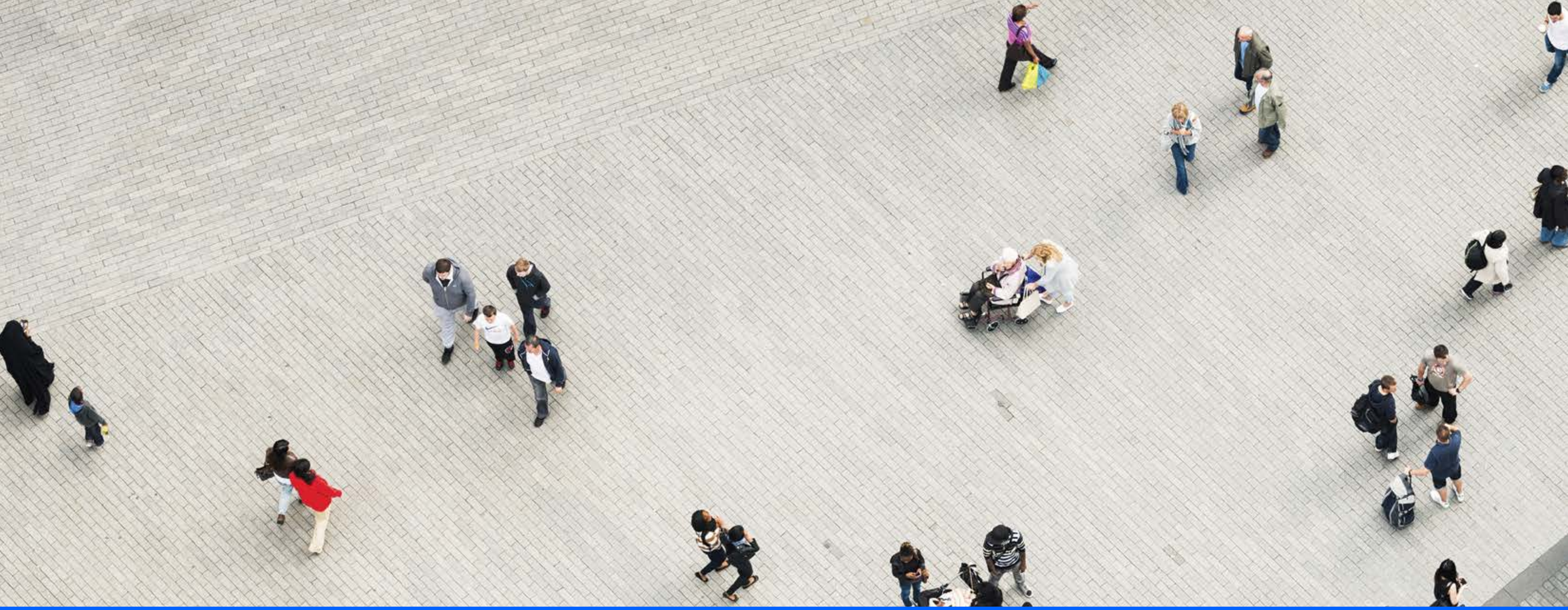
Transforming government with cloud technologies

IBM



Contents

Get started >

1.Introduction

The cloud is ubiquitous. Whether we think about it consciously or not, almost all of us are using cloud services. That could be a music service such as Spotify, storage such as Dropbox, communications via Gmail, or a software-as-a-service application such as Salesforce. Cloud services touch all of our lives.

But these examples only hint at the importance and impact of the cloud. Cloud technologies such as infrastructure-as-a-service and platform-as-a-service are redefining how government information technology organizations develop and deliver solutions to employees and citizens. By leveraging the cloud, government can become more efficient in its use of technology, and can innovate more quickly and effectively to advance its mission.

IBM has helped thousands of organizations securely and successfully leverage cloud capabilities. We know that it’s not easy. Government organizations, especially, are faced with seemingly never-ending budget pressure, legacy systems, and workforce challenges. We’ve seen clients struggle to formulate a successful cloud adoption strategy, and we’ve worked with them to overcome the hurdles in implementing that strategy.

For most agencies, the initial forays into the cloud were ad hoc efforts. Basic applications were moved to a cloud-based infrastructure in order to cut costs, or application teams circumvented their own IT departments to directly access cloud services. As a result, government IT environments are often composed of isolated silos with little communication between them.

According to our research, only about 10 to 20 percent of government workloads have moved to the cloud.[1] While some agencies are already enjoying the efficiency and agility that a multicloud environment can yield (see figure 1), the majority are still unsure how to tackle modernization. Agencies tell us that they are wrestling with the process of merging existing assets—such as infrastructure, applications, workloads and data—with cloud-native efforts.

But there's no doubt that the cloud has arrived. Agencies are already running an average of two to five clouds.[2] To enable greater security and accelerate innovation to advance their missions, agencies need to be able to move and manage data, services, and workflows seamlessly across their on-premises and cloud environments.

As with any strategic shift, there is no one-size-fits-all strategy to help governments move seamlessly and efficiently to the cloud. Instead, each organization will move at its own pace, making its own decisions about how various clouds can best fit their particular needs, today and in the longer-term. Significant technological and process challenges will have to be overcome. For governments, as for any organization, cloud adoption is a journey.

This ebook is for those who are—or aspire to be—catalysts for digital transformation in their organizations. It's inspired by a book, *The Cloud Adoption Playbook: Proven Strategies for Transforming Your Organization with the Cloud*, written by our colleagues Moe Abdula, Ingo Averdunk, Roland Barcia, Kyle Brown, and Ndu Emuchay, and to whom we are most grateful for their contributions.

Both book and ebook are based on IBM's years of experience helping thousands of organizations leverage the cloud's capabilities and securely transform their IT organizations to best achieve their objectives. The ebook focuses on critical contemporary issues in cloud adoption, such as strategy, architecture, security, governance and hybrid, multicloud approaches. Our hope is that this ebook will help guide you in deciding how to continue on your cloud journey, which important dimensions need to be considered, and how to make holistic decisions that improve your chances of success while reducing risk.

Multicloud usage improves government performance

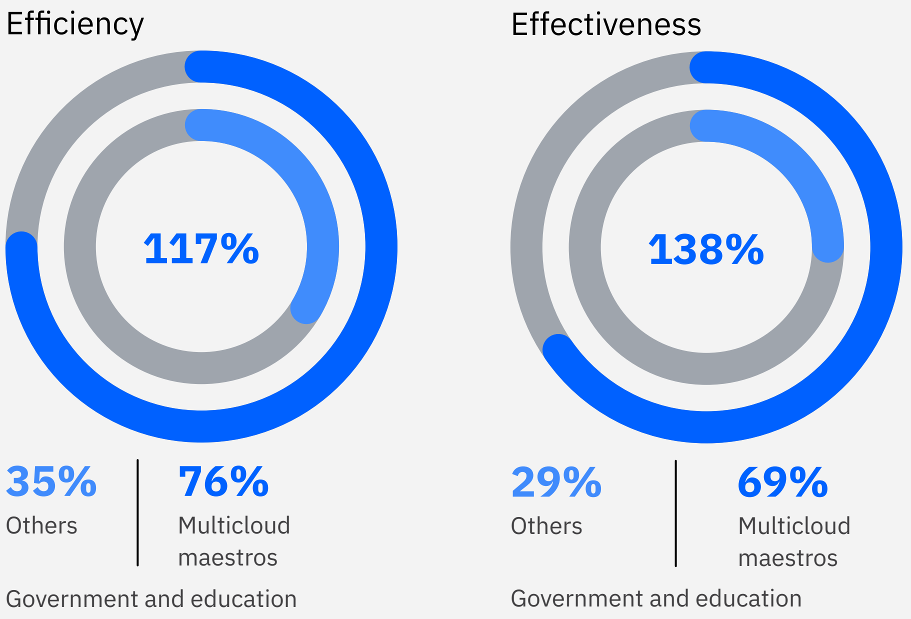


Figure 1: Government and education multicloud maestros are organizations that routinely use multiple clouds to deliver business functions and they outperform peers who do not.[3]

Source: Percentages reflect government and education survey respondents asked to rate the efficiency and effectiveness of their organization compared with their peers over the past three years.

Learning the lingo: Talking about cloud technologies has become so common that it’s easy to forget there are real definitions behind the terms.

Cloud computing

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider or service provider interaction.[4]

Private cloud

A model of cloud computing where IT services are provisioned over private IT infrastructure for the dedicated use of a single organization.

Public cloud

A cloud computing environment in which access to standardized resources, such as infrastructure, multi-tenant hardware, and services, is available to subscribers on a pay-per-use basis.

Hybrid cloud

A cloud computing model in which an organization uses a combination of on-premises, private cloud and public cloud technologies and architecture.

Multicloud

An approach to cloud computing utilizing more than one cloud service, public or private, from more than one cloud vendor.

2. The cloud advantage

As the cloud market has matured, the advantages of cloud adoption have multiplied. Although the cloud may first have been seen as a means to cut costs, it now offers broader, more strategic benefits to support government missions.

Cost savings

Government is constantly asked to do more with less, and cloud technologies can help agencies accomplish this. Creating real efficiencies, though, requires that you go beyond simply shifting the cost burden. Swapping decreased capital expenditures for increased operating expenditures may not ultimately save money. Eliminating redundant infrastructure or unneeded software licenses will.

Speed and agility

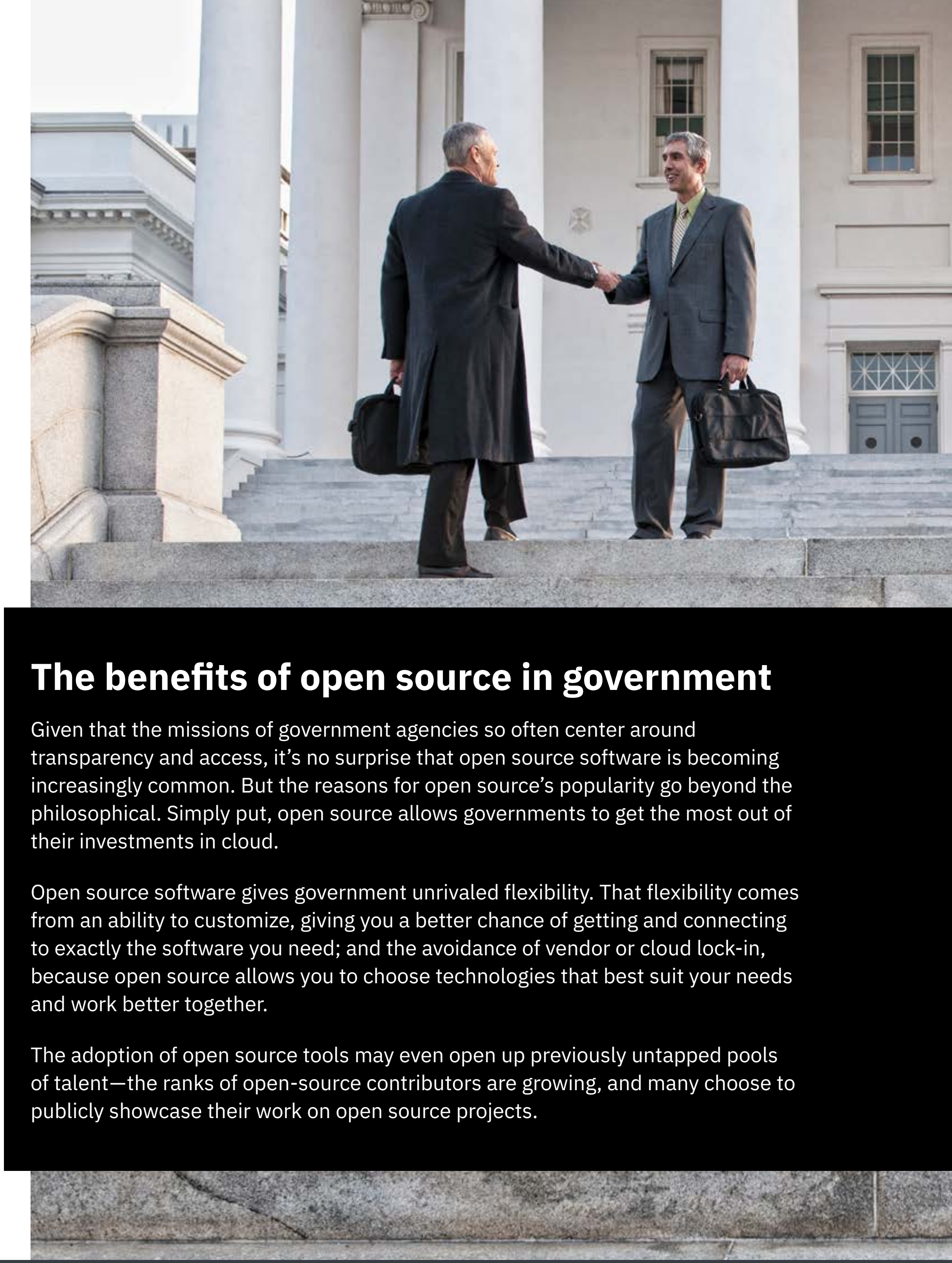
Whether it's a proof-of-concept or a new application under development, cloud technologies allow agencies to innovate and react to change more quickly. They also enable agencies to more nimbly respond to new business and mission realities.

Better services for citizens

Citizens expect the same level of digital services from government as they do from private enterprises such as Apple or Netflix. Hybrid capabilities enable agencies to integrate existing on-premises investments with cloud services such as analytics and artificial intelligence. The result: innovation that improves the user experience for citizens and employees, and accelerates time to value.

Consistent application management

Agencies' IT environments are becoming increasingly complex as they build new apps in the cloud, adopt software-as-a-service, and migrate and modernize existing apps to run on an increasing range of clouds and vendor platforms. Open, cloud-native standards and multicloud management tools enable continuous delivery of new features and ensure consistency in service quality and security.



The benefits of open source in government

Given that the missions of government agencies so often center around transparency and access, it's no surprise that open source software is becoming increasingly common. But the reasons for open source's popularity go beyond the philosophical. Simply put, open source allows governments to get the most out of their investments in cloud.

Open source software gives government unrivaled flexibility. That flexibility comes from an ability to customize, giving you a better chance of getting and connecting to exactly the software you need; and the avoidance of vendor or cloud lock-in, because open source allows you to choose technologies that best suit your needs and work better together.

The adoption of open source tools may even open up previously untapped pools of talent—the ranks of open-source contributors are growing, and many choose to publicly showcase their work on open source projects.

3. Strategy

To fully reap the benefits of this transformational technology, you need a deliberate, holistic strategy to support consistent cloud adoption across the enterprise. Your cloud strategy needs to consider mission needs and goals, your team's capabilities, and government's unique responsibilities with regard to trust and security.

Agencies need to consider lift, shift & optimize. Lift and shift is a good first step and should be followed by optimization of both data center and workload consolidation. Once in the cloud, agencies can realize the true value of cloud technology by refactoring applications into containers and microservices to achieve automation and manage higher density with DevOps. More on this later.

The lift & shift conundrum

One common approach for government has been to lift and shift applications to the cloud. It's an appealing approach for any government entity thinking about cloud adoption—it offers a fast, less resource-intensive way to move your workloads to the cloud. But it's rarely simple, and, by itself, it won't lower costs or bring other benefits such as consolidation or standardization.

Five steps to develop your cloud adoption strategy

No matter where your organization is along its cloud journey, the following five-step cloud strategy approach will establish a road map to achieve your vision for a transformed enterprise.

As you work through each step, keep a few things in mind. First, the cloud is a means to an end. It's a delivery platform for new capabilities. Your most important task is to define that end—the mission and business goals you want to achieve. Next is to understand that a cloud transformation, like any similarly ambitious initiative, is a journey that evolves over time. This isn't going to be achieved in a month or even a year. Yes, you'll want some quick wins on the board, to build buy-in and fortitude. But you're in search of strategic outcomes that will serve you well over the long haul. As you begin to adopt cloud more thoughtfully, you will also need to establish organizational structures, policies, and procedures that will support your long-term goals.

1 Define mission and business objectives and constraints

What do you hope to accomplish with cloud technology? The answer will define your organization's vision for digital transformation. It will also define your organization's priorities, and how they will be addressed. Given the unique missions of groups even within single government departments, there will be many objectives for what can be achieved. Cloud offers opportunities to break down silos—or at least work across them—to gain clarity on what is needed for a strategy to be viable. Remember that it's just as important to acknowledge regulatory and cultural challenges as it is to define the grand vision.

2 Complete analysis of your workload portfolio

The next step is to analyze your workloads, a capability or combination of IT capabilities and services that can make up an application. The goal is to identify and prioritize workloads to move to cloud. Some workloads will qualify as immediate quick wins that will help build evidence and gumption needed to support more complex, long-term efforts. Other workloads will require more planning to ensure optimal performance: perhaps the data stays in an on-premises data center but is accessed via an API and front end that is built specifically for the cloud. (For a deeper dive into workload analysis, see Architecture & technology).

Importantly, some workloads and applications won't be good candidates for the cloud. But all legacy applications can be extended into the cloud. For workloads that are hard to enhance or extend and are difficult to maintain and secure, moving to the cloud is an opportunity to embrace new, modern capabilities. On the other hand, complex applications that don't lend themselves to lift-and-shift can either be exposed through hybrid cloud services (i.e. API's), or moved into a managed cloud environment, where they can be integrated with cloud native services to extend their life.

3 Envision your future state and analyze your current state

Once you've agreed on goals, identified the obstacles, and determined which applications and workloads will be transitioned to cloud, conduct a gap analysis of your current and future states. Focus on the value you want to create for end-users. This aligns stakeholders around improving the user experience. In understanding the current state, it is critical to take a holistic, cross-functional view of your proposed transformation. For example, how long does it take a citizen or employee to complete a task? By examining an end-to-end process flow, you can begin to see where your bottlenecks might be.

4 Assess your organization's readiness

To make sure you can actually execute on your strategy, you need to shift your attention to the dimensions of organizational readiness:

- **Cultural readiness**. Culture, as we all know, eats strategy for breakfast. Stakeholder buy-in, the ability to accept risk, new collaboration models, and new organizational models are all part of getting the most value from the cloud.
- **Resource readiness**. Can you achieve your goals on time, using existing resources? How well do you understand your current commitments? Especially in the early stages of a transformation, outside partners can be an important resource.
- **Budgetary readiness**. Expectation management is critical here. Make sure you can show how early investments in cloud will lead to lower total costs of ownership and contribute to government transformation over the long term.
- **Technology readiness**. Technology readiness goes beyond workload assessments. Use a methodical approach to assess your readiness in terms of architecture, infrastructure, platform, and your entire ecosystem of third-party-supplied services.
- **Process readiness**. Process readiness begins with the changes your IT team needs to make in the way they build, run, and manage apps. It extends to security, compliance, risk, finance, legal, human resources, procurement, service desk, and operations.

5 Build an execution roadmap with defined strategic milestones

This roadmap will outline your key activities and technology investments and lay the groundwork for realizing your cloud vision. Your roadmap serves as a baseline for reviewing the plan with various stakeholders. It should be updated as priorities shift or as execution changes. We recommend that the road map be reviewed every 90 days and adjusted to accurately reflect the progress made.

4.Culture and organization

Organizational culture is the combination of shared values, beliefs, and social norms in an organization, resulting in the behaviors, practices, and customs followed by members of the organization. And it can make or break your cloud transformation.

Many agencies adopt cloud to lower cost, drive innovation and improve citizen services. But they don't always understand the elements of their existing culture that are needed to make cloud adoption successful. There are four specific cultural factors that will either hamstring or propel your efforts.

Willingness to embrace change

Some organizations view the ability to quickly embrace change as an asset that allows them to nimbly respond to changing business conditions. Others are more deliberative. Teams that embrace change often embrace too much of it, too quickly, and don't give changes time to work. If failure seems imminent, they may reject all the changes at once. Teams that are overly deliberative often fall into analysis paralysis.

To avoid either extreme, use your strategy as a guide and encourage experimentation and learning. Embrace incremental change and follow a data-driven decision process. Before adopting a change, identify the benefits you hope to gain and the metrics you'll use to measure them.

Decision-making style

Decision-making often arrives as one of two extremes. Centralized decision-making tends to be top-down and hierarchical, with clear roles and responsibilities. Decisions can be made quickly, but as they move up the chain, they can lose their grounding in necessary local and specialized knowledge. Consensus-driven decision-making is found at different levels of government and is where everyone feels that their voice has been heard.

In both scenarios, teams need well-defined levels of autonomy. They need to know which decisions they can make on their own, and which need to flow upward. Even within a consensus-based approach, teams need to be able to end debates, break ties, and move on.

Attitude toward risk

A culture of caution becomes a hallmark of an organization when any deviation from tried-and-true processes can be subject to scrutiny by regulators, auditors, or even peers. This attitude can extend to the smallest decisions, with the team (understandably) refusing to try anything new. Other organizations have a fear of missing out. Every decision becomes an excuse to experiment with the latest and greatest technology or fad, making consistency elusive.

The solution is to encourage local autonomy on small decisions, but with enough consistency to allow teams to work together. You also want to conduct controlled experiments: Define boundaries of each experiment in terms of time, money, and resources. That limits your losses if an experiment doesn't work out.

View of failure

Closely related to an organization's view of risk is its view of failure. For the other three cultural factors discussed here, an organization can successful even if they are near either of the competing poles. This is not true of an organization's view of failure. Some organizations view failure of any sort as a personal shortcoming. That makes it nearly impossible to adopt the new technology and new policies that align with agile DevOps and cloud deployment models.

Organizations need to view failure as something that both people and organizations can learn from. Only if small failures are viewed as learning experiences can a team move on to larger, more ambitious experiments with potentially larger payoffs.

5. Architecture and technology

As cloud technologies have matured, it's become appropriate to regard "the cloud" more as set of capabilities than as a location that hosts data and code. To take full advantage of the cloud, it's necessary to understand and carefully manage the relationship between various deployment models, workloads, and cloud-native technologies. This is especially true for agencies trying to modernize monolithic legacy applications.

Deployment models

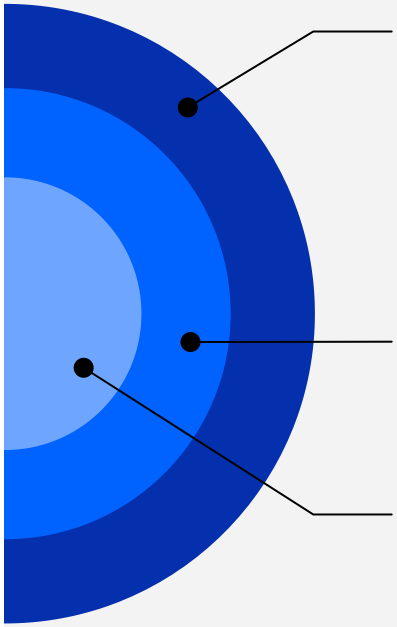
Government organizations are more likely to meet their mission and business needs if they're able to carefully select the particular cloud platform best suited for each workload. The evolution and maturity of cloud computing has led to a diversity of deployment models, starting with public and private clouds—although the divide between the two is becoming increasingly blurry. Public and private are further delineated into shared public, dedicated public, hosted private, managed private, and on-premises private. Different workloads are best-suited to each.

Particularly notable is the emerging space of private cloud, or a cloud operated solely for a single organization. Even for on-premises deployments, agencies are moving from virtualized or traditional on-premises environments to containerized private clouds. This can be a safe first step for many agencies on the road to a hybrid cloud environment. Private clouds can be managed internally or by a third party and hosted externally.

A private cloud may be especially suitable for workloads that face regulatory and legal requirements. Private cloud offers the benefits of a public cloud, including rapid deployment, scalability, ease of use, and elasticity. But private cloud gives organizations greater control, predictable costs, tighter security and flexible management options.

Figure 2 illustrates which types of workloads commonly run on public and private clouds, and which might be better left in place but exposed through APIs.

Cloud model



Public cloud

- DevOps
- ERP
- Front office/desktop
- Backup & archive
- Big data & analitycs
- Risk & compliance services
- Disaster recovery
- Customer service

- Third-party applications
- Web applications & e-commerce
- Development & test workloads
- Enterprise social solutions
- Isolated compute workloads
- Mobile applications
- Noncore business processes
- Digital experience solutions

Private cloud

- Mature workloads
- Existing database workloads
- Workloads needing low latency on back ends

- Applications with sensitive data
- Regulation-intensive applications
- Information-intensive applications
- Batch processing

Maintain & evolve

- Applications with complex processes and transactions
- Highly customized applications
- Not yet virtualized applications

Workload type

Figure 2: Which types of workloads should run on a public cloud or private cloud, and which ones can be left in place and exposed through APIs.

If your organization is like most in government, you'll find that a combination of cloud providers and clouds—public, private, software-as-a-service—best suit your needs. Often, organizations choose public clouds to develop applications; private clouds to maintain the highest levels of security and availability for mission-critical data and processes; and, in many cases, traditional on-premises IT for highly custom or complex applications. Such a hybrid platform can enable consistent management of applications, improved security, efficiency, and governance.

Analyzing your workload portfolio

Some workloads will migrate, some will be modernized, and some will need to be reconceptualized. Some won't currently be good candidates for the cloud at all. Each process requires a different level of effort and cost. This assessment, and the process of matching the right workload to the right deployment model, represents one of the most critical elements of any cloud strategy.

We recommend a two-level approach to assessing your workloads. This will help you determine the right cloud deployment model for each. You will want to look at your existing workloads as well as those on your roadmap, and include both applications and data. You'll first analyze the workload itself, and then consider available migration strategies.

Your initial questions will address mission or functional value:

1. **What is the real cost benefit of moving these workloads to cloud?**
2. **How will any move affect the ecosystem?**

Next, you should consider the risk profile of moving workloads:

3. **What existing (known) risks could this move exacerbate?**
4. **Are there new categories of risk that my organization might be exposed to?**

Finally, you should consider the technical aspects:

5. **Does the workload require strong controls to meet compliance or regulatory requirements?**
6. **Is the application designed in a way that is compatible with cloud services?**
7. **How self-contained is the workload? Is it technically feasible to "disentangle" the application from others?**
8. **What are the data transfer requirements?**

Your organization may have hundreds of applications. Auto-discovery tools can be a huge help in assessing your applications and estimating how easy—or difficult—it might be to move a particular workload to the cloud.

Migration strategy

Once you decide that a workload is a candidate for cloud deployment, the next challenge is to choose a migration strategy. The three main application migration strategies are to migrate, modernize, or innovate. You'll also need to consider your data as part of any migration strategy.

Migrate:

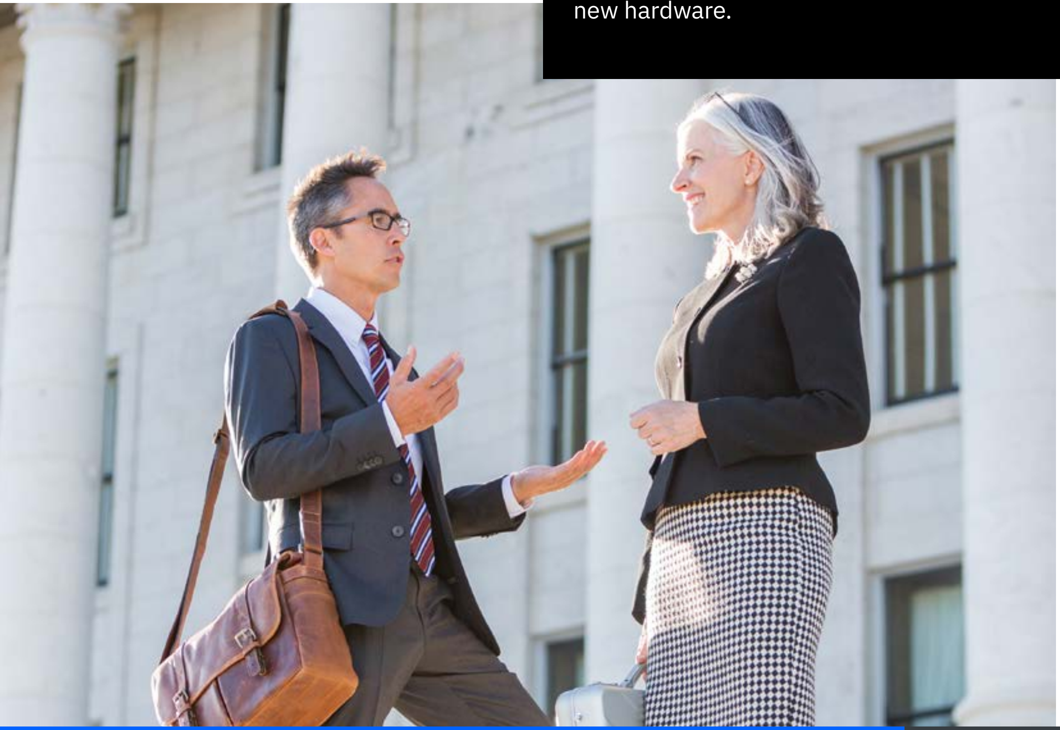
Migration is the process of lifting and shifting existing applications or data to the cloud, without redesigning them. This method is most often used for less complex, off-the-shelf applications that do not have extensive dependencies, such as email. The advantage of this approach is that, by renting cloud infrastructure or storage, it typically avoids the purchase of new hardware.

Modernize:

To modernize an application, your team will rewrite some or all of it to run on the cloud in a more native way. For example, by using containers and microservices, you're essentially making the application easier to update and easier to move.

