Your Roadmap to IT Modernization
# Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Executive Summary</td>
</tr>
<tr>
<td>4</td>
<td>IT Modernization &amp; the New Administration</td>
</tr>
<tr>
<td>5</td>
<td>A Look at the IT Modernization Fund</td>
</tr>
<tr>
<td>6</td>
<td>Department of Energy’s 10 Steps to IT Modernization</td>
</tr>
<tr>
<td>8</td>
<td>The Role of DCOI in IT Modernization</td>
</tr>
<tr>
<td>11</td>
<td>Taking Advantage of the Application Economy at Your Agency</td>
</tr>
<tr>
<td>12</td>
<td>How Agencies are Modernizing</td>
</tr>
<tr>
<td>15</td>
<td>The Definition of IT Modernization</td>
</tr>
<tr>
<td>16</td>
<td>PLAY 1: Assessment &amp; Roadmap</td>
</tr>
<tr>
<td>18</td>
<td>PLAY 2: Modernization Readiness</td>
</tr>
<tr>
<td>20</td>
<td>PLAY 3: Modernization Execution</td>
</tr>
<tr>
<td>22</td>
<td>PLAY 4: Modernization Deployment</td>
</tr>
<tr>
<td>24</td>
<td>PLAY 5: Post-Modernization</td>
</tr>
<tr>
<td>26</td>
<td>Conclusion</td>
</tr>
<tr>
<td>27</td>
<td>About &amp; Acknowledgments</td>
</tr>
</tbody>
</table>
Information technology (IT) modernization is one of the hottest topics across government today. IT modernization has revolutionized efficiency, convenience and effectiveness for all users. That’s why agencies within federal, state and local government are eager to take advantage of all that modernization efforts can offer. Frankly, IT modernization for government is a must. Modernization is important to deliver the necessary levels of security, functionality and efficiency to help government employees in their roles. More important, modernization will help government deliver better services to the American public.

But due to poor management of technology investments, costly IT projects that often result in failure and the delivery of technologies that are obsolete by the time they are completed, government has largely missed the mark on this needed transformation. Of the $82 billion in federal IT spending planned for 2017, approximately 78 percent ($63 billion) is dedicated to maintaining legacy IT investments.

But even with all the focus on IT modernization, there still seems to be a lot of confusion, especially with a new administration coming in with new ideas and policies. What does modernization really look like? Is it the same for every agency? Is modernization even achievable with limited budgets and an uncertain future for federal government?

GovLoop’s latest playbook answers those questions and more. This guide provides agencies with:

- A five-play roadmap to help government employees, both IT professionals and non-IT professionals alike, get a better sense of where to start on modernization projects;
- An overview of the Information Technology Modernization Fund (ITMF);
- Featured government success stories highlighting their modernization projects; and
- The IT Modernization Lifecycle, based on the recent report by the American Council for Technology-Industry Advisory Council.

Ultimately, this guide provides agencies with a plan for defining IT modernization for their unique needs and infrastructures. It provides concrete steps to help you plan for the future, even amid resource constraints and administration changes.
With the election of Donald Trump, there are questions about how the new administration will handle technology policy. What will the new president do to continue IT innovation and modernization? What can policymakers, agency leaders, employees and IT staff as well as the general public expect moving forward?

While we may not know all the answers to these questions yet, one thing is certain: IT modernization is just as imperative for government and the new administration as it ever was before.

According to the Information Technology and Innovation Foundation, President Trump has argued that the U.S. has obsolete capabilities and has expressed that cyber should be in the “nation’s thought process.” The new president has also vowed to “enforce stronger protections” against foreign hackers.

Cybersecurity-related hiring was a top IT priority in the last year of President Barack Obama’s administration. It followed high-profile government security breaches, including some 20 million records stolen from the U.S. Office of Personnel Management.

In terms of the IT workforce, President Trump recently signed an executive order preventing the filling of vacant positions across federal government except when necessary to meet national or public security responsibilities. This may raise some questions as to how government could sustain IT modernization projects without the necessary staff to manage new equipment and technologies.

However, defense agencies and other big users of IT may actually be largely unaffected by the executive action. This is because hiring is still a major impetus at civilian agencies. Depending on how broadly the government defines IT jobs related to “public security,” there could still be quite a bit more hiring. Specifically, opportunities with federal IT contractors may open up.

When it comes to technology modernization, President Trump seems to be largely in support of public-private partnerships and innovation. This was demonstrated by his praise of tech leaders in a recent summit that brought together many heads from Silicon Valley.

In fact, advocates for innovation in government are optimistic that President Trump will continue the push to use technology in order to enhance government. According to Rob Atkinson, President of the Information Technology and Innovation Foundation, “Whereas Obama tried to use IT for innovation in government, Trump will probably try to use IT for efficiency and cost-cutting in government,” he said.

Overall, it is difficult to predict the exact future of IT modernization so early in the Trump administration. Legislation may change, budget priorities may be shifted and agencies may increase or cut IT staffs depending on the impact of hiring freezes. Regardless, technology modernization will continue as more innovations, like apps and cloud platforms and new devices, develop in the years to come. Though it’s unclear exactly what direction the new administration will take, signs currently point to modernization continuing under the Trump agenda.
A comprehensive review of federal cybersecurity last year found that government largely still relies on legacy systems, software, applications and infrastructure, which are harder to defend against sophisticated cyberthreats and are less cost-effective. Currently, civilian agencies spend 71 percent ($36 billion) of their IT budget maintaining legacy IT investments, which limits funding for the development of more secure and efficient technology solutions.

To address such issues, the Obama administration recently proposed legislation to establish a $3.1 billion Information Technology Modernization Fund (ITMF). As the name suggests, that fund would help the nation modernize its IT infrastructure and further improve its cybersecurity posture.

