McKinsey & Company

Public Sector Practice

Defining a public-cloud strategy: An interview with Michael Ørnø, of Denmark's Statens IT

Statens IT, the Danish government shared-service center for IT, has established a comprehensive government data center. The next step is to embrace the opportunities and challenges of the public cloud.

by Matthias Daub and Niels Gotfredsen

June 2019

Governments around the globe are going digital to improve citizen services and reap efficiencies. Public clouds,[1] in particular, offer unique opportunities of flexibility, scalability, and sophisticated on-demand services. At the same time, they raise concerns of data protection, challenges of complex change management, and confusion around the financial business cases.[2] Successful migration to public clouds therefore calls for a structured and well-thought-through approach.[3]

In this interview, Michael Ørnø, director at Statens IT, describes the urgent need for governments to follow Denmark's lead and define a cloud strategy. The Danish strategy recognizes the importance and large potential of tapping into public clouds while also acknowledging the risks, stressing the need to reduce complexity and risk for the individual government agency. Ørnø explains how an IT shared-service center can work as a service integrator to enable agencies' secure and economically sound access to public-cloud services.

McKinsey: What is the essence of the public-cloud strategy you just launched?

Michael Ørnø: Our overall strategy is to reduce complexity for the users. The use of public clouds offers many advantages, and staying out is not a realistic option. But it also introduces a high level of complexity and fragmentation where a large number of systems need to be integrated and work together. This makes it very difficult, for example, to locate errors. But the user should not care about where the problem is, only that it is being fixed. Another important issue is access control—using a different access control for every new system you approach is not efficient, so we need to provide a single sign-on, preferably with the users' existing active directory (AD).

McKinsey: What are the advantages of the public- and private-cloud[4] services for the government sector? And where do you see the differences between public and private cloud?

Michael Ørnø: In my opinion, both private and public clouds provide huge flexibility advantages, as they offer a new level of self-service for the users. Cloud solutions enable users to manage agile projects with smaller deliverables and provide the option to adapt and scale to changing conditions instead of being dependent on a classic (somewhat rigid) waterfall sequential model. For governments, there is a financial potential, as there can be huge scale advantages when consolidating data centers—from shared rent to more efficient power use, and so on. And if you consolidate services, then you can really drive efficiency to another level with platforms as a service and less unused capacity on servers.

Comparing public and private clouds, I think there are three important differences: the functionality, the regulatory framework, and financial risk. For public clouds, the functionality is fundamentally different, with the number of services for public clouds being higher and continuously increasing. Public clouds, in addition, offer many services that are exclusive to them—so even if you wanted to stay out of public clouds, it is probably not a viable long-term strategy. The larger number of services and complex functionalities, on the other hand, typically introduces a higher number of log-ins in public clouds.

The second difference between public and private clouds is the regulatory framework—and this is, in my opinion, the largest challenge for public clouds compared to private clouds. The regulatory framework includes the question of where data is

[1] The public cloud consists of computing services (such as storage, applications, or virtual machines) offered by third-party providers over the public internet, making them available to anyone who wants to use or purchase them. They may be free or sold on demand. Examples include Microsoft Azure, Amazon Web Services, and Google Cloud Platform.

[2] See Arul Elumalai, James Kaplan, Mike Newborn, and Roger Roberts, "Making a secure transition to the public cloud," January 2018, McKinsey.com.

[3] See Mark Gu, Krish Krishnakanthan, Anand Mohanrangan, and Brent Smolinski, "The progressive cloud: A new approach to migration," August 2018, McKinsey.com.

[4] Private cloud refers to proprietary cloud-computing architecture dedicated to a single organization or authority, such as a group of government agencies. A private cloud differs from the public cloud as it serves as an extension of a company's existing data center and is accessible only by that company.

Michael Ørnø

Michael Ørnø has been the director at the Danish government IT shared-service center since 2012. Michael is also a board member at the highly influential professional organization Danish IT. Earlier experience includes eight years at PostNord, the Danish–Swedish joint postal service, where he was vice president, service and infrastructure management.

stored, who operates it, and if there's compliance with GDPR [General Data Protection Regulation]. The regulatory framework in Denmark is not yet completely clear, which is a challenge. A related issue is how to handle sensitive data. Of course, a part of the solution is encrypted data. But with encryption technologies evolving, it is vital to have sufficient guidance on the approach to sensitive data.

The third important difference between public and private clouds is the cost side. The public clouds are typically rather complex and the demanded services difficult to forecast, so the spending can get out of control. This, combined with the necessity of shutting down the services when they are no longer utilized, often makes the cost drivers rather complex and calls for quite sophisticated financial and contract management. The risk of contract lock-in is also imminent as sophisticated services are increasingly reserved for the cloud.

McKinsey: Which services do you expect to run out of the public cloud? And which do you expect to keep?

Michael Ørnø: I think there are two overall considerations here: one on the type of data and one on the type of functions.

For data, segmentation is necessary. If we opt for high security on all kinds of data, then it is simply going to be too expensive. Instead, data should be segmented to represent different security levels. You could imagine a scenario where data from some public entities could be placed in a public cloud. These could be entities that are related to nonpersonal data such as geo data, environmental data, traffic data, et cetera. For other public entities that handle more sensitive data, such as highly personalized data and foreign affairs, it is probably not likely that they could transfer their data to the public cloud.

For functions, I would also expect that the type of service influences whether it is in a public cloud. For servers with a very low capacity usage, public clouds could be relevant; whereas for servers with a very high capacity usage, it may simply become too expensive with today's price structure in the public cloud. Personally, I believe that for services related to product development and testing—especially where you need the agility and flexibility—public clouds can be the right approach. On the other hand, for services that are more production heavy, with a lot of transactions and users, an ordinary private cloud is probably more appropriate.

McKinsey: Do you see migration to public clouds as a way of gradually outsourcing a government shared service?

Michael Ørnø: In my opinion, there will be some services that may be outsourced and others may not. On the production side, there will be a case for migrating to public clouds and base more on service delivery instead of ownership. It is important, however, not to introduce too much complexity on services that are crucial to the everyday work of thousands of employees. And to keep an eye on cost.

The **public cloud** is computing services such as storage, applications, or virtual machines offered by third-party providers over the public internet, making them available to anyone who wants to use or purchase them. They may be free or sold on demand. Examples include Amazon Web Services, Google Cloud Platform, and Microsoft Azure.

A **private cloud** is a proprietary cloud-computing architecture dedicated to a single organization or authority, for instance, a group of government agencies. A private cloud differs from the public cloud, as it serves as an extension of a company's existing data center and is accessible only by that company.

On the other hand, governance and control are highly important to keep internal. This raises the question of whether you can have control without having technical capabilities. If you outsource all the production- and technology-heavy areas, then you end up in a procurement role, mainly doing contract management. The challenge here is specifying requirements and how to challenge prices and conditions.

One of the reasons why we are successful in negotiating agreements on, for example, servers is that we have the in-house technical skills negotiating directly with the suppliers. So I would say that you can probably outsource some of the areas and services, but you need to ensure that you still have the governance and the necessary level of technological skills. In that sense I see our current government shared-service center as a strong asset in moving to public clouds rather than something to be replaced.

McKinsey: What are your next steps toward public-cloud migration?

Michael Ørnø: The next couple of years are extremely important. As a shared-service center, we need to continue to deliver value for the government agencies that are our customers as a service integrator. And to stay relevant for our users, we need to be a part of the journey toward public cloud. If we are not successful in the role of service integrator, then we may see that in five to six years, the whole public sector has more than 200 different agreements with cloud suppliers—a very expensive and chaotic scenario.

Right now we are doing a number of proof of concepts with a couple of customers and vendors and expect to migrate to Office 365 in August 2019. As always, we start by testing the setup on ourselves. On contractual setup, we have managed to use existing frame agreements for some vendors and are presently investigating setups for vendors that do not respond to RFPs [requests for proposal].

The setup is not perfect yet, but the aim is to ensure that licenses and services can be shared across the public sector and that each public entity does not have its own agreement with the cloud suppliers. When our customers start moving toward using public clouds, we need to support that journey, too.

Michael Ørnø is director of Statens IT. **Matthias Daub** is a senior partner in McKinsey's Berlin office and **Niels Gotfredsen** is an associate partner in the Copenhagen office.

Designed by Global Editorial Services