DECOUPLE TO INNOVATE
How federal agencies can unlock IT value & agility by remediating technical debt
Fueled by the emergence of cloud computing, digital technologies and agile methods, the pace of technology innovation is accelerating dramatically. The more adaptive, service-based architectures that are emerging—what Accenture calls Exponential IT—will empower agencies to deliver more innovative, customer-focused solutions and operate more sustainably and securely as well. The roadblock? **The need to break free of monolithic core systems that are especially common in government.**
The Imperative to Decouple

While federal IT leaders have long recognized the need to modernize, modest progress to date is creating a potential crisis for many agencies. Continued reliance on legacy platforms and systems threatens their ability to perform core functions. For example, the Pentagon warned in September 2017 that failure to keep pace with commercial technology innovation could allow potential adversaries to “surprise us or overtake our military advantage.” And as former Social Security Administration CIO Rob Klopp testified to Congress in 2016, “… the interest payments on [our] 30-year-old technical debt are compounding, and in the next five years, we could face a crisis keeping our systems running.”

One way to gauge the need for modernization is to look at the current level of technical debt—essentially the money it would take to upgrade legacy systems—an organization has accumulated over time. Accenture’s analysis of CAST Appmarq data shows government had the highest average technical debt ($1.5 million) per application, which is up to five times greater than the 11 other industries examined. According to former Federal CIO Tony Scott, this equates to $7.5 billion in hardware and software having reached end-of-life in 2016, which doesn’t include functioning but outdated systems that significantly constrain operations.

There are many contributing factors unique to government agencies that lead to higher debt levels; these include irregular or prolonged funding cycles, reliance on homegrown legacy systems, persistent skill gaps, leadership turnover, and risk-averse cultures that hinder modernization efforts. Over time, these factors have created a situation where a disproportionate amount of agency investment goes to maintaining legacy systems. According to the GAO, the federal government spent over 75 percent of its FY15 IT budget on operations and maintenance (O&M), creating a crowding-out effect that is driving down investment in new development, modernization, and enhancements (DM&E).
The Accenture Federal Services Digital Decoupling Study examines this modernization conundrum, shedding light on the magnitude of the problem, identifying the key impediments, and revealing how best to break down the barriers to innovation and adoption of new technologies.¹

**The survey findings revealed three key themes:**

- **Legacy systems are putting agencies in danger.** 58 percent revealed that they experienced between 2-3 major disruptions or outages over the past decade, with just 4 percent avoiding any discontinuities over this time period.

- **Technical debt and resulting IT discontinuities impede innovation and agility.** 83 percent indicated that technical debt severely limits their ability to be innovative and 79 percent report that it inhibits their responsiveness to change.

- **Agencies need to implement decoupling strategies to unlock the value inside legacy IT.** 87 percent responded that they want the best of new IT and legacy by navigating to new technologies in a way that secures the best of both worlds, but only 36 percent said they have a clear strategy.

While presenting a sobering view of the significant challenges agencies face, the survey results do indicate some optimism on the part of agency heads supported by the fact that they understand the dangers of technical debt, have begun to measure these risks, and have implemented more agile methods to accelerate modernization efforts.
Modernization as a Strategic Priority

Modernization of federal IT systems is an imperative due not only to security and cost factors but also mission capabilities. For every day that upgrade decisions are deferred, agencies are less able to deliver improved, citizen-centric or mission-critical services.

According to the survey results, approximately one-third of “core, mainstream systems” are considered legacy and require 21 percent of the overall IT budget to maintain. In fact, some of these systems are built on outdated technology more than 50 years old and support tens of millions of US citizens.

These legacy systems present two strategic threats for federal agencies:

An inability to move as fast as the mission requires. Speed, agility and innovation were overwhelmingly identified (top three overall choices and 4 of the top 6) as being “severely hindered by your legacy system (multiple responses)”.