The fund is housed under the Cybersecurity National Action Plan (CNAP), which outlines short- and long-term strategies to enhance cybersecurity awareness and protections, protect privacy and maintain public safety. The ITMF specifically would help retire, replace and modernize the federal government’s IT legacy systems, which are costly and difficult to secure.

To address such challenges, the proposed ITMF would be administered by the General Services Administration (GSA) to fund a governmentwide transition to more secure and efficient modern IT systems and infrastructure. Additionally, the fund would establish a self-sustaining mechanism for federal agencies to regularly refresh their IT systems based on up-to-date technologies and best practices.

More specifically, the ITMF proposal addresses the challenges associated with legacy IT in a number of unique ways:

- **Governmentwide prioritization:**
  An independent board of experts will identify the highest-priority projects across government, ensuring that the federal government’s most pressing and highest-risk systems are targeted for replacement.

- **Self-sustainment:**
  Agencies would be required to repay the funds, ensuring the ITMF is not only self-sustaining, but also can continue to support modernization projects over the long term. As a result, $3.1 billion in seed funding for fiscal year 2017 will address at least $12 billion in modernization projects over the first 10 years and will continue to remain available in the future.

- **Expert management:**
  Experts in IT acquisition and development at GSA will provide modernization expertise to help agencies as they’re implementing their modernization projects. Every investment that receives funding will allow agencies to receive oversight and expertise to improve the chances of successful projects.

- **Transition to common platforms:**
  In order to reduce risks and save money, the ITMF would facilitate a transition to common platforms across government. By collecting modernization proposals from many agencies, the board can identify opportunities to replace multiple legacy systems with a small number of common platforms – something that is relatively difficult for agencies to do on their own.

- **Strong incentives:**
  By establishing a central fund that agencies must apply to and compete for, the legislative proposal would provide strong incentives for agencies to develop comprehensive, high-quality modernization plans. Additionally, the funding allows for more long-term thinking than costly one-off fixes.

Ultimately, the ITMF would be a $3 billion kickstart fund to help agencies by relieving extra costs for their modernization efforts. The legislation would be an important first step in changing the way federal government manages its IT portfolio, would help save money and strengthen security.

Regardless of whether the legislation passes, modernization is an inevitable part of the future and government agencies need to be ready to take the plunge.
Department of Energy’s 10 Steps to IT Modernization

While legislation like the ITMF comprehensively addresses government IT, some agencies are already tackling modernization according to their unique needs. Take a look at the Department of Energy (DOE), for example. As early as 2012, the DOE Chief Information Officer (CIO) and the National Nuclear Security Administration (NNSA) CIO were jointly tasked with developing a strategy to modernize DOE’s IT environment. They were to identify opportunities to share services, reduce costs and leverage new technologies.

What emerged was DOE’s very own IT modernization strategy with three overarching objectives, including:

**Transform.**
Use existing and new activities to enable new technologies to be inserted into the overall architecture in a lean and agile manner. The goal was to improve effectiveness and fiscal efficiency.

**Protect.**
Leverage the DOE’s Joint Cybersecurity Coordination Center to improve information-sharing, provide better operational awareness of security for corporate infrastructure, respond to incidents and proactively build cybersecurity into new technology investments. The goal was to ensure new technologies were appropriately secured throughout their lifecycle from design to retirement.

**Advance.**
Leverage the national laboratories’ world-class research and development capabilities through the cornerstone of the Cyber Sciences Laboratory (CSL). CSL is a virtual research and development (R&D) center that combines the capabilities of national laboratories, academia and industry to investigate the theory behind cyber.
Under these three objectives are 10 direct steps DOE developed to execute its modernization strategy:

**Transform**

1. **Consolidate and connect networks and services to create the DOE “Cloud of Clouds.”** Reduce the number of redundant infrastructures and services (i.e., data centers, email systems and collaboration tools) to create an optimum suite of services that leverages commercial providers. This helped the agency better meet mission support requirements.

2. **Align IT management and governance.** Address structure, process and people to improve management and decision-making effectiveness by aligning IT personnel and resources to optimize their use as well as decision-making to mission outcome.

3. **Establish architecture, policy and standards that embrace platform and device diversity.** Establish the DOE CIO as broker-advisor who coordinates the architecture, policy and standards necessary to enable mission outcomes.

4. **Streamline, simplify and reduce the cost of IT solutions and acquisition.** Reduce the number of product and service procurement vehicles. Leverage the collective buying power of DOE to simplify and reduce the cost and complexity of acquisitions.

5. **Develop a corporate data and information management strategy.** Create a data and information lifecycle plan that ensures the right information is available at the right time. This helped improve mission effectiveness by enabling data-driven decision-making.

**Protect**

6. **Strengthen cybersecurity risk management, including understanding and managing the IT supply chain.** Establish structures, processes and people to continuously improve DOE’s management of cybersecurity risk, including risk imposed by non-trusted supply chains.

7. **Establish full operational capability for information-sharing, shared analytics, reporting and collaborative incident response.** Leverage the collective, collaborative power of DOE contractor expertise to provide site and enterprise cyber situational awareness and cyber incident response.

8. **Improve cybersecurity training and awareness.** Address the weakest link in the cybersecurity value chain by delivering a rich training and awareness program that is tailored to the roles and responsibilities of each individual.

**Advance**

9. **Establish and advance the cyber sciences laboratory and establish a cyber innovation center.** The CSL was to establish and sustain an enduring, national cybersecurity R&D center of excellence at the National Laboratories to address cybersecurity threats to the nuclear deterrent, energy infrastructure and the nation’s reliance on cyber infrastructure at large.

10. **Enlarge and leverage the best of government, industry, academia and innovators.** Improve the effectiveness and efficiency of modernization efforts by establishing structures and processes that maintain collaborative relationships with the best of government, industry, academia and innovators.

