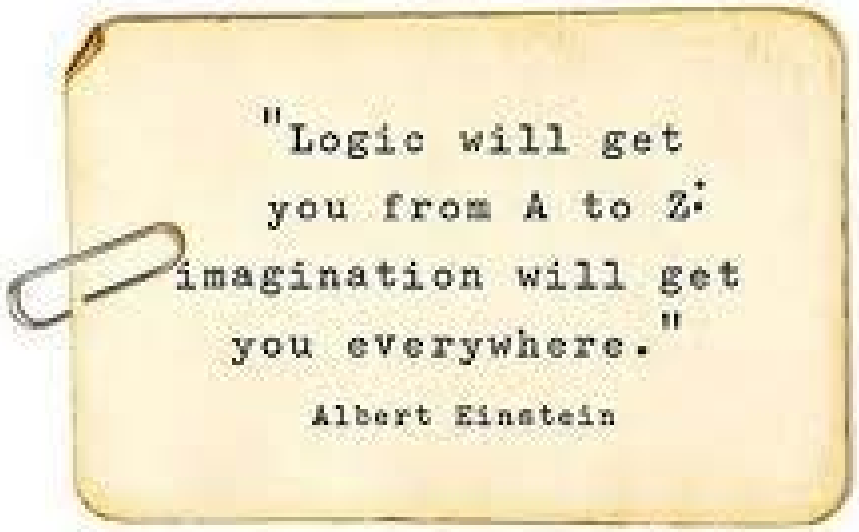
Hey, you, get off of my cloud!

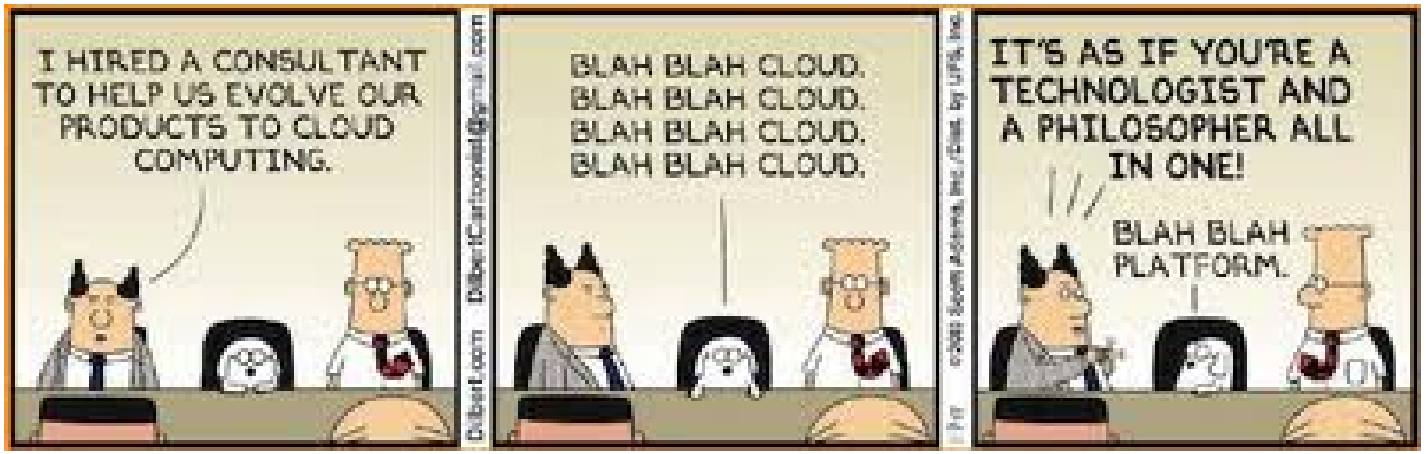
Negotiate your cloud contract to get what you need and mitigate risk

Presented by:
Sabrina M. Segal, USITC,
Counselor to the Inspector General and Assistant Inspector General for Investigations
Sabrina.segal@usitc.gov

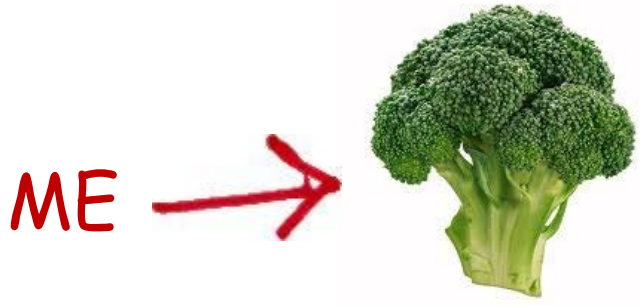
Imagination Time



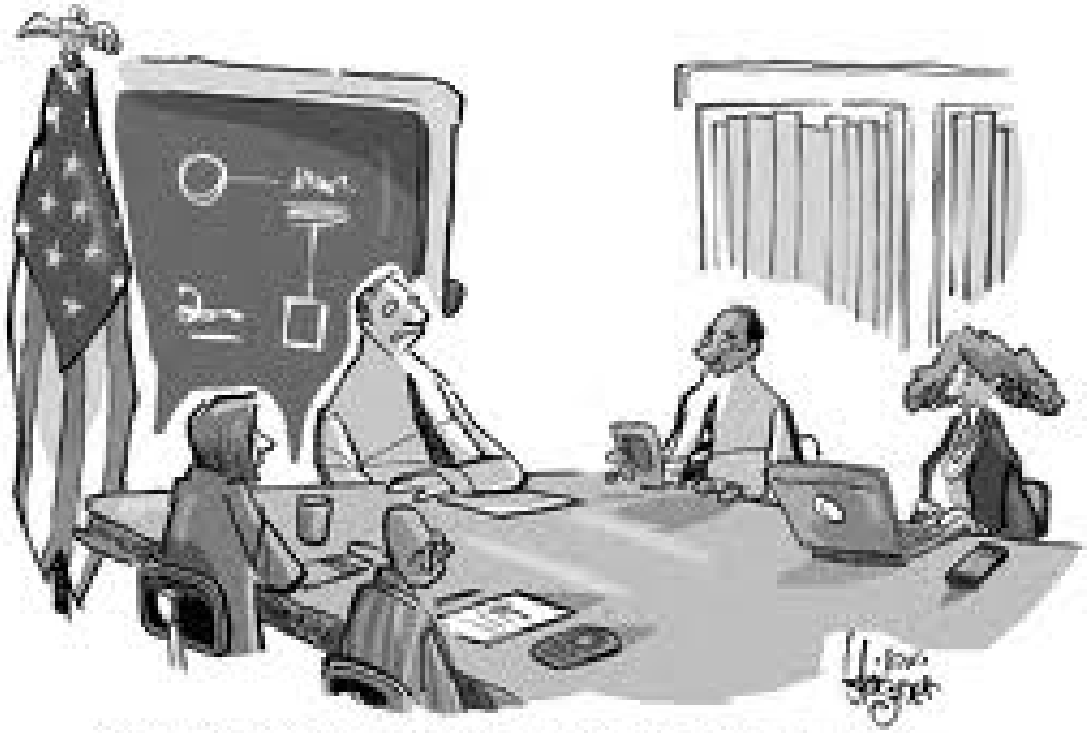
Caveat Emptor



Be careful from whom you ask and receive advice….



Is this you?


"IT'S NOT THAT I DON'T WANT TO TRY WEB 2.0 TECHNOLOGY. IT'S JUST THAT I'M STILL GETTING USED TO THE FAX MACHINE."

Or is this you?

Remember, you can't outsource responsibility.

Cloud Computing:

What is it?

So what is this “cloud”….?

“The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. … The computer industry is the only industry that is more fashion-driven than women's fashion. Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish. It's insane. When is this idiocy going to stop?”

Larry Ellison, CEO of Oracle, 2008

http://news.cnet.com/8301-13953_3-10052188-80.html

So what is this "cloud"….?

I'm from the Government and I'm here to help…

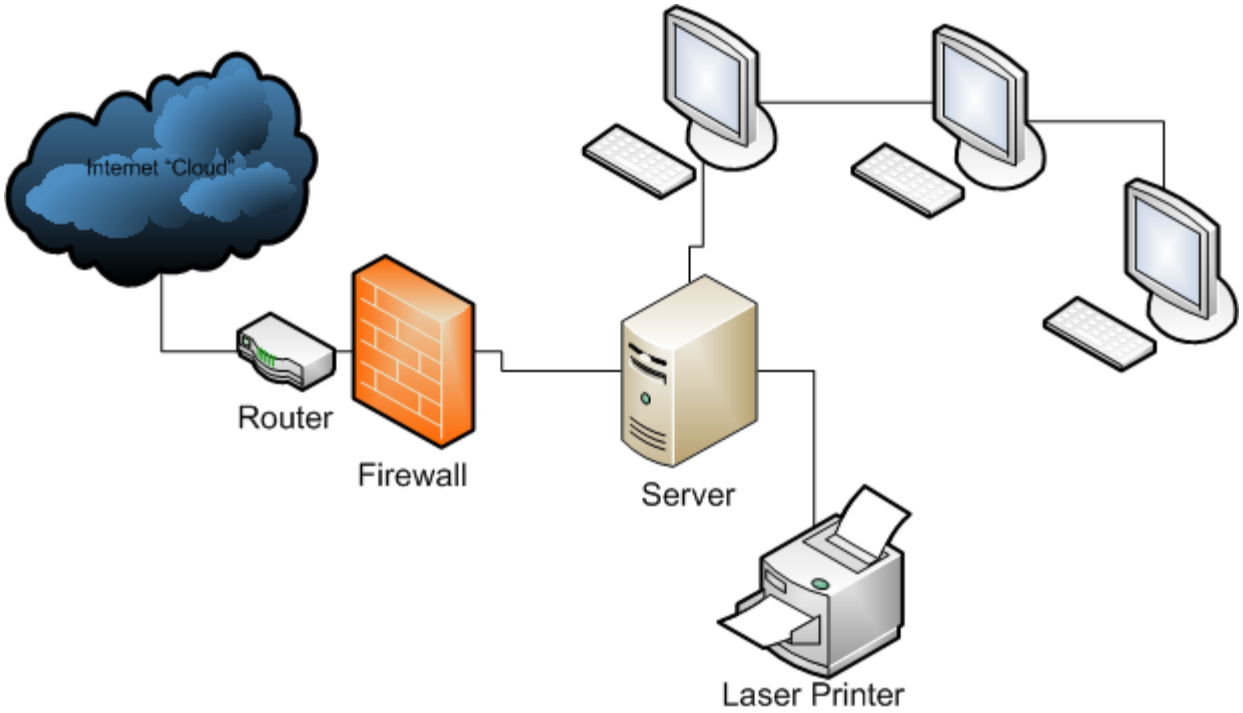
"Cloud computing is a model for enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."

- NIST Definition of Cloud Computing, September 2011

Helpful, right?

Traditional Computing v. Cloud Computing

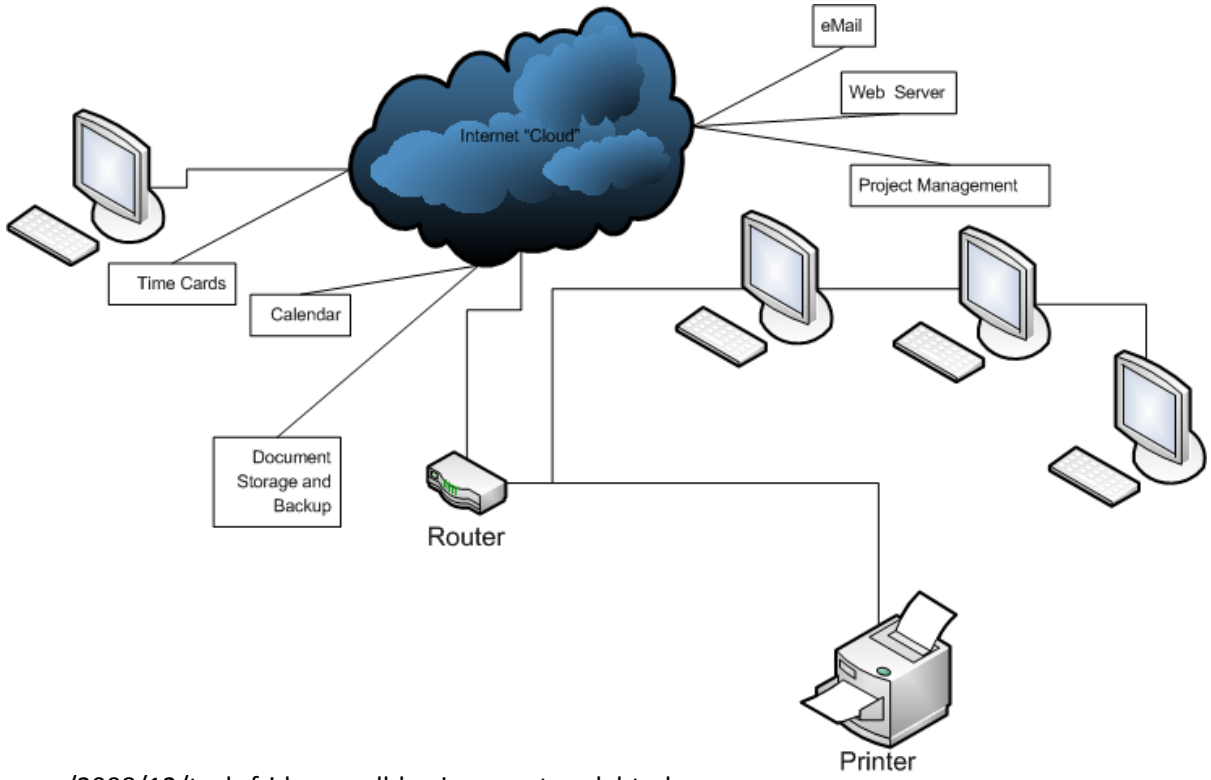
In the traditional model of computing, both data and software are fully contained on the user's computer.



