

A “Tomorrow Ready” Strategy for Government Technology

Future proof IT transformation can only come through open architecture hybrid cloud approaches

By Fletcher Previn, IBM Chief Information Officer

There is no doubt that technology has incredible potential to transform the way governments serve citizens and accomplish critical missions. But while governments are some of the world’s largest organizations with diverse and complex technology needs, agencies often are hampered by legacy IT systems that are difficult and expensive to modernize. Add to that agency missions that are constantly evolving and the growing expectation that government technology, public facing and otherwise, be just as innovative and intuitive as consumer-facing apps, and the challenges for government IT leaders are immediately clear.

Tomorrow Ready IT strategies give governments maximum flexibility to meet changing needs. Governments should not deconstruct and rebuild their agency’s IT systems based on any one technology provider’s business model. This misdirects scarce modernization resources in a way that benefits vendors, not government agencies.

The only way to meet those challenges is through investments today to transform government IT systems to be **Tomorrow Ready** – flexible to evolve as mission requirements grow and shift over the long-term, and open to the broadest possible range of innovations. No one vendor, platform, or cloud can do all that.

To advance their missions with a recognition that no one can fully predict future requirements, the world’s largest commercial enterprises are embracing Tomorrow Ready technology strategies built on hybrid cloud architectures. By following that example and making hybrid approaches the rule versus the exception in public sector IT, leaders in government can realize a broad range of benefits that enhance citizen experiences and essential government operations, such as:

- Allowing citizens to use a common digital ID across multiple agencies to simplify processes such as student loan applications, filing taxes, applying for Medicare, or renewing a passport.
- Using that same common digital ID, coupled with predictive analytics, to proactively anticipate citizens’ needs.
- Boosting defense sector productivity, helping military ships navigate sea lanes more efficiently and safely by leveraging AI, which shows great promise for autonomous shipping.
- Enabling defense and homeland security agencies to use emerging technologies to derive greater insights from their supply chains and make critical decisions.

Using hybrid cloud to power Australia’s myGov platform

In Australia, citizens can access a wide range of government services including Medicare, veterans service, taxation, disability insurance, and health records through a single, secure platform called myGov. Australian citizens have a single login and a secure inbox where they can receive correspondence from multiple participating government agencies. As of July 2020, more than 60% of the Australian population use the myGov system.

One obstacle many governments agencies currently face is decades old infrastructure and applications, written in outdated programming languages and layered from years of adapting to policy changes. As the COVID-19 response has shown, citizens and government workers remain frustrated with systems that

are out of synch with evolving technology use or less resilient due to years of deferred modernization.

Amidst the COVID-19 response, government workers performing sensitive missions were suddenly working remotely. As governments responded to the crisis, IT systems were heavily stressed by increased workloads. While many agency IT leaders accelerated modernization, systems and networks were still pushed to their limits. This impacted mission-critical operations and diminished government's ability to respond to the crisis. The ways that leaders have accelerated modernization during the COVID-19 response have shown that IT systems need to enable entirely new ways of operating.

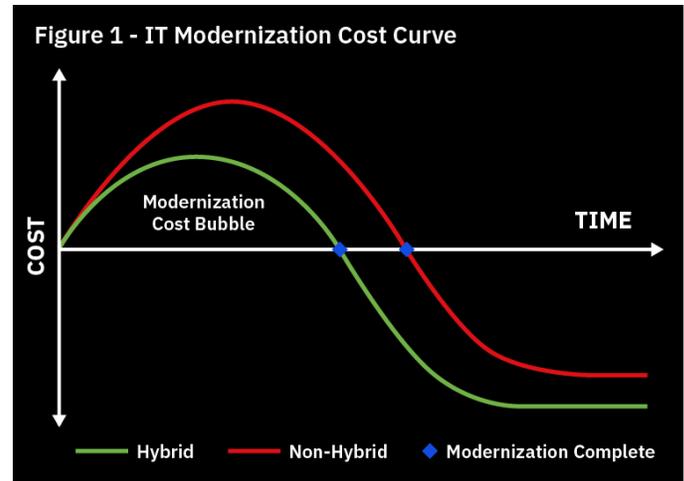
“Moments of crisis almost always carry lessons and if there is anything the COVID-19 pandemic has taught us, it’s the critical importance of technology solutions that enable speed, flexibility, insight, and innovation.” - IBM CEO Arvind Krishna