As the agency that manages the nation’s electric grid systems, it seems requisite that DOE stay ahead of IT modernization. But laying out a modernization strategy certainly helped. Within a year, DOE made strong progress toward its outlined goals and has since continued working toward moving away from maintaining legacy systems to developing new solutions and platforms that are up to date.

Agencies like DOE certainly set high standards and precedents that other government agencies can look to for their own modernization strategies.
The Role of DCOI in IT Modernization

A large part of IT modernization for government is using, sharing, storing and managing data more efficiently. A significant challenge for agencies has been the exponential growth of datacenters, which has become increasingly complex and costly for government to manage. The growing number of datacenters has now become unsustainable for government. That’s why understanding the role of the Data Optimization Initiative (DCOI) in IT modernization can help agencies get a better sense of how to prioritize data and IT needs while also figuring out where to put all their data as part of their modernization efforts.

Before the DCOI, there was already a focus on reversing the unsustainable growth of datacenters. In February 2010, OPM established the Federal Data Center Consolidation Initiative (FDCCI) to consolidate datacenters. The Initiative sought to curb datacenter increase by reducing the cost of datacenter hardware, software and operations and shifting IT investments to more efficient government platforms, like cloud or shared services.

The results of this initiative were a mix of positive and negative. During its nascent stages, the tally of datacenters run by the federal government rose from around 1,100 in 2009 to over 3,100 in 2015. However, by October 2013, 640 centers had been closed. A further 470 closures were scheduled to happen by September 2014. The FDCCI also aimed to save $3 billion to $5 billion by 2015.

While the FDCCI was initially off to a great start, the datacenter count only continued to skyrocket. A look at some FDCCI statistics from Data.gov shows that even though 746 closures had been completed by 2014, there was a final tally of datacenters that exceeded 7,000.

Some argued that the FDCCI was a noble effort met with some successes but ultimately too inefficient to yield real results. That’s why the initiative eventually evolved into the Data Center Optimization Initiative (DCOI), which supersedes the original FDCCI. The DCOI requires agencies to:

1. **Develop** and report on their datacenter strategies;
2. **Transition** to more efficient infrastructure, such as cloud services and inter-agency shared services;
3. **Leverage** technology advancements to optimize infrastructure; and
4. **Provide** quality services for the public good.
To prioritize and measure agency progress for this initiative, OMB plans to focus on two key goals as the primary metrics: optimization and cost savings. Agencies would submit to the inventory on a quarterly basis.

Goal 1: Optimization

In order to push agencies to reduce manual recording and entering of data, the DCOI encourages agencies to instead install automated monitoring tools that can monitor and report information directly. OMB combined server utilization and automated monitoring as a single metric under optimization. This metric shows how well agencies’ servers are being utilized, discounted by the fraction of servers being monitored by automated tools.

Physical Datacenters

In addition to cost savings and optimization, agencies are expected to cut down their physical datacenters for the sake of reducing their environmental footprint. The DCOI provides that rooms with a least one server (whether in a production, test, stage, development, or any other environment) are considered datacenters.

Datacenters are also categorized into two groups: tiered datacenters and non-tiered datacenters. Tiered datacenters are defined as locations that use a separate physical space for IT infrastructure, and uninterruptible power supply, and an independent cooling system and a backup power generator in case of power outages. All other datacenters are considered non-tiered datacenters.

Agency Metering and Power Efficiency

The DCOI mandates that agencies install automated energy metering tools by 2018 so that agencies can report their energy usage in their datacenters. OMB will then monitor the energy efficiency of datacenters through a Power Usage Effectiveness (PUE) metric. Energy metering tools would then enable the active tracking of PUE for the datacenter.

Agency CIOs are required to ensure that existing tiered datacenters achieve and maintain a PUE of less than 1.5 by September 30, 2018. Effective immediately, all new datacenters must implement advanced energy metering and be designed and operated to maintain a PUE no greater than 1.4.

Automated Infrastructure Management

As part of OMB’s optimization goal, agencies are expected to eventually replace manual collections of reporting systems, software and hardware inventory housed within datacenters. These are to be replaced with automated monitoring, inventory and management tools (such as data center infrastructure management) by the end of fiscal year 2018.

These tools can measure progress toward the server utilization and virtualization metrics laid out in the DCOI. Additionally, agencies should include automated infrastructure management requirements for all new datacenter service contracts or procurement vehicles. Any new datacenter contractor procurement vehicle must require the contractor to report to the contracting agency.

The DCOI serves as a strong initiative and incentive for agencies to consolidate datacenters and IT infrastructures and use their datacenters more efficiently. Not only can this initiative help agencies save on costs, but more importantly, keep up with the latest in IT modernization.
The application economy is changing everything.

Learn more at ca.com
Technology has changed and will continue to change the way government reaches out and communicates with citizens. Gone are the days when faxing forms to a central government office was the norm. In today’s application economy - a connected, mobile application-based world enabled through software - citizens want quick and reliable services at their fingertips, on any device they choose.

In order to better understand how agencies can thrive in this software-driven environment, GovLoop sat down with Jeremy Rissi, Senior Director of Digital Transformation Solution Sales at CA Technologies, a company that provides software to modernize and secure applications.

“Citizens expect immediacy and they expect better efficiency from government services, whether that’s applying for a permit, paying taxes, or registering a business,” Rissi explained.

As a result, the public sector is leveraging application programming interfaces, or APIs, to build applications that allow them to deliver the services citizens expect in a quick, reliable, and secure manner. An API is an interface that lets one software program “talk” to another one, exchanging data behind the scenes. Using APIs agencies can link previously siloed legacy systems, eliminate boundaries between departments, improve internal processes, and most importantly provide a more efficient way of building new services.

