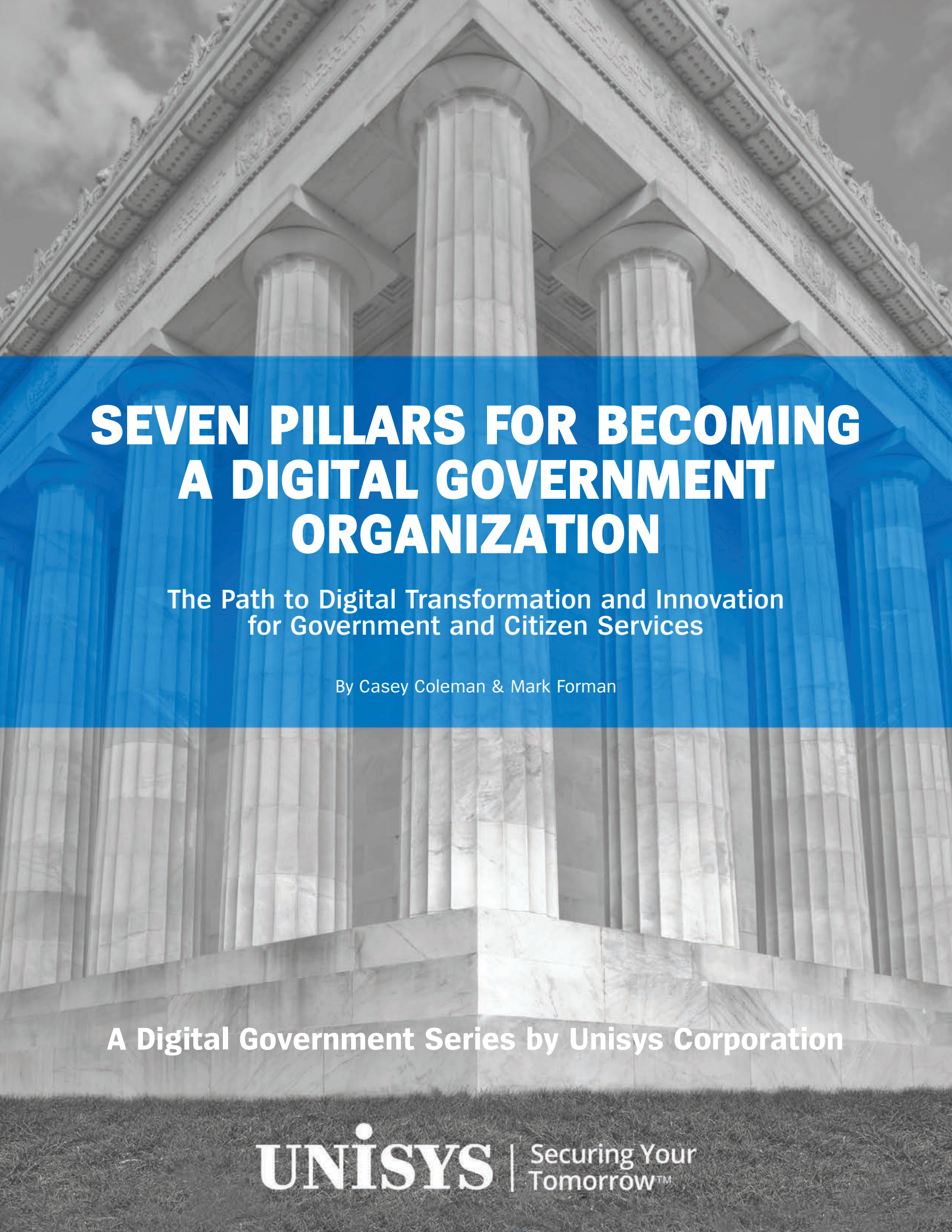


SEVEN PILLARS FOR BECOMING A DIGITAL GOVERNMENT ORGANIZATION

The Path to Digital Transformation and Innovation for Government and Citizen Services

By Casey Coleman & Mark Forman

A Digital Government Series by Unisys Corporation

UNISYS | Securing Your Tomorrow™

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Digital transformation is driving new business models and disrupting long-standing norms. Innovative startups such as Uber, Airbnb, and Waze are harnessing digital technologies—e.g., cloud, virtualization, advanced data analytics, and mobile—to transform traditional business models and displace competitors by delivering superior service at dramatically reduced costs.

