Cloud Computing in the Federal Sector: What is it, what to worry about, and what to negotiate.

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

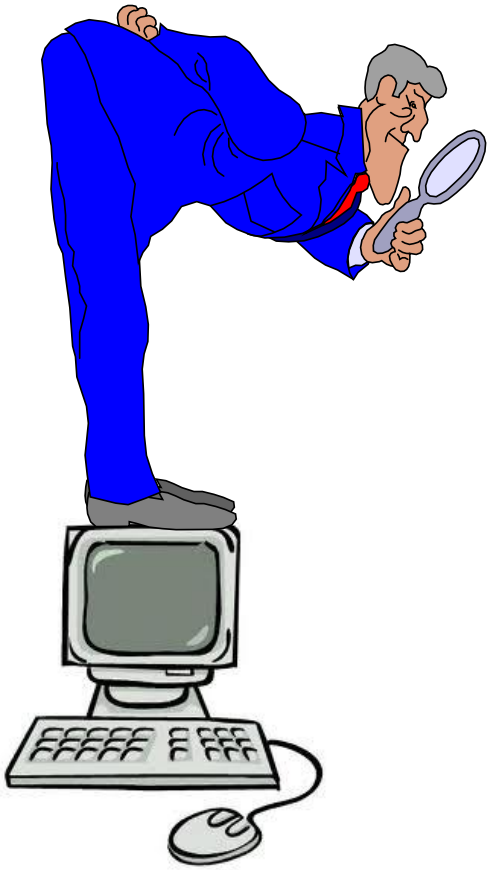
Gartner Hype Cycle: Where are we now?

Cloud Computing:

What is it?

So what is this "cloud"….?

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



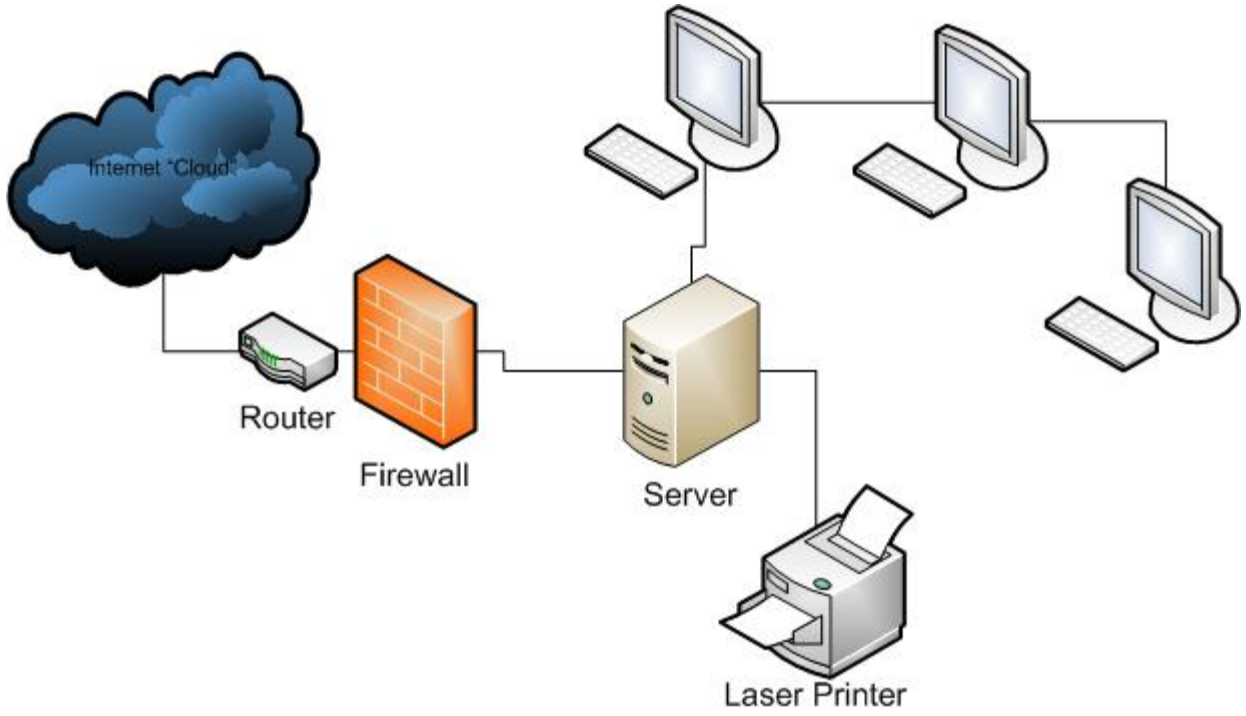
Cloud computing is defined by the National Institute of Standards and Technology (NIST) as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." NIST has identified five essential characteristics of cloud computing: on-demand service, broad network access, resource pooling, rapid elasticity, and measured service.