“Users don’t care about IT systems, about software applications, or about where data resides. They care about the things they want to accomplish; the tasks they expect to get done. Agencies must use APIs to separate functions and capabilities from the applications and the data sources” said Rissi.

As agencies increasingly rely on APIs to deliver citizen-centric experiences, they will need a means to efficiently create and manage these APIs. API management tools allow agencies to realize the benefits of APIs while mitigating the inherent security risk that come with opening up the enterprise.

First, API management tools speed up application development which according to Rissi is a challenge for the public sector. “Slow application development is a huge obstacle. Many agencies are taking anywhere from one year to 18 months to create applications. In today’s application economy, agencies have to be more agile, and show iteration month after month”, said Rissi. API management tools simplify development and allows for seamless integration. When developers want to build a new service, they don’t have to start from scratch. API management tools allow services and components to be reused which in turn cuts the time it takes agencies to deploy new services to citizens.

API management tools also help make the capabilities of an agency more accessible to developers and constituents alike. When asked about how CA Technologies addresses this challenge, Rissi said, “At CA, accessibility is achieved by helping our clients make systems themselves less complex and by taking advantage of the application economy”. CA Technologies’ management tools provide catalogs of available APIs as well as instructions. This in turn makes systems easier to maintain, allows internal developers to access agency systems and innovate around their APIs, and makes agency services more available to citizens.

Most importantly, API management tools help agencies to eliminate data and security risks and Rissi assured that CA Technologies’ tools and services have security built into it. “When we talk about security, we are talking about authorization, authentication, and access,” he explained. Thinking through these security paradigms as agencies build out new systems allows them to integrate security into the IT maturity model and IT department as a whole. An API management tool can secure and control access from a single interface allowing agencies to protect its data without sacrificing user convenience.

In addition to providing the tools agencies need to modernize their IT infrastructure, CA Technologies and Three Wire Systems, an application development systems integrator and trusted CA partner, also provides expertise to agencies on their modernization journey. “Agencies need to think about what services they provide to their constituents, how they want to deliver those services, and the ecosystem of capability that makes this possible,” Rissi said. Three Wire Systems works with agencies to clearly define what they want to achieve and who the stakeholders in the delivery will be to make sure agencies set clear objectives for their IT modernization projects from the start.

Looking forward, government can benefit from the continued growth of the application economy by collaborating with private sector partners, like CA Technologies and Three Wire Systems, to integrate their IT infrastructure and efficiently develop and manage their applications. By leveraging solutions that help unlock the value of data, accelerate development, and reduce data and security risk, agencies will be able to better drive their mission and thrive in today’s application economy.
How Agencies are Modernizing

Modernization looks different for every agency. The following case studies feature agencies that have made significant efforts in modernizing their IT infrastructures. Each modernization project was aligned to the agency’s unique needs and goals.

NASA’s Enterprise Service Desk

NASA’s modernization project focused on helping its employees deliver better services and allowing outside users to easily navigate the website and interact with the agency.

As early as 2012, NASA decided to update its IT services to help create a one-stop shop for both internal employees and the public to easily access. NASA’s Information Technology Infrastructure Integration Program (I3P) has transformed NASA’s IT infrastructure to a standard, enterprise-based management and provisioning model shared across the agency. The scope of I3P is broad, entailing consolidation and central management of IT services in the areas of Tier-0/1 (faster level of storage) service desk and ordering, web services and technologies, enterprise business and management applications, integrated network/communications services and end-user services.

To get a better understanding of the need for this modernization effort, GovLoop sat down with Paul Rydeen, Engineering Services Contract (ESC) Program Officer at NASA. Rydeen acknowledged that while the need to modernize might seem obvious, it might not be as obvious to everyone in your organization. “However, it’s important to get buy-in ahead of time to encourage more user acceptance and deliver a better user experience,” Rydeen said.

What does modernization mean to NASA? In order to save on costs while updating platforms for the shared services center, NASA moved many of its services to the cloud. “For us, [modernization] meant moving to the cloud, finding the right software and virtualization,” Rydeen said.

At the NASA Shared Services Center (NSSC) provides services across the agency in five functional areas, including agency IT services and selected activities in financial management, human resources and procurement and business support services. The Tier-0 website acts as a gateway for NASA users. Employees or citizens with NASA accounts can access hundreds of knowledge articles, submit a ticket, check the status of a ticket, order a new service, check order status and view notifications.

“We have two help desks on either side of the hall. One is about IT, and one is for the non-IT work we do for HR procurement,” Rydeen said. “This desk overall helps generate and track a lot of calls from members of the public.”

Takeaway:

The NSSC helps employees and citizens alike easily access NASA’s vast array of services. Modernization projects that compartmentalize services into one resource center can help agencies deliver better services to citizens while also improving their employees’ experiences and overall productivity.

If your agency is looking to modernize by consolidating your IT resources in a shared services center, you may want to consider the following examples from NASA:

• Get user buy-in from the beginning.
• Consider moving services to the cloud to save on costs.
• Ensure enough staff is available to answer questions internally and to citizens accessing your agency from outside.
The Federal Communications Commission (FCC)'s modernization program centered around a seven track strategy to improve the agency's IT infrastructure while promoting the cultural change needed for success.

The FCC is often touted as the golden agency for its massive IT overhaul efforts. As the agency responsible for setting modernization standards in IT and Internet/Wi-Fi access, the FCC leads by example.

In an interview with GovLoop, Dustin Laun, Contractor and Technology Expert, explained what modernization at the FCC looks like and some of the challenges presented. “Modernization can mean a number of things like updating your technology stack but also updating your mindset about how that should work, how you should work and your methodologies,” Laun said. “It’s a total transformation from both the technology and mental aspects.”