Innovate:

This is the process of building new applications in the cloud or extending existing on-premises applications by leveraging new cloud-based features. These applications are increasingly built to be cloud-native, in that they are designed specifically to run in and benefit from cloud environments.



Keep in mind that innovating and migrating are relatively straightforward processes and provide agencies with easy entry points for their cloud journey. Modernizing is a somewhat more complex process, but it takes agencies to the next level on their cloud journey—advancing their mission and tapping into higher-value services.

As agencies increasingly build new apps on the cloud, adopt software as a service, and migrate and modernize existing apps to run on an increasing mix of clouds and vendor platforms, multicloud and hybrid management become critical. Organizations must adapt tools, processes and skills to enable continuous delivery of new features and ensure the same level of service quality and resiliency.

Cloud native technologies

Government, or anyone else, won't get the complete benefits of cloud technology without using containers and microservices. Microservices and containers are a fast-emerging industry standard that give you flexibility and portability to move data and workloads in and out of different clouds, to deploy more quickly, and to manage applications and data across environments.

Microservices belong to a type of architecture in which your applications are split into component pieces, each of which performs a specific fine-grained function. Microservices run inside containers, which include everything a microservice needs to run, such as code, dependencies, and libraries. Containers provide optimal portability across cloud and on-premises environments.

Container platforms provide a system for automating deployment, scaling and management of containerized applications. Kubernetes has become the de facto standard for container orchestration across cloud platforms.

You'll want to look for a multicloud management platform using Kubernetes, which will help your organization build a private cloud, and access cloud services quickly and securely.

It can be helpful to compare microservices to the older monolithic development style of applications, where all of an application's components and functions are in a single instance.

Many government applications are still essentially monoliths. Agencies should try to identify applications where microservices could be used to improve performance. In these cases, the application should be incrementally broken down into smaller deployable components. A container and microservices based architecture used consistently across on-premises, private, and public cloud environments provides the ability to seamlessly and securely run workloads across any cloud platform while using a vendor's cloud services, thereby increasing interoperability and helping avoid the risk of vendor lock-in.

Monolithic architecture vs Microservices architecture

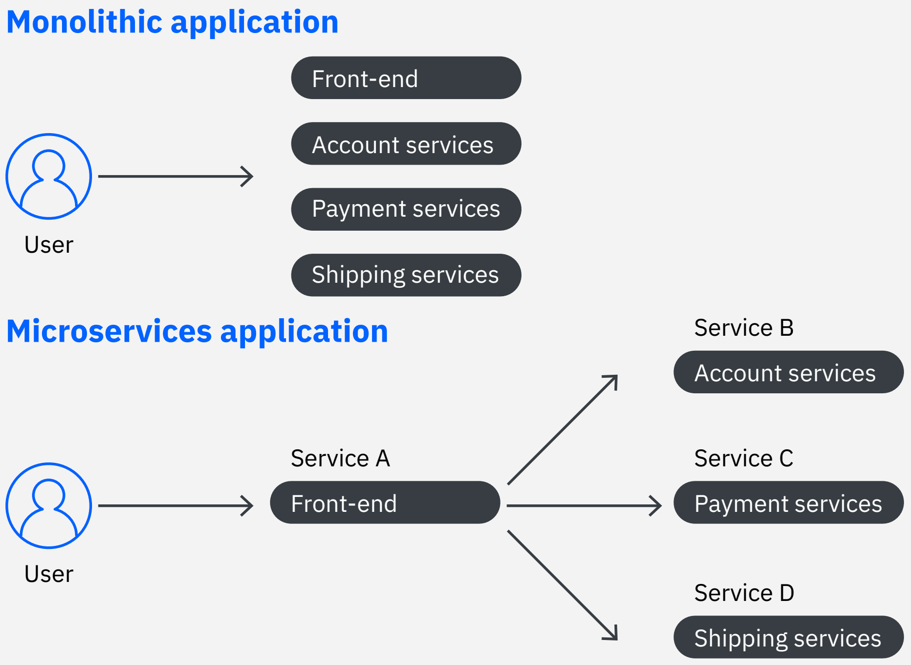


Figure 3: A microservices architecture splits your application into multiple services that perform fine-grained functions. Microservices is a more modern approach in an application's architecture compared to a monolithic architecture where all your application's components and functions are in a single instance.

6.Security and compliance

Security and compliance are two of the most crucial, yet misunderstood, requirements of any cloud migration. While the cloud requires you to think differently about security, with proper planning and execution, the cloud can be made more secure than your on-premises environment. Here, your security team is your partner. They'll help you think through the security implications of the particular data being collected, and the functions of the particular application.

The foundation of a secure cloud environment is a solid knowledge of data and workloads. What are the contents? Are those contents governed by regulations? If so, what are the requirements of those regulations?

Using a reputable cloud vendor enables you to pass along some security concerns, because the vendor will perform maintenance and upgrades, significantly reducing risk. Containers also strengthen security. That's because access to containers is controlled, and because they are write-once, read-many, requiring the creation of a new container to make changes.

Compliance, security and cloud adoption

Compliance, in general, means conforming to a set of standards. For security in the cloud, the theory goes that if agencies adhere to standards that aim to mitigate cybersecurity risks, they will be secure. If security is a lock on a door, compliance is knowing that there is a lock.

In reality, just because you are in compliance doesn't necessarily mean you have adequate security. Security requirements change quickly, but compliance does not. Compliance will tell you what is necessary in certain situations, but it isn't designed to cover everything. Your security team needs to be proactive, rather than waiting for mandates to be handed down from compliance. In the cloud, both security and compliance must be managed in cooperation with your cloud provider.

In today's world of increasing cyber threats, security needs to come first. The lock on the door may be compromised even if your organization is in compliance. Both security and compliance must be regularly reviewed and should be managed in tandem.

Six true or false questions about security

Your processes, tools, and approaches need to adapt to a cloud environment. You'll need to test your assumptions about security as well.

