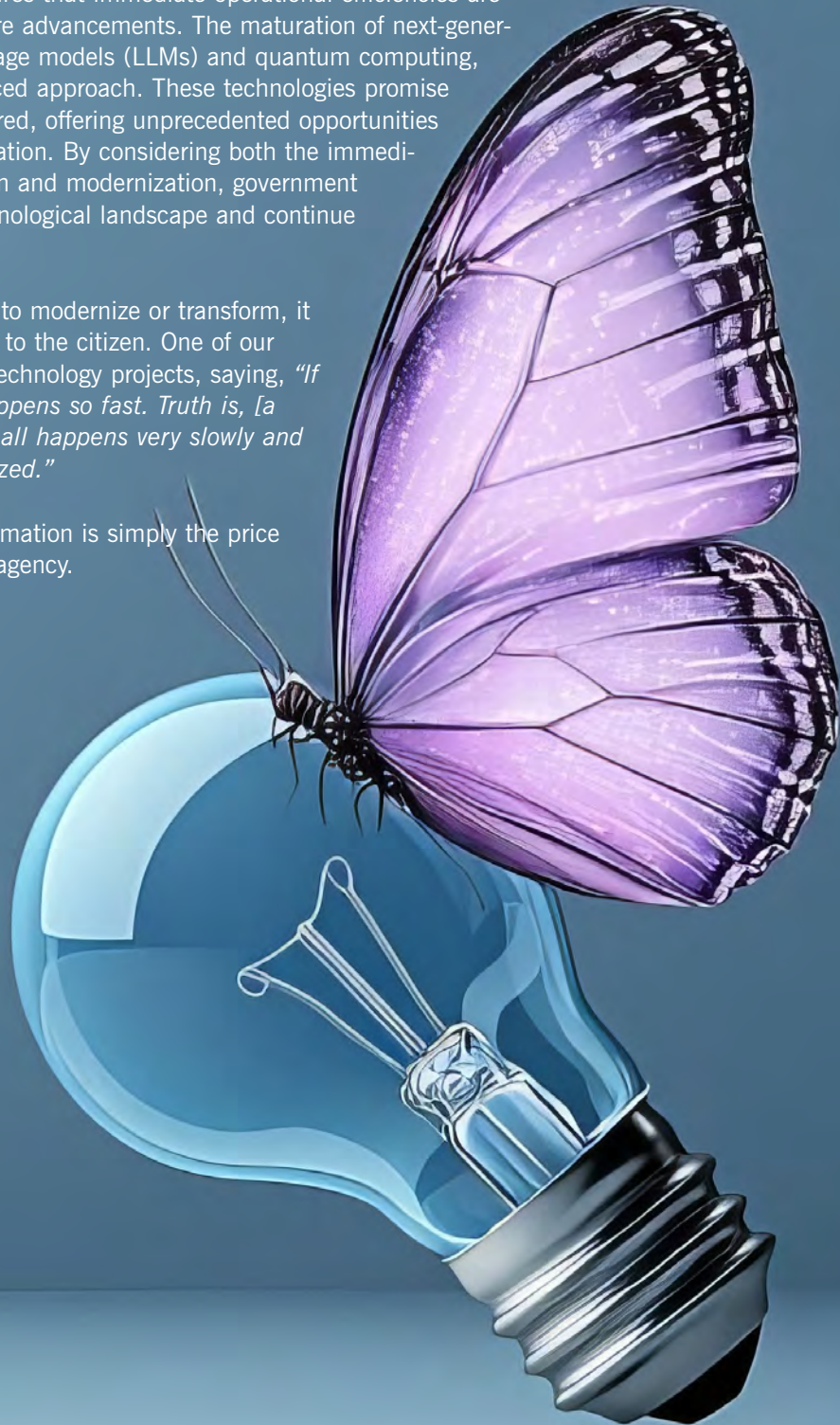
- To remain curious, focus on understanding the project's purpose and impact while connecting it to your personal and professional growth.
- Break the work into manageable milestones, proactively seek opportunities to learn about related technologies, and ask thoughtful questions to deepen your understanding.
- Collaborate with diverse teams to gain fresh perspectives, and regularly reflect on how your contributions drive meaningful outcomes for stakeholders.
- Staying organized, celebrating progress, and embracing challenges as learning opportunities will help you sustain curiosity and engagement throughout the process.