http://blog.techfornonprofits.com/2008/12/tech-friday-small-business-network.html

Traditional Computing v. Cloud Computing

In cloud computing, the user's computer may contain almost no software or data (perhaps a minimal operating system and web browser only), serving as little more than a display terminal for processes occurring on a network of computers far away.



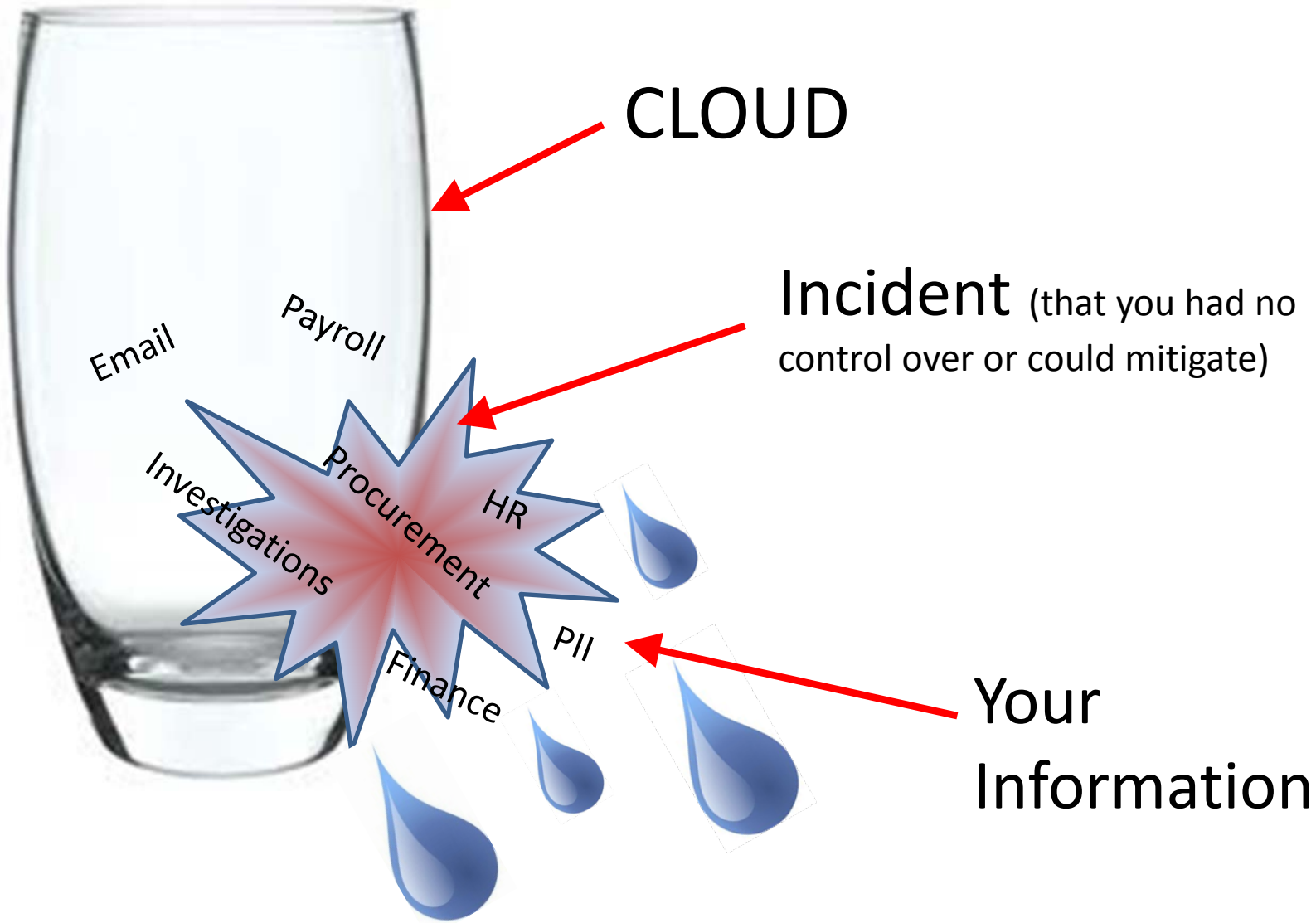
http://blog.techfornonprofits.com/2008/12/tech-friday-small-business-network.html