Government organizations, often following the pace of innovation in the private sector, are adopting these same technologies with hopes of achieving similar gains in cost reductions and mission performance. The goal is to become digital organizations that operate at higher levels of efficiency, speed, innovation, and agility than possible today.

But for government organizations, the path to digital transformation is inherently different. Unlike a newly formed startup, government organizations are engaged in vital missions whose disruption—even for a short time—could seriously damage national interests and public trust. New technologies can also pose risks for agencies bound by strict requirements for privacy, security, and reliability. These factors alone inhibit experimentation and innovation in government business models.

Most government agencies are traditional "brick and mortar," with huge infrastructure investments in hard assets such as buildings and legacy information technology (IT) systems. In the e-Government era, many longstanding processes were "web-enabled" leading to some benefits, such as 24x7 access to services and information. But major gains require major change. Disrupting the norm while keeping the "lights on" is daunting, leading some to wonder whether digital government can deliver anything significant, except in small, unique pockets of the public sector.

Yet, it's not all doom and gloom—a path and vision toward digital transformation is emerging. The key to success is a hybrid approach, essentially a blend of old and new, where the show goes on while incremental transformation is happening and building toward a big finale. The hybrid approach marries existing stable systems with digital technologies and operating models. Under this approach, an organization aggressively incorporates new digital capabilities while continuing to leverage existing systems components and capabilities. Digital government is not an either/or proposition. Rather, it's a powerful and growing set of capabilities that enable government organizations to transition—smartly and efficiently—to new, transformative business models.

The transition to digital government is supported by seven essential building blocks built upon a strong foundation of IT governance:

- Hybrid IT environments that leverage public cloud, private cloud, and dedicated IT infrastructure assets to deliver IT services through unified management and security.
- Security that extends protection and management controls efficiently into the expanding digital environment.
- Advanced data analytics that exploit growing stores of data to improve citizen services, operational efficiencies, and mission performance.
- IT Service Management that provides a comprehensive, unified view of the hybrid IT environment for robust service orchestration and delivery, including End-User Support (EUS).
- Application services that leverage DevOps, reuse of common IT services, and modularity to rapidly develop and deliver innovative solutions.
- Mobility services that ensure rigorous management and security while providing users with seamless access to applications and data any time, anywhere, and on multiple devices.
- User-centered design of interfaces and business processes that provide services government workers need to perform their jobs more effectively and citizens need to get quicker and better service.

With these seven pillars in place, government leaders can confidently and boldly explore opportunities for expanding their digital capabilities within a hybrid environment. Government agencies can become digital organizations that successfully blend modern and legacy technologies to transform their ability to deliver mission-critical services.

DEFINING A DIGITAL ORGANIZATION

Digital technologies such as cloud, virtualization, advanced data analytics, and mobile offer numerous benefits in terms of cost savings and efficiencies; insights for improved decision making; enhanced customer service; and more. Many government agencies are already realizing these gains in small amounts or a few key areas. But simply adopting digital technologies does not necessarily create the transformative power of new business models and new ways of delivering services.

Recent Gartner research on large institutions, including government organizations, indicates that the emerging models will be enabled by a technical architecture that is a hybrid of legacy and digital models.

So what does it mean to be a digital organization?

Well-known startups provide instructive examples of how digital technologies can transform traditional service delivery models. For example, Waze connects hundreds of thousands of drivers, vehicles, and other sensors to crowd source information about traffic conditions, fastest routes, and other highway information. Airbnb has made it easier for people to find and book travel accommodations, giving them more choices and lower costs by creating an online community marketplace where people can offer and obtain accommodations. And Uber connects riders to drivers with applications that make the transaction simple for both riders and drivers without having to pay rates established by taxicab commissions disconnected from the market place. None of these three businesses required huge investments in office space or other physical capital. Each transformed traditional business models by exploiting mountains of data and the vast connections among people, businesses, and things.