Closing Thoughts

As government technology leaders navigate the complexities of digital transformation and modernization, both short-term and long-term strategies need to be balanced in creating and maintaining public value. This dual focus ensures that immediate operational efficiencies are achieved while laying the groundwork for future advancements. The maturation of next-generation digital technologies, such as large language models (LLMs) and quantum computing, will only amplify the importance of this balanced approach. These technologies promise to revolutionize how public services are delivered, offering unprecedented opportunities for innovation, efficiency, and public value creation. By considering both the immediate and future impacts of digital transformation and modernization, government agencies can better navigate the evolving technological landscape and continue to meet the needs of their citizens effectively.

Whether government technology leaders want to modernize or transform, it has to be done to provide the required service to the citizen. One of our interviewees put it best in speaking of major technology projects, saying, *“If you see [a project completed] on TV, it all happens so fast. Truth is, [a modernization project] is way more boring. It all happens very slowly and you realize how much of it [on TV] is dramatized.”*

Achieving successful modernization or transformation is simply the price of being a technology leader of a government agency.



About the Authors

**Dr. Gregory S. Dawson**

Clinical Associate Professor
Center for Organization Research and Design
Arizona State University
300 E Lemon St.
Tempe, AZ 85287

Email: GregorySDawson@gmail.com

Dr. Gregory S. Dawson is Clinical Professor in the School of Accountancy in the W. P. Carey School of Business at Arizona State University. 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.

His research is primarily focused on emerging technologies 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. In addition to his role as a Professor, Dr. Dawson also actively consults with clients around the world on their use of technology.



James S. Denford

Professor of Management Information Systems
 Management Department
 17000 Stn Forces Kingston
 Ontario, ON K7K 7B4, Canada

Email: jim.denford@rmc.ca

James S. Denford is a Professor of Management Information Systems in the Department of Management at the Royal Military College of Canada. He holds a PhD from the Smith School of Business at Queen's University and two degrees from the Royal Military College of Canada. Following a 24-year career as an Army Signals Officer in the Canadian Armed Forces, he moved from practice to academe. His research interests are in the areas of information systems and knowledge management leadership, strategy, governance and innovation, particularly in the public sector, and he has a strong interest in non-dominant paradigm research methods. His research has appeared in leading research outlets such as Information Systems Research, the Journal of Management Information Systems, the Journal of Strategic Information Systems, and the Journal of Knowledge Management among others. He has also published practice-oriented work in top outlets such as Brookings Institution and the IBM Center for The Business of Government.



Kevin C. Desouza

Professor, Business, Technology and Strategy
 School of Management, QUT Business School
 Faculty of Business and Law
 Queensland University of Technology

Email: kevin.c.desouza@gmail.com

Web: <http://www.kevindesouza.net>

Kevin C. Desouza is a professor of Business, Technology and Strategy in the School of Management at the QUT Business School at the Queensland University of Technology. He is a nonresident senior fellow at the Brookings Institution. He formerly held tenured faculty posts at Arizona State University, Virginia Tech, and the University of Washington and has held visiting appointments at the London School of Economics and Political Science, Università Bocconi, Shanghai Jiao Tong University, the University of the Witwatersrand, and the University of Ljubljana.

Desouza has authored, coauthored, and/or edited nine books. He has published more than 150 articles in journals across a range of disciplines including information systems (*Journal of MIS*), information science (*Journal of the American Society for Information Science and Technology*), public administration (*Public Administration Review*), political science (*Studies in Conflict and Terrorism*), technology management (*Technology Forecasting Social Change*), and urban affairs (*Cities*). Several outlets have featured his work including *Time*, *Sloan*

Management Review, Financial Times, Stanford Social Innovation Research, Harvard Business Review, Forbes, Businessweek, Wired, Governing, Slate.com, Wall Street Journal, BBC, USA Today, NPR, PBS, and Computerworld.

Desouza has advised, briefed, and/or consulted for major international corporations, nongovernmental organizations, and public agencies on strategic management issues ranging from management of information systems to knowledge management, innovation programs, digital transformation, and leadership development. Desouza has received over \$2.25 USD million in research funding from both private and government organizations.