- Federal Cloud Computing Strategy, February 8, 2011

Helpful, right?

Traditional Computing v. Cloud Computing

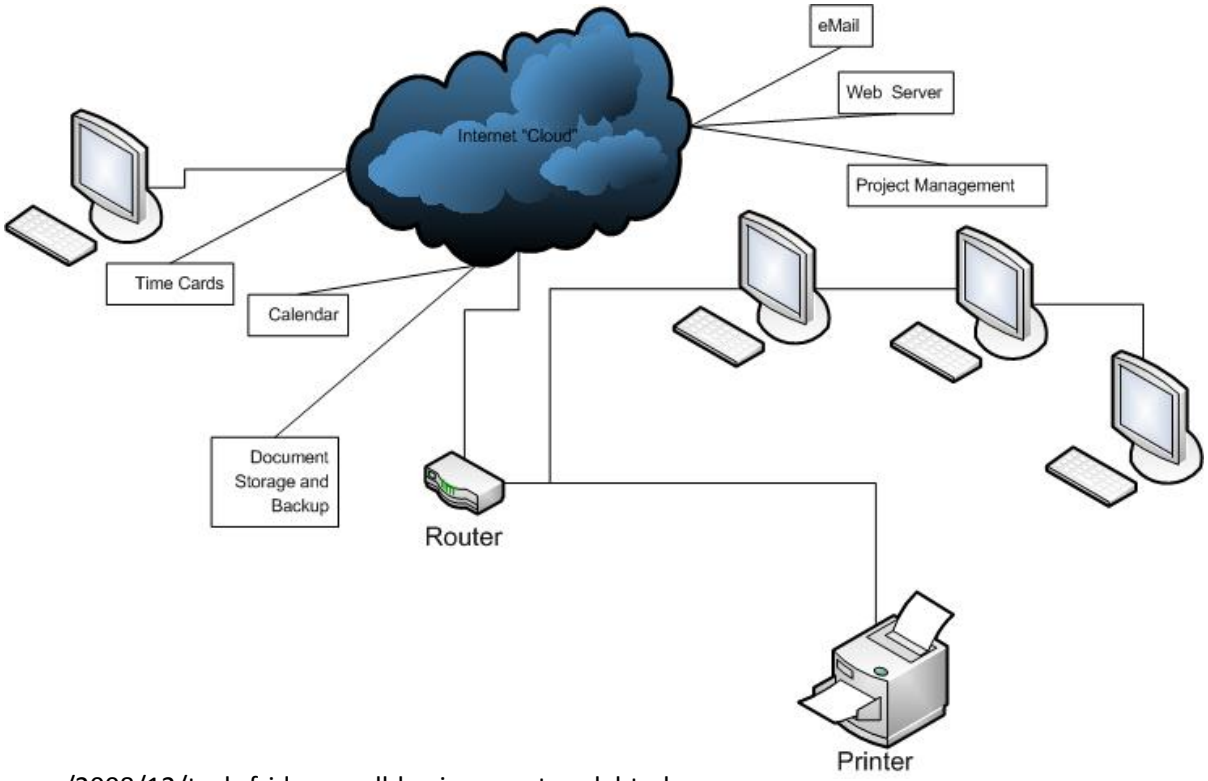
In the traditional model of computing, both data and software are fully contained on the user's computer.



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.



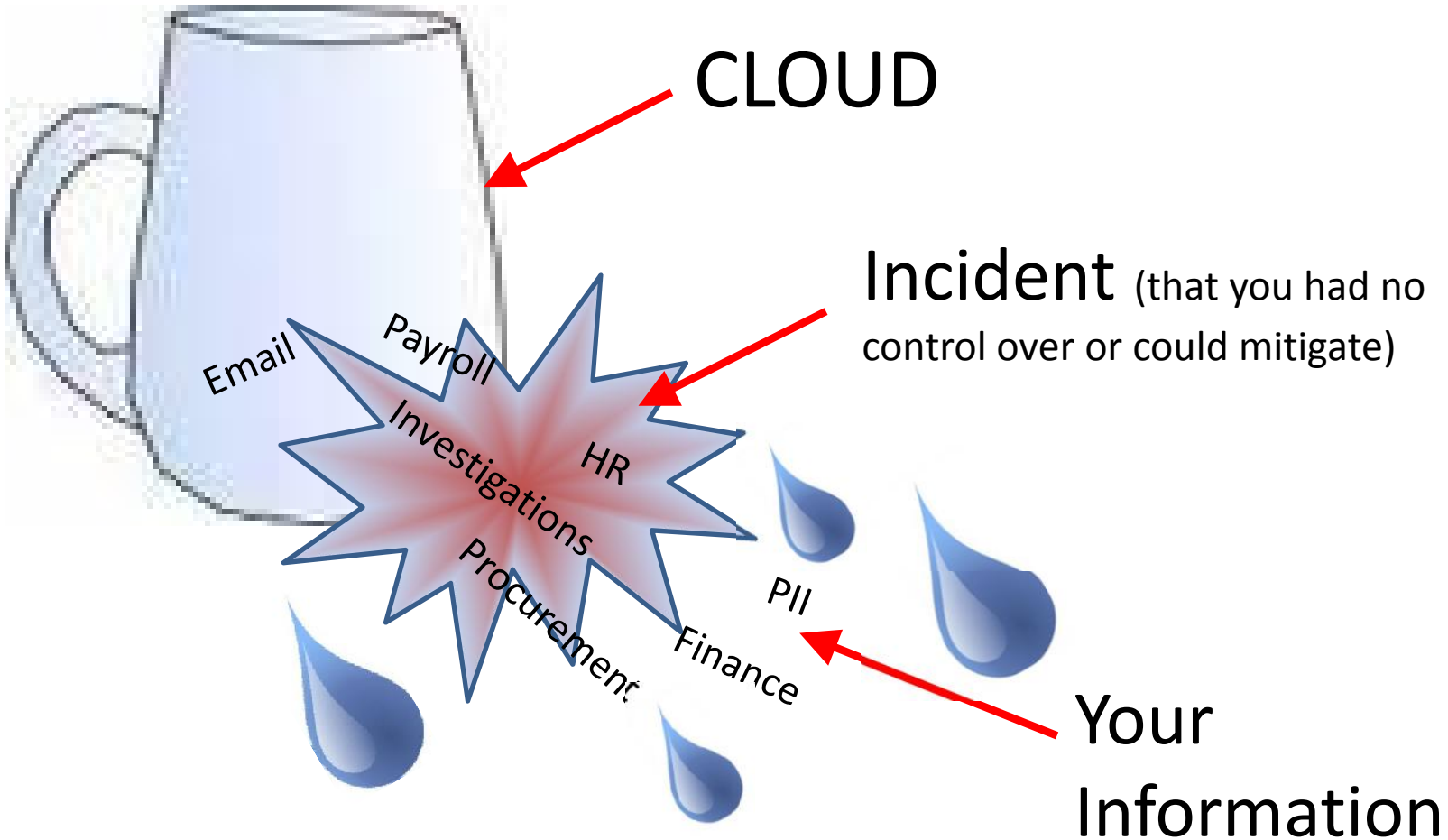
http://blog.techfornonprofits.com/2008/12/tech-friday-small-business-network.html

One last attempt to explain the Cloud….

Your Information

CLOUD

One last attempt to explain the Cloud….