One last attempt to explain the Cloud…

Your Information

CLOUD

One last attempt to explain the Cloud…



Types of Clouds

Types of Clouds

RISK

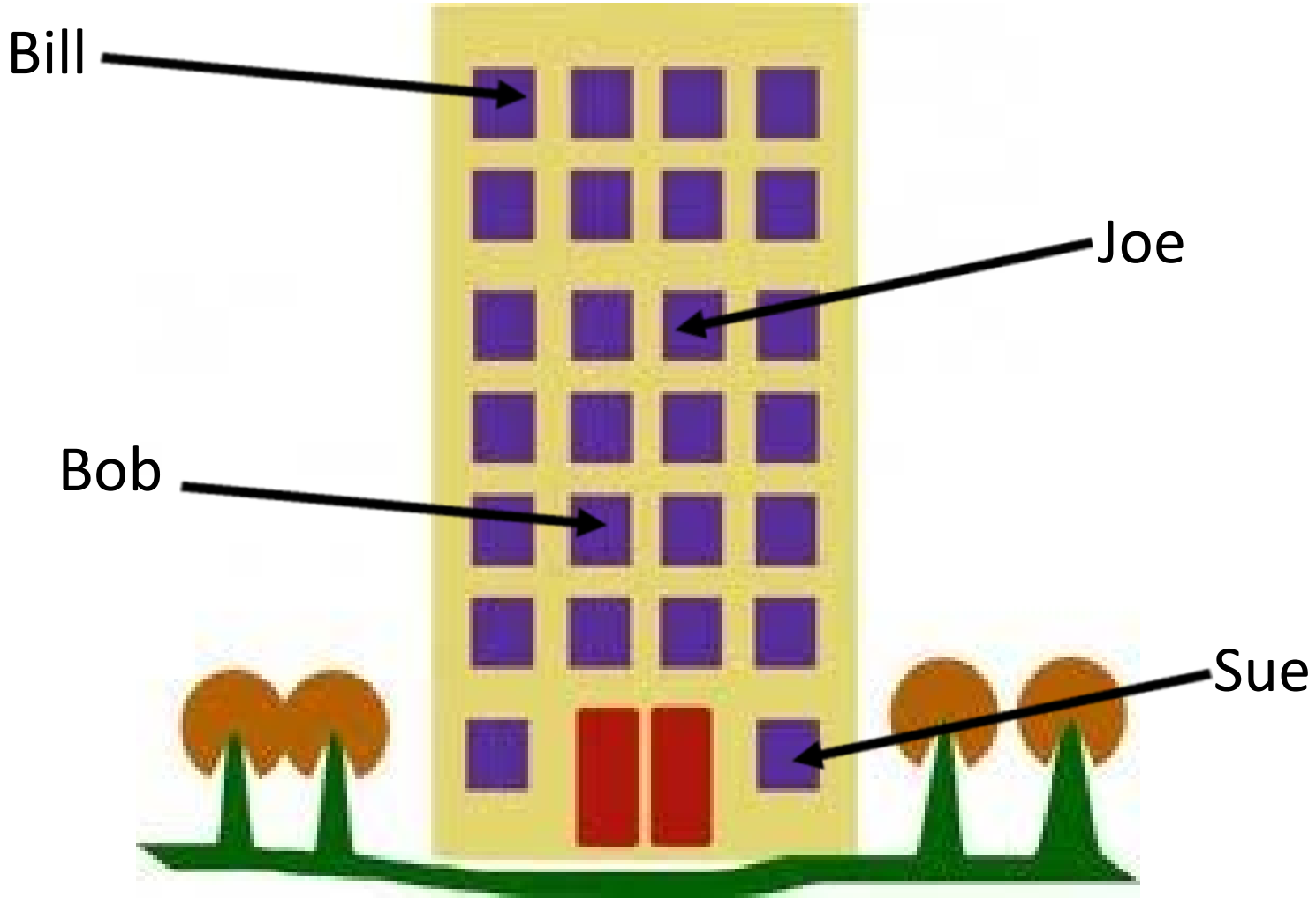
Public cloud - The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Community cloud - The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

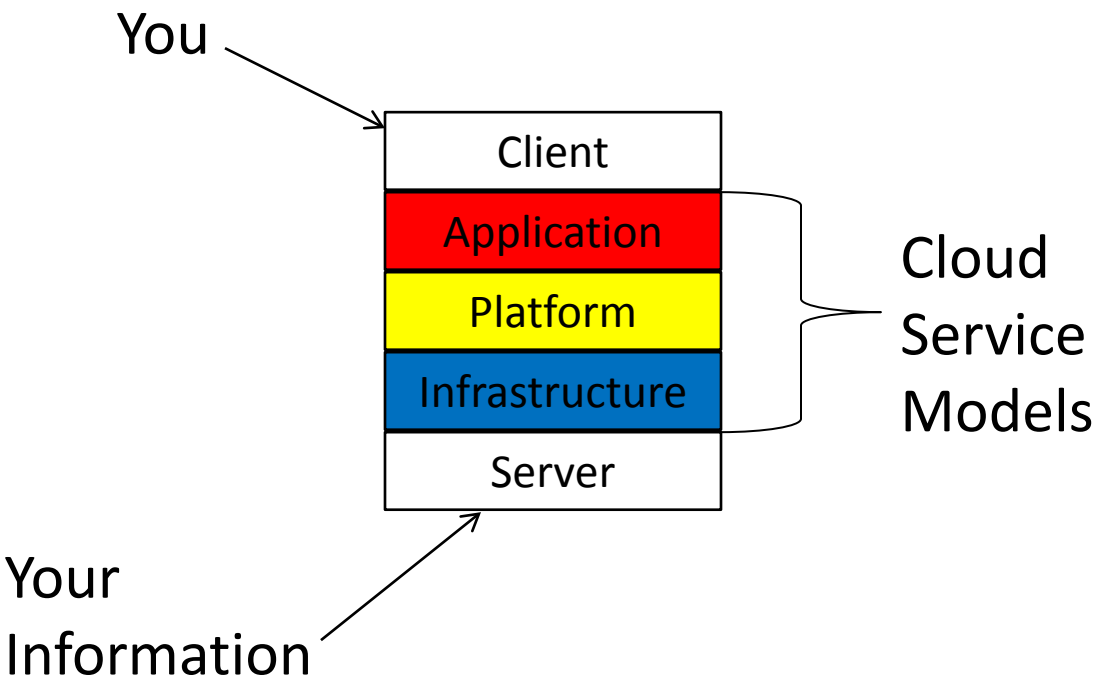
Private cloud - The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Hybrid cloud - The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Public Cloud, Multi-tenant Environment



Cloud Computing Service Models

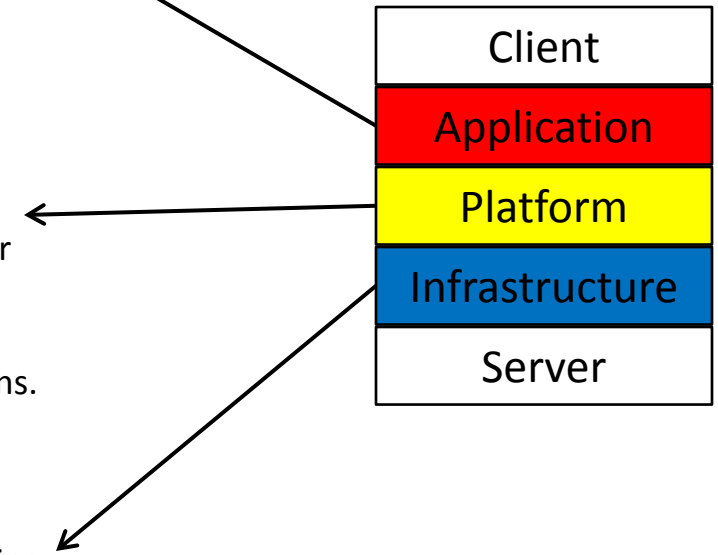


Cloud Computing Service Models

Cloud Software as a Service (SaaS) - applications are accessible from various client devices through an interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS) - the ability to deploy consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS) – provides processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).



