ACT-IAC
Accelerating Government

IT Modernization:
Lessons Learned and Best Practices

Case Studies from Representative Government Agencies

IT Management & Modernization Community of Interest

Released: February 24, 2021

Synopsis

This white paper discusses representative case studies from Federal government agencies and organizations, detailing their mission objectives and lessons learned as they modernized business processes and applications.

These case studies cover a variety of programs, ranging from custom application development to replacement of legacy functionality with software as a service (SaaS). Both civilian and military organizations are represented.

The case studies in this white paper provide a set of lessons-learned that can be used by government stakeholders as they plan modernization strategies. These are real-world examples that illustrate a topic that is often discussed in abstract terms.

Readers will find information in these case studies that can assist them with modernization efforts. This white paper provides names and resources that can offer transition guidance and mitigate the risks associated with modernization efforts.

The choices of vendors and solutions made by represented Government agencies and organizations are based on program-specific selection criteria. The IT Management & Modernization Community of Interest respects the independence of these choices and does not itself advocate any one vendor or solution over another.

This page is intentionally blank

American Council for Technology-Industry Advisory Council (ACT-IAC)

The American Council for Technology-Industry Advisory Council (ACT-IAC) is a non-profit educational organization established to accelerate government mission outcomes through collaboration, leadership and education. ACT-IAC provides a unique, objective, and trusted forum where government and industry executives are working together to improve public services and agency operations through the use of technology. ACT-IAC contributes to better communication between government and industry, collaborative and innovative problem solving, and a more professional and qualified workforce.

The information, conclusions, and recommendations contained in this publication were produced by volunteers from government and industry who share the ACT-IAC vision of a more effective and innovative government. ACT-IAC volunteers represent a wide diversity of organizations (public and private) and functions. These volunteers use the ACT-IAC collaborative process, refined over forty years of experience, to produce outcomes that are consensus-based.

To maintain the objectivity and integrity of its collaborative process, ACT-IAC welcomes the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of technology. For additional information, visit the ACT-IAC website at www.actiac.org.

IT Management & Modernization Community of Interest

The IT Management & Modernization (ITMM) Community of Interest (COI) advises and equips government with best practices and lessons learned, focused on strengthening IT management and implementation and accelerating legacy IT modernization. The COI covers all aspects of IT management and modernization to include strategy and policy making, governance, Capital Planning Investment Control (CPIC), Federal Information Technology Acquisition Reform Act (FITARA) implementation, and operations management.

Disclaimer

This document has been prepared to contribute to a more effective, efficient, and innovative government. The information contained in this report is the result of a collaborative process in which several individuals participated. This document does not – nor is it intended to – endorse or recommend any specific technology, product, or vendor. Moreover, the views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development. Every effort has been made to present accurate and reliable information in this report. However, neither ACT-IAC nor its contributors assume any responsibility for consequences resulting from the use of the information herein.

Copyright

Table of Contents

Introduction and Executive Summary

Many Federal agencies rely on decades-old, obsolete technologies to support mission critical programs, essential functions, and daily operations. In some cases, these technologies will be a challenge to support moving forward.

Additionally, agencies have different levels of experience with, and are in varying stages of, IT modernization. The government workforce has different levels of skills and experience with respect to new technologies and approaches associated with modernization readiness (e.g., microservices, agile, the transition from project to product, culture).

ACT-IAC recognized that sharing best practices and lessons learned can assist Federal government agencies in lowering risk and accelerating the successful modernization of their IT portfolios. Accordingly, ACT-IAC tasked the IT Management & Modernization (ITMM) Community of Interest (COI) with a project to:

- Research and interview departments and agencies that have experience with IT modernization;
- Document case studies from the research, highlighting the challenge, approach, and results;
    - Construct a taxonomy by modernization approach
    - Understand approaches to DevSecOps sustainment
- Synthesize results into a set of best practices and lessons learned to provide input to agencies for initiating and executing IT modernization.

The ITMM COI created a project team to solicit case studies from government leaders. Upon completing five case studies, the team project discovered common themes that had emerged which would be of value to other agencies considering modernization efforts. These include the importance of **employee engagement**, the need for **incremental and manageable modernization efforts**, the *centrality* of the **cloud**, the ubiquitous concern for **cybersecurity**, and the benefits of leveraging industry **best practices**, particularly in application development.

Recommended Guidance

ACT-IAC recommends reading these case studies and pairing them with the requirements matching your organization's mission. The following questions will help in assessing specific situations:

1. What is my organization's overall mission and where does modernization better help us meet our mission needs?
2. Who are our stakeholders? This includes management, peer agencies, and oversight committees.
3. Who are our users and what are their requirements?
4. What are our security requirements? What is our plan to meet them, and who will we engage from the appropriate communities to both educate and monitor compliance?
5. How will we manage change? What communities will need to announce the transition, and will we need to communicate with on an ongoing basis? What is the frequency and means of regular progress updates during the transition?
6. What type of training will we need to provide?
7. Have we thoroughly evaluated the availability of proven commercially available or established federal shared service solutions before moving to a custom development effort?
8. Have we considered the impact of our transition on the full ecosystem of workloads impacted by the scope of the modernization?
9. What is our current capital and operational budget? How much additional budget will we need during a transition (i.e., before the legacy implementation is retired)?
10. What are the long-term cost implications, post-transition?
11. Should we consider changing our organizational structure or operating model to improve execution and management of our modernization efforts?
12. Most importantly: Have we scoped the effort to be successful, including a manageable scope with clearly defined and attainable measures of success, the achievement of which will be viewed as success by all of our constituents?

Case Study Taxonomy

Scope Categories

Category	Subcategories
Infrastructure Services	Device management, routers, switches, circuits, network gateway consolidation, IPv6 implementation, etc.
Network Operational Services	IT service management and helpdesk; national and regional operational centers
Mission/Business Services	Applications and support services; partner gateways; micro services and data exchanges
Mission Employee/Associate Environment (Back Office Services)	Virtual data center; applications (including digital workplace applications, email, etc.) and support services; partner gateways (payment systems); learning management systems; HR, payroll, etc.
Data Center Services	Data center optimization; resource rationalization
Cybersecurity Protection	Network-level; platform/gateway level; application-level; data level
Enterprise Mobility	Enablement; consolidation
IT Commodity Management	Software/hardware licensing; asset management; agreements; privacy; and other compliance

PMA Categories

The President's Management Agenda (PMA) from the previous administration laid out a long-term vision for modernizing the Federal government in key areas that will improve the ability of agencies to deliver mission outcomes, provide excellent service, and effectively steward taxpayer dollars on behalf of the American people. To drive these management priorities, the Administration leveraged Cross-Agency Priority (CAP) Goals to coordinate and publicly track implementation across federal agencies.[i] [ii]

PMA Category/ Case Study (blue shading indicates the PMA goal was addressed)	ARMY IRMIS	GSA	DOE	VA	Department of Education
Key Drivers of Transformation					
IT Modernization					
Data, Accountability and Transparency					
People - Workforce for the 21st Century					
Cross-Cutting Priority Areas					
Improving Customer Experience					
Sharing Quality Services					
Shifting From Low-Value to High-Value Work					
Functional Priority Areas					
Category Management					
Results-Oriented Accountability for Grants					
Getting Payments Right					
Federal IT Spending Transparency					
Frictionless Acquisition					
Mission Priority Areas					
Modernize Infrastructure Permitting					
Security Clearance, Suitability, and Credentialing Reform					

Case Studies

Department of the Army: Integrated Resource Management Information System (IRMIS)

Title of Project: Integrated Resource Management Information System (IRMIS)

Organization: Army

Lead: John Bergin, Deputy Assistant Secretary of the Army Financial Information Management

Vision: Accelerate financial management innovation within the Army, and beyond, that enables the greatest advantage to the warfighter and provides the best return on investment for the American taxpayer.

Mission: To strengthen fiscal stewardship and support the Army's priorities through financial information management reform, analysis, and innovation.

Functions:

- Integrate Army Financial Management (FM) Systems into a Simplified and Standardized Environment
- Deliver Big Data Analytics to FM Domain Decision-Makers
- Enable Visibility and Transparency of Financial Information
- Provide Enablers to Automate Manual Processes
- Assure Federal Financial Management Improvement Act Controls and Compliance to Ensure Data Integrity
- Retire Legacy Systems

Challenge: Transform financial legacy systems

Goals/Objectives: To transform the legacy system to a cloud-native system that improved the efficiency of reporting and users.

Solution:
The project is called IRMIS (Integrated Resource Management Information System), a legacy end of life system this is not cloud-native and considered technically obsolete.

Mr. Bergin leveraged an existing contract to procure services for the project. Army and contractors worked collaboratively to develop the new system.

Mr. Bergin required a new cost-effective solution with built-in security policies to create a better user interface and experience. Army redesigned the system with new modules and developed new processes to make it technically compliant and user friendly.

Mr. Bergin's had several concerns when developing the Modernization Strategy. Mr. Bergin was concerned with end-user adoption. The current team was used to the legacy systems; he wondered how he could get the team excited about the new system. Mr. Bergin was concerned about the cost and schedule and the backlog of additional requirements.

Mr. Bergin's vision was to transform the legacy system into a serverless /cloud design to address security risks. Cybersecurity was built into the system by using DevSecOps methodology. Cybersecurity was discussed in every conversation with the team as well as in the requirements. The Army used a Zero Trust Model in the Cloud. This design strategy was new to the Army; Mr. Bergin taught the team the new approach.

Mr. Bergin embodied “servant leadership”, the practice of leading through service to the team, by focusing on understanding and addressing the needs and development of team members to enable the highest possible team performance.

Mr. Bergin restructured the team at the beginning of the project. He used agile methodologies on how to structure the team, including: Scrum Master, Product Owner, User Experience Analysts, and additional cross-functional team members.

Mr. Bergin led the team by enabling project leaders to become more agile and facilitate the team's success by promoting self-awareness, listening, serving those on the team, helping people grow, coaching, promoting safety, respect, and trust; and promoting the energy and intelligence of others.

Successful agile teams embrace the growth mindset, where people believe they can learn new skills. When the team and the servant leaders believe they can all learn, everyone becomes more capable.

Methodologies that drove the project to a successful completion included Agile Development Methodology, Twelve-Factor App Methodology (a methodology for building software-as-a-service application), Microservice (API) architecture, and DevSecOps.

Mr. Bergin stated that the project took 12 months to complete; the first capability was deployed rapidly in 48 days. The Army obtained 99% access control; the API passed the audit. The Army produced continuous value delivery within every sprint, enabling the team to become excited about their work and progress they had accomplished. Legacy systems were removed, Army moved over 49 servers to the Cloud. The modernization incorporated real-time reporting. The Army has access to daily transactional data, which are reviewed regularly to identify any resource issues. Army achieved reporting functionality in two to four months. Kanban became a useful tool in support of development as a whole, and it proved to be an excellent catalyst for promoting improvement; it was a major catalyst to success. User acceptance testing was the most significant risk; it is the last phase of the software testing process that verifies whether a product or software is fit for the purpose it was built for in the first place. With User Acceptance Testing, the business use case, requirements, code, testing, and cosmetic errors should be correct; it is a risk that requirements may change, new code may have to be developed, and more cosmetic design issues may have to be fixed. The team issues encountered included a remote user

acceptance testing; the Army team is working remotely due to the COVID-19 Pandemic. Army developed training to teach the team how to perform user acceptance testing to alleviate the challenges.

Mr. Bergin leveraged an existing contract to procure services for the project. Army and contractors worked collaboratively to complete the project. Mr. Bergin stated that "*there is never enough budget when implementing modernization; we had to prioritize our projects, we canceled projects and non-valued added contracts*."

IRMIS is utilized globally; the Army ensured success by writing exceptional code and developing comprehensive use cases.

Which PMA Cap Goal does the solution address and how does the solution line align with, support, or relate to these goal/s? (If applicable)

1. IT Modernization
2. Data, Accountability, and Transparency
3. People – Workforce for the 21st Century
4. Improving Customer Experience
5. Getting Payments Right
6. Federal IT Spending Transparency

Outcomes/Results:

Mr. Bergin's stated Army's IT Management Maturity increased; as the team learned this new approach to modernization, they started taking on more projects and utilized a 10-12 month model for implementations.

The modernization has increased operational effectiveness by resulting in better visibility, improved data calls, better management of $176 billion, increased mission capability, and decreased risk.

Lessons Learned:

Mr. Bergin stated "*We thrived on the processes we used—agile development, DevSecOps, serverless computing, and organizational change management. We would improve on the employee campaign that the modernization would make their job easie*r."

General Services Administration: IT Modernization

Title of Project: IT Modernization

Organization: GSA

Mission: "Deliver value and savings in real estate, acquisition, technology, and other mission-support services across government."

Vision: Effective and efficient government for the American people.

Lead: Mr. David A. Shive is the Chief Information Officer for the U.S. General Services Administration. Mr. Shive oversees GSA IT - formerly known as the Office of the Chief Information Officer (OCIO) - and information technology operations and budget, ensuring its alignment with agency and administration strategic objectives and priorities.

Challenge: GSA required a robust, flexible technology portfolio that would improve efficiency, interoperability, transparency, and collaboration across the organization.

Goals/Objectives: GSA's modernization includes a series of projects that were undertaken year by year. GSA started modernizing in 2011. GSA started small with discrete projects that they could test, create goodwill, and utilize as a springboard for additional modernization projects.

Solution: In 2017 through 2018, GSA began modernizing by transforming the email. The current email system was not interoperable. GSA transformed its email system into a cloud-based system, Google Mail. GSA was the first in government to use the new Google solution. GSA began A3 - Anywhere, Any Device, Anytime—users were not constrained by a facility. GSA started the implementation of the project by transitioning 100 users at a time. GSA used the Public Building Service to start the journey, and then the new solution was phased into the other departments.

Secondly, GSA moved the back office to the cloud into Salesforce. They transformed business processes during the transition. GSA went from 1800 applications to 250 (9 to 1 ratio) applications through rationalization. They found significant duplication when going through the rationalization process. They utilized government employees' ideas on how to improve since they know firsthand what they need to increase the effectiveness and efficiency of their jobs.

Mr. Shive stated, "GSA's goal was to do no harm to the business nor people during the modernization." Organizational Change Management was a part of the Modernization Strategy. GSA had to restructure as part of its modernization efforts. Originally all GSA departments had separate IT departments, including 27 CIOs. Now GSA has only one CIO, one infrastructure, one IT shop, and several business executives working collaboratively to exceed the mission.

GSA gave their employees a voice to be heard, provided extensive training, and built a collaborative business partnership. Soon employees got really excited about the modernization projects. Employees got comfortable performing work in a certain way -- employees forget about improving the process. GSA is exceptional at acquisition, good stewards of taxpayer dollars. Mr. Shive wondered how the team could be a part of that success. GSA used design thinking and User eXperience/Customer eXperience (UX/CX) practices to develop productive outcomes. The security users were paired with the engineers. GSA developed best practices of cross-communication. GSA was forward-leaning regarding business and technology and used the process to get their employees excited about new technology.

As a foundation to most of its Modernization efforts, GSA started using a hybrid cloud model over seven years ago. The flexibility of the cloud enabled GSA to utilize the commercial cloud for 53% of its portfolio and 10% of its portfolio in a private cloud. Mr. Shive stated, "*GSA is seven times ahead of its government peers*."

GSA understood the criticality of having best in breed cybersecurity policies, processes, and tools early on in the modernization process. GSA used to build cybersecurity functionality due to a business issue; that reactive process wasn't efficient. In the modernization phase, GSA began to build cybersecurity throughout the design of the system from beginning to end. GSA moved to continuous monitoring. GSA used to monitor systems on 1 to 3-year increments but wanted to be proactive by creating a minute cycle constant assessing model of cybersecurity. GSA transformed how they performed cybersecurity. They also retooled and retrained cybersecurity staff.

GSA is using emerging technologies as part of its modernization efforts. GSA has successfully implemented artificial intelligence and machine learning in its infrastructure. GSA has over fifteen current engagements with ten additional projects in the pipeline. GSA is exploring the usage of machine learning and artificial intelligence in cybersecurity. GSA is also utilizing helpdesk and email bots that feel like a real person (There is a learning curve, a bot has to learn just like a new employee). GSA is also the home of the Artificial Intelligence Center of Excellence in collaboration with JAIC/DoD. GSA is also the Robotic Process Automation Center of Excellence Leader. Mr. Shive stated, "*The White House is interested in sharing the capabilities of GSA's proven concepts in emerging technologies*."

GSA internalized and implemented many commercial best practices in its modernization efforts including: Digitization, Design Thinking, Lean Six Sigma, Customer Experience/User Experience (CX/UX), TIME (Tolerate, Invest, Modernize, Eliminate) Model, EOA (Eliminate, Optimize, Automate).

GSA developed a digital-first mindset. GSA continuously assess its systems for value and embraces the ability to develop API's to connect to other systems. GSA was one of the first agencies to change paper forms to web forms. GSA is a digital-first organization, and Mr. Shive said it is the most efficient way to accomplish their goals. GSA developed a well-defined process with fully open, transparent data, and restructured to develop the new reality. GSA's efforts resulted in eliminating duplication, saving money and time by becoming one GSA, collaborative culture, increased interoperability, and flexible, futuristic-designed infrastructure.

GSA's goal is to shift low value to high-value work. Pushing paper from point A to Point B and other manual processes can be transformed with automation. Mr. Shive stated, "*We are transforming our employees to knowledge workers to increase the value and efficiency of public service resulting in better properties, policies, and acquisitions.*"

Which PMA Cap Goal does the solution address, and how does the solution line align with, support, or relate to these goal/s? (If applicable)

1. IT Modernization
2. Data, Accountability, and Transparency
3. People – Workforce for the 21st Century
4. Improving Customer Experience
5. Sharing Quality Services
6. Shifting from Low-Value to High-Value Work
7. Federal IT Spending Transparency

Outcomes/Results: GSA's IT maturity matured to Strategic (achieving IT operational excellence and taking a strategic role in driving business innovation. Mr. Shive's position as CIO allows him to be a trusted, strategic partner to every area of the business. Before the first modernization business owners and technologists worked in silos. Now at GSA, the business owners and technologists work hand in hand on every significant project, which allows GSA to integrate technology, business, and data.

GSA measures the effectiveness of the modernization by surveys and a managed budget. GSA used to measure functions like server density or power consumption. Three years ago, GSA decided to revise its performance metrics. GSA wanted to establish metrics that would show the effect on technology within the business. GSA pivoted to purely business measures including click rate, transaction time, happiness of the workforce, and net promoter score.

Lessons Learned: Modernization is never really completed. GSA has transformed from the classic model of modernization ($200 million big bang system modernization) to a more manageable incremental improvement model for system modernization, eliminating the spending peaks of the appropriations. With Continuous Integration Continuous Deployment (CIDC), GSA manages a $10-$20 million budget for new capability annually to meet ever-evolving business needs. The result of GSA's new modernization model included happier employees and customers, better-managed budget, better partnerships, and reduced costs.

Even the best performing agencies are still seeking solutions, unknown to most, GSA is the largest purveyor of arts and antiquities in the world. It is a massive ecosystem; GSA has not identified a cloud provider to manage its vast collection.

Department of Energy: Transforming the Digital Customer Experience

Organization: US Department of Energy

The Department of Energy (DOE) is responsible for advancing the energy, environmental, and nuclear security of the United States; promoting scientific and technological innovation in support of that mission; sponsoring basic research in the physical sciences; and ensuring the environmental clean-up of the nation's nuclear weapons complex.

Within the DOE, the Innovation Community Center (ICC) is a digital hub and innovation platform for accelerating mission outcomes through collaborative innovation exchange, market research, and sandboxes for rapid prototyping, proof of concepts, and production pilots.

Lead: Pam Isom, Department of Energy, Deputy CIO for Architecture, Engineering, Technology, and Innovation

Challenge:

In accordance with the 21st Century Integrated Digital Experience Act (IDEA), the ICC was asked to reimagine how external customers interact with the department through its websites. Legacy technology supported antiquated processes (some still paper-based) and lacked modern capabilities. Additionally, the current culture and processes can be resistant to change. This ambitious effort will produce a better external customer experience working with the department to receive products and services. The effort focuses on making the departments websites consistent, modern, and mobile-friendly provided through an industry-standard, secure connection.

Goals/Objectives:

The project's purpose was to produce mission value in 4 ways:

1. Increase workflow automation to improve productivity, simplify and update design elements for web forms (e.g. hover effects);
2. Empower the use of analytics as well as AI and machine learning to generate website and form improvements;
3. Ensure adherence to accessibility requirements across DOE web presences (e.g. Section 508 compliance, GSA web standards); and
4. Improve the overall customer experience for both internal users and external customers.

Solution:

To accomplish the objectives, the digital modernization enables:

- New Web Standards
- Digitized Forms and Services
- Use of E-Signatures and Digital Signatures
    - External e-signing to comply with privacy act
    - Internal digital signature with the PIV card to validate workflow steps are complete

A proof of concept and a pilot were executed for two use cases to achieve the desired results: 1) Privacy Act Form and 2) Off-boarding Workflow of Federal Employees

Proof of Concept: The DOE ICC completed the process of testing viability:

- Validated vendor capabilities and functionalities
- Validated functionality and capabilities of on-premises environment as well as cloud services
- Achieved OneID internal authentication leveraging Single Sign-On capabilities
- Leveraged eSignatures where appropriate as well as digital signatures
- Leveraged the shared login.gov authentication capability to authenticate external customers

Pilot: ICC completed phase one process, digitizing public facing forms with electronic signatures and internal forms with digital signatures:

- Obtained virtual machine (VM) environment to install the forms solution
- Integrated the forms and OneID
- Used vendor cloud environment to demonstrate public facing forms and eSignatures
- Validated workflows as well as signature validation to include user acceptance testing

In phase 2, the team is moving the first forms wave, out of six total waves, to production.

Which PMA Cap Goal does the solution address and how does the solution line align with, support, or relate to these goal/s? (If applicable)

1. IT Modernization
2. Data, Accountability, and Transparency
3. People – Workforce for the 21st Century
4. Improving Customer Experience
5. Sharing Quality Services
6. Shifting from Low-Value to High-Value Work

Outcomes/Results:

The desired results were achieved through the use case pilots for privacy act forms and off-boarding workflows of federal employees:

1. Increased workflow automation to improve productivity, simplifying and updating design elements for web forms (e.g. hover effects);
2. Empowered the use of analytics as well as AI and machine learning to generate website and form improvements (e.g. analytics captured the length of time it takes users to complete form elements providing valuable information to guide improvements);
3. Adhered to accessibility requirements and verified standards were met (e.g. Section 508 compliance, GSA web standards); and
4. Improved the overall customer experience for both internal users and external customers.

- Phase 1 Results:
    - Form Conversion: Two official DOE forms digitized in phase 1, 200+ slated for phase 2

  - Incorporated workflows into each DOE Form providing efficiencies as well as providing transparency in provided service
  - eSignature and Digital Signature Enabled: Leveraged an electronic signature solution for web-based forms
  - OneID Authentication: Achieved multifactor authentication for internal customers
  - Login.Gov was tested for use with external customers for authentication and ID proofing

- Phase 2 – in progress
  - Web Modernization: High cost savings potential in paper reduction and efficiency anticipated on Energy.gov with over 26 million visits/month, with Section 508 compliance. 27 additional sites identified to standardize web presence
  - Optimal Citizen and Employee Experience: Ability to scale interactions and real-time data insights, enabling rapid delivery and improved user experience
  - Leverage AI capabilities in development of forms and database by identifying existing fields during conversion process

Lessons Learned:
Through the effort, the team recognized the following items as having an important role in facilitating the project's success:

- Use of Proof of Concept and Pilot: This approach enables the team to determine whether the proposed solution would meet the desired objectives and helped refine requirements. The pilot helps determine fit for the environment as well as provides a more complete view of cost.
- Resource Support: Having the right resources allocated (e.g. a full-time project manager to drive project tasks and an Information System Security Officer for security requirements/documents) separates a success project from a stalled effort.
- Communication and Collaboration: Stakeholder synthesis, collaboration and communication is critical for technical evaluations and to produce a common agenda among stakeholders. Those stakeholders involved need to have decision making authority for the areas of the project that affect their organization / work. Use of multi-channel communications enables to the team to reach the right stakeholders at the right times.
- System: Legacy system reconfigurations are required to enable a turnkey solution.
- Architecture: Technical architecture modifications will be needed for integration.
- Security: Considerations are needed to match compliance with firewall security configurations.

Additionally, the team noted the implication on the department's Learning Agenda:

- Workflows: The Workflow Learning Agenda addresses questions related to tailoring, automating, and streamlining document workflows.
- Tool Acclimation: The Tool Acclimation Learning Agenda addresses questions related to best practices and use of digital tools.
- Staffing: Personnel need to be trained on use of the solution, cloud platform, and services.
- Business processes: Identifies areas for improvement in business processes.

Agency Disclaimer: The appearance of this U.S. Department of Energy case study does not imply or constitute an endorsement by the Department.

Department of Veteran Affairs Franchise Fund: Automated IT Financial Management Leveraging the Technology Business Management (TBM) Standard

Title of Project: Automated IT Financial Management leveraging the TBM Standard.

Organization: Veteran Affairs Franchise Fund

Lead: Ryan Woodward, Director, VA Franchise Fund Budget Office Infrastructure Operations

Challenge: The Veterans Affairs Department spends more than $7 billion a year on information technology. This number was roughly $5B until the onset of COVID. VA's IT spending is now at $7B with an additional investment towards TeleHealth/TeleMedicine in support of veterans.

Most of VA's efforts to understand costs were manual through many spreadsheets taped to walls. The process was tedious and there was a need to send out monthly bills to VA stakeholders for the shared services provided. The end-users felt the bills were difficult to interpret and took too long to produce. VA wanted to shift to a repeatable, sustainable, automated SaaS system to modernize manual processes.

Goals/Objectives: By applying Technology Business Management (TBM) standards, VA's goal was to understand its IT spending two or three levels down to drive better decisions and cost savings.

Solution: One of the very basic first steps we took was pulling all budget lines and all labor costs by full-time equivalent and by contractors and mapping every single one of those and employees to the TBM taxonomy. That's really a basic foundational exercise. That forms the foundation for migrating to an IT financial management solution and start aggregating your costs in accordance with TBM taxonomy. You start to see total cost for a platform or for storage once you have that initial mapping done.

The use of automated TBM resulted in a better understanding of how VA's costs to use cloud services compare to private sector costs.

Ryan Woodward, Director, VA Franchise Fund Budget Office Infrastructure Operations stated that "*data is helping VA decide which applications should go to the public cloud as well as understanding the return on investment for moving to the cloud*."

"*It's helping us understand our costs in a more granular manner so there are some applications that for the near term will probably stay on-premise legacy infrastructure*," Woodward said. "*Through our analysis with TBM and comparing our costs to [commercial] cloud costs, we are understanding the drivers of our costs better, so we are able to optimize our on-premise spend while those things either wait to be migrated or stay on legacy infrastructure for the foreseeable future*."

More specifically, Woodward said using the TBM data helped VA not invest in more storage equipment because there was either plenty available on-premise or the data or applications could be moved to the cloud.

Which PMA Cap Goal does the solution address and how does the solution line align with, support, or relate to these goal/s? (If applicable)

1. IT Modernization
2. Data, Accountability, and Transparency
3. Improving Customer Experience
4. Shifting from Low-Value to High-Value Work
5. Category Management – Leveraging Common Contracts and Best Practices
6. Federal IT Spending Transparency

Outcomes/Results:

A good example is that VA went from having basic cost data related to call centers or budget object codes or congressional projects to now having data about specific services they are providing. For example, compute, storage and networking. VA is able to describe that in much more detail.

"*That's where you can start automating this process of converting general ledger cost data into more useful, granular and transparent data that is being displayed in the TBM taxonomy format*," Woodward said. "*Once you have that down, then you can start conducting broader activities related to analyzing the data and trending the data over time for applications*."

Woodward said the use of TBM resulted in a better understanding of how VA's costs to use cloud services compare to private sector costs.

He said this data is helping VA decide which applications should go to the public cloud as well as understanding the return on investment for moving to the cloud.

Woodward said the early analysis shows the agency is paying at least 10% less for commercial cloud storage.

"*We recently migrated some important VBA applications from an off-premise third-party data center to the cloud and that was a big win for the agency because we saved many millions of dollars*," he said. "*We were able to cut those costs by half, at least*."

Lessons Learned: VA has been implementing TBM for the better part of two-plus years. Started by seeing what data is available first and then filling in the gaps. "*One of the very basic first steps we took was pulling all budget lines and all labor costs by full-time equivalent and by contractors and mapping every single one of those and employees to the TBM taxonomy. That's really a basic foundational exercise*," Woodward said. "*That forms the foundation for migrating to an IT financial management solution and start aggregating your costs in accordance with TBM taxonomy. You start to see total cost for platform or for storage once you have that initial mapping done*."

- Overcommunicate
- Understand current state versus future state
- Identify key stakeholders of data owners
- Update all players often
- Identify key stakeholders of end users
- Identify key stakeholders of who will benefit most
- Be clear on what will change and why
- Automate through COTS

An interesting lesson was the relationship between the CFO and CIO's shop was an important collaboration to make TBM more valuable. For example, VA created a standard mapping structure for budget object codes to cost pools in the taxonomy, which made it easier to map the data to the categories. One method, one conversation.

Department of Education: The Enterprise IT Modernization

Title of Project: The Enterprise IT Modernization

Organization: US Department of Education
The Department of Education's mission is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.
In 2016 the department and its Office of the Chief Information Officer (OCIO) began its enterprise IT modernization journey – a journey that began by focusing on the basics, advanced to addressing IT systems, and now has evolved to employing emerging technologies in support of automation.

Lead: Jason Gray, Department of Education Chief Information Officer (CIO)

Challenge:
The department was facing old equipment, slow and cumbersome IT, and cloud sprawl. Laptops were taking 20 minutes to boot. The size of the cyber footprint was a concern and causing significant extra work to secure. The department's IT-service delivery is contractor-owned, contractor-operated making it a 100% cloud-based environment. At the same time, the number of cloud providers had become unwieldy and troubling. Understanding that a change was needed, an enterprise IT modernization journey began.

Goals/Objectives:
The enterprise IT modernization purpose was to produce mission value in 3 ways:

1. Improve the basic IT user experience;
2. Enhance cyber security; and
3. Attack inefficiency.

Solution:
To accomplish the objectives, the department's efforts focused on:

- infrastructure and cloud consolidation;
- systems rationalization; and
- modernization and automation.

The department's approach to accomplish these objectives was a deliberate and methodical process that included assessment, partnership, planning and execution.

The Assessment – The department completed a thorough, independent assessment of its IT and systems to generate an accurate picture of the state of IT. The results:

- provided a visual of what IT looked like to be communicated throughout the department;
- mapped systems to laws, policies and priorities; and
- identified important matters such as personally identifiable information (PII) and high value assets.

The Partnership – Understanding that the journey would have its challenges, a spirit of collaboration and partnership was cultivated across:

- departmental leadership beginning with the Secretary, Deputy Secretary and importantly the Assistant Secretaries;
- the OCIO team;
- system owners; and
- service providers.

The Plan – With the evidence and the support in place, the department created the TO-BE vision and the plan to achieve it. The plan was detailed and communicated extensively.

The Execution – The challenge demanded execution excellence combined with joint problem solving. At one point, the effort encountered an unexpected budget challenge. Faced with the issue, the department's leadership immediately came together as a team to find a resolution.

Which PMA Cap Goal does the solution address and how does the solution line align with, support, or relate to these goal/s? (If applicable)

1. IT Modernization
2. Data, Accountability, and Transparency
3. People – Workforce for the 21st Century
4. Improving Customer Experience
5. Sharing Quality Services
6. Shifting from Low-Value to High-Value Work
7. Federal IT Spending Transparency
8. Improve Management of Major Acquisitions

Outcomes/Results:

Through partnership, rigorous planning and execution, the desired results were achieved:

1. Improved the basic IT user experience;
2. Enhanced cyber security by reducing the IT footprint; and
3. Improved efficiency.

At every point of interaction with technology, customers form or re-affirm their perception of IT. Beginning with the moment customers turn on their IT workstations, they expect reliable access to the basic technology needed to accomplish their mission. The Infrastructure modernization completed in 2019 produced a secure cloud environment and deployed ~5,000 new laptops. As a result, users saw an approximately 95% reduction in laptop boot up time. And the cloud environment is generating $20M in server storage savings over 5 years. Additionally, the overall IT footprint has been reduced enhancing the department's cyber security posture. Beyond the efficiency gains in laptop and compute performance, the department has identified $200M in potential savings from automation.

The Pandemic – In this unexpected and challenging time, the planning and hard work have paid off as demonstrated in the department's recent successfully move to 100% remote work with minimal impact.

The department's upgraded IT infrastructure proved to be critical to this success. Challenges encountered in the move were manageable and quickly addressed including solving PIV/onboarding complexities in 5 days instead of weeks.

While much has been accomplished, the journey continues. The department has recently introduced a new five-year roadmap for its continued enterprise IT modernization.

Lessons Learned:
Through the effort, the team recognized the following items as having an important role in facilitating success:

- Collaboration and Partnership: Knowing that any modernization effort of this size and complexity will have unwelcome challenges along the way, the department's leadership collaborated every step of the way. The effort became less CIO's modernization and more the department's modernization. Because of this, the significant issues were addressed as a department. Highlighted factors:
    - Support from senior leadership
    - System owners and stakeholder involvement every step of the way
    - Communicating possible things IT can do for you, not what will be done to you
    - CIO reporting to the secretary or dep secretary
- The importance of planning: Planning begins with a thorough understanding of the IT landscape in terms of assets and state. Bring the problems to the front to be planned and worked together. Emphasize transparency. For the department, the upfront assessment and associated picture of IT showed what IT looked like and provided the evidence to support what was being done and why. From that point forward, be transparent all along the way.
- Creating the vision, communicating the vision: The vision develops a picture of the future and the direction IT needs to move. It needs to be easy to communicate and address the stakeholders – basing it on the data will make it that much stronger.
- Getting the basics right, earning credibility: Starting with the basics and making progress there is viewed as 'critical' as it earned the team the credibility to launch more ambitious modernization efforts.
- Starting small, avoid 'boiling the ocean': Avoid taking on too ambitious of an undertaking. Beginning with smaller efforts and showing evidence of progress early provided the confidence to expand over time.

Summary and Lessons Learned

The selection of Federal modernization initiatives in this paper provides the opportunity to draw general "best practice" conclusions. While the scope of the projects is broad, ranging from stakeholder engagement, to the back office, to cost and financial management, these success stories enable us to provide guidance to those undertaking such projects in the future.

Lesson 1: While it is IT modernization, humans make it happen

Focus on engagement and collaboration

In each of the five case studies, the interviewees emphasized that success was contingent upon concern for end-user adoption and/or employee engagement. Where longstanding practices and processes need to be replaced by new methods, these successful leaders anticipated and overcame resistance in the culture and in the embedded processes.

- **GSA** change agents emphasized the following:
    - The firsthand understanding of process which their employees brought.
    - Restructuring: from separate IT departments within each department (including 27 CIOs), to one CIO, one infrastructure, one IT shop, and several business executives working collaboratively.
    - Measurements of effectiveness, based on surveys and a managed budget: From, for example, server density or power consumption, GSA has changed its approach to establish metrics that demonstrate the impact on technology within the business. It does this through purely business measures, including click rate, transaction time, happiness of the workforce, and net promoter score.

- The **Department of Energy** found synthesis, collaboration, and communication among empowered stakeholders critical for technical evaluations and to produce a common agenda.

- The **Army** found a "servant leadership" model to be optimal for developing energy and belief in the success of teammates and, in retrospect, would be even stronger on its employee campaign.

- The **VA** found enhanced value in collaboration between the CFO and CIO organizations, advised over-communication, identification of stakeholders of data owners, end user and project beneficiaries, and regular updates as best practices.

- The **Department of Education** cultivated a spirit of collaboration and partnership across departmental leadership, beginning with the Secretary, Deputy Secretary and, most important, the Assistant Secretaries, the OCIO team, system owners, and service providers.

Each team took great care to assign resources who had both the skills and the time to devote to a successful project.

Lesson 2: Incremental rather than "big bang"

Incremental, rather than "big bang" or comprehensive modernization, delivers results quicker and mitigates risk

Three of the five case studies call this out explicitly. The project team believed this to be a foundational point. Specifically:

GSA's modernization includes a series of projects that were undertaken year by year, beginning in 2011. GSA started small with discrete projects that it "can test, create goodwill, and utilize as a springboard for additional modernization projects" (from the case study in this whitepaper).

The **Department of Education** learned to "Start small, [and] avoid 'boiling the ocean': Avoid taking on too ambitious of an undertaking. Beginning with smaller efforts and showing evidence of progress early provided the confidence to expand over time" (from the case study in this whitepaper).

The **Department of Energy** also began with proof of concept and pilot, to be followed by six waves moving into production. Overly ambitious project scoping can result in increased levels of complexity, which drives execution risk and longer timelines, leading to longer payback periods. These combine with the higher levels of required funding to reduce overall satisfaction with a modernization effort.

While these initiatives featured manageable projects, which built support and confidence, both initiatives had a clear long-term view of what modernization meant to the agency.

This practice conforms to the eighth FITARA scorecard which "*reward(s) agencies for using iterative, agile and incremental development*," according to Kevin Walsh, a Government Accountability Office analyst who assembles the data that go into the scorecard.[iii]

The value of this approach to the successful acquisition of project funding is discussed by Gartner's Thomas Klinect in "How to Build a Business Case for Application Modernization."[iv]

Lesson 3: Cloud Approaches

One or more Cloud approaches will be part of the Modernization project

In January 2018, ACT-IAC published a paper entitled, "Cloud Migrations-Lessons Learned," which discussed a number of the challenges facing the government's adoption of this technology.

In today's connected world, the cloud has moved from novelty to necessity and has become transparent as it pervades both individuals and infrastructure.

> In the government world, things are not quite as smooth and easy. The mission needs of government are unique and vertical. Differing user bases have unique requirements that are bounded by security, internal connectivity, legacy applications, specific authentication needs, auditing mandates, training concerns, and privacy regulations. Significant foresight and planning are required for any government cloud transition. There are often many roadblocks – some are based on policy and process, others on fear and perception. While FedRAMP and FISMA provide a great framework, the overall process from inception to the final Authority to Operate (ATO) can be daunting, even to the most seasoned CIO and CTO. Where do I start? How do I manage the process? What services do I need? How will I staff and manage this new environment? These, and many others, are the questions that keep government cloud strategists awake at night.[v]

In autumn 2020, not three years after these concerns were recognized, cloud is at the center of each of the five modernization case studies. The range of cloud adoption is from:

- Custom development for Army IRMIS
- Software as a service (SaaS)
    - First-in-government use of SaaS email
    - Back office conversion to SaaS Customer Relationship Management (CRM)
    - TBM (Technology Business Management) SaaS solution
- The Department of Energy's use of vendor cloud environments to demonstrate public-facing forms and eSignatures
- The Department of Education, noting not only that cloud was central, but that the organization actually saw a need for rationalization to reduce cloud sprawl

Lesson 4: Focus on Cybersecurity is Foundational

As IT modernization frequently results in the transition from decades-old legacy systems to the cloud, it is understandable that cybersecurity was a principal concern in each of these undertakings.

Many, if not most, industry analysts believe that the public cloud in 2020 is at least as secure as the on-premises data center. This was not the case at the outset of a number of these case studies, so an extra burden of care fell upon the change agents. Even today, stakeholder concerns must be addressed; operations, data, and privacy protected; and regulatory requirements satisfied.

Insights from the case studies include:

The **Department of Energy** identified having an Information System Security Officer (ISSO) for security requirements/documents as a key to separating a successful project from a stalled effort.

The **Department of Education** called out the "enhancement of cybersecurity" as an objective and noted that the objective was achieved and that the reduction of the overall IT footprint had contributed to it.

The **Army** chose a serverless/cloud design in part to address security risks, discussing cybersecurity in every conversation with the team and in the requirements, employed DevSecOps methodology, as well as introducing a Zero Trust Model in the cloud.

GSA recognized early the value of best in breed cybersecurity policies, processes, and tools. It had previously built cybersecurity functionality reactively; in modernization, GSA began to build cybersecurity throughout the design of the system. It moved to continuous monitoring, retooled, and retrained cybersecurity staff.

Lesson 5: Embrace Proven Management Practices That Provide a Blueprint for Success

The agencies in the case studies utilized established and sound project and program management approaches to their modernization initiatives. Specifically:

The **Army** initiative included Agile Development Methodology, Twelve-Factor App Methodology (a methodology for building SaaS applications), Microservice (API) architecture, and DevSecOps.

The **VA** initiative was based on Technology Business Management (TBM) standards.

The **GSA** project alone incorporated digitization, design thinking, Lean Six Sigma, Customer Experience/User Experience (CX/UX), and the TIME (Tolerate, Invest, Modernize, Eliminate) Model (helpful in prioritizing modernization initiatives) and EOA (Eliminate, Optimize, Automate) models.

And even with all of these efforts, some modernization solutions remain difficult to find. For example, **GSA** still struggles to find a solution for its vast collection of artwork.

Authors & Affiliations

This white paper was written by a consortium of government and industry. The organizational affiliations of these contributors are included for information purposes only. The views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development.

Government Sponsor
David Chiles, United States Patent & Trademark Office

Authors and Contributors

- Eric Stogoski, Ernst & Young
- Rich Byrnes, Global Technology Solutions Group
- Tanesia Barrow, Barrow Wise Consulting, LLC
- Bob Carter, Apptio, Inc.
- Daniel W. York, General Services Administration
- Prasad Kanigicherla, KPSoft, Inc.

The project team extends its gratitude to the following government executives who provided valuable information regarding their IT modernization case studies

- John Bergin, Department of the Army
- David A. Shive, General Services Administration
- Pam Isom, Department of Energy
- Ryan Woodward, Department of Veterans Affairs
- Jason Gray, Department of Education

Appendix: Supplemental Information on Key Terms

In Support of Lesson 5, Management Practices:

Advanced Data Sciences: applies advanced analysis and logic-based techniques, including machine learning, to interpret events, support and automate decisions, and take actions[vi]

Modern Development practices and techniques, including:

- Agile Development Methodology: a development approach that delivers software in increments by following the principles of the Manifesto for Agile Software Development[vii]
- Design thinking: [the] balance [of] intuitive originality (the hallmarks of great designers) with analytic mastery (the hallmarks of business leaders and engineers) to create business-focused outcomes that generate transformative, innovative and strategic change[viii]
- Twelve-Factor App Methodology (a methodology for building a SaaS application)[ix]
- Microservice (API) architecture: based on service-oriented application components tightly scoped, strongly encapsulated, loosely coupled, independently deployable and independently scalable [x]
- DevSecOps: integration of security into emerging agile IT and DevOps development [xi]
- Kanban: provides an effective and efficient route to continuous delivery and Lean software development [xii]

Organizational Change Management (OCM): a strategic approach for managing and integrating people to align with the future state vision and goals. OCM is used to prepare, adopt, and implement fundamental and radical organizational changes, including its culture, policies, procedures, and physical environment, as well as employee roles, skills, and responsibilities[xiii]

Robotic Process Automation (RPA): a productivity tool that allows a user to configure one or more scripts (which some vendors refer to as "bots") to activate specific keystrokes in an automated fashion[xiv]

Use of Proof of Concept and Pilot: as articulated by the Department of Energy, "enabling the team to get a closer view of the fit for the environment, and refine requirements, as well as providing a more complete view of cost"

In Support of Lesson 4, Cybersecurity:

FedRAMP simplifies security for the digital age by providing a standardized approach to security for the cloud. In its case study, the Department of Energy specified a minimum of FISMA Moderate (loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals)[xv]

OneID Authentication, a "digital identity management service that provides a repository for usernames and passwords, eliminating the need for people to remember numerous arcane character sequences"[xvi]

- Zero-Trust: an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location.[xvii]

References

[i] https://www.performance.gov/PMA/PMA.html, retrieved 3 September 2020
[ii] PMA CAP goals from https://www.performance.gov/CAP/overview/, retrieved 23 November 2020
[iii] https://www.nextgov.com/it-modernization/2019/08/what-expect-future-fitara-scorecards/158886/, retrieved 24 November 2020
[iv] https://www.gartner.com/smarterwithgartner/how-to-build-a-business-case-for-application-modernization/, retrieved 15 September 2020
[v] ACT-IAC Cloud Migration Lessons Learned, released 24 January 2018 https://www.actiac.org/act-iac-white-paper-cloud-migrations-%E2%80%93-lessons-learned
[vi] https://www.gartner.com/en/information-technology/glossary/artificial-intelligence, retrieved 16 September 2020. Gartner defines "Advanced Analytics" as Advanced Analytics is the autonomous or semi-autonomous examination of data or content using sophisticated techniques and tools, typically beyond those of traditional business intelligence (BI), to discover deeper insights, make predictions, or generate recommendations.
[vii] https://www.gartner.com/en/information-technology/glossary/agile, retrieved 16 September 2020
[viii] https://www.gartner.com/en/information-technology/glossary/design-thinking, retrieved 16 September 2020
[ix] For more, see https://12factor.net/ as retrieved 3 September 2020
[x] https://www.gartner.com/en/information-technology/glossary/microservice, retrieved 16 September 2020
[xi] https://www.gartner.com/en/information-technology/glossary/devsecops, retrieved 16 September 2020
[xii] https://www.gartner.com/en/documents/3892280/adoption-guide-to-second-generation-agile-with-kanban, retrieved 16 September 2020
[xiii] https://www.techopedia.com/definition/13996/organizational-change-management-ocm, retrieved 16 September 2020
[xiv] https://www.gartner.com/en/information-technology/glossary/robotic-process-automation-rpa, retrieved 16 September 2020
[xv] https://www.govinfo.gov/content/pkg/GOVPUB-C13-9af73460e5ff9ede8820abdf3a50041d/pdf/GOVPUB-C13-9af73460e5ff9ede8820abdf3a50041d.pdf, retrieved 15 September 2020
[xvi] *https://whatis.techtarget.com/definition/OneID*, retrieved 2 September 2020
[xvii] https://www.nist.gov/publications/zero-trust-architecture, retrieved 14 September 2020