To help the American public, the FCC regularly updates modernization efforts, which includes projects such as ULS (Universal Licensing System) that aim to help enhance the way licensees currently interact with the agency as well as create an exceptional end user experience.

When FCC started their modernization program, it laid out seven tracks and supporting goals:

1. **Improve secure employee and telework mobility.** Help personnel work from anywhere, anytime, on any device without compromising security.

2. **Secure internal and external collaborations.** Expand storage capabilities of email and use other cloud-based solutions to improve collaboration.

3. **Strengthen IT security posture.** Improve security of networks and privacy of user information by baking-in automated alerts, compartmentalized controls and system resiliency.

4. **Transform access to enterprise data.** Modernize systems by implementing web-based user interfaces as well as application programming interfaces (APIs) to make data more open to public and partner organizations. FCC wanted to establish a working group that extracts data from old legacy systems.

5. **Modernize legacy systems and tracking.** Update FCC’s 200-plus systems by encouraging the bureaus and offices as well as relevant partners to storyboard their desired “to be state”. Then, produce modular components for systems and desired workflows.

6. **Improve FCC.gov and complaint reform.** Identify most useful parts of FCC.gov by outreach to the public and partners as well as data-driven analytics.

7. **Increase transparency and system usability.** Pursue mobile and cloud-based applications to make more open data available to others.

The FCC journey to modernization certainly didn’t come without its challenges. “It’s always hard starting out on the track of modernization because people are really resistant to change,” Laun said.

To address such challenges, Laun emphasized the importance of documenting every small win and sharing every step of the modernization project. That made the project both more feasible and widely accepted.

**Takeaway:**

By simultaneously addressing both the technological and cultural aspects of IT modernization, the FCC can successfully roll out projects like ULS. IT transformation can be increasingly successful with detailed plans, like the seven tracks that the FCC used for its modernization program.

To address both technology and culture through your agency’s modernization project, here are some examples you can take from the FCC:

- Assemble a detailed plan with steps for each stage.
- Document small wins every step of the way.
- Share progress of your efforts with all stakeholders involved.
Illinois Consolidates IT

The state of Illinois’ modernization project centered on creating a new agency to consolidate all information technologies and tools into one place.

Illinois started its innovation journey in 2015. Last year, priorities included consolidation, customer-centric culture and cybersecurity. To achieve this, the state rolled out the Department of Innovation and Technology (DoIT), a new agency that brought the entirety of the state’s IT under one umbrella.

Under this effort, the state managed to consolidate 38 IT silos into the new agency. This effort brought together 1,700 employees and a billion-dollar spend into a coordinated department.

In an interview with GovLoop, the state’s CIO, Hardik Bhatt, shared Illinois’ new IT priorities and the state’s progress. “Our entire journey as an IT department can be mapped out in three steps: improving the business of IT, improving the business of the state using IT and finding areas where we can leapfrog,” he said.

In addition to consolidation, DoIT will provide high-value, customer-centric technology to agencies to foster collaboration and empower their employees to provide the best services to their citizenry.

While modernizing the nuts and bolts of Illinois’ technology has been beneficial, it’s equally important that cultural innovation take place. “We are focusing on building a borderless culture,” Bhatt said. “In order to do this, we brought together all the CIOs of different agencies and put them together in groups of five to seven and gave them enterprise strategy responsibility.”

These groups include topics like cybersecurity, backend development and analytics. The working groups bring together technology leaders from across the state, further breaking down silos and creating a borderless culture across the state.

As Illinois continues to champion innovation, Bhatt and his team want to mirror the governor’s priorities. “Our governor wants to make Illinois compassionate and globally competitive while providing the best citizen experience possible,” he said. Instilling these values into the state’s core IT mission allows Illinois to persistently champion IT advancement.

Takeaway:

Illinois’ modernization project is an example of how consolidation across IT departments and collaboration among IT leaders and professionals can improve the citizen experience.

If your agency’s modernization aspirations are consolidation, or even creating an entirely separate IT department, here are some tactics you can take from Illinois:

- Identify your agency’s mission, business goals and areas where you know your agency could excel.
- Foster collaboration by bringing CIOs and IT professionals from various departments to strategize and brainstorm ideas for modernization.
- Create working groups to focus on specific issues for your project, like cybersecurity or the analytics components.
The Definition of IT Modernization

As the previous case studies illustrate, modernization can mean a variety of things to different agencies. But with so many different takes on modernization, it can be hard to agree on what exactly modernization should comprise.

**IT modernization has been defined as the continuous evolution of an organization's existing application and infrastructure software, with the goal of aligning IT with the organization's ever-shifting business strategies.**

For government, alignment means increasing cost efficiency while reducing expenses. IT modernization also lets organizations maximize their existing application assets as they move toward a more open, complete and integrated application and infrastructure platform.

In simpler terms, an IT modernization project aims to create new business value from new and/or existing applications or systems. According to the American Council for Technology-Industry Advisory Council (ACT-IAC), a successful modernization program is one that combines business processes, people and technology to reduce risks, promote adoption and realize potential benefits.

Modernization means agencies become more efficient and effective in performing the functions that support their missions. Modernization projects require frameworks that are pre-built, pre-modeled and pre-tested to accelerate transformation, reduce costs and mitigate operational risks. All modernization frameworks should provide processes, tools, resources and assets that reduce much of the risks of modernization. Such risks include deployment failure or security risks moving data to new systems.

Using frameworks for modernization projects, agencies have more opportunities to be proactive in generating demand for updated enterprise architecture. Frameworks not only help agencies better plan but also better inform users and stakeholders. Anyone who is affected by the project in question can easily follow along with a framework. This, in turn, aligns with long-term organizational objectives and enables managed adoption of enterprise architecture standards. Some agencies may need to completely overhaul current applications and systems. Others may need new platforms or databases.