This is why, as governments plan their pandemic recovery, policymakers should reorient and accelerate modernization to transform government IT systems to become Tomorrow Ready. No one knows what the next emergency will be or how specific agency missions will evolve. But with the right foundation, they don't need to. If that infrastructure is flexible and built to open architecture standards, it can adapt quickly to new demands. If it is open, and not locked into any one vendor environment, it can rapidly bring the best technology to bear as challenges arise. Tomorrow Ready puts the agency, not specific technologies or vendors, at the center of IT modernization.

IBM recommends a three-step approach to advance a Tomorrow Ready technology strategy:

1. Adopt Hybrid Cloud Architecture

Government IT is too big, varied, and disparate for one cloud computing provider to effectively serve all its needs. Instead, an open and hybrid approach will build in the necessary flexibility to allow agency heads and CIOs to make tech decisions based on how agency missions are evolving, rather than because they're locked into a contract with one vendor.



Leading global enterprises want clouds that are flexible, provide access to the best applications from multiple vendors, and can smoothly transition legacy systems. Modernizing legacy IT systems can be a daunting task. It requires planning for up-front costs that only deliver financial savings down the road (see Figure 1). Many government agencies have security, privacy, and mission needs that require specialized government computing centers. The preferred modernization approach will often keep workloads in those centers due to unique operational needs and benefits, while other applications will clearly benefit from lifting to commercial clouds.

Sharing information on EU travelers using open architecture containerization

European Union member states are collaborating to build an open architecture, hybrid cloud environment to allow data on traveler entry and exit from the Schengen area to flow smoothly between member states, reinforcing security and the fight against terrorism and crime. By leveraging open architecture containerization, different systems across multiple clouds can connect today and later innovations across different clouds can be integrated in the future.

The best way agencies can reduce initial modernization cost, time, and complexity is to use a hybrid cloud

architecture to modernize applications to run in the cloud setting with maximum citizen service and mission benefits. As shown in Figure 1, implementing a non-hybrid strategy will result in higher upfront costs due to the expense of added “lifting and shifting” of applications to commercial cloud and reduced future savings if the lift to a less optimal cloud setting brings lower benefits. **Governments should not deconstruct and rebuild their agency’s IT systems based on any one technology provider’s business model. This misdirects scarce modernization resources in a way that benefits vendors, not government agencies.** In the cloud computing context, this often equates to cloud migration without modernization. Governments should pursue Tomorrow Ready hybrid cloud strategies that rationalize each application’s modernization path based on a full assessment of the mission needs and through open architecture preserve flexibility in long-term IT decision making by avoiding being needlessly locked-in to one cloud environment.

Agencies should plan their modernization as an evolution that culminates with their entire cloud portfolio under a single consistent multi-cloud management model across public, private, and hybrid cloud providers. IBM and other leading organizations have proven in their own transformations that a Tomorrow Ready cloud approach that aggressively drives to a single consistent multi-cloud management model across public, private, and hybrid cloud will create labor efficiencies, better cyber hygiene and network observability, and greater resiliency. These elements are exactly what is needed to “future proof” government IT systems to respond to unexpected challenges.

Improving the U.S. Veterans benefits experience through automation

In the U.S., a veteran’s benefits application experience is shaped by how applications enable claims evaluators. Manual processes (i.e. transcribing data from paper forms) add time, complexity, and error. The U.S. Veterans Administration has used automation to reduce claims processing times from more than 10 days to just a few hours. More than 350 claims assistants were able to upskill to focus on more complex claims adjudication activities.

Tomorrow Ready hybrid cloud strategies must also enable government workers to perform their mission anywhere. A Tomorrow Ready hybrid cloud approach will move agencies beyond the constraints of static data center firewalls with software defined networks that bring mission critical application access to workers anywhere – whether that be agency field offices, a remote base, or their homes – while providing security and visibility to the end of the network. This ensures agencies can smoothly reposition workers when future challenges demand it. It also allows them to recruit talented professionals who want to work in a modern and flexible environment that drives innovation and a healthy work culture.