<table>
<thead>
<tr>
<th>Innovations hindered by legacy systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which of the following, if any, are severely hindered by your legacy systems?</td>
</tr>
<tr>
<td>Quickly creating innovative new products or services</td>
</tr>
<tr>
<td>Quickly creating innovative new operating models</td>
</tr>
<tr>
<td>Quickly creating innovative new operational processes</td>
</tr>
<tr>
<td>Securing government systems and data from cyber threats and attacks</td>
</tr>
<tr>
<td>Improving efficiency</td>
</tr>
<tr>
<td>Responding quickly to changing mission conditions and needs</td>
</tr>
<tr>
<td>Enhancing our citizens experience</td>
</tr>
<tr>
<td>Partnering with other organizations including those in our ecosystem</td>
</tr>
<tr>
<td>Collaborating across agencies to provide personalized customer services</td>
</tr>
<tr>
<td>Augmenting our employees’ capabilities with new technologies</td>
</tr>
<tr>
<td>Achieving the full benefits of analytics-driven insight</td>
</tr>
<tr>
<td>Building citizen trust</td>
</tr>
</tbody>
</table>
**Significant risk of a cyber incident or outage.** In addition to the 37 percent indicating that outdated technology hinders their ability to protect against cyber threats, 46 percent separately reported that outages within their legacy system involved a security breakdown.

As a result, **85% of these IT leaders** believe that their agency’s future will be threatened if they don’t update their technology.

The primary challenge agencies face is accurately assessing the costs and risks buried in their systems. When evaluating legacy systems, the risk may not be just a function of age, but rather the ability to meet current and emerging requirements. In fact, older systems can continue to function properly and co-exist with modern ones if maintained properly.
Overcoming Barriers to Modernization

Technical debt accumulating in legacy systems is a key barrier to modernization. Accenture’s analysis of Appmarq data from CAST, a leading provider of software intelligence solutions, shows that it is 2.5 times more expensive to manage legacy applications that are ten years or older compared with new applications.⁸

Assessing the level of accumulated technical debt is the starting point for agencies trying to gauge their modernization challenge. Technical debt is a concept that draws from a technique that is quite familiar to organizations and individuals: Borrowing money to fund current expenditures. Just as readily available credit has led to economic expansion and significantly higher standards of living, excessive debt has led to bankruptcy and contraction when borrowers are unable or unwilling to make the required payments.

Technical debt can be created through the standard trade-offs associated with software development as one feature is prioritized over another. However, it accumulates rapidly when subsequent decisions to upgrade systems are deferred, meaning the required “payments” are not made. Over time, these missed payments lead to discontinuity points where systems slow down or break down entirely and become constraints on the broader organization and strategy. Or, to use the financial example, they become bankrupt.

It’s important to note that technical debt is not bad per se, but just like financial debt, it must be properly managed and leveraged. It reflects the necessary trade-offs made when running large complex organizations trying to balance multiple priorities.

Key survey findings related to technical debt:

- IT Leaders are well aware of technical debt. 96 percent of IT leaders understand how technical debt is being managed within their agency.

- Technical debt stands in the way of innovation and migration to New IT. Eighty-three percent believe technical debt limits innovation, 80 percent say it severely limits their ability to enhance current systems and 81 percent cite the need to remediate technical debt before migrating to the cloud.
More can be done to manage technical debt. Leaders haven’t developed a clear consensus on how best to deal with technical debt, with the top method—tracking when new systems are taking on technical debt—listed by less than half of respondents. Approaches that agencies are currently using to manage technical debt include (multiple responses):

<table>
<thead>
<tr>
<th>Technique</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking when new systems are taking on technical debt</td>
<td>46%</td>
</tr>
<tr>
<td>Reporting on technical debt to a C-suite executive committee</td>
<td>44%</td>
</tr>
<tr>
<td>Assigning responsibility for technical debt to an executive or manager within IT</td>
<td>43%</td>
</tr>
<tr>
<td>Educating line managers running their own systems about technical debt</td>
<td>42%</td>
</tr>
<tr>
<td>Assigning responsibility for technical debt tracking and reporting to finance executive</td>
<td>41%</td>
</tr>
<tr>
<td>Developing or following explicit guidelines to manage technical debt</td>
<td>41%</td>
</tr>
<tr>
<td>Estimating the cost of remediating technical debt</td>
<td>38%</td>
</tr>
<tr>
<td>Tracking which existing systems have technical debt</td>
<td>37%</td>
</tr>
<tr>
<td>Prioritizing technical debt remediation efforts</td>
<td>36%</td>
</tr>
<tr>
<td>None of the above</td>
<td>1%</td>
</tr>
</tbody>
</table>

Technical debt becomes a problem when you don’t monitor or actively manage it. Agencies need to be mindful of the policies, practices, decision-making processes, and culture that help create technical debt. Common debt drivers found in agencies include the need to move quickly to address emerging threats, the desire to innovate and experiment, deferred investments due to budget uncertainty, poor governance and architecture, and organizational restructuring.