A HYBRID MODEL FOR DIGITAL GOVERNMENT

Unlike digital startups, government agencies are not starting from a blank slate. While making the transition to digital organizations, they must continue delivering mission-critical services related to national security, economic well-being, and public health, safety, and welfare of citizens. Government agencies must also adhere to strict requirements for privacy and security that may inhibit the wide-open information sharing and experimentation that characterizes the modern digital organization. Agencies have already made huge investments in physical and IT infrastructures that support their missions. Shifting to a new business model would entail not just implementation of new technologies, but also new policies, processes, skills and training—all of which could disrupt ongoing mission activities. Many challenges stand in the way of a smooth transition to digital government.

How can governments shift their business models and make this complex transition, but do so without interrupting essential services or abandoning systems that continue to serve them well? Recent Gartner research on large institutions, including government organizations, indicates that the emerging models will be enabled by a technical architecture that is a hybrid of legacy and digital models. That is, organizations cannot completely abandon their legacy systems. It would be too costly and disruptive. And so they will continue running many of their legacy systems while they bring transformative digital solutions into their environment—thus managing the old and new together in what Gartner calls "bimodal IT."[1]

The hybrid or bimodal model should not be used as an excuse to slow innovation. For government agencies, this approach ensures the stability of mission-critical services and operations while they expand—as aggressively as possible—their digital capabilities within the enterprise.

CRAFTING A STRATEGIC PATH TO DIGITAL GOVERNMENT

Many government organizations have already begun implementing cloud, mobile, data analytics, and other digital technologies. Many federal or central governments have mandates such as the Cloud First policy, the Big Data Research and Development Initiative, and Digital Government Strategy for guiding agency efforts. But incorporating digital technologies into an integrated, secure environment requires preparation, planning and change management skills. For example, to establish the most cost-effective hybrid IT model, an organization must carefully assess its legacy infrastructure to determine what should remain or be modified as it expands its digital capabilities. Similarly, an organization cannot simply "lift and shift" its services into the cloud. An effective migration will require re-architecting of applications as well as rewriting the architecture to support Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Servcice (SaaS). Moving applications to the cloud also does not eliminate the need to do applications management and maintenance, and few gains can be realized unless consolidation of technologies occur as applications are modified to take advantage of common platforms and open application program interfaces. Mobile applications will also have to be integrated into the environment. Security remains a top concern in all activities. And most importantly, an organization will want to tightly align its new digital services and tools with its business and mission goals.

The question is, "how does an organization ensure it pays attention to all of the issues surrounding the adoption of digital technologies?" The answer is with strong IT governance that aligns the organization's business and mission strategy with its evolving IT architecture so the organization's information technologies—including its new digital capabilities—deliver continuous value to workers, citizens and other stakeholders.

1 Mary K. Pratt, "Bimodal IT: A Two-Pronged Approach to Delivering Innovation and Maintenance," *Computerworld*, September 21, 2015.

THE TECHNICAL PILLARS OF DIGITAL GOVERNMENT

What technical capabilities must agencies have to begin building digital government? In our experience working with public and private sector organizations throughout the world, we have found that successful organizations put in place seven essential building blocks for expanding their digital operations and capabilities. Each is described below.

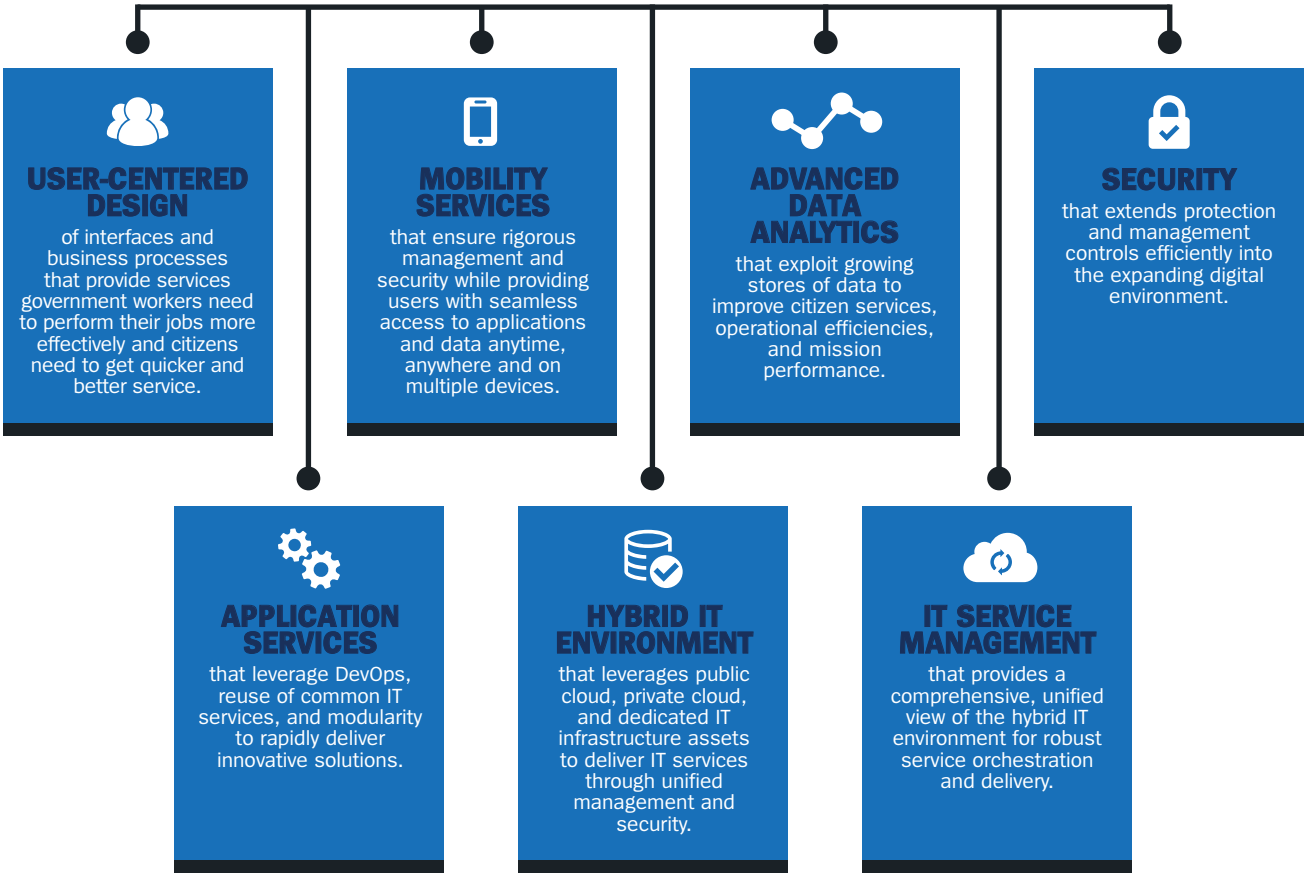
1. Hybrid IT environments that leverage public cloud, private cloud, and dedicated IT infrastructure assets to deliver IT services through unified management and security. The hybrid IT environment allows organizations to take advantage of new, cost-efficient services in the public cloud while making appropriate choices to leverage existing investments in on-premises or vendor managed private clouds. Such a hybrid model typically consists of internal and external infrastructure. Some infrastructure will be deployed as IaaS or PaaS cloud platforms, while other IT assets will continue to perform more traditional roles as either general purpose or specialized functions.

As agencies transition to hybrid IT, their mission-critical systems will no longer be siloed, proprietary technology that is restricted to a few core applications. Instead, those systems will be part of an agile and flexible fabric running on low-cost, industry-standard platforms that can support today's highly consumerized applications and tomorrow's Internet of Things (IoT).

