Expert Insights

IBM **Institute for Business Value**

Government on open hybrid multicloud

Boosting both flexibility and security to enhance citizen services

IBM

Experts on this topic

Marc Fiammante

IBM Fellow
Global CTO Government, IBM
linkedin.com/in/marc-fiammante
marc.fiammante@fr.ibm.com

With his team, Marc Fiammante is addressing the practical, relational, analytical, and experimental aspects of the technologies that apply to governments, particularly the high-performing, highly secured hybrid cloud solutions with cognitive workloads. Marc's specialties are Watson, AI, public sector, police, and defense.

Chris Nott

CTO Government, IBM EMEA
linkedin.com/in/chris-nott-8840851
chris_nott@uk.ibm.com

Chris Nott wants to make citizens feel connected to government. With IT solutions that exploit the power of data using analytics and AI on cloud, Chris ensures that tax is spent on the right services by the right people. He has created an information exchange in defense to facilitate cross-force communications, has defined novel analytics patterns to optimize use of government resources, and is currently leading a cloud-enabled transformation.

Gregory Spargo

Associate Partner
Global Government Solutions Architect
linkedin.com/in/greg-spargo
gregspar@uk.ibm.com

Greg Spargo specializes in the business of government and applying emerging technology to improve services, public safety, security, and citizen experience. He brings experience of large-scale, technology-driven government transformation with an outcome-focused approach to deliver measurable value. His focus areas are hybrid multicloud adoption, digital transformation, and cybersecurity.

Dennis Stotts

IBM Distinguished Engineer
Global Government Cloud CTO
linkedin.com/in/dennis-stotts-77b1193
dlstotts@us.ibm.com

Dennis Stotts is the lead global technology executive responsible for IBM's cloud strategy for the government industry. Dennis is an innovative thought leader promoting the implementation of hybrid cloud, analytics, and IT modernization solutions to address transformation objectives for government organizations.

Open hybrid multicloud with confidential computing is a logical solution for governments, offering flexibility, and addressing security and cost concerns.

Key takeaways

Accelerated transformation

Governments have been accelerating their digital transformations over the past year. They are modernizing operations, automating business processes, taking measures to maximize tax receipts, and developing ecosystems to form novel services.

Balancing act

In building this new digitally agile architecture, governments are challenged to balance their infrastructure platforms' need for flexibility to support business model innovation and digital transformation with high security, privacy, data protection, and compliance requirements. An open, hybrid multicloud environment based on confidential computing (see "Confidential computing") is ideally suited for the government ecosystem.

Getting there from here

While the benefits of moving to a secure open hybrid multicloud are clear, the path—which workloads to move, and when and where to move them—is a bit muddier. An industry-tailored approach designed to prioritize workflows according to both technical and business criteria can help clear the way with a map toward success.

—

Governments' path to cloud

Governments typically target delivering the best possible services for their citizens by addressing user centricity and transparency. However, a bewildering array of technologies and development methodologies is advancing at a rapid pace. This opens up opportunities for governments to engage with citizens in new ways and unlock value from new technologies.

But as governments face generational—even existential—challenges, from the COVID-19 pandemic to climate change, how can leaders decide what's important and how to prioritize? In addition to a challenging macroeconomic environment, governments face ever-evolving demands for new and improved services and experiences from both citizens and businesses in the increasingly digital world.

Other industries are catering to those "customer" expectations through innovative business models that can reduce friction between industry value chains and spawn innovative ecosystems. Not surprisingly, citizens expect the same from their governments. At the same time, the continued proliferation of data, heightened compliance requirements, growing security threats, and changing workforce dynamics continue to impact the e-government services landscape.

In response, governments have been progressively transforming themselves, building new digital capabilities to compete in today's era of platforms. Similar to other organizations experiencing the shift to market platforms, governments face technology challenges associated with infrastructure, applications, processes, data, and customer engagement. However, governments also must contend with some of the most stringent standards involving industry security, protection from foreign intelligence, privacy and confidentiality, and compliance, all of which add further complexity.

Confidential computing[1]

Confidential computing protects data during processing, and when combined with storage and network encryption with exclusive control of encryption keys, it provides end-to-end data security in the cloud. It isolates sensitive data in a protected CPU enclave during processing. The data being processed—and the techniques used to process it—are accessible only to authorized programming code and are invisible and unknowable to anything or anyone else, including the cloud provider.