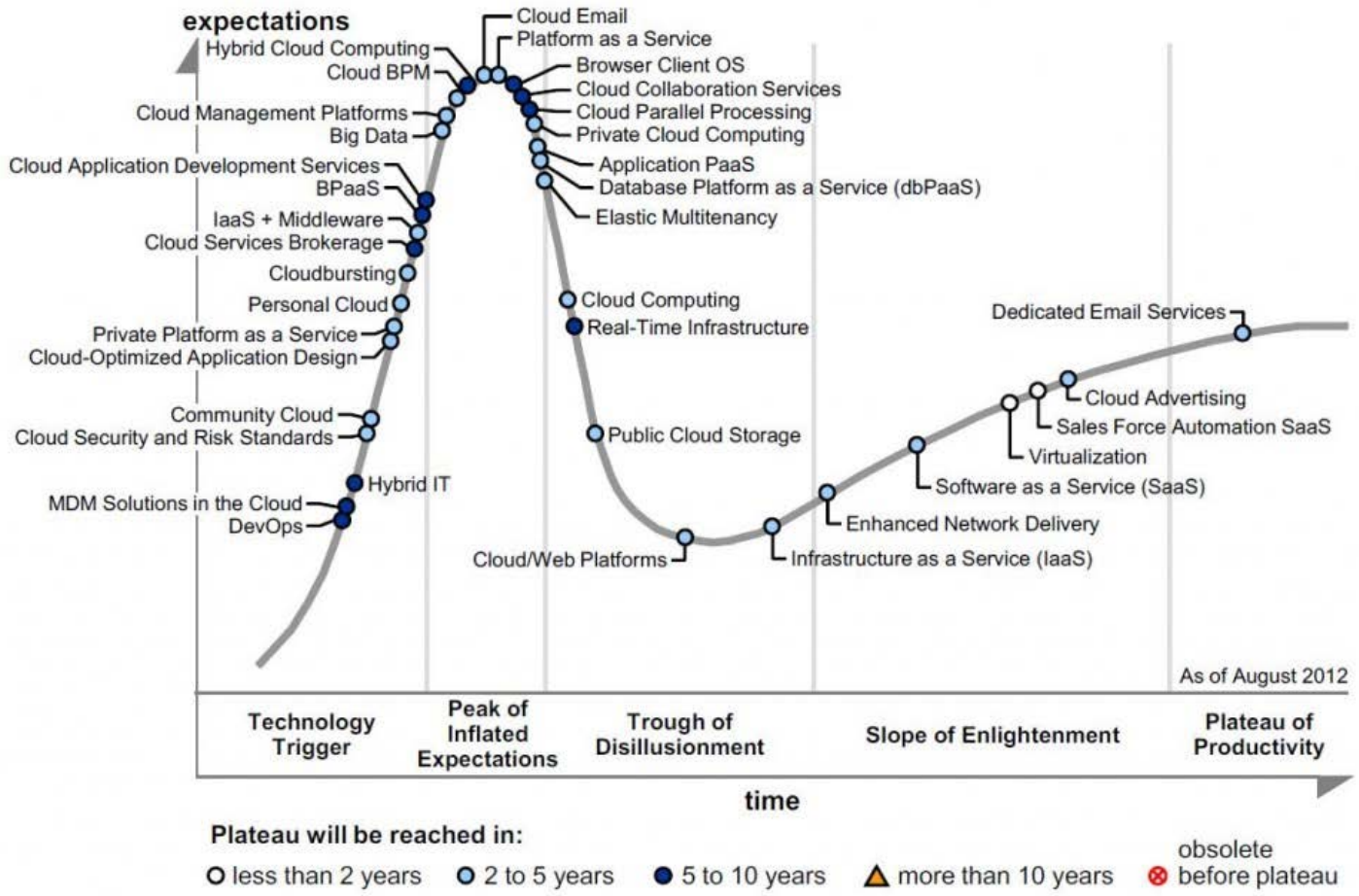
Cloud Computing:

What to worry about?

Gartner Hype Cycle

Gartner Hype Cycle: Where are we now?

Figure 1. Hype Cycle for Cloud Computing, 2012



Source: Gartner (August 2012)

Two Baseline Questions to Ask Yourself Before You Move to the Cloud

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?

Eight Risks to Address Upfront

1. Data Security/Sovereignty
2. Compliance
3. Termination & Transition
4. Asset Availability and Bandwidth
5. Maintenance
6. Pricing and Time
7. Intellectual Property
8. Inspector General needs (aka – audit, investigation, and validation)