2. Security that strengthens protection and extends management controls efficiently into the digital environment. Security in the digital environment will be increasingly fine-grained and identity-based, rather than device-based. Remote and mobile users—government employees, businesses and citizens—are now accessing applications and data anytime, anywhere and from multiple devices. Consequently, the traditional model of perimeter security that relied on high castle walls and deep moats, which was already growing obsolete, has become even more untenable in a digital environment.

To address modern security challenges, government organizations should move away from an over-reliance on firewalls and other perimeter-based defenses which often create a Rubik's cube of convoluted protections. Instead, they should redirect their security toward a much simpler and more cost-effective approach called micro-segmentation. Intruders who breach firewalls typically move laterally through the ecosystem with the goal of finding critical assets, and then exfiltrating and/or destroying the assets. Micro-segmentation contains them within a tiny compartment. They will not have access to an organization's critical assets outside of the tiny segment they

SEVEN PILLARS OF DIGITAL GOVERNMENT



have entered. The potential damage caused by malware is significantly limited and overall risk is minimized.

3. Advanced data analytics that exploit growing stores of data to improve citizen services, operational efficiencies, and mission performance. Agencies should strive to move analytics beyond mere analysis to predictive analytics that drive improvements in government processes, policies, and performance. The goal is to derive actionable insights with analytic tools that are easy to use and deliver rapid results to decision makers.

How might government agencies use predictive analytics to improve operational and mission capabilities? To exemplify, predictive analytics can guide the awarding of grants for education and other purposes by tying grant funding to anticipated and/or demonstrated results. Predictive analytics can provide rigorous, risk-based assessments that strengthen border protection and fraud prevention while also automating and speeding screening processes. It can also help regulators determine whether they are collecting the right data to protect the environment and enable relief agencies to quickly determine—even anticipate—where and what kind of aid is needed following a disaster. Developing algorithms that can generate predictive insights is the key component to transforming government operating models.

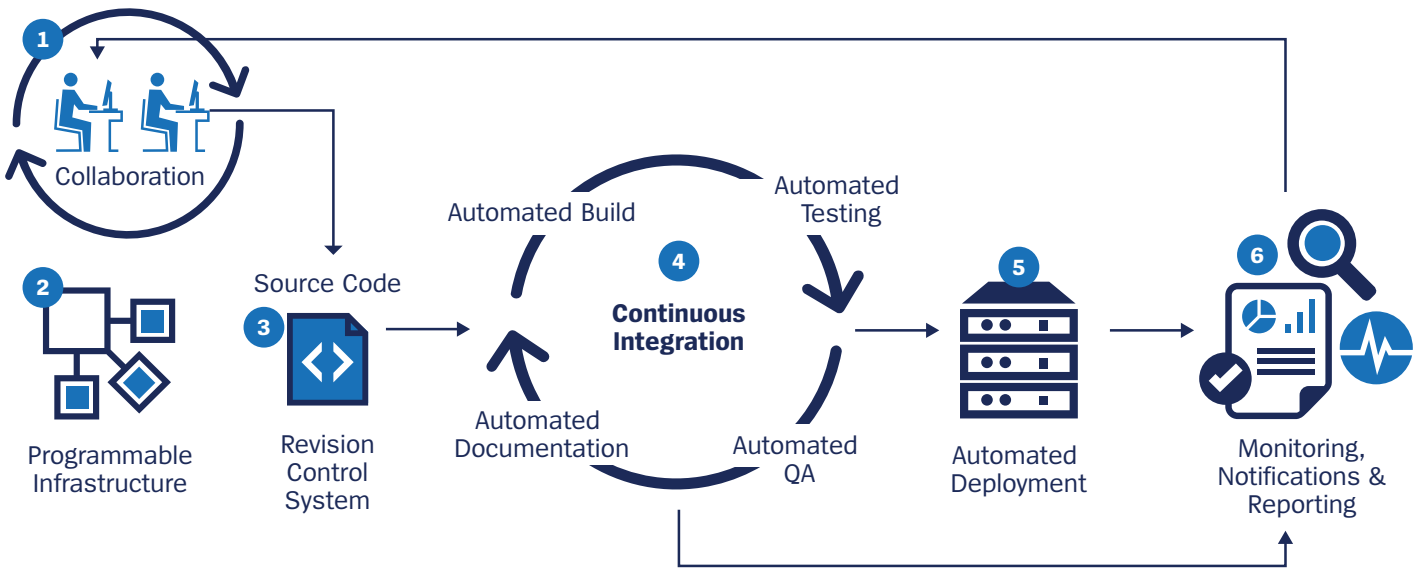
4. IT Service Management that provides a comprehensive, unified view of the hybrid IT environment for robust service orchestration and delivery, including End User Support. One of the key challenges when transitioning to a digital organization is effectively managing a complex environment. The environment will consist of both legacy and digital systems. It likely will include a mix of PaaS, IaaS, and SaaS deployed within a hybrid cloud managed by multiple cloud providers. The applications and systems will serve a diverse set of government, business and citizen users who will be accessing data and services from multiple types of devices. Consequently, agencies need IT Service Management (ITSM) that can provide a comprehensive view to ensure that all IT resources are working together in the most efficient manner.