Agencies can use the following tactics to define their modernization strategies

**Rehost.**
IT managers can shift an application to another platform while leaving the old system and agency-specific customizations largely untouched.

**Rearchitect.**
Software engineers and managers can use tools to recover and reassemble the business-relevant code from legacy applications while eliminating technology-specific code.

**Replace.**
Managers can switch legacy applications with new ones if the legacy application does not incorporate unique agency data and functionality.

**Integrate.**
Architects can wrap legacy applications (support old systems that can’t be retired) and create a Service-Oriented Architecture (SOA) – a style of software design where services are provided to the other components by application components, through a communication protocol over a network. SOA can then be used to operate on a new platform but is implemented by the existing code.

**Migrate.**
For some legacy applications, IT professionals can automate the migration to new technologies without changing the application design.
This stage incorporates analysis of current and future business processes and capabilities to assess the extent to which the IT portfolio meets those needs. Based on this analysis, create a roadmap of application dispositions. You may decide to decommission, retire, remediate, re-platform, consolidate or enhance applications. Such actions can help optimize the portfolio to align with your agency's constraints, dependencies, priorities and budget profile.

To determine application dispositions, consider the best assessment topics for your agency. You may want your applications’ assessment topics to include security, functional health, technical health, strategic alignment and financial impact. Examining such topics provides your agency with the data-driven insight needed to make better decisions concerning applications.

The assessment provides detailed understanding of the current environment, including individual application characteristics, and establishes a baseline scope and roadmap to reduce risk. During the assessment phase, the first step is to understand your IT modernization project scope and complexity.

For example, suppose a system runs through one agency, i.e., the Department of Energy, and provides data to a second agency, i.e., Department of State, for reporting. The first agency wants to modernize its system, but the receiving agency cannot accept the data in a new format – what happens then? Does the second agency have to modernize too? That scenario illustrates why an assessment is so important as the first step in determining your best modernization approach.

Next, the roadmap process should include an analysis of alternatives to help you consider the full range of feasible options and determine the best strategy before you invest. The roadmap breaks down the preferred option in multiple “waves” to plan, design, build, test and implement smaller components of the application, rather than modernizing the entire system all at once.

Developing a modernization roadmap is critical, as it presents a comprehensive view of your agency's technology strategies in the right sequence. Ideally, your roadmap should include multiple dimensions, including the application modernization technical approach, governance and lifecycle management functions and methods for closing any technology gaps. It should highlight enterprise-level information requirements, cross-enterprise and business partners' integration needs, enterprise-level security and operational support measures.

Ultimately, your assessment and roadmap will provide you with both a timeline for the expected modernization to occur and estimated costs. This is especially important for helping you make sure that cost and time estimates are based on a genuine assessment of your existing architecture rather than just guessing.

By assessing your current infrastructure and drawing out a roadmap for your IT modernization project, you’re more likely to have a realistic estimate for the scope of work and a more successful project overall.
Steps to Implement

Conduct an assessment.
Analyze your agency’s current state of IT. Understand your IT inventory (i.e., apps and legacy systems) from the top leadership in your agency to the bottom.

Understand the project scope and complexity.
Consider to what extent you want to modernize your IT systems. You may want a hybrid approach where you still maintain some of your agency’s legacy systems rather than a massive overhaul to entirely new systems. Finalize what you want the future state of your IT architecture to look like.

Analyze alternatives.
Conduct a risk analysis of each of your project alternatives. Once you identify a project with the lowest risk and highest payoff, select your preferred alternative (outcome) for your modernization project.

Outline a roadmap.
Consider the lifecycle costs and time constraints for your preferred alternative and plan accordingly. Break the path to your preferred option into manageable chunks or waves.
At the beginning of this stage, agencies need to identify if they are working with a pre-existing framework or not. If your agency does not have a common architecture stack, you should define it here. Agencies that do have an existing architecture framework should be evaluated for capabilities required for the modernized system.

Once your agency has a framework in place, you can make your high-level roadmap (from stage 1) and extend it to include the detailed steps needed to track and deliver the project at a more micro level. These steps include developing a staffing and communication plan.

When developing a staff plan at this level, it’s also critical to establish a team with key management oversight in each discipline. The leadership roles needed for a successful modernization initiative include:

- strong project manager
- business lead
- system architect
- data architect
- security architect
- development and integration manager
- test manager
- configuration manager
- operations manager
- contracting officer

Of those positions, the project manager is the most important role. This person has to work with other stakeholders and the executive board on key decisions throughout the project. The best way to ensure modernization governance and cooperation is through a single, transparent reporting relationship between the project manager and oversight governance board.

Empowering agency leaders allows them to make decisions that bind their organization while simultaneously fostering stronger partnerships between the other stakeholders, i.e., employees and citizens. The modernization governance board should not try to take over for the project manager, but instead act as a forum where the project manager can elicit feedback on critical issues and trade-off decisions. The board should be informed, empowered and vested in the program’s success and should view the project manager as a trusted advisor and subject matter expert.

After a modernization team is established, you can start developing mechanisms to drive alignment and proper decision-making for all stakeholders involved in the modernization effort. Many IT programs fail because of poorly defined and inadequately managed requirements through the program lifecycle. So, getting key stakeholders to agree on desired outcomes and the approaches to meet those outcomes at the beginning of the initiative is crucial.

It is also important, however, to stay agile as you prepare to launch your modernization effort. This consensus-building isn’t a one-time exercise. Alignment is an ongoing process throughout the strategic planning, design and development and implementation of the modernization initiative. For complex IT systems, it’s important to align IT, finance, procurement, legal, security and privacy teams. Ensuring communication and cooperation between these groups is necessary to facilitate a successful modernization effort.
Steps to Implement

**Plan the project.**
Have a strategy for how the project manager, project leadership, key stakeholders and executive board are going to communicate. Define expectations early to avoid miscommunication on requirements later in the project.