** *Always consider mission specific issues*

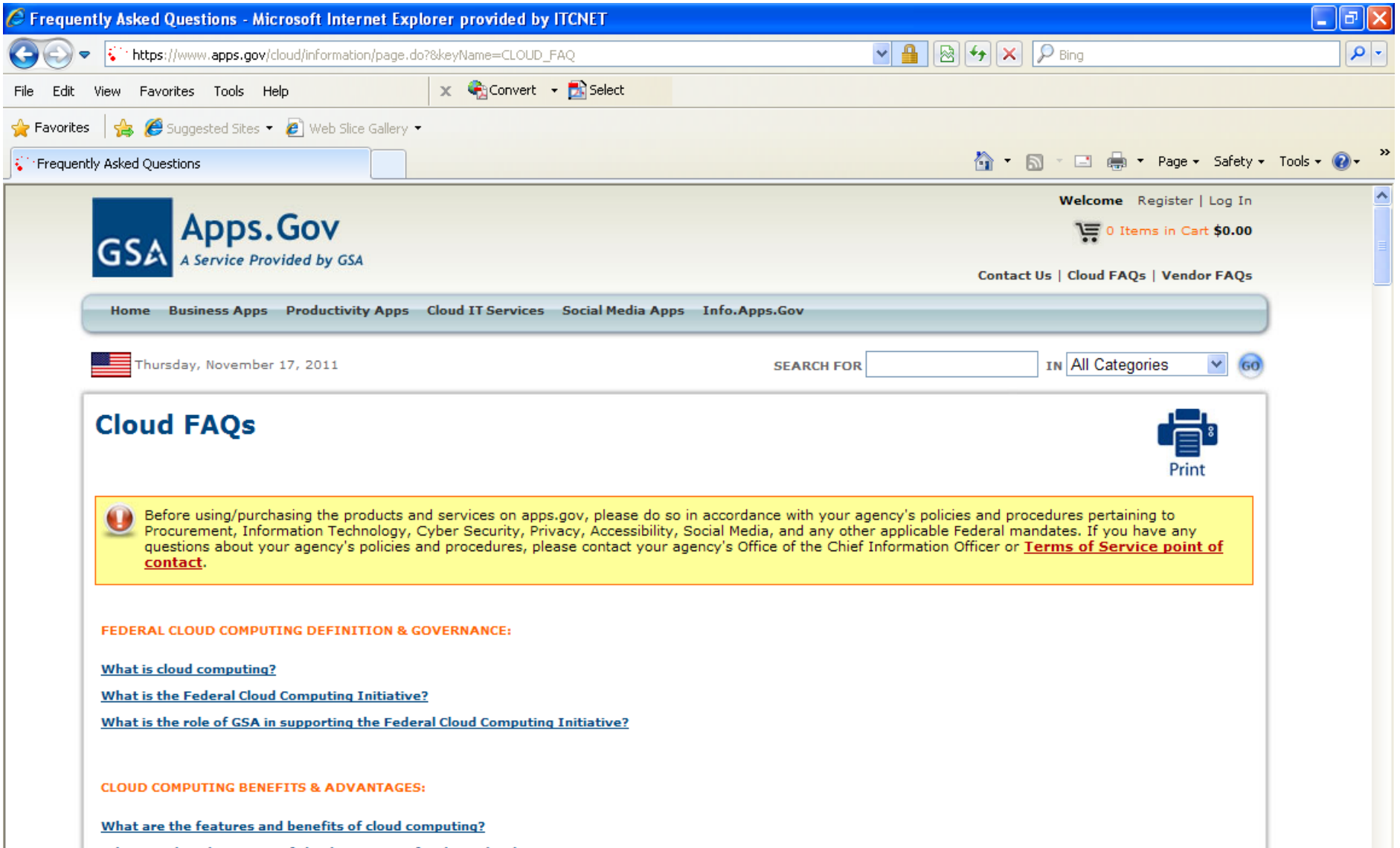
But how do I do that?

Negotiate!

1. Data Security/Access

- Access to live and backup data (ie – encryption, location, destruction, etc.)
- Access to network traffic (ie – monitoring, law enforcement, EINSTEIN, TIC, etc.)
- Incident Response (ie – timing, reporting, forensics, etc.)
- Proper configuration?
- Encryption in motion? At rest?
- Physical security and data sovereignty (location of data, ie – CONUS?)
- Vendor obligations and duties
- Disposal of data (and hardware)

Fair Warning?



2. Compliance

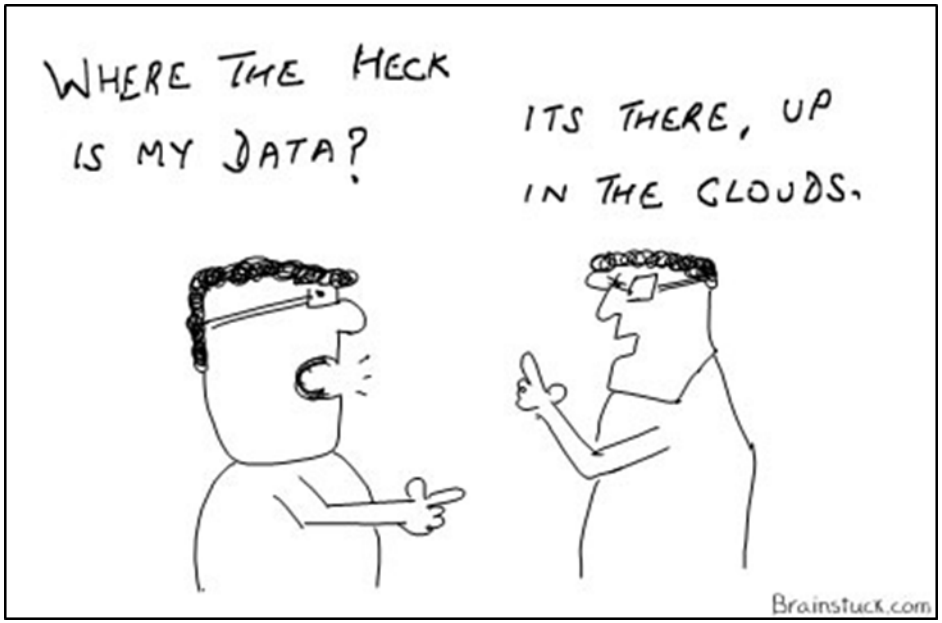
- Statutorily Required Compliance (ie - Privacy, transparency, e-discovery, accessibility, etc.)
- Law enforcement, intelligence data, CJIS compliant?
- Non-disclosure agreements, background checks
- Timeliness
- Treatment of non-public information
- Government Indemnification

3. Termination & Transition

- How will data be protected, conveyed, and destroyed? Proof?
- What are the lasting data sensitivities after a contract ends?
- In what format will the data be provided for transition?
- Timing for termination and transition?
- Bankruptcy, sale, merger of provider?

4. Asset Availability and Bandwidth

- Data availability/disaster recovery?
- Hardware/software compatibility with agency?
- Software updates?
- Hardware refresh?
- Estimated outage time and frequency?
- Response time if an emergency takes system offline?
- Bandwidth capabilities?



5. Maintenance

- Patching?
- Version control?
- Compatibility with legacy hardware and software?

6. Pricing and Time

- Additional cost for information access (ie – transparency, litigation, IG, LE needs, etc.)?
- Address time requirements for compliance?
- Cost for “out of the box” v. government requirements?
- Cost for back up cloud?

Actual costs?

Cloud Savings!