The challenge for many federal agencies is sustaining a long-term, ongoing focus on technical debt remediation. For example, 68 percent of agencies reported having 3 or more CIOs over the past ten years and only 29 percent plan their IT strategy and vision extending five or more years into the future. Furthermore, while nearly all agree that it is important to continuously manage technical debt, only 36 percent actually do so.
Understanding Technical Debt

To accurately track and measure technical debt, agencies need to agree upon a standard definition of what it is, what specific components are included, and the methods available to remediate this debt.

Let’s start with a definition of technical debt. It includes the cost to renew legacy systems for current requirements and maintain software quality for acceptable risk, performance, and agility—in other words, to make these systems fit for today’s operating environment.

**Accenture’s Technical Debt Model breaks down the component costs as follows:**

**Principal** – This is the largest and easiest to measure and includes the cost to remediate and maintain legacy systems. Like financial debt, you make measurable progress in debt reduction by paying down principal.

**Interest** – These are the workaround costs such as staffing, delays, and redundant systems that must be maintained because decisions to integrate or retire older systems have been deferred. By not paying down principal, interest costs mount.

**Liability** – When systems are fragile and vulnerable, outages, breaches, or data corruption can occur, creating significant costs to patch software, restore systems, or in some instances replace hardware. Similar to deferred maintenance on a home, other issues surface that create additional, unforeseen expenditures.

**Opportunity Costs** – These costs are the most difficult to measure, but are nonetheless essential to understand, as they represent borrowing from the future due to the inability to support benefit-producing initiatives today. Current gaps in cost, performance, and security grow wider for every year modernization is deferred.
Monitoring and Mitigating Technical Debt

Technical debt is often described in monolithic terms. The reality is that it exists at many levels within an agency with different implications for various types of technical debt. For example, excessive technical debt can either constrain program operations, increase IT support costs, create a security or business continuity risk, or all of the above.

While agencies need a systematic means for measuring and managing their technical debt, most (70 percent) report that they do not have a fully-integrated approach. As a starting point, it is often easiest to distinguish between application-level and structural-level (either system or system-of-systems) technical debt. This is due, in part, to the fact that application-level debt can often be addressed discretely while structural debt generally requires more integrated remediation. At the same time, agencies also require better approaches to managing their ongoing accumulation of new technical debt.

Application Portfolio Management (APM) can provide analysis and benchmarking for understanding where application-level technical debt exists in the organization. APM is typically used to assess mission and business alignment, functional performance, technical health, cost-to-maintain, cloud and modernization readiness, and potential security vulnerabilities for each application in the enterprise. When this information is consolidated, such as in a dashboard, organizations can quickly assess different categories to identify the most significant gaps and constraints.

For applications showing the most severe performance impact, more detailed diagnostics can be used to better understand and account for specific risks. Modern, automated approach can also be used to determine total technical debt and cost-to-remediate, and to evaluate the impact of potential fixes on overall performance.

As one example, the CEO of a large commercial organization decreed a 10 percent across-the-board cost-cut for all departments in response to increasing competition. Recognizing the impact of legacy applications on support costs, the CIO pursued a 12 percent reduction in total application technical debt. Her team was able to actually reduce technical debt 15 percent, which lowered overall support costs by 10 percent.
The interdependencies inherent within infrastructure and related systems creates challenges in assessing their technical debt. As a common utility, their requirements and constraints may not be entirely variable, as a fixed cost may be incurred to support one or a hundred systems. In this scenario, modeling to future capability models and cost structures can play an important role in assessing current structural debt.

For example, consider your target architecture and to-be operating model, which should reflect anticipated mission, business and operational requirements. By mapping it against your current baseline capabilities, structural gaps that need to be addressed can be identified.

As important as remediating past technical debt is the management and avoidance of new debt. Currently, 46 percent of agencies track when new systems take on technical debt. The concept of a backlog within agile software development makes this issue explicit, as the tradeoff between increased velocity and functionality versus added debt is an everyday decision. Beyond tracking its accumulation, agencies need to create acceptable performance standards or ranges for technical debt and dynamically test to ensure that unaccounted debt isn’t being created.
Beyond monitoring the accumulation of technical debt in new development, agencies also need to ensure that existing systems do not accumulate excessive debt as they age. With a better sense of the near and long-term costs of deferred remediation, agencies can justify shifting more O&M spending to the maintenance component of the equation to reduce operational costs. Strategies like enterprise cyber hygiene that enforce a systematic approach towards maintaining systems to current standards can pay significant dividends.