**Communicate throughout the project.**
Know who your key stakeholders are and involve them. Constant communication is key to understanding alignment and decision-making at every step of the effort.

**Organize and staff the project.**
A strong project manager and governance team leading the modernization effort is the single most important ingredient to success. Create a strong modernization management team by thoughtfully filling each of the leadership roles to make the subsequent modernization steps smoother.
For example, the Federal Communications Commission moved hundreds of servers and apps, plus terabytes of storage, to a new platform by outsourcing data center operations and upgrading infrastructure. Key to the project’s success was a strong engagement with industry, agile implementation and a solid governance approach.

During the execution phase, agencies are primarily focused on designing, building and configuring the new IT environment and applications, all while keeping cybersecurity top of mind. You’ll want to ensure any configuration efforts align with government standards and policies that minimize risk and reduce your agency’s overall attack surface, or the paths and methods that hackers can use to exploit vulnerabilities.

“Integrating security is critical for the modernization program,” according to the ACT-IAC report. “It is imperative to begin early in the lifecycle and use an architectural review of applications security measures to identify and address potential security vulnerabilities. This involves leveraging proven security strategies and using security testing processes, such as code testing, code reviews, and vulnerability/penetration testing throughout the modernization program to proactively identify and remediate security vulnerabilities.”

The overall strategy for modernization execution will vary based on the agency and can include different approaches for installing hardware and software. But despite these differences, there are common themes that span across all implementations:

- **Comply** with the organization’s System Development Life Cycle (SDLC) process, which defines the various steps for developing information systems. It’s important to comply with this process to ensure that modernization efforts are subject to and enforced by the established rigor for any application development or maintenance activity.
- **Modify** and standardize across all modernization programs, especially if the current SDLC does not map to the modernization process.
- **Enforce** compliance with the organization’s architecture guidelines so that it is easier to maintain modernized applications. All agencies should have an enterprise architecture, which is a blueprint that guides how their information technology and information management elements work together to accomplish their mission.
- **Incorporate** early performance tests, especially when moving hardware to a new platform or hosting environment, to verify that the modernized application will deliver required performance once it’s placed into production.

Testing for a modernization program is a complex task. Many systems lack documented requirements and test cases for applications. These test cases should define the steps and preconditions needed to determine if that system functions correctly.

The testing strategy should also identify the test case sources and the environment in which the system will be validated. Keep in mind that the testing strategy also depends on the modernization strategy, which can vary by project and agency. At the Housing and Urban Development Department (HUD), for example, the agency used a phased approach with shared services for its modernization strategy.

When it comes time to execute your modernization project, communication and stakeholder inclusion are key. Integrate security early on from the get-go, incorporate numerous tests and be sure that as you’re modernizing, you’re also standardizing across all programs.
Steps to Implement

**Define your strategy for modernization execution.**
Each strategy has unique business cases, business drivers and strengths and weaknesses, so evaluate carefully.

**Align the strategy with your agency’s SDLC process.**
Doing so will help to ensure your system meets agency standards for development and maintenance.

**Make cybersecurity a priority.**
Review the architecture of applications early on in the process to identify and address potential security vulnerabilities.

**Execute a solid testing strategy.**
Use test cases for your systems that define the steps and preconditions needed to determine if that system functions correctly before it’s placed in an operational environment.
Modernization Deployment

Deployment during the modernization lifecycle can be a period of complex, interdependent, concurrent activities that need to be carefully orchestrated. This is a time where things may or may not go smoothly, so it’s good to be prepared for a variety of outcomes.

Such outcomes can range from smooth transitions with satisfied users to deployments fraught with mistakes and dissatisfied users (even disruption to business). The difference between these results ultimately depends on the quality and execution of your deployment plans. Deployment can affect personnel, government and business processes, IT infrastructure and operations, data and even support functions like finance and contracting.

Deployment can also “involve coordination with and reliance on external third parties introducing new relationships, additional complexity and potential risks,” according to the ACT-IAC report. “If anything is going to go wrong, the middle of a transition is when it is most likely to happen. There are several deployment strategies that can be applied to improve user adoption. Techniques that have been successful in both commercial and government sectors include A/B deployments to expose increments of capabilities to smaller sets of users and ‘dark launches’ that deliver specific increments of functionality to the users.”

Dark launching is the practice of deploying the initial version of a service into a production environment well before project or product release. This way, you can test your project and find any bugs before you make functionality available to your users.

For example, HUD overcame previous modernization failures and decommissioned outdated systems by focusing on phased replacement. It deployed its new program in increments and did a few dark launches before making the product available to its users. It’s especially important to deploy in stages so that any errors can be immediately addressed.

You’ve assessed your current IT infrastructure, drawn out a roadmap, prepared your modernization project and begun execution. Now it’s time to launch your new tools and strategies.

“The important thing is to make sure you’re understanding what you’re doing, why you’re doing it and educating yourself and your users,” Dustin Laun, Technology Expert from the FCC, said.

During the deployment stage, it is also essential to carefully plan all of the steps required and communicate throughout the process with users. Involve employees and end users alike throughout the process. User acceptance is particularly critical. They need to be informed about what to expect, what will change and how it will affect the performance of their jobs. To better ensure success of the modernization project, users also need to receive timely training, support and assistance that is well-packaged and easily accessible and understood.

It’s important that agencies plan in advance to provide sufficient support staff both during and immediately after deployment. Such staff needs to be readily available to answer questions for users and ensure a smooth transition as well as positive outcome. This is enabled best by strong governance, agile development methodologies and seamless communication from start to finish.

“Take baby steps if you can and minimize customization,” Rydeen, ESC Program Officer from NASA, said.