Digital technology can also support a new self-service approach that significantly enhances EUS by enabling users to quickly resolve problems on their own. The self-service approach leverages social media, such as YouTube videos and communities of practice, so users can get the help they need without going through a help desk or other channels, which may result in unproductive wait times. Agencies can integrate social media with traditional EUS to provide users with more effective but less costly support.

Agencies can also use analytics to tailor their services to address users' specific needs. For example, analytics can reveal how and when users access applications and data; the storage and processing capacity they need; the types of problems they typically encounter; and similar issues. With this knowledge, organizations can customize EUS to their users' profiles or personas, thus enhancing all EUS channels to create more satisfied, productive employees.

5. Application services that leverage DevOps, reuse of common IT services, and modularity to rapidly deliver innovative solutions. Traditional methods of development and operations often slow innovation. While the development teams typically push to deploy new features and functionality as quickly as possible, IT operations professionals prefer to follow standardized processes that ensure stability, predictability, and quality performance. DevOps is a method for development that recognizes the interdependence of software development and

Automation is Critical for DevOps Success



IT operations—hence "DevOps." DevOps methodology brings together these two groups to collaboratively develop and deploy new software products and services.

Digital technologies make DevOps possible because developers and operators can work with and test small pieces of code in the cloud rather than having to wait until a solution is completed. Much of this integrated process is automated—e.g., building, testing, quality assurance, and documentation—to speed development while assuring the stability and quality that IT operations need.

Taking a modular approach to modernizing applications and systems is key to gaining the expected efficiencies and process improvements from DevOps. That is, agencies should recognize that their IT systems actually consist of many discreet modules or functions. Rather than simply "ripping and replacing" an entire system, they can keep legacy applications whose functions—such as large-scale, back-end data processing—are performing well. At the same time, agencies can replace outdated system functions with higher performing digital applications. This hybrid environment of legacy and digital applications yields the greatest value. The ease with which digital modules can be developed and deployed through DevOps will increase the speed of digital innovation—at lower costs and higher quality—for government agencies.

The hallmark of a digital organization *is its ability to leverage free flowing information through an interconnected world.*

6. Mobility services that ensure rigorous management and security while providing users with seamless access to applications and data any time, anywhere and on multiple devices. The development of HTML5 markup language enables organizations to shift more computer functions—such as data collection, analytics, and applications—from servers to the mobile device. These capabilities will empower mobile users to perform functions and make decisions from remote locations thus extending the power and reach of government to deliver mission services.

A key challenge for government organizations is determining which applications (or modules) to implement for mobile use as well as how to adapt them for mobile use. Embedding mobile devices with too many functions may overwhelm users. And processes that are easy to follow on a PC may be too convoluted for mobile users and devices. Organizations must tailor their mobile applications, including the processes that support them, to users' expectations and needs to create the most effective mobile experience.