Insight: Defining open hybrid multicloud

Open hybrid multicloud is a foundational environment enabling effective digital transformation that integrates traditional computing platforms with private, public, and managed cloud services. In essence, a hybrid cloud becomes a virtual computing environment that aligns workloads and interfaces with the most appropriate computing platform. All these services need to be managed as though they were designed to behave as a single unified environment.

Confidential computing helps protect data in use by performing computation in a secure and isolated environment designed to prevent unauthorized access or modification of applications and data while in use, thereby increasing the security assurances for organizations that manage sensitive and regulated data.

Measures taken in response to the pandemic have forced big increases in remote working, virtual learning, and the use of online services. Furthermore, governments are taking the opportunity to modernize operations and automate business processes, take measures to maximize tax receipts, and develop ecosystems to form novel services.

For many years now, government leaders have been looking at cloud to meet their infrastructure needs for both business flexibility and the rigors required for security and compliance. According to a 2019 report on cloud usage in the industry, however, only a small percentage of government institutions are actively using cloud services today, mostly private cloud. As an example, only about 11% of US federal IT systems are running on a cloud.[2] In addition, very few mission-critical, regulated government or defense workloads have shifted to a cloud environment.

The scalability and agility available through a cloud-based infrastructure can better equip an organization to rapidly make adjustments and respond to situational changes, such as those associated with the pandemic. Pragmatic leaders are taking this lesson a step further with an open confidential computing hybrid multicloud approach, embracing multiple interoperable platforms that offer the combined security and flexibility required. A successful migration to an open hybrid multicloud environment requires examining, through the lens of the governments' unique requirements, which platform is appropriate for each application or service.

Traditional government systems are not particularly flexible, making it expensive to adopt new technologies or deploy new functionality.

Time for a change... in architecture

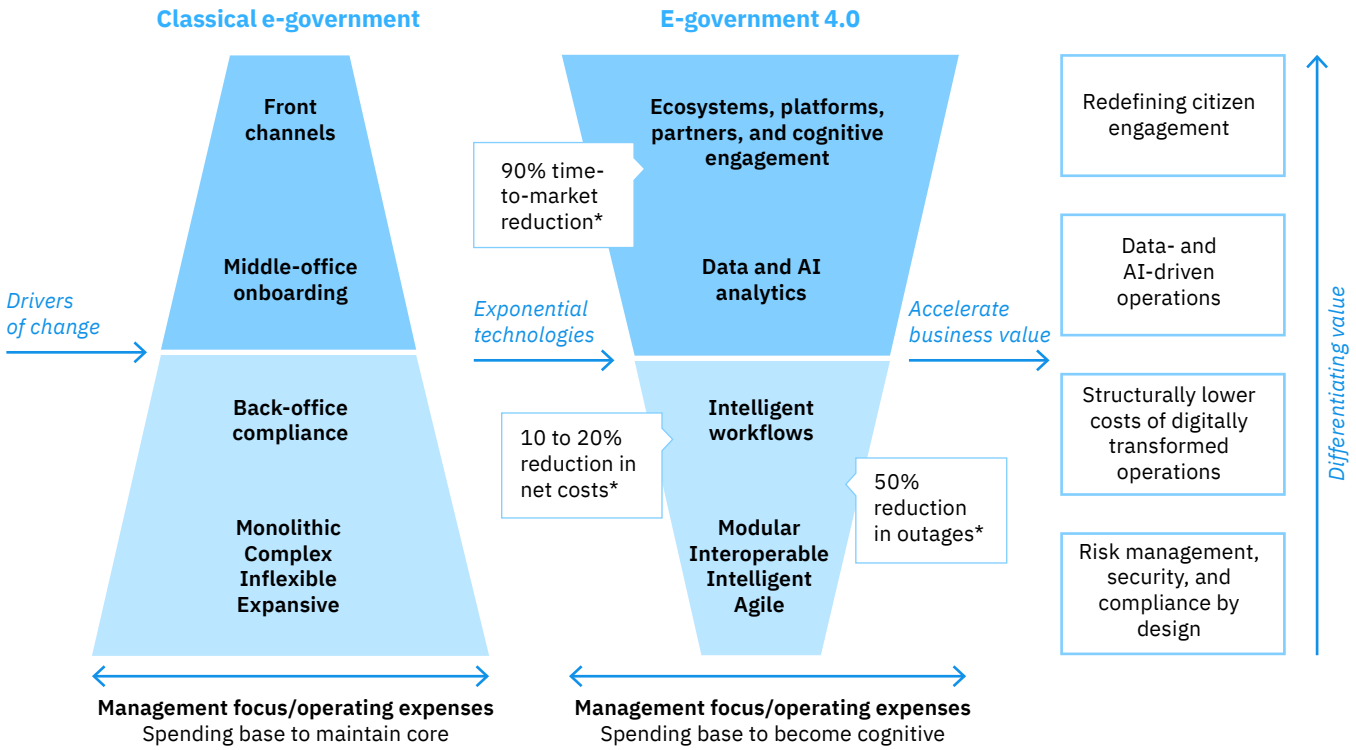
Today's governments are challenged to reshape the citizen's experience through new platform-driven engagement models while also lowering operating costs. Concurrently, they must remain agile to rapidly respond to changing situations and citizens' insights. This need for flexibility requires operational transformation to support continuous iteration and business model calibration. At the same time, government organizations must continue to optimize risk management, compliance, and security strategies, embedding them throughout their operations.

