

Delivering Government Services


Key Considerations

- **Cost reduction.** Transferring services to the cloud could improve public access to government services and potentially drive down their costs.¹
- **Higher consequences of disruption.** Yet it simultaneously increases the costs and risks inherent in disruption, denial, or biasing of services, requiring special vigilance and contingency planning.
- **Risk of inequitable access.** Inequitable availability of broadband infrastructure and uneven abilities to use digital technologies will result in unequal access to cloud-dependent government services, risking adverse political, social, and economic consequences. However, the potential for these consequences might incentivize stakeholders to upgrade and extend broadband infrastructure to underserved communities.
- **Risk of vendor lock-in.** The size of governmental e-services contracts enhances their initial leverage over cloud providers to secure favorable arrangements. But the complexity of these arrangements and their contracting rigidity also create a serious lock-in challenge (and ensure reverse leverage).

Background

The growing popularity of cloud-hosted applications is bringing twenty-first-century efficiency to a range of citizen-facing services. For example, it is enabling governments to more efficiently store and manage the data needed to distribute unemployment insurance and manage state identity records.² Likewise, the promises of smart-city systems, which themselves rely on the collection and processing of vast quantities of data, cannot go unnoticed. However, as governments begin to migrate IT operations from internal servers to off-site data centers and deploy “digital-first” services, anxieties surrounding the security of the systems and equal access to those services, among other concerns, become more acute. Data breaches or power outages could impair these government functions and, along with uneven access to broadband, deny their populations access to essential services. Moreover, the cascading effects of such breaches in other critical sectors, such as finance and healthcare, remain a prime concern for legislators and law enforcement agencies alike.

Beyond protecting against technical compromises, however, governments must also consider the impact of broad digitization on the inclusiveness of their services. Digitization certainly can make government services more inclusive. It can enable access for those who struggle to



physically travel to government buildings, harness technology to offer services in less-common languages to underserved populations, and do it all in a cost-effective manner for the government. However, digitization does not guarantee inclusiveness. If governments do not consciously couple their digital transformation initiatives with inclusive and equitable measures—such as extending high-speed broadband connectivity, accounting for language barriers or physical and cognitive impairments, or increasing public access to computers and cellular devices—the benefits of cloud-hosted programs become limited in their scope and impact. Moreover, in the move to digital services, governments risk losing the accessibility of physical services, on which senior citizens and others with less technological familiarity depend. The cloud is clearly not a one-size-fits-all solution, and governments must consider using e-services in tandem with traditional modes of service delivery, such as offices and stations, as opposed to entirely replacing physical infrastructure.

Additionally, cloud computing can enable constant data sharing between government agencies and can obscure such practices from the public. In bureaucracies with lax rules about interagency data sharing, services that ought to be kept separate to protect individual privacy, such as law enforcement and other citizen-facing services, could become easier to combine. As governments migrate their services to the cloud, they might consider revisiting the rules on how sensitive data is stored and who may access it. Careful attention to this issue can also help them build these protections into the design of their new cloud-based systems.

Notes

¹ Office of Management and Budget, “Cloud Smart,” Office of Management and Budget, June 24, 2019, <https://www.fedscoop.com/final-cloud-smart-policy/>

² Phil Goldstein, “How the Cloud Can Help States Process Unemployment Claims Faster,” *StateTech*, May 8, 2020, <https://statetechmagazine.com/article/2020/05/how-cloud-can-help-states-process-unemployment-claims-faster>