An effective mobile program will also extend the digital pillars to the mobile environment. That is, agencies will want to protect their mobile data, services, and devices with fine-grained micro-segmentation security. They also will want to bring their mobile devices under their IT Service Management (ITSM) and EUS services umbrella. This will enable IT administrators to exercise the same level of management control over mobile users while also providing them with the access and services enjoyed by wired users. Agencies will also want mobile users to have access to their data and analytics tools. As government organizations more fully exploit IoT data and connections, they will need to integrate their mobile and IT environments to provide a secure, seamless experience for defense employees, civilian employees and citizens, regardless of the mobile device they use.

7. User-Centered Design. A user-centered design supports and unifies the other six pillars because a digital organization is a people-centric organization. Its leaders recognize that their employees perform the mission-critical services, and so they strive to empower workers with applications and data that enhance performance. Similarly, agency leaders recognize that government services must be delivered according to citizens' expectation and needs. User-centered design also takes into consideration the users' devices, both capabilities and limitations, to ensure the best interaction.

The failure to adequately consider users can prevent agencies from realizing the benefits of digital initiatives such as agile development. When developing a new application or service, agencies often mistake the process—e.g., filling out a form—for the end goal when the real goal is helping the user accomplish a task such as renewing a license or obtaining a permit. Consequently, they simply digitize a process rather than transform the process to help users obtain the desired service quickly and efficiently. Advanced analytics that provide objective measures of user activities can enable government organizations to fine-tune their applications and accompanying processes to create user-centric, digital government.

THE UNISYS SERIES ON DIGITAL GOVERNMENT

Becoming a digital government organization

The transition to digital government is not an all-or-nothing proposition. Agencies will continue to optimize and leverage their legacy environments while they identify opportunities to implement new hosting models; strengthen data collection, integration, and analytics; and expand their digital capabilities throughout the enterprise. The hallmark of a digital organization is its ability to leverage free flowing information through an interconnected world.

The next step for government agencies is to build on their experimentation and initial deployments to create a digital government roadmap. The lessons learned from earlier programs will help agency leaders establish priorities and identify the benefits they want to achieve. This planning will also help them create the governance mechanisms to manage their digital programs and keep them moving forward.

Digital government organizations will enjoy many benefits. Agencies will realize cost savings and operational efficiencies to help them meet expanding mission requirements even as budgets tighten. And the ability to collect and analyze the enormous amounts of data will generate insights for improving the mission capabilities of warfighters, civilian employees and government systems. Overall, digital government will empower employees to bring forward the most advanced and innovative solutions for spending taxpayer dollars wisely, serving citizens, and performing governments' many missions.

For more information on Digital Government:
http://www.unisys.com/digital-government

ABOUT UNISYS

Unisys is a global information technology company that specializes in providing industry-focused solutions integrated with leading-edge security to clients in the government, financial services and commercial markets. Unisys offerings include security solutions, advanced data analytics, cloud and infrastructure services, application services and application and server software. For more information, visit www.unisys.com.

ABOUT THE AUTHORS

Casey Coleman is the Group Vice President of Unisys Federal Systems Civilian Agencies. In this role Casey leads and manages the overall business for key civilian agencies including Justice, Treasury, IRS, GSA, FDIC, Interior, USDA and the Executive Office of the President. Widely recognized as an innovator during her tenure as GSA's CIO from 2007 to 2014, Casey led several modernization initiatives, including the agency's move to a cloud-based email and collaboration platform.

Mark Forman is Global Head, Vice President, and General Manager of Unisys' Public Sector business. Mark has a long record of accomplishments in government management reforms, spanning a variety of government and industry positions. He served under Presidential appoint as the first U.S. Administrator for E-Government and Information Technology and the federal Government's Chief Information Officer. He is a respected speaker on government use of cloud computing, IT risk management, enterprise architecture, data center consolidation, e-government and social media tools.

12/16 16-0509