**Addressing Discontinuity Points**

What Accenture calls discontinuity points is what happens when an organization fails to address technical debt. These are critical inflection points where constraints move beyond IT to threaten core mission, business and operational programs. They occur when accumulated technical debt causes these critical systems to either chronically break down, decline or become so inadequate, sluggish or inflexible that the organization is forced to halt or significantly slow down investments on innovative new systems until it consolidates, replaces or rearchitects its existing IT systems.

The leading causes of these events are aging legacy systems, lack of skills to upgrade and modernize, and the inability to integrate systems as well as data. Other contributing factors include poor maintenance, inadequate investment, the inherent complexity of the systems, and changing mission requirements.

According to the survey, 96 percent of agencies have experienced one or more discontinuity points in the past decade, including 58 percent that experienced two or three incidents and 9 percent with 3 or more. In 46 percent of cases, more than 25 percent of citizen users were impacted. Beyond the internal IT costs to fix broken systems, the downtime causes agencies to incur additional operating costs, fines, and uncollected revenues.

### Widespread discontinuity within the past 10 years

*How many times has your organization experienced a discontinuity point with the past 10 years?*

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never</td>
<td>4%</td>
</tr>
<tr>
<td>Once</td>
<td>29%</td>
</tr>
<tr>
<td>2-3 times</td>
<td>58%</td>
</tr>
<tr>
<td>More than 3 times</td>
<td>9%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>1%</td>
</tr>
</tbody>
</table>

**DEFINITION:**

Points in time where business-critical systems either chronically break down, decline or become so inadequate, sluggish or inflexible that the organization is forced to suspend or significantly slow down investments on innovative new systems until it consolidates, replaces or rearchitects its existing IT systems.
Embrace Digital Decoupling for Continuous Modernization

Agencies are eager to move forward with 81 percent indicating that they would tear up and replace all of their organization’s core systems if they could. However, they also understand that they are often dependent upon (and therefore, vulnerable to) them, especially the large monolithic systems that operate their agency’s core functions. These include large benefits and payment systems, legacy electronic health record platforms and command & control networks within the military. In many cases, these home-grown systems have grown in fits and starts for up to fifty years, resulting in systems that are as mission-critical as they are unmanageable.

While these systems are vulnerable, they also possess an agency’s DNA, meaning that they cannot be simply abandoned. For example, 82 percent of survey respondents indicated that their “legacy systems contain trapped value—data and capabilities that can be used for innovative new products, services, processes and business models but are not being leveraged.” However, they also overwhelmingly believe (87 percent) that although legacy systems hold information that is critical to their organization, they must navigate to new technologies in a way that secures the best of both worlds.

So, what is getting in the way? According to the survey, the top impediments to modernization included:

- Concerns about security or data loss (38%)
- Inconvenience, disruption or new requirements imposed on citizens (38%)
- Time required to migrate from legacy to new systems (36%)
- Difficulty of integrating with legacy systems (32%)

What agencies are learning is that using “big bang” or “lift and shift” methods to modernize legacy systems is not always feasible due to the disruption, cost, risk and delay that it entails. This is especially true for mission-focused core systems. Instead, a hybrid approach that allows legacy systems to run in parallel with new technologies as modernization initiatives roll out over time with continuous technical debt reduction is often a better fit.

Digital decoupling is a process of using new technologies, development methodologies and migration methods to build new systems that execute on top of legacy systems. For example, open application programming interfaces (APIs),
Agile DevOps, cloud migration factories and data lakes. Using these and other approaches, organizations can gradually decouple their core systems, migrating critical functionality and data to new platforms at a pace the agency requires and can support. Over time, this allows agencies to evolve towards Exponential IT, which is marked by unlocked value in terms of data and functionality, increased IT agility and more seamless collaboration with mission, business and operations stakeholders.

At its core, digital decoupling encompasses three key elements:

- **Creating a Platform or Ecosystem Vision** – In many instances, the end goal is to transform a monolithic core system into a service-based platform to fully unleash its value while eliminating current constraints. This requires understanding both future mission, business or operational requirements as well as plans for the agency’s digital environment. This will guide both needed enhancements and target architecture.