Cloud Costs

Reality

Cloud Costs

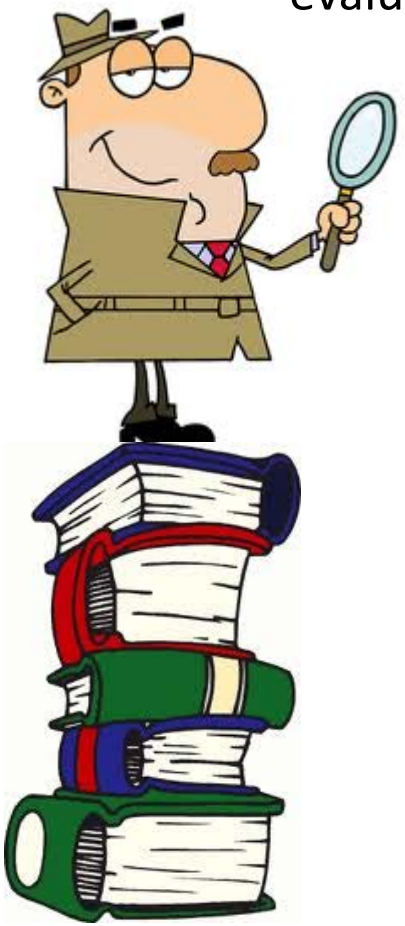
- Cloud Savings!
- Back-up for the Back-up
- Data Access / transparency / e-discovery
- Incident Response

7. Intellectual Property

- Protect government and set boundaries for vendor
- How will infringing material be handled if found on the network? Third party requests for removal?
- Level of indemnity provided by vendor or government if infringement? Third party claim?
- Access to vendor IP (especially for IG investigations and audits)?
- Data confidentiality and Trade Secrets protection?
- Pre-filing protection, liability for breach?

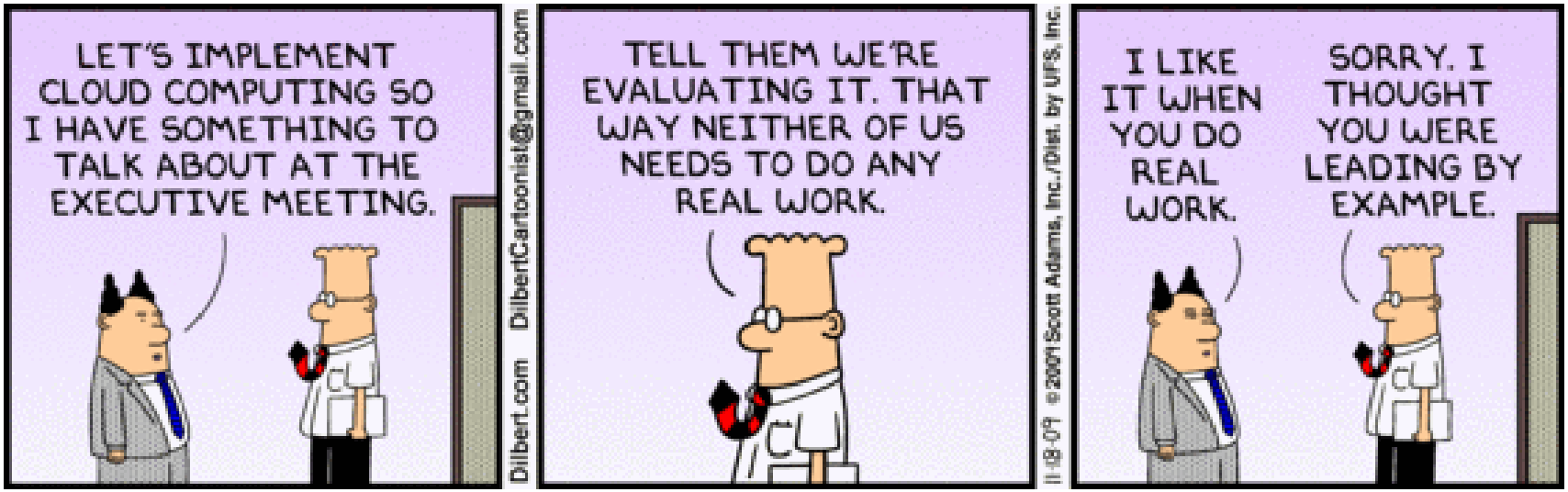
8. Inspector General needs

Inspectors General are responsible for promoting and preserving efficiency, effectiveness, and integrity within the agencies over which they have jurisdiction. They do this by conducting audits, evaluations, inspections, and criminal investigations.



- Clear and clean access to agency information and vendor facilities
- Ability to conduct criminal investigations (Wiretapping? Network monitoring?)
- Provider agreement to procedures and processes (information preservation, reporting, etc.)
- Unencumbered auditability of systems
- IG access at no additional cost

Ridiculously funny, but probably true…



Is this your CIO?

Cloud Computing:

What to negotiate?*

*** EVERYTHING!**

Have the right people at the table…

REALLY IMPORTANT →

- OCIO
- Client Office
- General Counsel
- Info Sec
- Management/Administration
- Inspector General

And identify what matters.

- Is the contract directly with a cloud vendor or is there an integrator (middleman/reseller)?
- Arbitration? Open indemnities? Advertising?
- Vague terms? (E.g., “industry standard,” “commercially reasonable,” “promptly notify”) Is everything defined?
- Make sure the contract/ToS/SLA/T&C/SLO etc. doesn’t rely or reference other agreements or policies which can be changed at any time. E.g., “Acceptable Use Policy,” “Domain Service Terms,” “Technical Support Services”
- If you have an integrator, what are the requirements /obligation of their agreement with the vendor?
- Who are the parties? “Affiliates?”

REMEMBER!

You can't outsource responsibility

Present ALL aspects of the technology to decision makers – pros and cons. If any aspect is withheld, especially cons, it will be impossible to defend the decision.

Thank you for your attention!

Questions?

Sabrina.segal@usitc.gov

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

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; (3) and 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 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 or integrator 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?

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

iii. Is data-at-rest readable by on-site staff? Is it encrypted? Where are the keys stored?
iv. Is data encrypted in motion? At rest?
v. Who has physical access to the live data? How are they vetted/cleared?
vi. Will vendor or integrator employees be required to sign NDAs?
vii. How is data destroyed? Who ensures that it is destroyed and how is it documented?

b. Access to backup data:
   i. Are backups to tape encrypted? Where are the keys stored?
   ii. Who has access to these tapes? How are they vetted/cleared?
   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? Where are the keys stored?
   iii. Who can decrypt the network traffic? Who has authority to use the keys?
   iv. Who controls access to the network?
   v. How is the network monitored?
   vi. TIC compliant?