1 Everything is contained within your network

False This is not true in the cloud. If you're running anything on the internet, you're already running on a public network. There will always be at least some parts of a government presence that are public-facing, even if it's only an informational web site. In a hybrid, multicloud environment, you'll be dealing with a set of connections between your existing physical network, the cloud provider's network, and the public internet.

2 Your team is responsible for everything

False When you were running your own data centers exclusively, your team was responsible for everything. The cloud is different. In a cloud environment, your cloud vendor will maintain an infrastructure and ensure that the environment meets all required standards.

3 All your data must be stored locally

False Your data does not need to be stored locally, although your data storage may need to meet certain standards. For example, if you want to develop something that is easy for the public to use and accessible via mobile, you could do the development in the cloud with test data. Additionally, some data may need to stay on premises. You need to know what your data is, the rules around it, what is confidential, and what is not.

4 Your developers need to be security experts

False In cloud-native development, developers need to bake security into the application code. That doesn't mean your developers need to be security experts, but it sure makes sense to put a security person on the development team. Beyond that, developers need a secure development framework. They should take advantage of approved, hardened security services available in the cloud.

5 Multicloud cannot be as secure as a single cloud

False Multicloud can be as secure as a single cloud or as an on-premises solution, but it requires a collaborative approach with your vendors. Make sure the vendors you are working with have the necessary infrastructure-as-a-service certifications in place (AICPA SOC1 and 2, ISO27001, NIST800-53, etc.).

You need to completely understand how your applications will work in a multicloud environment. You must ensure that configuration and deployment of your applications are what you believe them to be. And consider placing edge security devices at the point of presence so that you can confirm that network traffic flows are being monitored in accordance with your policies and procedures.

Managing security between multiple clouds may require you to balance and orchestrate workloads between multiple providers. The key, as is always the case with security, is knowing where you put your stuff. The right tools will help enable security orchestration and integrate security services in a multicloud environment.

A private cloud alleviates many security concerns. It automates the process of protecting your services, dedicates firewalls specifically to your needs, and ensures that your policies and procedures are satisfied.

6 All data must have top-level security

False Not all workloads require the same level of security. An address, which is publicly available, doesn't need to be protected in the same way that a social security number should be. If you don't understand your data fully, and where and how it's being used, you might end up putting the highest-level security on everything, which is expensive and unnecessary.

7.Service management and operations

Independent of where applications run—in traditional IT data centers or in the cloud—they must be managed to ensure availability, security, and adequate quality of service. How can a process-heavy, mature operations team evolve to support modern agile and cloud-oriented approaches? This transformation has implications in four areas: organization, process, technology, and culture.

Organization

The primary organizational transformation needed to support cloud technologies lies in the relationship between the operations and development teams. Governments are gradually adopting the DevOps model, which is an approach to software delivery that brings together development, operations and even testing to improve agility and reduce the time needed to address customer feedback. DevOps enables continuous delivery, continuous deployment and continuous monitoring of applications by iteratively following the stages of think, code, deploy, run, manage and learn.[5]

Depending on the state of your legacy technology, you might not be able to use DevOps throughout your entire organization. Your legacy technology may still require longer upgrade and maintenance cycles. In that case, you'll need regular check-ins between the two to maintain coordination.

Process

The cloud enables teams to adopt agile processes, a way of producing software in short iterations on a continuous delivery schedule. In a cloud environment, architecture and operations are tightly linked. If you have to rollback or change deployment, you need to have a container-based architecture that can easily support this. Just as important, it allows you to innovate, upgrade, and fix continually rather than relying on infrequent bet-the-farm releases.

As cloud environments grow and become more complex and more heavily used, automation and standardization become increasingly essential. Automation can be used to design and build blueprints, giving developers a fixed set of configuration options. Without automation, costs for environments and for staff will increase. The cloud is about airtight standard operating procedures. More automation equals less chance of human error.

Technology

While we've already discussed many of the technology changes brought by the cloud, one additional area is in the use of monitoring tools. Especially when managing workloads that cross multiple clouds, cloud management platforms provide management, visibility, automation and orchestration across cloud providers using policy-based tools. Effective platforms present a single, self-service interface that enables configuring, provisioning and deployment of development environments, as well as the integration of service management and monitoring, backup and security. There also needs to be a shift in focus, from resource-centric monitoring to application- and service-oriented monitoring such as response time, latency, error rate, and saturation. These metrics should be easily accessible via dashboards.

Culture

Cultural changes can make or sink a cloud adoption strategy. Traditional IT service management is often characterized by a precisely defined and structured approach, which often conflicts with the more agile and iterative development style enabled by the cloud. The journey agencies are on as they adopt cloud will gradually create cultural changes often aligned to those in figure 4.

Operations transformation—culture change

Traditional IT	Cloud-native
Planned, process-oriented	Iterative, agile
Goal to look good—“*it's not me*”	Goal is to learn: no-blame or finger-pointing
Savior syndrome, “heroes”	Learning organization
Goals per business unit	Common goals across all units
Expertise	Collaboration, sharing
Be protective of information	Transparency
Be comfortable in static environment	Be comfortable with change and dynamics
Risk-averse	Empowered and collaborative
Reaction to challenge: helplessness	Reaction to challenge: resilience
Default attitude is “*no*”	Default attitude is “*yes*”

Figure 4: Traditional IT service management can have a precisely defined approach, which is often in conflict with an agile and iterative development approach.

8. Cloud governance in a hybrid, multicloud world

Defining a governance model

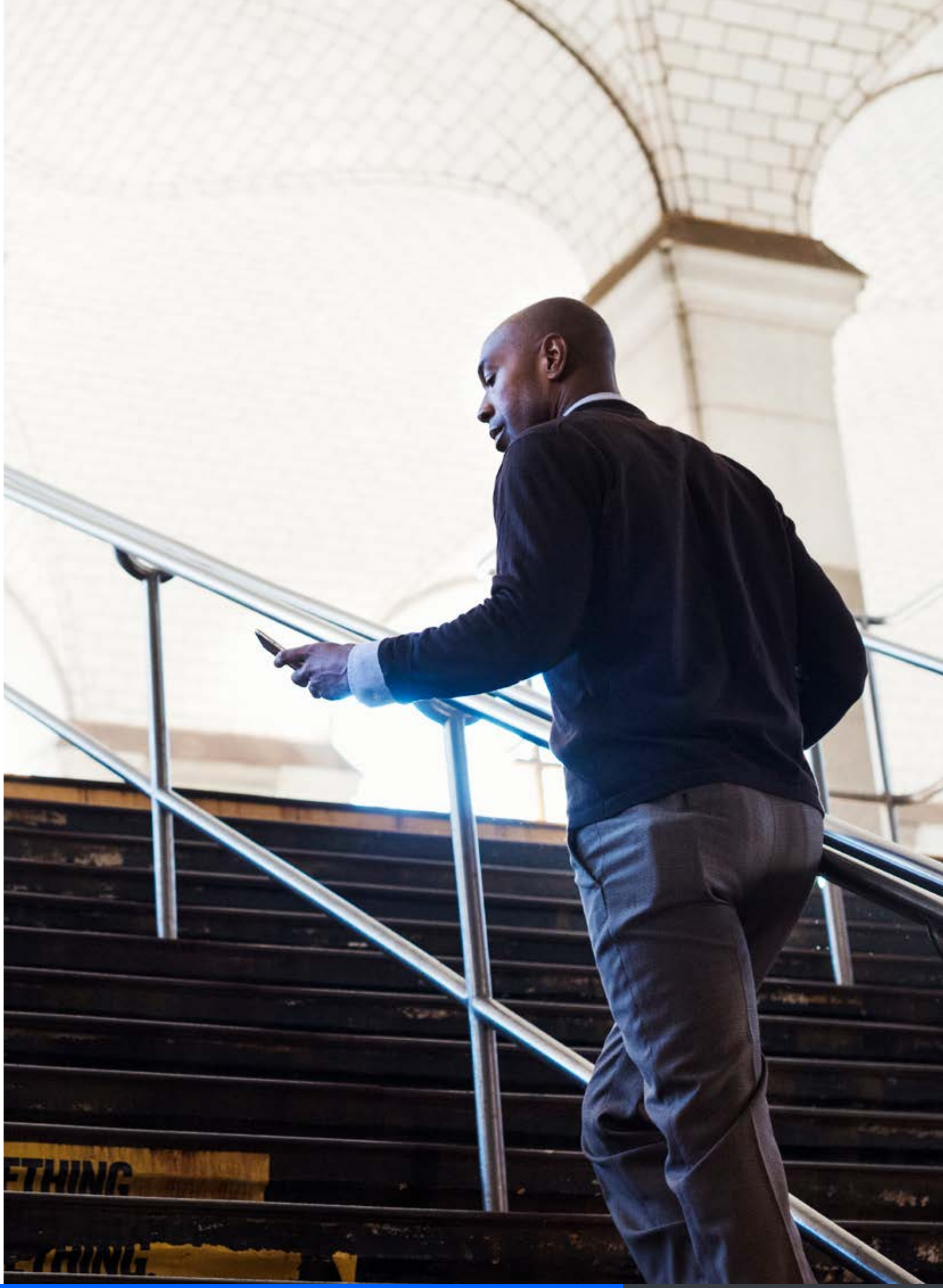
Your governance model should clearly establish core principles and standards for cloud-related decisions. It must also align with your desired strategic outcomes, so that it becomes an essential tool to help manage risk and maximize value. Based on our experience working with clients, we recommend a governance model that does the following:

1. **Enables you to identify, manage and mitigate risks**
2. **Helps ensure regulatory compliance**
3. **Helps you drive towards standardized solutions in a concerted way**
4. **Promotes consistent cloud adoption throughout your organization**
5. **Drives synergy through sharing and reusing processes that work, captured as best practices**

Each organization is going to have its own model of successful governance, because each organization will have different goals and metrics for success. A lack of effective cloud governance can create unchecked, costly cloud sprawl, shadow IT, and increased security risks. It's too easy to end up with a proliferation of resources that are being paid for across multiple environments, but without a comprehensive view of what those assets and resources are. This results in an operational nightmare that is difficult to maintain, update, and integrate.

To help a system of governance take root, consider establishing a center of competency, even if you don't officially designate any group of people as a center of competency. This approach acknowledges that you can't get everyone working in the cloud, using cloud-native technologies, tomorrow. Instead, start with a small group of developers, project managers, and analysts who work hand in hand to develop standard processes you'll apply throughout your cloud adoption journey. Decide which tools will be used and devise process and policies around those tools. Once this group is comfortable with the technologies and associated policies they've chosen, they'll slowly roll them out—along with guidance—to other groups. It's a good way to diffuse new knowledge and consistency throughout an organization.

Common standards, and agreements on which technologies will be used, maintained, and supported, are crucial to achieving higher levels of operational efficiency, greater resilience, higher levels of customer and citizen satisfaction, and the reductions in cost that are possible with the cloud.



9.Conclusion

Throughout this ebook, we have tried to reinforce how cloud is rapidly maturing and how it has become a central part of the transformational journey for government entities of all sizes and types.

We are passionate about the potential of the cloud to transform government and its ability to provide services to citizens using new business models. We also realize that the journey to reaping the benefits of the cloud can be longer than anticipated. The next phase of cloud, where agencies will need to develop ways to manage hybrid, multicloud environments may seem daunting, but the rewards will be significant: decreased IT costs, less downtime, fewer outages, improved citizen experiences, shared services and new business models and revenue streams.

This ebook is intended to help you continue your cloud adoption journey in the right direction. To learn more about how IBM can help you on your journey, visit ibm.com/cloud/government.

Sources:

[1] Assembling Your Cloud Orchestra, IBM Institute for Business Value, 2018

[2] Center for Digital Government Survey, sponsored by IBM, forthcoming study

[3] Assembling Your Cloud Orchestra, IBM Institute for Business Value, 2018

[4] The NIST Definition of Cloud Computing

[5] What is DevOps? Think, Code, Deploy, Run, Manage, Learn., Accessed on 12/18/18

< Back