Meeting these challenges requires a new business architecture. Traditional industry models are not well-suited for today's digital reality, which is dominated by rapid innovation, customer centricity, and mobile-first interfaces. Monolithic and complex in nature, traditional systems lack flexibility, making it expensive to adopt new technologies and deploy new functionality. In addition, they drive a disproportionate amount of focus and operating expense on middle- and back-office activities, as opposed to those closer to the customer interface that can deliver higher returns on equity.

Essentially, traditional government systems don't support extended ecosystem engagement, AI-powered systems and processes, and intelligent workflows. Governments need to build new modular, interoperable, intelligent operating environments that embed risk management, security, and compliance in their core (see Figure 1).

Figure 1

Targeting a new government-to-citizen architecture



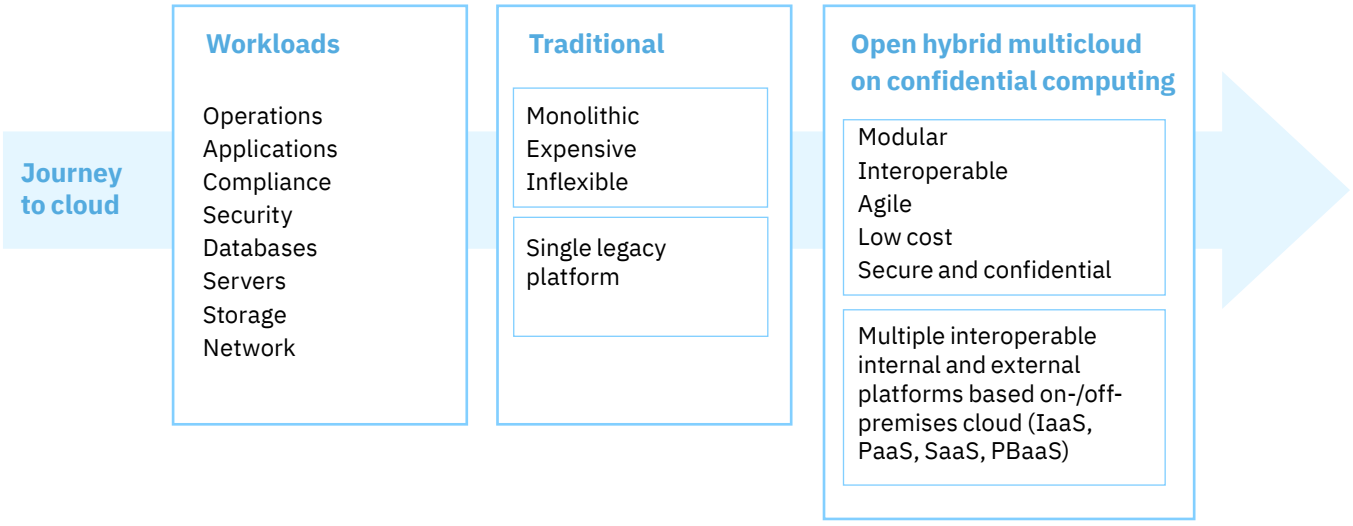
Source: "How public-sector tech leaders can speed up the journey to the cloud." McKinsey & Company. October 19, 2020

An open hybrid multicloud approach that includes a mix of public cloud flexibility and private cloud and on-premises security can provide the needed efficiency. Adoption of confidential computing across all clouds allows governments the freedom to extend beyond their data centers and into cloud services without restricting them to a single technical solution platform or provider. While delivering confidence in data privacy and confidentiality, this can help structurally reduce cost of operations, as well as balance ownership and flexibility with regulatory adherence. It also enables portability of workflows and data accessibility.

Successful migration to an open hybrid multicloud environment requires in-depth knowledge about the functional requirements of many industry workloads and the capabilities of different infrastructure platforms. These include infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), and public blockchain as a service (PBaaS, see Figure 2).

Figure 2

Migrating workloads to alternative cloud environments



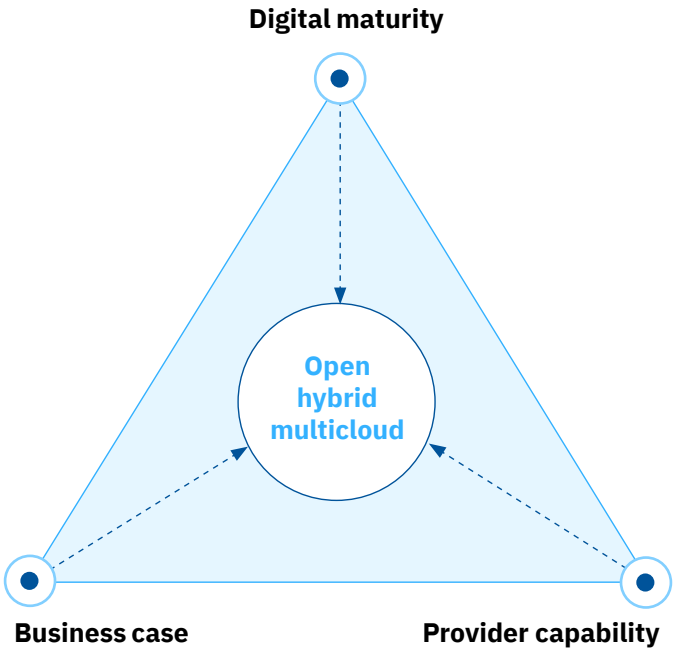
An open hybrid multicloud approach allows governments to extend into cloud services without restricting them to a single solution or provider.

Scaling migration hurdles

Part of building a successful digital transformation and workload migration strategy involves evaluating 3 key areas: business case, digital maturity, and provider capability (see Figure 3).

Figure 3

Migration considerations



Business case

Governments are challenged to strike a balance as they consider business needs against IT capabilities and constraints. On one hand, there is a need to transform e-government processes and reduce costs, risks, and complexities. On the other, there is an equally important need for flexibility to support business model innovation, ecosystem engagement, and rapid response. A key part of developing a migration strategy involves weighing the costs and benefits of a new platform against existing legacy investments and costs to migrate.

Digital maturity

Governments have to determine if they are truly ready for open hybrid multicloud. They have to evaluate their application portfolio and architecture and identify which workloads are candidates for decoupling. A high level of digital maturity typically corresponds with workload clarity and simplicity, making it feasible to decouple workloads into subcomponents and microservices that can run off different, yet interoperable, environments.

Provider capability

As governments consider migrating workloads to public cloud, a key hurdle involves finding hosting providers that can deliver the necessary operational requirements related to resiliency, responsiveness, security, privacy, and compliance. Governments have to identify providers that can offer an enhanced public cloud environment, with confidential computing, that is tailored to meet their industry-specific and workload-specific requirements.

Open hybrid multicloud for governments: A logical solution

The business logic behind an open hybrid multicloud approach centers around improving business performance while balancing business needs with IT requirements and cost constraints. Migrating to an open hybrid multicloud environment helps mitigate future costs to move (featuring high interoperability of cloud-native applications and workflows), while helping reduce new costs to build (leveraging security and legal compliance by design) and managing costs to run.