Agencies must also ensure that modernized applications can integrate emerging technologies like blockchain, AI, and quantum computing that will drive the next revolution in government and enable future missions. Modernizing applications using interoperable “containers” based on open architecture standards achieves this by allowing data to flow to any future applications that are built to those same standards. Containers also enable a “modernize once, run anywhere” approach that allow key applications to be shared across multiple agencies or even different layers of government. To achieve more flexible IT systems, governments should update cloud adoption and data center investment strategies to prioritize hybrid cloud and application containerization based on open architecture.

2. Increase adoption of commercial technology

IT applications enable business processes that support missions and citizen services. **Modernization of those applications should focus on adopting commercial automation technologies to reduce manual processes, give leaders the data they need to make smarter decisions, and enable entirely new ways of delivering services.**

Real progress may require policy changes to break down structural barriers to automation. However, the benefits are clear. The U.S. General Services Administration estimates that agencies could save \$3 billion a year if automation gave federal workers just 20 hours back per year to focus on more mission critical tasks.

Agencies should target near-term modernization on business processes that are commonly used across multiple agencies,

such as logistics, claims processing, and mission support operations. Agency CIOs should work with program leaders to link modernization outcomes to clear services and mission improvements. Policymakers should update IT modernization laws to encourage a greater focus on business processes and outcomes and incentivize agencies to devote more IT spending to Tomorrow Ready modernization.

3. Enhance the role of CIOs in leading IT modernization decisions

Modernization requires intense coordination of investments with inevitable tradeoffs. While agency mission leaders should have clear authority on “mission” system functions, such as benefits portals or supply chain systems, CIOs must have a clearer role in guiding choices on modernization funding and strategy. Because they have a vantage point over all agency enterprise systems, CIOs can weigh modernization decisions that will optimize the full portfolio of agency applications. This is especially important with strategies to coordinate cloud migration of mission and “enterprise” (i.e. computing centers) applications.

Highlighting this challenge, in the U.S. only about 20 percent of the \$92 billion the U.S. government spends annually on IT is devoted to modernization. Further, IT oversight scorecards show that even after years of legislative mandates to elevate and clarify CIO authorities, many CIOs still often lack authority to review IT contracts and evaluate their entire agency’s IT portfolio.

To shift the trend from patching legacy systems to a better ratio of spending on modernization and sustainment, **government CIOs should have greater authority to direct IT modernization investments, as part of a robust shared governance process with other agency chiefs.**

In addition to a sharper focus on modernization, governments must also find ways to stretch limited budgets. Governments should encourage and authorize agencies to use procurement models that employ multi-sector partnerships that allow non-government partners to assume short-term costs and share long-term savings. This should include more flexibility to fund rapid modernization pilots.

Tomorrow Ready IT infrastructure that is flexible, open, and cost-effective will make government nimbler and more responsive to society’s changing needs. And while government leaders have made progress modernizing IT systems, they can accelerate modernization by following the example of the private sector in adopting the hybrid cloud approaches at the center of a Tomorrow Ready approach. Government agencies do some of the world’s most mission-critical work, and they should have the flexibility to do it in the most cost-effective way possible with the technologies that make the most sense for their organizations.

IBM has proudly assisted governments in embracing new technologies for our entire history. We believe in Tomorrow Ready as the only effective way to drive long-term transformation of government technology because if IT modernization strategies are built around specific platforms, technologies, or a given public cloud model, they ultimately are putting a vendor first, not the agency mission. We welcome the chance to discuss the Tomorrow Ready policy framework in more detail with forward thinking government leaders worldwide.

Connecting public health surveillance systems across Canada

In Canada, the Panorama system connects dozens of legacy health surveillance systems across the country to allow better sharing of immunization records and vaccine inventories. Health care providers have better access to patient immunization records and public health leaders have better data needed manage vaccine supply in response to health events. Panorama covers more than 75% of the Canadian population and is available to all Canadian provinces.