- **Prioritizing Near-term Constraints** – Identifying current chokepoints, liabilities and risks to establish where near-term intervention can have the most significant and immediate impact. For example, some systems may prioritize a modernized user experience (UX) that support human-centered design (HCD); others may require underlying technical changes to shift functionality to lower-cost or more secure platforms; and for many, ensuring more accessible and interoperable data is the key driver.

- **Adopting Continuous Modernization** – Large scale application modernization projects have a well-deserved reputation for cost overruns and failure. A shift to an agile model using DevOps for iterative development and incremental delivery can reduce risk while accelerating time-to-value.
The shift to digital decoupling and continuous modernization is critical for three reasons. First, it allows IT to be more responsive to changing requirements, shifting priorities as needed to deliver needed capabilities more quickly. Second, it helps to guard against the accumulation of additional technical debt through a regular and ongoing process of updating core components as needed. Finally, an iterative approach allows agencies to capture benefits incrementally so that initial cost savings can be reinvested to fund subsequent phases of the project.

As more and more systems are decoupled, agencies can evolve towards a true service-based Exponential IT architecture that maximizes agility. Furthermore, this creates a more “AI-friendly” environment where contextual data and insight can be used more readily to supplement or replace rules-based decision-making.

Figure 1 shows a common legacy system. In Figure 2, core functionality is being decoupled for migration to more modern platforms while new capabilities are layered onto the existing system. Figure 3 is the target future state environment.

Existing legacy systems can be modernized iteratively. Near-term, core functionality can be decoupled for migration to more modern platforms while new capabilities are layered onto the existing system. The future state vision reflects a complete shift to a more modular architecture.
The Time is Now

Given the scope and scale of the federal government, building momentum for modernization efforts can be daunting. However, as the Accenture Federal Services Digital Decoupling Survey results reveal, there is reason to believe that agencies can adopt the necessary practices and techniques, such as digital decoupling, required for modernization. These practical, agile approaches provide a way forward for government agencies that control costs, mitigate risks, and deliver critical new capabilities.

Further bolstering the case for optimism are developments in the standardization of IT cost categories and reporting represented by the TBM Council, as well as legislative changes brought about by the recent passing of the Modernizing Government Technology Act that may provide further fuel to accelerate agency efforts.

To make modernization a reality, agencies need to:

- **Adopt digital decoupling** as a rational approach for agencies to focus on modernization in a way that gradually migrates systems away from legacy while effectively managing cost and risk.

- **Utilize application assessments** that are well grounded in commercial experience and use modernization roadmaps that offer transparency and risk reduction critical for business-line executive accountability.

- **Educate to build awareness and acceptance** of a modernization approach that has high success rates in improving government’s cost efficiencies while maintaining service excellence.

As barriers to modernization continue to fall, change will continue apace, giving agencies more running room to innovate like never before.
Let’s get to work together

Author
David McClure, Ph.D.
Principal Director, Federal CIO Advisory Services
Accenture Federal Services
david.mcclure@accenturefederal.com
@drdavemcc
https://www.linkedin.com/in/damcclure/

Research
Carla Kusel
Lynn LaFiandra

Contributors
Sara Abiusi
John Conley
Dominic Delmolino
Tom Greiner
Aaron Jeanguenat
Saurabh Srivastava
Craig Wright

Notes
4. The Accenture Federal Services Digital Decoupling survey was fielded to 185 federal IT decision-makers in October 2017. All were employed by agencies of the U.S. Federal government as either a political appointee, Senior Executive Service (SES) or career employee (GS-13 to GS-15 or O-1 to O-10). All reported having legacy environments within their agency. Within this group, 45% reported that they were extremely knowledgeable and 54% very knowledgeable “…regarding their organization’s plans for legacy systems AND adoption of new technologies such as cloud computing and new techniques such as agile development and DevOps.”
5. Based on analysis of CAST Appmarq data from 1177 applications.

About Accenture Federal Services
Accenture Federal Services, a wholly owned subsidiary of Accenture LLP, is a U.S. company with offices in Arlington, Virginia. Accenture’s federal business has served every cabinet-level department and 30 of the largest federal organizations. Accenture Federal Services transforms bold ideas into breakthrough outcomes for clients at defense, intelligence, public safety, civilian and military health organizations.

About Accenture
Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world’s largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 449,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

Copyright © 2018 Accenture. All rights reserved.
Accenture, its logo, and High performance. Delivered. are trademarks of Accenture.