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 what time limit must the vendor notify the agency? Hours? Days?
   ii. Does the vendor or integrator have a duty to collect and retain information that is relevant to security incidents?
   iii. Who is responsible for incident investigation? Vendor, integrator, or agency?
   iv. Is the vendor or integrator responsible for providing a written report concerning the incident? Within what time limit? Hours? Days? Must the report contain any remedial action taken or planned to be taken to mitigate damage?
   v. Can the agency independently run forensic tools on the cloud system?
   vi. Is the vendor or integrator required to cooperate in any post-incident administrative or legal proceedings?
   vii. Does the vendor or integrator have a duty to cooperate in the investigation and resolution of security incidents? Can the agency control the investigation?

e. Geographic status / data sovereignty:
   i. What are the geographic boundaries of the physical footprint? Where are the servers located? CONUS? Is the vendor or integrator required to notify the agency if the location of the serves changes? Advance notice?
   ii. Even if physical footprint is overseas, can data be restricted to CONUS? How is this confirmed?
   iii. How will the location impact the access and security of the data? Third party / foreign government access?

f. Additional data:
    i. Does the vendor or integrator have an obligation to implement additional security or other safeguards identified by the agency? Will there be any additional costs?
    ii. Can/will third parties run security audits on the vendor or integrator's system? Will the agency receive copies of any third-party security audits conducted on the vendor or integrator's cloud system?
    iii. Who as access to audit logs?

2. Compliance
    a. Statutorily Required Compliance (including but not limited to)
        i. Privacy Act compliant? Privacy Impact Assessment?
        ii. Federal Records compliant? 5015.2 compliant?
        iii. HIPAA and HITECH compliant?
        iv. 508?
        v. HSPD-12?
        vi. FISMA?
        vii. Financial (Credit cards?)
        viii. Treatment of CBI/BPI information?
        ix. E-discovery?
        x. FOIA?
        xi. Does the vendor or integrator have a duty to cooperate with government or law enforcement 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 or integrator 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 (ie – encryption)? Is "nonpublic" information still nonpublic if it's on a public cloud?
3. Termination & Transition
    a. How is the contract with the vendor or integrator cancelled and the data / applications migrated? What type of notice is required? Timeframe?
    b. What is the guarantee that the data and/or applications will work once outside of the integrator or vendor's systems? Proprietary software? APIs?
    c. 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?
    d. How long does the vendor or integrator retain the information after termination? What are the lasting data sensitivities after a contract ends?
    e. What happens in the event of bankruptcy, sale, or merger of the integrator or vendor?

    f. What happens when the contract with the integrator ends but the cloud provider continues? Vice versa?
4. Asset Availability and Bandwidth
    a. Where are the servers physically located?
    b. What is the data availability and disaster recovery plan for the vendor or integrator?
    c. How will hardware/software compatibility with the agency be ensured? What happens if the vendor or integrator deploys something not compatible with the agency?
    d. What types of software updates is the vendor or integrator responsible for? What is the agency responsible for? Hardware?
    e. Will the vendor or integrator maintain "state-of-the-art" communication protocols?
    f. If there is an outage and the vendor or integrator knows ahead of time, how much notice must they give the agency?
    g. If there is an outage and the vendor or integrator did not know about it, how long is an acceptable time to be down before a reduction in cost? What type of communication and when must the vendor or integrator provide to the agency regarding the outage?
    h. What is the definition of "down time?"
    i. What is an acceptable response time if an emergency takes the system offline?
    j. Does the agency have a back-up cloud provider keeping in sync with primary vendor or integrator?
    k. What are the bandwidth requirements? What happens when there is an overload?
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 or integrator to install updates in a timely fashion?
    d. What types of software updates is the vendor or integrator 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 (ie – 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 or integrator 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/days) must the vendor or integrator notify the agency if they receive a subpoena or other legal process?

e. What is the additional cost for compliance requiring vendor or integrator personnel?
f. Will the agency have access to all agency related metadata?

7. Intellectual Property
    a. What are the boundaries for access to data for the vendor? Are there any boundaries for the agency accessing vendor or integrator systems?
    b. How will infringing material found on the system be handled?
    c. What is the level of indemnity provided by the vendor, integrator, or the government? Is it open-ended (consider Antideficiency Act)?
    d. Are there restrictions to vendor or integrator IP (consider IG investigations and audits)?
    e. Data confidentiality and Trade Secrets protection?
    f. Patent pre-filing protection, liability for breach?
8. System Transparency / Integrity
    a. How will electronic forensic tools run on the cloud? Will they be allowed?
    b. Will there be an extra cost or restrictions on the type and depth of investigations and audits the agency can do on the system? Does the agency have access to the logs?
    c. Are there any boundaries for the agency accessing vendor or integrator systems? Are there restrictions to vendor IP (agency inspections and audits)? Will the vendor provide a diagram of the network configuration?
    d. Does the vendor or integrator have a duty to cooperate with the agency? Have they agreed to procedures/processes? Can the agency control security investigations?
    e. How frequently and to what depth will the agency be able to audit the cloud system? Will standards such as SAS-70 or ISO 27002 be set?
    f. Will the agency be required to provide notice when accessing the cloud system? Will the agency have the same unrestricted access to information as they do on agency owned systems?
    g. Does the vendor or integrator have an obligation to implement additional security or other safeguards identified by the agency? Will there be an additional cost?
    h. What type of search and authentication is provided by the vendor or integrator?
    i. Will there be an extra cost or restrictions on the type and depth of investigations and audits the agency can do on the system?
    j. Are the vendor's partners/subcontractors as transparent and accessible?
9. Inspector General / Investigation Concerns
    a. How will law enforcement and intelligence data be protected? Who will have access?
    b. Will there be an extra cost or restrictions on the type and depth of investigations and audits the IG can do on the system? Does the IG have access to the logs?
    c. Are there any boundaries for the IG accessing vendor or integrator systems? Are there restrictions to vendor IP (consider investigations and audits)? Will the vendor provide a diagram of the network configuration?
    d. Does the vendor or integrator have a duty to cooperate with the IG? Have they agreed to procedures/processes? Can the IG control the investigation?
    e. 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?

f. Will the IG be required to provide notice when accessing the cloud system? Will the IG have the same unrestricted access to information as they do on agency systems?
g. Does the vendor or integrator have an obligation to implement additional security or other safeguards identified by the IG? Will there be an additional cost?
h. Will there be an extra cost or restrictions on the type and depth of investigations and audits the IG can do on the system?