CLOUD FIRST, BUT NOT ALWAYS

*When* Government Should Move *What* to the Cloud

by: John Druitt and Wagish Bhartiya

November 2017

www.reisystems.com
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>When and Why Private Companies Use the Cloud – Rules of Thumb</td>
<td>2</td>
</tr>
<tr>
<td>Some of Those Rules of Thumb Apply to Government</td>
<td>6</td>
</tr>
<tr>
<td>Conclusion</td>
<td>10</td>
</tr>
</tbody>
</table>
Executive Summary

While there are many known benefits to cloud computing, it is not always the right option for Government agencies. Some types of applications should be moved to the cloud earlier, and some can reasonably be deferred, while others may need never move to the cloud. In this article, we advise agencies to look to the private sector for motivations and examples of when companies move to the cloud, and what they move. Then, we demonstrate how lessons from those motivations and examples can be applied to Government. Finally, we provide specific recommendations how the Government can encourage and facilitate the right cloud computing decisions.

Introduction

President Obama introduced a cloud first strategy in 2011, when then US CIO Vivek Kundra directed agencies to consider a cloud computing option first. Any decision to spend funds for a traditional on-premise solution vs. a cloud alternative was required to be “fully justified.” President Trump is continuing the emphasis on cloud with the (draft) August 2017 “Report to the President on Federal IT Modernization.” Despite this attention, Government has been slow to move toward the cloud. In a Government Business Council survey just 19% of respondents indicated that their agency “extensively uses applications developed for the cloud” or is “piloting some applications developed for the cloud.” The remaining clear majority – 81% – acknowledged that their agency had not yet begun a substantial move to the cloud, or were not aware of progress. The pace of movement toward the cloud by government has been slow... but why? We believe that the managers and IT leaders of these agencies are rational. The benefits of the cloud aren’t always clear, the potential costs can be substantial, and not everyone understands the risks, obstacles and how to succeed. People are hesitant to move all their agency’s IT to the cloud immediately. We believe that Government is right to hesitate, and to act carefully. Some types of applications should be moved to the cloud earlier, and some can reasonably be deferred, while others may need never move to the cloud. In evaluating options, it is helpful to look to the private sector for motivations and examples of when companies move to the cloud, and what they move. In many instances, lessons from those motivations and examples can be applied to Government.

---

1. That report plans for government to Enable use of commercial cloud, Accelerate adoption of cloud email and collaboration tools, and Modernize Trusted Internet Connections (TIC) and the National Cybersecurity Protection System (NCPS) Program to Enable Cloud Migration.

2. Survey published in 2017, 368 responses from subscribers to Government Executive, Nextgov, or Defense One who are senior employees representing more than 30 departments and agencies.

3. We define “the cloud” to be an IT hosting infrastructure that is off-premise from the user’s organization, that is shared by multiple organizations, and that may offer different levels of service (e.g., platform and commodity software applications may, or may not be included).
When and Why Private Companies Use the Cloud – Rules of Thumb

Private companies move their IT applications, data and operations to the cloud in ten instances:

- **Unpredictable growth is likely.** When Uber and Netflix first launched, each company had aspirations of enormous growth in their business, and in the need for IT to support that business volume. But it would have been imprudent for either company to bet on the specific volume of business they expected, and purchase IT servers for that volume, because there was too much uncertainty.

- **Demand fluctuates significantly.** Amazon (along with Macys, Best Buy, and many other retailers) need more processing capacity for a limited time – e.g., November, December and early January – because of peaks in seasonal sales volume. They rely on cloud resources because they can use the cloud during periods of peak demand, but not pay for it at other times. (As a cloud service provider, Amazon Web Services owns its resources, but “rents” more of the resources to others during non-peak periods.)

- **Limited resources (capital, or calendar time).** Companies more often rely on the cloud if they have scarce resources and are in a hurry (e.g., they want to get
to market before competitors). In that case, companies do not want to dedicate funds to capital investments in IT, particularly during their first few years. This is most typical of start-up companies such as LinkedIn, which need to spend money on product development and marketing – not IT infrastructure. Paying only for what they use is a secondary benefit. Note that, as companies mature, gain easier access to capital and more predictable demand for IT, some transition from exclusive reliance on the commercial cloud to meeting part or all their infrastructure need with data centers that they operate themselves, “in-house.”

- **Lack of available expertise.** Companies that do not have (or do not want to maintain) the technical or management expertise to launch or manage a data center consider the cloud as less risky alternative. One example is video game developer Zynga (maker of Farmville), which first launched its services on the cloud in 2007, transitioned to in-house data centers in 2011, but determined it did not have / could not attract sufficient expertise and thus transitioned back to public cloud hosting in 2015.⁴

- **Fear of security risks from in-house hosting.** A number of companies, (e.g., British American Tobacco) prefer to rely upon security practices, tools and experts from cloud computing providers, rather than establish and keep such practices up-to-date themselves. Those who do this tend to rely on cloud providers with heavily-used and well-protected IT assets in many geographies. They particularly rely on cloud providers to manage employee (and customer/partner) access to computing resources. Companies that choose to use the cloud to reduce cyber/hacking risks often include businesses with geographically dispersed employees.⁵

- **Desire for early access to technological innovation.** Many companies (such as AIG Edison Life Insurance) whose primary mission focus is not technology still feel a need to be at the forefront of technological innovation in order to appeal to youthful customers with convenient service formats, and to manage perceptions so as to appear as a modern and innovative brand. In AIG Edison’s case, the company wanted thousands of customers to have access to mobile applications and customer support via smartphone, and to offer the same accessibility to its sales representatives. Rather than relying on

---

⁴ See: https://www.sparkpost.com/blog/aws-instead-data-center/

its own infrastructure, or “bare metal” cloud servers, the company elected to acquire both cloud hosting and platform services from SalesForce.\(^6\)

- **Expectation of lower total cost of ownership: more efficient, lower price from cloud hosts.** It is challenging to construct an apples-to-apples comparison of cloud hosting costs to self-operated data center costs (particularly because capturing labor effort and wage costs for self-operation is difficult, and because amortization of capital costs rarely occurs in government). Never the less, subject matter experts (and many lay people) perceive that economies of scale have a strong potential to make cloud costs lower – if the purchaser negotiates effectively and if the cloud provider passes along cost savings to the customer in the form of economical pricing. This perception is illustrated in a study from the UK’s Bournemouth University, which found that SMEs identified “Cost Reduction” as the most frequent reason to use cloud computing services.\(^7\)

- **Desire for access to proven, economical support applications.** A significant proportion of 550 commercial startups surveyed make heavy use of support applications that are bundled with and provided on cloud infrastructure, including QuickBooks (71%) for accounting, Google Analytics (70%) for BI, Salesforce.com (59%) for customer relationship management, and Dropbox (39%) for storage and backup.\(^8\)

- **Highly reliable physical proximity to data is needed in many geographic locations.** If a very fast response time is critical to a business model, but a company’s IT users are geographically dispersed in many locations, it is unlikely to be economical to own and operate an efficient data center if just a few users are served in each location. In 2015, for these reasons, Netflix closed its last in-house data center in favor of Amazon Web Services’ public cloud, together with a content delivery network (cloud) that Netflix has been building.\(^9\)

- **An emergency back-up hosting facility is needed for business continuity purposes.** Many businesses with a primary location and data center in Texas and Florida find it valuable to

\(^6\) See: [https://www.enterpriseinnovation.net/content/insurance-company-moves-cloud](https://www.enterpriseinnovation.net/content/insurance-company-moves-cloud)


have an available cloud back-up facility in a different geography so that their business can sustain disruption by events such as hurricanes Harvey and Irma.

In contrast, private companies frequently operate their own data center in several other circumstances:

- **A core, base portion of IT needs are stable/unlikely to change.** For the core, stable base portion of a company’s IT needs, where those needs are substantial, a company may choose to own and operate data center(s) to support those core/base needs. Companies like The Hartford Insurance Company, and Delhaize (operator of Food Lion and Hannaford grocery stores) supplement that base capacity with cloud hosting for specialized uses – such as big data analytics, surges of business volume, or business continuity disruptions.¹⁰ For several companies, the resultant approach is to use a base of in-house data centers, supplemented by cloud infrastructure to meet surge capacity, specialized or geographically remote needs, and to provide emergency back-up capability. The motivation is driven in part by a perception that stable in-house hosting capacity may be less costly than capacity offered by a commercial cloud provider. Note, however, that a careful price/cost comparison is likely warranted. In-house costs may not necessarily compare well to efficient commercial cloud pricing. This can be true because the scale of a commercial cloud data center tends to be much larger than the entire capacity need for many companies. For example, a single Amazon Web Services data center location typically houses 50,000 to 75,000 servers. In comparison, the entire Federal government uses approximately 60,000 servers – fitting into less than one AWS data center vice the thousands of data centers currently used by the Government. Thus, commercial cloud providers can operate quite economically by spreading fixed costs over several separate companies or agencies (though they may not always reflect this efficiency in their pricing.). The potential efficiency draws from economies of scale - e.g., just one DCIM software tool, and one Data Center Director are needed for a single large data center, vs. needing 25 DCIM tools and 25 data center managers to provide the same capacity using 25 data centers if each operates a more typical 2,000 to 3,000 servers.

• **Extremely sensitive data.** Some companies, such as JP Morgan\(^{11}\) want to maintain complete control over their “crown jewels” – i.e., their most sensitive data and systems. Of course this is not always effective: for example, the Equifax, was unable to protect extremely sensitive data regardless of its hybrid hosting arrangements.

• **The organization uses an extraordinary volume of infrastructure/hosting service that is integral to their business and competitive advantage** (e.g., Apple, Google, Amazon). Such companies may become vendors of cloud services, in addition to their core business.

---

**Some of Those Rules of Thumb Apply to Government**

If we apply that same basic logic to government, even under a cloud-first policy, they don’t produce a conclusion of cloud always. In fact, they produce some helpful ideas about when the government may want to move to the cloud. We have included an arrow icon (⇒)next to the rules of thumb that apply most frequently and/or strongly in government.

• **Unpredictable growth.** Breakaway growth is rare in government. Most government activities aren’t subject to the kind of growth that was the specific goal for Uber and Netflix. Exceptions may be disaster response and recovery, immigration functions (i.e., in times of a change to benefits), or the military in case of preparation or war.

• **Demand fluctuates seasonally.** Again, this is not common across government, but might well be the case for a few agencies such as the IRS during tax return processing season, the SEC around filing deadlines, or grant-making agencies when grant applications are statutorily due.

⇒ **Limited resources (capital, or calendar time) to buy/build data centers.** This might be a big motivation for government – in the current constrained budget environment, there’s little chance to obtain appropriations for a large capital expenditure to upgrade or construct a modern data center. Thus, the cloud is a mechanism that allows government to “pay-as-you-go” subject to a contractual ceiling, rather than paying up-front for the hardware that will be used to support government computing needs. But, many government agencies – including some with relatively modern infrastructure and operations – have data centers with extra capacity already in place. Some existing government centers have a marginal cost that may be less than the price for equivalent

---

infrastructure capacity available in the commercial cloud.

- **Lack of available expertise.** Federal agencies seem at least as likely to face this challenge as are private sector companies, and perhaps more so.

- **Fear of security risks from in-house hosting.** Federal agencies have not typically feared for security from in-house hosting – perhaps because the government has established security standards there are clearer than those applied in many parts of the private sector. Thus, a desire for security has not significantly motivated government agencies to move to the cloud. Perhaps, however, agencies have an unjustified sense of comfort with the security of in-house computing – data breaches of databases hosted in-house at the Office of Personnel Management and the Department of Veterans Affairs illustrate that in-house security may not be as robust as is assumed.

- **Desire for early access to technological innovation.** Government’s desire for access to innovation via the cloud is a strong motivator. In part, federal agencies tend to look to the private sector as an experimentation and proving grounds for innovation before the risks are known well enough for the government to adopt a new technology. As well, investments in new technology, tools, and expertise is usually required to foster innovation. Government tends to be risk averse about making such investments, and neither capitalizes nor depreciates the costs of the investment. The result is that agencies and individual technologists in government often look to outsourcing – the cloud – for their first opportunity to access innovation. Some may eventually seek to bring a particular innovation to in-house government-owned data centers, but that typically occurs only after the technology is well proven.

- **Expectation of lower total cost of ownership: more efficient, lower price from cloud hosts.** Many in government perceive that costs of cloud computing will be lower than costs for in-house data centers, motivating some agencies to move toward the cloud. However, analysis by the non-profit Rand Corporation does not confirm the perception that cloud is cheaper. Rand’s 2014 study, titled “Cost Considerations in Cloud Computing,” was funded by the US Army. It compared a base alternative (government-owned and -operated hardware, with several incremental improvements) to comparable alternatives offered by two commercial vendors for a hybrid cloud option.

12. See: [https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE113/RAND_PE113.pdf](https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE113/RAND_PE113.pdf)
Pricing for the first commercial vendor’s offering was slightly lower than the government-owned/operated option, while the second commercial vendor’s pricing was substantially higher.

- **Desire for access to proven, economical support applications.** Federal agencies seem resistant to sharing applications for support services. Payroll processing is the only cloud-hosted support service for which more than half of federal agencies choose to share rather than self-provide. Perhaps setting and incentivizing targets for shared service market penetration (i.e., agencies should rely upon shared service providers for at least half of their support applications) would increase the government’s efficiency.

