Bond Case Briefs

Municipal Finance Law Since 1971

Government in the Cloud: Minimizing the Risks.

A new report provides a checklist of a dozen issues that need to be addressed when governments contract for cloud-computing services.

Many governments find the lure of cloud-based solutions — the delivery of computing services such as email, data storage and online forms over the Internet — to be highly compelling. Government leaders are finding they can lower their information-technology costs and expand services while improving performance and security.

But as with any form of government contracting, there are risks to be considered. Do governments lose control over their data? Do they risk losing access to it? Are they locked in to a single vendor? The key to success is writing and negotiating a strong contract. A recent report for the IBM Center for the Business of Government by researchers at the University of North Carolina at Chapel Hill analyzes contracting issues that state and local governments face when adopting cloud-computing services.

The study's authors, Shannon Tufts and Meredith Weiss, interviewed pioneering users of cloud services in local governments and state agencies in North Carolina to find out first-hand what works and what doesn't. Based on their research, Tufts and Weiss developed a 12-part checklist of issues that should be addressed whenever writing or negotiating a cloud-computing contract:

1. Pricing. "Pricing for cloud services," they write, "typically includes initial or upfront costs, maintenance and continuation costs, renewal costs, and volume commitments." Some contracts also include caps on the increases in costs permitted over time.

2. Infrastructure security. This encompasses "the supplier's responsibilities in the areas of information security, physical security, operations management, and audits and certifications."

3. Data assurances. In addition to determining responses to data breaches, Tufts and Weiss identify a number of related issues, including "ownership, access, disposition, storage location, and litigation holds."

4. Governing law. If there is a dispute, whose law will govern the case? Contracts should specify how and where any legal disputes will be settled, and should take into accounts different jurisdictions' laws. For example, the researchers note, North Carolina law "voids contract provisions that require disputes under contracts to be litigated outside of the state."

5. Service-level agreements. Cloud contracts should specify not only service-level parameters but also specific remedies and penalties for non-compliance.

6. Outsourced services. The contract "should require the vendor to inform the government of any outsourced functionality and its provider" while holding the primary vendor "directly responsible for all terms of the contract, regardless of outsourced functions."

7. Functionality. Cloud contracts should not only specify the functionality of the service being

purchased but should require advance notice if a function is to be changed or deleted along with a notification period to allow time to switch vendors if necessary.

8. Disaster recovery. Contract language concerning disaster recovery and business continuity should specify processes and safeguards "to protect the contracting public entity's data and services in the event of system failures."

9. Mergers and acquisitions. What will happen if the vendor becomes involved in a corporate merger or buy-out? Contracts should "articulate the responsibilities and transferability of contracts or contract terms."

10. Compliance with laws. In addition to language related to warranties and liabilities, cloud contracts should ensure that the vendor will comply with laws and regulations "of import to the contracting entity."

11. Terms and conditions modifications. Noting that many cloud contracts incorporate terms and conditions that are posted online and could be changed by the vendor at any time, Tufts and Weiss recommend that "the active terms and conditions at the time of contract signature should be incorporated as an exhibit for future reference purposes."

12. Contract renewal and termination. "Since switching cloud vendors can be costly and involve significant planning," Tufts and Weiss write, "contract renewal and termination clauses are critically important." For example, "the contract should specify how data will be retrieved/returned upon termination by either party."

Based on their interviews, evaluation and analysis of various public-sector contracts, Tufts and Weiss identify three key lessons for those considering the transition to cloud computing:

First, IT professionals should not select cloud solutions without legal and procurement help. IT staff can evaluate a contract based on its technical merits but generally have limited knowledge of legal and procurement issues that public-sector officials must be aware of to minimize exposure to legal risk.

Second, agencies should negotiate their contracts rather than merely accepting the cloud solutions being offered via vendor-supplied master service agreements.

And to effectively negotiate a cloud contract, the public entity "has to be willing to seek alternative providers or solutions in the event that the government's contract terms cannot or will not be met," note the authors. The bottom line: All contracts involve some degree of risk.

Read the report at:

http://www.businessofgovernment.org/sites/default/files/Cloudy%20with%20a%20Chance%20of%20Success.pdf

BY JOHN M. KAMENSKY | JANUARY 2, 2014