Cloud Computing – Questions to Ask

Pursuant to the Federal Cloud Computing Strategy[1] and the Cloud First policy, agencies are required to "evaluate safe, secure cloud computing options before making any new [technology] investments."[2]

The Cloud First policy lists "security, service and market characteristics, government readiness, and lifecycle stage" as "key considerations" when determining whether to migrate to the cloud.[3]

In light of these cited policies and concerns, I compiled some questions to ask to ensure that agencies and components review all risks and costs of the cloud technology accurately and thoroughly before deciding to move data into the cloud. These questions provide a baseline to determine if remedial action needs to be taken or if unacceptable levels of risk were ignored outright or accepted inappropriately.

Sabrina M. Segal
Counsel to the IG, USITC

Baseline Questions

1. Is there a business case for moving into the cloud?
2. Is the business case sufficient?
    a. Sufficient =
        i. Has a business need been identified?
        ii. Has a cost/benefit analysis been completed?
        iii. Have all risks and costs to mitigate those risks been addressed?

Risks

The risks listed below are a starting point and not an exhaustive list. The risks will change depending on:

(1) the information, applications, or data that an agency is moving to the cloud;

(2) the result should that information be compromised; and

(3) the level of mitigation acceptable to the agency.

Agencies should be sensitive to the "cost to mitigate" these risks and this cost should be included in the cost/benefit analysis. For example, if it costs an agency $300,000 to run their

[1] Vivek Kundra, Federal Cloud Computing Strategy, February 8, 2011.
[2] Id., p.2.
[3] Id., p.12.

email system and it will only cost $30,000 in the cloud, an agency should take into consideration that it will cost another $30,000 every time they need to access the cloud system to respond to a litigation or FOIA request, an additional $100,000 to have a backup cloud system on standby incase the primary one goes offline, etc. In the end, instead of $270,000 in savings, the agency may find that the actual savings are much smaller.

1. Data Security

    a. Access to live data:

        i. Can the vendor access or use the agency's data? Singularly or in aggregate?

        ii. What other third parties will have access to the agency's data? For what purpose?

        iii. Is data-at-rest readable by on-site staff? Is it encrypted?

        iv. Who has physical access to the live data? How are they vetted?

        v. Will all vendor employees be required to sign NDAs?

        vi. How is live data destroyed? Who ensures that it is destroyed and how is it documented?

    b. Access to backup data:

        i. Are backups to tape encrypted?

        ii. Who has access to these tapes? How are they vetted?

        iii. How is backup data destroyed? Who ensures that it is destroyed and how is it documented?

    c. Access to network traffic:

        i. Is all network traffic encrypted?

        ii. How is it encrypted?

        iii. Who can decrypt the network traffic?

        iv. Who controls access to the network?

        v. How is the network monitored?

        vi. How will TIC impact the cloud system?

d. Security incidents:

    i. How is incident response handled? Definition of incident response? Timeliness of incident response? Type of notice provided when incident occurs? Within how many hours must the vendor notify the agency?

    ii. Does the vendor have a duty to collect and retain information that is relevant to security incidents?

    iii. Who is responsible for incident investigation? Vendor or agency?

    iv. Is the vendor responsible for providing a written report concerning the incident? Within how many days? Must the report contain any remedial action taken or planned to be taken to mitigate damage?

    v. Can the agency run forensic tools on the cloud system?

    vi. Is the vendor required to cooperate in any post-incident administrative or legal proceedings?

    vii. Does the vendor have a duty to cooperate in the investigation and resolution of security incidents? Can the agency control the investigation?

e. Geographic status:

    i. What are the geographic boundaries? Where are the servers located? CONUS? Is the vendor required to notify the agency if the location of the serves changes? Advance notice?

    ii. How will the location impact the access and security of the data?

f. Additional data:

    i. Does the vendor have an obligation to implement additional security or other safeguards identified by the agency? Will there be any additional costs?

    ii. Will the agency receive copies of any third-party security audits conducted on the vendor's cloud system?

2. Compliance

a. Statutorily Required Compliance

    i. Privacy Act compliant?

    ii. Federal Records compliant?

    iii. HIPAA and HITECH compliant?

    iv. Does the vendor have a duty to cooperate with government compliance requirements?

b. Special Data

    i. What will happen when there is a classified spill onto the unclassified system?

    ii. How will law enforcement and intelligence data be protected? Who will have access?

c. Will the vendor indemnify the government for harm done should data be lost or leaked?

d. Will information on the cloud continue to be “nonpublic” without some additional protection (i.e., encryption)?