- **Highly reliable physical proximity to data is needed in many geographic locations.** Few agencies have a business model that requires such speedy processing that physical proximity of IT hosting is an issue for them. Exceptions may include supercomputing resources used by DOE National Laboratories, health data needed for urgent care by the Veterans Health Administration, weather data storage by the National Oceanic and Atmospheric Administration, and certain military or law enforcement activities where time is of the essence.

- **An emergency back-up hosting facility is needed.** This need to use the cloud is important for government, just as it is for the private sector. It is most important where people’s lives, health and/or safety depends on continuity of an agency’s services. And – several of the reasons private companies retain responsibility for operating data centers can also be applied to government.

- **A core, base portion of IT needs are stable/unlikely to change.** Few Federal agencies are start-ups with the accompanying instability. And, relatively few should plan for their IT infrastructure based upon an assumption that they will need to carry out a dramatically increased or decreased volume of work (though perhaps such an assumption might be valid for agencies that oversee the Affordable Care Act). Thus, many agencies may reasonably plan to meet a core, base portion of their IT infrastructure needs using in-house data centers – if those data centers are modern, secure and efficient. (As noted above, however, few Government data centers are likely to be as efficient and low cost as commercial cloud operators. Thus, a careful cost comparison is likely to be called for, since other motivations for moving to the cloud are not strongly present.
• **Extremely sensitive data.** Several types of Government agencies use extremely sensitive data. These include, for example, law enforcement, the intelligence community, the military, and agencies that manage personally identifiable information. The Government naturally should take much greater care before moving these sorts of applications to the commercial cloud. That great care is embodied in FISMA standards, and FedRAMP criteria.

• **Organization uses an extraordinary volume of infrastructure/hosting service** that is integral to their business and competitive advantage. A few government agencies use intensive amounts of data (Social Security, Census Bureau, National Weather Service), or rely upon unusual infrastructure for a competitive advantage (e.g., NASA, and DOE’s National Laboratory supercomputing facilities). These agencies may find that they operate at a scale, can keep deep expertise on staff, and may not be well served by public cloud because of their unusual needs. As with the private sector, some of the agencies may find that they can share the cost of their infrastructure by acting as a cloud provider (shared service provider) themselves – presumably supporting other government agencies. (Full disclosure: The authors’ employer, REI Systems, supports GSA in its role as Managing Partner of the Government’s Data Center Optimization Initiative.)
Conclusion

Our conclusion is that it is not reasonable to expect Government agencies to move all IT applications, platforms, and infrastructure to the cloud – private companies don’t, and it just doesn’t make sense.

The most prominent reasons for an Agency to move IT to the cloud include:

- Limited resources (capital, or calendar time) to buy/build data centers
- Lack of available expertise to manage infrastructure in-house
- An emergency back-up hosting facility is needed

Agencies should be more hesitant to move to the cloud – and carefully compare costs and plan to ensure that the choose a cloud option tailored to their needs if:

- A core, base portion of IT needs are stable/unlikely to change.
- Extremely sensitive data may be moved to the cloud

Our recommendations are:

1. Encourage/Create Government-Owned and Operated Cloud Infrastructure Offerings: To facilitate Agency decisions on whether to move to the cloud for their infrastructure needs, OMB and GSA should help encourage/create several government-owned and operated cloud infrastructure offerings that achieve efficiencies like those available from commercial cloud providers. Several government Data Centers are well-prepared to do this already.
   - USDA’s National IT Center in MO
   - NASA’s Stennis Space Center in AL
   - SSA’s Urbana Data Center in MD
   - DoJ/FBI’s Data Centers in WV and TX

2. Authorize Agencies to Make Investments in Efficient Public Cloud Infrastructure: Congress should authorize more agencies (for example, SSA, and DoJ/FBI) to operate enterprise funds that will enable them to (continue to) make investments in IT infrastructure, as well as recoup those investments over more than one year by charging other agencies for use of their efficient “public cloud” infrastructure. Congress should also consider modifying the MGT Act to allow new funds to be used to support inter-agency shared services.

3. Require Agencies to Use Approved Cloud Infrastructure Providers: GSA should competitively select a few appropriate “commercial cloud” providers, negotiate substantial volume discounts for guaranteed usage volume, and (with a directive from OMB) require agencies to direct their cloud use toward only those providers until those volume guarantees have been met. If the government relies on every agency individually to procure and oversee government use of the commercial cloud, the Government is unlikely to receive a pricing benefit from the economies of scale available from the cloud.