Marc E. Barda Picavet

Postdoctoral fellow in digital innovation and governance
School of Management, QUT Business School,
Queensland University of Technology

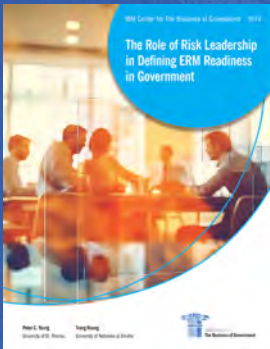
Email: marc.bardapicavet@qut.edu.au

Dr. Marc E. B. Picavet is a postdoctoral fellow in digital innovation and governance at the School of Management of the Queensland University of Technology (QUT), Australia. Picavet has a PhD in Public Administration and Government at the School of Business Administration of São Paulo (FGV EAESP) and recipient of a FAPESP scholarship. His background includes a master's in Political Economy from the Chinese University of Hong Kong and a BA in Economics from Insper in Brazil. At QUT, he participated in several projects on digital transformation and the use of artificial intelligence in government. One of these works resulted on the report about artificial intelligence government strategies in Indonesia published in IBM Center for The Business of Government. During his PhD, he participated in the Belmont Forum project “Understanding Innovative Initiatives for Governing Food, Water and Energy Nexus in Cities” and in the FAPESP-funded project “Innovation for Creating Sustainable Value: Understanding Global Value Chains in the Amazon.” He has also international experience having worked several years for a consultancy in Hong Kong, and another consultancy in Brazil specialized in innovation. His research interests are innovation and collaboration in the public sector, artificial intelligence, sustainability and cities.

Acknowledgments

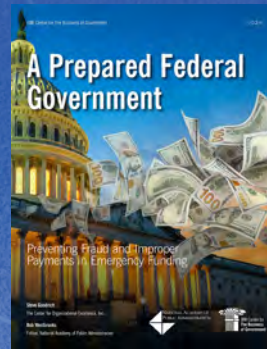
We would like to thank all interviewees and collaborators who took time to share their insights and experiences with us including Robert Osmond, Sylvia Burns, John Clarke, Anthony Kalkipsakis, Amardeep Sandhu, Peter Maroni, Ganesh Selvaraj, Dan Malarowski, Christoph Buck, Juniper Thren, Mary Tate, Rick Watson, Rob Perrons, and Anna Wiewiora. We are also indebted to Michael Keegan, host and producer of *The Business of Government Hour* who provided us with recordings of his interview podcasts with leading U.S. public sector executives. Finally, we thank all seminar participants who shared developmental feedback on this project including those at 25th Annual International Conference on Digital Government Research (dg.o 2024), Open Mic Series at the Queensland University of Technology's Centre for Future Enterprise, Bocconi University, and the City University of Hong Kong.

Recent Reports from the IBM Center for The Business of Government



The Role of Risk Leadership in Defining ERM Readiness in Government

by Peter C and YoungTrang Hoang



A Prepared Federal Government: Preventing Fraud and Improper Payments in Emergency Funding

by Steve Goodrich and Bob Westbrook



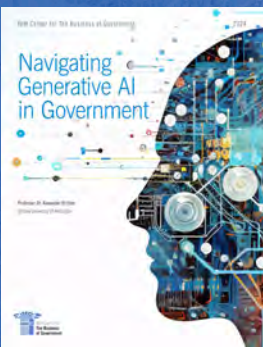
Resilience in action: Crisis leadership through innovation, collaboration, and human-centered solutions

by Challenge Grant Case Study Recipients



Preparing Governments for Future Shocks

by Lisa Schlosser



Navigating Generative AI in Government

by Alex Richter



Realising Trustworthy and Inclusive Artificial Intelligence for Indonesia

by Kevin C. Desouza and Marc E. Barda Picavet



Building future ready governments—Transformational lessons learned from a global shock

by Cristina Caballe Fuguet, Kee Won Song and David Zaharchuk



Building On Regulatory Foundations and Bridging to the Future

by Dan Chenok and Susan Dudley



For a full listing of our reports, visit businessofgovernment.org/reports

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 Consulting

With consultants and professional staff in more than 160 countries globally, IBM Consulting is the world's largest consulting services organization. IBM Consulting 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, D.C. 20005
(202) 551-9342

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

Stay connected with the
IBM Center on:

