

Accelerating Legacy System Modernization in Government

Costs and risks associated with government legacy systems continue to rise, as agencies and departments continue to leverage these mission critical systems without a modernization plan.¹ While the challenge of replacing these systems can be complex, there are highly pragmatic approaches to modernization that have proven very successful in government. This brief will identify risk factors associated with legacy systems, contrast different modernization approaches, and highlight best practices and recommendations for accelerating legacy system modernization initiatives.

¹ GAO Report 19-471 "Agencies Need to Develop Modernization Plans for Critical Legacy Systems," June 2019.

With the explosive adoption of predictive analytics and artificial intelligence in IT operations, security, and application data, the technology gap between the private sector and government continues to grow; and will continue to do so until these innovations are being addressed through modernization plans.

Technical and Cost Risk Factors

There are many concerning risk factors associated with legacy systems, as a June 2019 GAO report on critical legacy systems details.² These risk factors include outdated programming languages, unsupported hardware and software by vendors, operating with known security vulnerabilities, shortages of qualified staff, and others. These are significant by themselves, but are far too often compounding the risk associated with these systems. There are also other risk factors not discussed in the GAO report that are equally concerning. One example is the increasing opportunity costs of not modernizing these systems. With the explosive adoption of predictive analytics and artificial intelligence in IT operations, security, and application data, the technology gap between the private sector and government continues to grow; and will continue to do so until these innovations are being addressed through modernization plans. There is also risk associated with not being agile enough to respond to a future security vulnerability or breach, given the inability to quickly update or replace vulnerable code in these systems. Combined, these risks continue to drive up maintenance costs and increasingly, threaten the security of high value government data residing on these systems.

Legacy System Modernization Alternatives

Legacy system modernization is not a new challenge and several alternative approaches have been tried and tested up to this point, but with highly variable degrees of success. In fact, industry analyst Gartner Inc. defined five legacy modernization alternatives back in 2011; replace, rewrite, rehost, retain, and retire respectively.³ Since we already covered the increasing costs to retain a legacy system and the assumption you cannot simply retire these legacy assets without adverse impact to the mission, we can focus on the vastly different outcomes of the three remaining options for modernization.

Replace

Replacing the legacy system with a commercial off the shelf (COTS) package may seem like a promising alternative, but there are two significant challenges with this approach. First, it is likely the COTS package does not do all the things the legacy system does. After all, these systems were modified over many decades and simply cannot be swapped out. Additionally, all the things the legacy system does are not known or well understood, which is the second big challenge with replacing them. This explains the poor results of rip-and-replace modernization projects, as reported by the Standish Group⁴:

- **1 in 5** projects will be **cancelled** in their entirety
- **88%** projects **fail** to complete on time and budget
- **50%** projects will **cost 3 times** their original estimates
- **3%** projects with labor costs over \$10 million **succeed**

A record like this suggests the rip-n-replace modernization method will have the highest cost, significant risk, and in the end will fail to achieve the desired outcome.

² Ibid.

³ Gartner, Inc. Research "Migrating Applications to the Cloud," December 2010.

⁴ Standish Group Report "Modernization: Clearing a Pathway to Success," 2010.

Rewrite

The rewrite modernization option also suffers from not knowing what you do not know; that is, what exactly the legacy system does and how it does it. However with rewrite, this liability lies directly on you, instead of a COTS vendor with the replace option. This makes it the most risky option with similar high costs, since you are funding the entire development effort to replace the legacy system. Gartner summarizes this option by stating, *"Rewrite the application...and you get exactly what you want, the most expensive, highest risk, and most time [alternative]..."*⁵

Rehost

The only legacy system modernization alternative to show repeatable success and the predictability to stay on budget and on schedule is rehost. This option pragmatically shifts these legacy workloads to modern commodity platforms with as little change as possible. This equates to the least cost, lowest risk, and fastest time-to-value approach. In fact, by moving these workloads to commodity platforms, you quickly realize savings over legacy platforms and can start applying that savings to additional modernization efforts, such as moving more workloads or redesigning business processes, user interfaces, or integrations with other systems. This savings benefit is unique to this modernization approach and is credited with its growing adoption. According to industry analyst IDC, *"we are seeing a shift from a 'rip-and-replace' approach towards modernization strategies that are aimed at gaining significant business value in the form of agility, new business capabilities, and reduction in TCO and risk."*⁶

To accelerate modernization of legacy systems and achieve the best time-to-value for government agencies and departments, rehost is the only clear option. Rehost not only provides almost immediate cost savings other alternatives do not, but also has the least risk, fastest implementation, and most realistic path to innovation. Combine this with past performance and the increasing costs of the status quo and the only realistic, pragmatic approach is rehost.

Key Elements of Successful Legacy Modernization Strategies

Of course selecting the appropriate legacy system modernization method alone does not ensure success; there are also different project elements and best practices to make your modernization strategy successful. Carefully reviewing past performance suggests three key elements of successful legacy modernization strategies:

Application Estate Analysis is critical to identify what you do not know or understand about the legacy applications and the enterprise services and infrastructure that support them. The ability to view the entire legacy application estate holistically helps demystify large, complex legacy codebases and application portfolios and most importantly, understand the current value legacy applications provide.

3 key elements of successful legacy modernization strategies:

- **Application Estate Analysis**
- **Modernization Framework and Reference Architecture**
- **Measurable Continuous Improvement**

5 Gartner, Inc. Research *"Migrating Applications to the Cloud,"* December 2010.

6 IDC Whitepaper *"Modernization: A Flexible Approach to Digital Transformation,"* July 2018.

Legacy system modernization, no matter how complex, does not have to be the elephant in the room, as many successful government projects have shown.

Modernization Framework and Reference Architecture provides the end-to-end system roadmap and target blueprint respectively, mapping the migration of existing legacy system components to new target systems. This informs a pragmatic approach to modernization by defining the entire application holistically, including associated processes (i.e., devops, backup/recovery) and infrastructure (i.e., identity and access management, databases, platforms), in addition to application source code.

Measurable Continuous Improvement ensures the modern practices of Agile DevOps, delivering applications with the speed that the mission requires, are applied to all applications, including legacy applications and systems -- from mainframes to edge devices.

Government Modernization Best Practices

Legacy system modernization, no matter how complex, does not have to be the elephant in the room, as many successful government projects have shown. At Customs and Border Protection (CBP), they had a legacy mainframe system with escalating hardware and software licensing costs. This system also represented over one million lines of COBOL and assembler source code, nearly 100 batch processes, 800 million instructions per second (MIPS), and supported over 60,000 users – so it was imperative for CBP to get this right and leverage industry best practices:

- Analyze legacy application estate to inform modernization priorities and decisions
- Develop holistic modernization plan for applications, associated processes, and infrastructure they are dependent on
- Leadership commitment to modernization plan and buy in from all stakeholders
- Leverage rehost: Start by moving target dev and test workloads to commodity platforms
- Transition to agile devops processes for maintaining legacy applications
- Integrate security and predictive analytics requirements into the modernization plan
- Continuously measure, improve, and repeat

By following these best practices, CBP has achieved \$40 million in cost savings the first year and a 90% reduction annually for this particular system. Sixteen months after initiating this modernization project, they have aligned the IT infrastructure with standard platforms, such as migrating from the legacy hierarchical mainframe database to a new extensible RDBMS database while improving online and batch performance along the way. This enables new integration projects with open platforms and better positions CBP for future innovation – whether that be cloud migration, predictive analytics adoption, or enhanced security operations.

Measuring Legacy Modernization Progress

Sustaining if not accelerating forward momentum should be an objective of every modernization plan and is a key to successful transformation. Agile DevOps practices help deliver this, but not without providing all stakeholders with the visibility required to inform decisions and quickly respond to inefficient or ineffective modernization activity. The influencing factors for modernization decisions are Cost and Risk. Analysis of these factors provides the critical information needed to accelerate the modernization of legacy applications.

Cost metrics—It is important to consider all the associated IT and operational costs together. This includes the cost of the application platform, supporting software, including maintenance; the cost of wages and attributed overhead costs (e.g., datacenter expense). There are also downstream costs of current systems, e.g., likely system upgrades, leasing renewals, support staff contracts etc. Additionally, any 'new' system costs need to have been evaluated for comparison along the same lines. Typically, there is a new hardware CapEx element as well as the purchase of new system software. Retraining on any new system has to be considered and incorporated too.

Risk / operational metrics—Typically plotting 'cost' against 'value' will give you a reasonable measure of any system from a business perspective. However, there are dangers in ignoring the readily available and valuable operational data points:

- **rate of change**—number of issues 'solved' by the system on average. This gives a good view of the flexibility of any system
- **number of defects**—an overall measure of outstanding issues may indicate a level of robustness
- **rates of change**—the amount of recorded change made is an important factor
- **application complexity**—a number of standard metrics can be measured against applications to deduce 'complexity'
- **customer / user views**—customer opinion can be determined through help desk systems or surveys
- **strategic fit**—systems conform to an internal architectural blueprint to a lesser or a greater extent and this information is typically recorded in a way that allows it to be rated

Additional key performance indicators for tracking progress of legacy systems modernization:

- **cost-savings optimization index**—how much in cost-savings (\$) is being generated per dollar spent on modernization activity?
- **risk-reduction optimization index**—per dollar spent on modernization activity, how much reduction in risk has occurred?⁷
- **% have completed analysis**—of all existing legacy and mainframe applications, what percentage have had a completed analysis that specifically identifies the disposition, costs, code-level dependencies, and risks of the system?

The influencing factors for modernization decisions are Cost and Risk. Analysis of these factors provides the critical information needed to accelerate the modernization of legacy applications.

⁷ Reduction in risk as derived by the organizations Risk Management Framework (RMF).

Driven by customer-centric innovation, our software provides the critical tools they need to build, operate, secure, and analyze the enterprise. By design, these tools bridge the gap between existing and emerging technologies—enabling faster innovation, with less risk, in the race to digital transformation.

- **% have modernization plan**—of all existing legacy and mainframe applications, what percentage have an individual modernization plan?
- **% of modernization work on contract or working capital fund (WCF)**—what percentage of legacy and mainframe systems in the modernization plan are beyond the analysis phase and on an existing modernization contract or WCF?

Monitoring, tracking, sharing, and adapting to these indicators on a regular cadence over time is imperative for accelerating legacy system modernization initiatives.

About Micro Focus Government Solutions

Micro Focus helps organizations run and transform their business through four core areas of digital transformation: [Enterprise DevOps](#), [Hybrid IT Management](#), [Predictive Analytics](#) and [Security, Risk and Governance](#). Driven by customer-centric innovation, our software provides the critical tools they need to build, operate, secure, and analyze the enterprise. By design, these tools bridge the gap between existing and emerging technologies—enabling faster innovation, with less risk, in the race to digital transformation.

**Micro Focus Government Solutions
Headquarters**

8609 Westwood Center Dr.
Suite 700
Vienna, VA 22182 U.S.A.

Additional contact information and
office locations:

www.microfocusgov.com