“The important thing is to make sure you’re understanding what you’re doing, why you’re doing it and educating yourself and your users,” Dustin Laun, Technology Expert from the FCC, said.
Steps to Implement

Determine who will be involved.
Because of the complexity of the deployment process, it’s important to determine in advance who on your team will be responsible for each component. Decide whether there will be third parties (i.e., vendors or contractors) involved and introduce any new relationships to the deployment process accordingly.

Plan all of the steps required.
Make sure you carefully review your plan during the first three stages of the modernization lifecycle before you deploy. It’s better to take more time to address any issues now than having to fix errors in production later.

Do a dark launch.
Test your modernization project in a production environment before making it fully available to your users. Use A/B deployment to incrementally test new applications, websites or software so you can address any problems or user concerns as you go along.

Anticipate what might go wrong.
It’s almost impossible to avoid errors or mishaps during deployment. Develop contingency plans and fallback strategies so you’re ready for anything.

Loop in your stakeholders.
Communicate with every stakeholder to let them know what is happening during the duration of deployment activities. Inform involved team members, as well as the end users.
Post-Modernization

This is the follow-up stage to your IT modernization project. Vendors may be required to provide post-implementation support while agency employees are caught up to speed on the new system. They may even continue supporting the system indefinitely, depending on the agency approach.

Agencies need to create a process to deal with any glitches or defects accordingly. For example, if there was a specific new tool or software used during modernization (like Office 365) it’s important to plan for that tool and the relevant team to be available for sufficient duration after the modernization project is completed. This way, any defects detected after deployment can be efficiently addressed.

To put it more specifically, modernization involves new technology, infrastructure and hosting options. When core technology language will be replaced (e.g., an application modernized from Java), make sure that the relevant skills needed to manage such technology are in place.

For example, modernized applications that will be implemented in the cloud or private or public implementations will require changes in IT roles and responsibilities. Such changes subsequently will trigger organizational and cultural disruptions. It’s important to address such changes and the risks they may pose to an agency. Have contingency plans in place if business is interrupted or be sure to have extra staff on board to manage the new technology post-deployment.

Post-modernization also includes decommissioning legacy hardware and software that is no longer needed. Additionally, effective communication with those inside and outside your agency is critical to increasing the chance of success for your modernization project.

“As you document your strategies, wins and failures, hold open houses, communicate with the agency and press and keep talking about your modernization project,” Laun said. “Once you execute your project and get your wins, document your wins and tell people about them. That gets people excited about modernization.”

For example, the FCC decided to redesign its main website, FCC.gov, by moving to a new platform and new host for the site. To follow up and make sure that users were included in the aftermath of the modernization project, FCC made sure to allow users to provide feedback to the new site. As a result, 85 percent of new visitors left positive comments about the website, allowing the FCC to dedicate adequate time to outstanding issues for those who left negative comments.

A large percentage of modernization efforts result in failure due to lack of acceptance by users. According to a recent Meritalk report, only 29 percent of agencies have established an application modernization change management team. The CIO, senior IT management team and any senior managers, however, must consistently demonstrate commitment to the program. Without such leadership, agency employees may withhold support or actively oppose the effort.

Ultimately, the post-modernization stage can be boiled down to two essential areas of focus: Consider what is needed after the new system is implemented and create a process to deal with any issues or defects.

“As you document your strategies, wins and failures, hold open houses, communicate with the agency and press and keep talking about your modernization project. Once you execute your project and get your wins, document your wins and tell people about them. That gets people excited about modernization.”

Dustin Laun, Technology Expert, FCC
Steps to Implement

Make sure you have the necessary tools and staff available.
After deployment, be sure you have the relevant teams you need to address inevitable glitches, issues or any questions users may have about the modernization project.

Quantify the impact.
Explain how the change fits into the overall strategy, who will be impacted and how the change will affect the organization and budget. Then put those values into numbers and determine return of investment (ROI) by analyzing how the project will save costs for your agency.

Build the vision.
Inform users how things would improve after the modernization project has been implemented. Have a compelling story that would persuade sponsors and users to support the change.

Set up a communication plan.
Decide how you are going to continually involve end users so that they are aware of the entire modernization process. This includes when to expect regular communications (i.e., weekly, semi-weekly) and how they can provide feedback and ask questions.

Execute the change.
Generate a detailed training plan to avoid issues with end-user acceptance. Define how and when the training will take place and identify leads within the community who can help coach others.
Conclusion

Modernizing IT systems is an increasing imperative for federal, state and local governments to deliver better citizen services, support mission programs and improve security and efficiency. Funds are being dedicated to the effort, new positions are being created according to needs and agencies are working to provide tools and resources to all stakeholders involved.

It’s important to remember that there is no one-size-fits-all solution and that every agency’s IT modernization roadmap may be different.

Various modernization strategies exist today and careful evaluation is needed to identify the best one for your agency. This can certainly be an overwhelming process. Fortunately, the modernization lifecycle can help agencies get started with five concrete stages:

1. Assessment and Roadmap;
2. Modernization Readiness;
3. Modernization Execution;
4. Modernization Deployment; and
5. Post-Modernization.

With an IT modernization roadmap, agencies can execute their modernization efforts more confidently and increase the likelihood of successful projects.
About GovLoop

GovLoop’s mission is to “connect government to improve government.” We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

www.govloop.com  |  @GovLoop

Thank You

Thank you to Alfresco, Amazon Web Services, BMC, CA Technologies, Cisco, Commvault, DLT Solutions, HP, MuleSoft, and SolarWinds for their support of this valuable resource for public-sector professionals.

Authors

Francesca El-Attrash, Staff Writer
Courtney Belme, Editorial Fellow
Nicole Blake Johnson, Technology Writer
Michael Steinberg, Editorial Fellow

Designer

Kaitlyn Baker, Graphic Designer