In addition to balancing short-term economics with long-term value and operational costs with business and regulatory needs, an open hybrid multicloud approach reduces dependency on any single provider or technology preference. Instead of being restricted to running all workloads on a single platform, performance can improve with various workloads on multiple interoperable platforms.

Open hybrid multicloud offers the flexibility necessary for business innovation and improved customer experience, while also addressing security and cost concerns (see "Perspective: Open hybrid multicloud strategy benefits for governments"). It can serve as the necessary foundation for a modern government architecture by enabling internal and external data accessibility, workload flexible portability, and effective interoperability of analytics.[3]

An open hybrid multicloud environment can help government organizations boost the performance of other exponential technologies to support business-critical functions:

- *Robotic process automation (RPA).* Automating repetitive tasks inside standardized back-office operations.
- *Artificial intelligence (AI) for customers*. Improving relationships based on chat assistants, voice assistants, and automated advisors.
- *AI for workforce*. Improving work efficiency with sales assistants, client insights, and knowledge centers.
- *AI for controls.* Facilitating compliance to improve know your customer (KYC), prescriptive security, and policy and regulatory gap assessments.
- *Application programming interface (API) platforms.* Enabling distribution and servicing of e-government services and offers across third parties and non-governmental ecosystems.
- *Quantum computing.* Elevating cryptographic standards and breaking analytics barriers in high-frequency trading and risk analysis.
- *Blockchain.* Rebuilding infrastructures with trust-based digital interactions.
- *Internet of Things (IoT).* Building a network of physical objects embedded with analytics connectors to streamline shipping, trading, and finance operations.
- *Augmented reality (AR).* Allowing citizens and civil servants to engage within the context of their current environments.
- *Fully homomorphic encryption*. Enabling governments to perform encrypted calculations on encrypted data without decrypting it first, enhancing the level of efficiency and interoperability of any secured process on open hybrid multicloud.

An open hybrid multicloud environment can help boost the performance of other exponential technologies.

- *5G for workforce.* Allowing civil servants to both work efficiently from home and run automated processes across multiple locations without deteriorating performance.
- *Edge computing.* Enabling governments to process data closer to where it's stored, which can reduce response time and latency issues while revealing more immediate insights from connected devices and systems.
- *Confidential computing.* Protecting data in use by performing computation in secure and isolated environments that prevent unauthorized access or modification of applications and data while in use. Doing so thereby increases the security assurances for organizations that manage sensitive and regulated data.

Achieving an open hybrid multicloud environment requires cutting through barriers to move workloads—whether infrastructure or software processes—from a traditional construct to cloud constructs. The issue is less one of "why" government organizations should aim for an open hybrid multicloud environment than "how" they achieve it.

How do you break through the barriers? How do you determine which workloads to move selectively? And then how do you know which cloud platform best meets the requirements of that workload?

Roadmap to open hybrid multicloud

For many governments, the journey to cloud has been a stairstep decision-making process. First, they built private cloud environments to "lift and shift" on-premises workflows within secured, compliant, and fully owned technical frameworks. The digital revolution then progressively revealed how operating on public cloud could reduce operational costs and increase access to external ecosystems. However, governments had security, latency, integration, and compliance concerns about environments that were not tailored to the industry.

Today, the shift to platform economies requires governments to rapidly interact across departments and with an ecosystem of providers, such as multinational organizations, independent software vendors (ISVs), and data and other functionality providers. The challenge has become how to benefit from ecosystem innovation without having to closely approve, trace, and remediate third-party interactions with their constituents.

As organizations consider an open hybrid multicloud approach, the key question then becomes how to determine what functions sit on which platforms. The goal, obviously, is for each of the various environments to handle what it does best, with each workload in the right place for reduced risk and increased agility.

This requires not only looking at the puzzle from a technical point of view, but also considering the business objectives. An organization has to make decisions about which workloads to prioritize for public cloud, which ones to prioritize for private cloud, and which to leave on a more traditional platform. They also need to separate what can be done—in terms of ease and feasibility—from what should be done from a strategic standpoint.

Perspective: Open hybrid multicloud strategy benefits for governments

Cost reduction. Government organizations are better able to scale their data needs in real time, avoiding the expenses associated with maintaining a great deal of unused digital capacity.

Citizen experience. Governments can quickly move digital resources where they are most needed, allowing for swift response to shifting citizen demands.

Business innovation. Open hybrid multicloud enables consistency and portability of business-critical analytics, applications, and processes that can be used to design, mix, test, and deploy new solutions according to citizens' categories and geographical demands—where and when they are needed.

Security at core. Security threats change constantly, and an open hybrid multicloud infrastructure can provide access to confidential computing and AI-powered defense tools specifically designed for governments.

Aligning workloads with platforms

Making these decisions requires an industry-tailored approach and framework to evaluate workflows and determine the appropriate operating environment. By evaluating workloads according to industry-specific benchmarks, a government organization can align and prioritize each workload with an optimal platform—traditional, private cloud, public cloud, or public cloud designed to support a workload's unique requirements. Both operational and business criteria should be considered in workload evaluation, including resiliency, responsiveness, digital maturity, risk, security and compliance, and business case application.

The first step in evaluating workloads is actually defining the industry activities and processes that drive application workloads. While every government will have some customization and organization of operations, we find significant consistency across the industry. There are some government frameworks, open or proprietary, that could be leveraged as proxies for government workloads and serve as a starting point for a government's specific workloads. Such framework examples are from the European Interoperability Reference Architecture (EIRA) or North Atlantic Treaty Organization Consultation, Command, and Control (NATO C3) Taxonomy.

Discussions surrounding open hybrid multicloud for government are shifting their focus from “why” to the more complicated issue of “how.”

Once workloads have been identified, a robust multicriteria evaluation framework can be applied to them to determine the optimal platform for each workload. The evaluation criteria must evaluate critical elements such as:

- *Resiliency.* Evaluate the volume, stability, and business criticality of the data and transactions involved.
- *Responsiveness.* Consider the latency, response, and service requirements associated with the workloads.
- *Digital maturity.* Evaluate the evolution of the government institution’s digital transformation from monolithic operations to modular services. Workloads more easily decoupled from other workloads without loss of interoperability are candidates for migration.
- *Risk, security, and compliance.* Gauge the regulatory requirements and security features associated with a workload. These can vary significantly depending on a government’s security posture, and geographic and segment regulatory regime.
- *Business case.* Examine expected investment requirements, cost and revenue benefits, and potential impacts on competitive advantage and disruption.

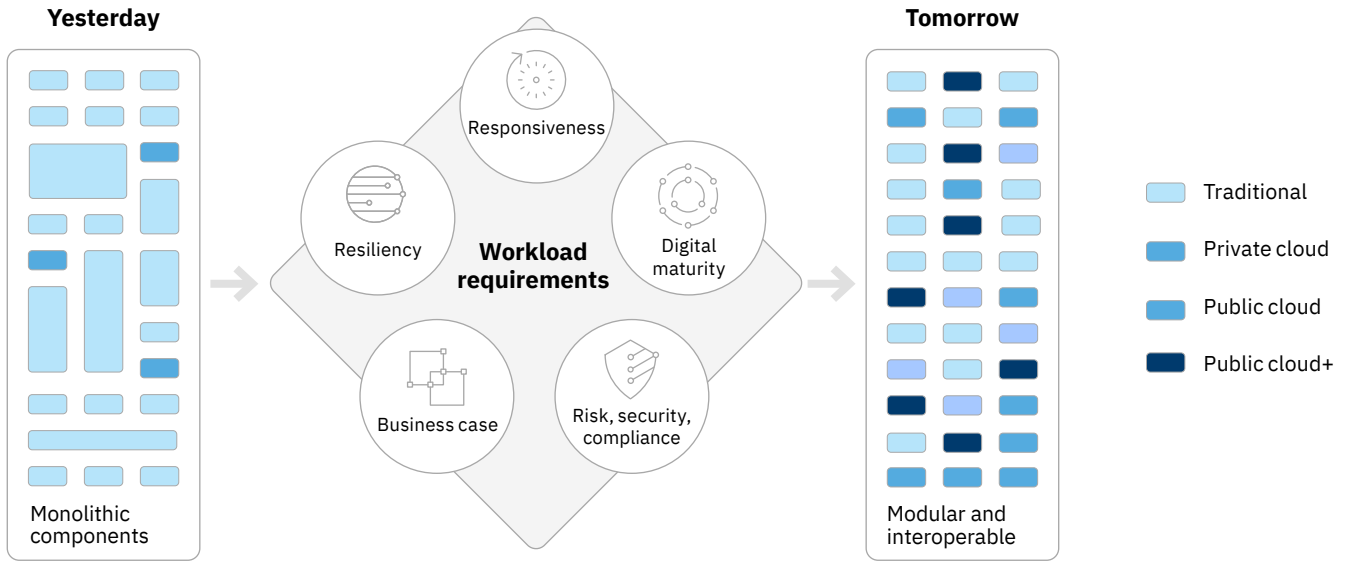
Every government institution organizes itself differently. So, the specific number of workloads will vary, but most government organizations will face decisions on several hundred workloads. Using the appropriate operational and business criteria, they can determine the most appropriate platform for each. The end result is a map defining which type of environment is appropriate for each workload or decoupled workload component (see Figure 4).

Each governmental organization must make its own individual decisions about how to configure and manage the sub-components of its operations and how much flexibility is built into the open hybrid multicloud setup it deems most advantageous. The evaluation criteria can help guide their decisions, identifying and mitigating real and perceived hurdles.

Clearly, cloud computing is more than just a technical infrastructure. The symbiotic combination of workload complexity, modernized applications, development methods, and cost-effective managed services enables digital transformation and secured platforms, while still enabling ecosystem engagement.

Figure 4

Evaluating workloads for migration to open hybrid multicloud



Forging ahead

Most government organizations are well aware of the flexibility, agility, integration, and scalability benefits of an open hybrid multicloud approach. Discussions surrounding open hybrid multicloud for government are shifting their focus from "why" to the more complicated issue of "how."

As they accelerate their journey to cloud, governments are challenged to balance the costs and benefits associated with a new platform against the cost to migrate and existing legacy investments. They also have to ask themselves if they are ready from a digital maturity standpoint as they consider which workloads are mature enough to decouple. And they have to find cloud providers that can deliver on industry-specific operational requirements and allow for interoperable platforms.

The road from recognizing the need for a new business architecture to successfully executing an infrastructure migration and application modernization can appear bumpy. However, with the right roadmap, government organizations can make the necessary move to open hybrid multicloud, transforming themselves into agile organizations fueled by data, guided by AI insights, and built for change.

Action guide

Government on open hybrid multicloud

Below are key steps to develop a strategy that balances flexibility with your security and compliance requirements. Consider a "big picture" view of the considerations related to a large-scale migration of processes to alternative cloud environments.

- *Evaluate your organization's digital maturity.* Determine your organization's digital maturity and identify what is possible, what is practical, and what is prudent from a technology standpoint.
- *Investigate provider capabilities.* Identify providers that can deliver the capabilities required through an enhanced industry-tailored cloud environment.
- *Define industry activities and processes.* Identify the operations—several hundred—that drive application workloads.
- *Build a framework.* Group these applications and services into the appropriate area: business development, distribution, production, operations, business infrastructure, or financial and risk management.
- *Evaluate workloads.* Determine the optimal platform—or operating environment—for each workload using business and operational evaluation criteria: resiliency; responsiveness; digital maturity; risk, security, and compliance; and business case.
- *Map each workload to its optimal platform.* Based on the evaluation criteria, determine the right environment for each workload for reduced risk, increased agility, and so on.

Notes and sources

1 Confidential Computing Consortium. Accessed June 14, 2021. https://confidentialcomputing.io; Nagaratnam, Nataraj. “Confidential Computing.” IBM Cloud Learn Hub. October 16, 2020. https://www.ibm.com/cloud/learn/confidential-computing

2 “Cloud Computing,” Table 2. United States Government Accountability Office. April 2019. https://www.gao.gov/assets/700/698236.pdf

3 “The European Commission adopts a new Cloud Strategy.” European Commission. May 28, 2019. https://ec.europa.eu/info/news/european-commission-adopts-new-cloud-strategy-2019-may-28_en

About Expert Insights

Expert Insights represent the opinions of thought leaders on newsworthy business and related technology topics. They are based upon conversations with leading subject matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America
July 2021