3. Termination & Transition

    a. How do we cancel the contract and migrate the data and/or applications? What type of notice is required? Timeframe?

    b. Can we terminate for convenience as well as cause?

    c. What is the guarantee that the data and/or applications will work once outside of the Cloud provider’s systems?

    d. How are data/applications and their media destroyed? How is the information “wiped?” How is hardware destroyed? What proof is provided that these steps have taken place?

    e. How long does the vendor retain the information after termination? What are the lasting data sensitivities after a contract ends?

4. Asset Availability

    a. Where are the servers located?

    b. What is the data availability and disaster recovery plan for the vendor?

    c. How will hardware/software compatibility with the agency be ensured? What happens if the vendor deploys something not compatible with the agency?

    d. What types of software updates is the vendor responsible for? What is the agency responsible for? Hardware?

    e. Will the vendor maintain “state-of-the-art” communication protocols?

    f. If there is an outage and the vendor knows ahead of time, how much notice must they give the agency?

    g. If there is an outage and the vendor did not know about it, how long is an acceptable time to be down before a reduction in cost? What type of communication must the vendor provide to the agency regarding the outage?

    h. What is an acceptable response time if an emergency takes the system offline?

    i. Does the agency have a back-up cloud provider keeping in sync with primary vendor?

5. Maintenance

    a. How are upgrades and maintenance handled? What type of notice is provided to the agency?

    b. Who is responsible for timing and implementation of major/minor updates and patches?

    c. How does the contract specify update timing requirements? What is the incentive for the vendor to do updates in a timely fashion?

    d. What types of software updates is the vendor responsible for? What is the agency responsible for? Hardware?

    e. How is version control handled?

    f. How will upgrades be coordinated to insure compatibility?

6. Pricing & time

    a. What is the baseline cost for the cloud system? What is the cost with the additional needs and requirements of the agency?

    b. Will there be additional costs for information access (i.e., FOIA, IG investigations, e-discovery, litigation holds, subpoenas, etc.)?

    c. How will e-discovery and FOIA be handled? Will the agency be able to ensure chain of custody and authenticity? Additional cost?

    d. Does the vendor have a duty to cooperate in any litigation involving the agency including a duty to preserve and cooperate with any discovery requests? How quickly (hours) must the vendor notify the agency if they receive a subpoena or other legal process?

    e. What is the additional cost for compliance requiring vendor personnel?

    f. Will the agency have access to all agency meta data?

7. Intellectual Property

    a. What are the boundaries for access to data for the vendor? Are there any boundaries for the agency accessing vendor systems?

    b. How will infringing material found on the system be handled?

    c. What is the level of indemnity provided by the vendor or the government? Is it open-ended (consider Anti-Deficiency Act)?

    d. Are there restrictions to vendor IP (consider IG investigations and audits)?

8. Investigation Concerns

    a. How will electronic forensic tools run on the cloud? Will they be allowed?

    b. How will law enforcement and intelligence data be protected? Who will have access?

    c. Will there be an extra cost or restrictions on the type and depth of investigations and audits the IG can do on the system?

    d. Are there any boundaries for the agency accessing vendor systems? Are there restrictions to vendor IP (consider investigations and audits)?

e. Does the vendor have a duty to cooperate with the IG/SEC? Can the IG/SEC control the investigation?

f. How frequently and to what depth will the IG be able to audit the cloud system? Will standards such as SAS-70 or ISO 27002 be set?

g. Will the IG/SEC be required to provide notice when accessing the cloud system? Will the IG/SEC have the same unrestricted access to information as they do on agency systems?

h. Does the vendor have an obligation to implement additional security or other safeguards identified by the IG/SEC? Will there be an additional cost?

i. What type of search and authentication is provided by the vendor?

j. Will there be an extra cost or restrictions on the type and depth of investigations and audits the IG can do on the system?

k. What type of search and authentication is provided by the vendor?

Please feel free to contact me if you have any questions about this subject.

Sabrina M. Segal
Counsel to the Inspector General
United States International Trade Commission
500 E St., SW Washington, DC 20436
Phone: 202-205-3360
Fax: 202-205-1859
sabrina.segal@usitc.gov