Types of Clouds

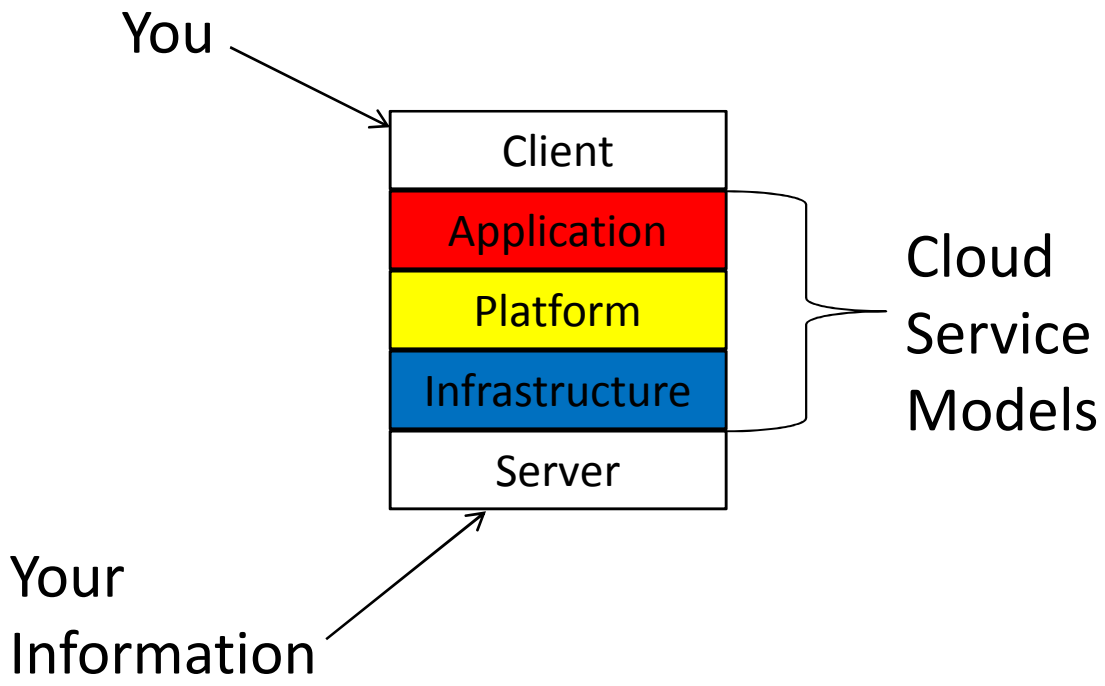
Private cloud - The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

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.

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.

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).

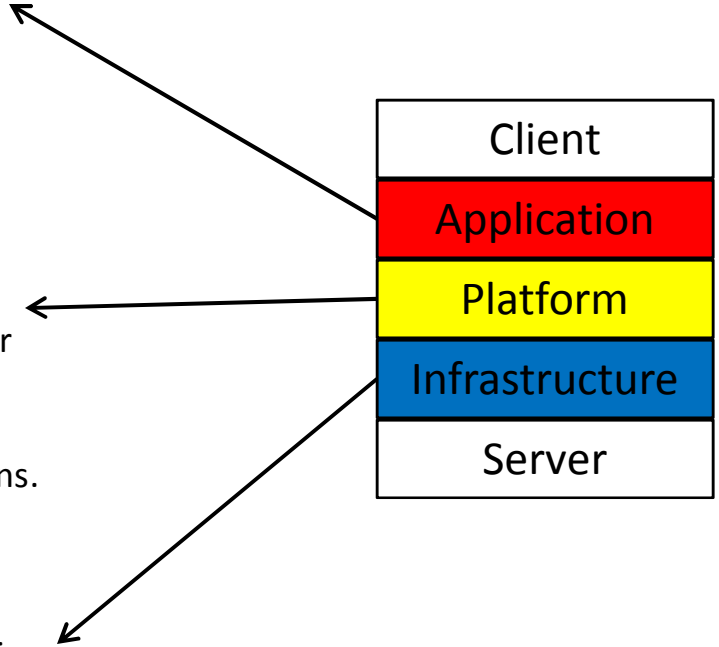
Cloud Computing Service Models



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?

Some Questions to Think About

- Who has access to the data, both in its live state and when backups are made?
- How is the data handled? Encryption?
- What are the vendor obligations?
- What are the geographic boundaries? Where are the servers located and how will this impact the access and security of the data?
- What are the incident response guidelines?
- How are the upgrades and maintenance handled?
- Can the vendor access or use the information in aggregate?
- How do we cancel the contract and migrate the information?
- How are data and media destroyed?

Eight Concerns to Address Upfront

1. Data Security
2. Compliance
3. Termination & Transition
4. Asset Availability
5. Maintenance
6. Pricing and Time
7. Intellectual Property
8. Inspector General needs

** *Always consider office specific issues*

But how do I do that?

Negotiate!

1. Data Security/Access

- Access to live and backup data (ie – encryption, access, destruction, etc.)
- Access to network traffic (ie – monitoring, EINSTEIN, TIC, etc.)
- Incident Response (ie – timing, reporting, forensics, etc.)
- Physical security and location of data (ie – CONUS?)
- Vendor obligations and duties
- Disposal of data (and hardware)

2. Compliance

- Statutorily Required Compliance (ie - Privacy Act, FISMA, Federal Records Act, FOIA, e-discovery, etc.)
- Classified Information (Spills?)
- Law enforcement, intelligence data
- Non-disclosure agreements
- 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?

4. Asset Availability

- 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?

5. Maintenance

- Patching?
- Version control?
- Compatibility?

6. Pricing and Time

- Additional cost for information access (ie – FOIA, IG 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 Savings!

Cloud Costs

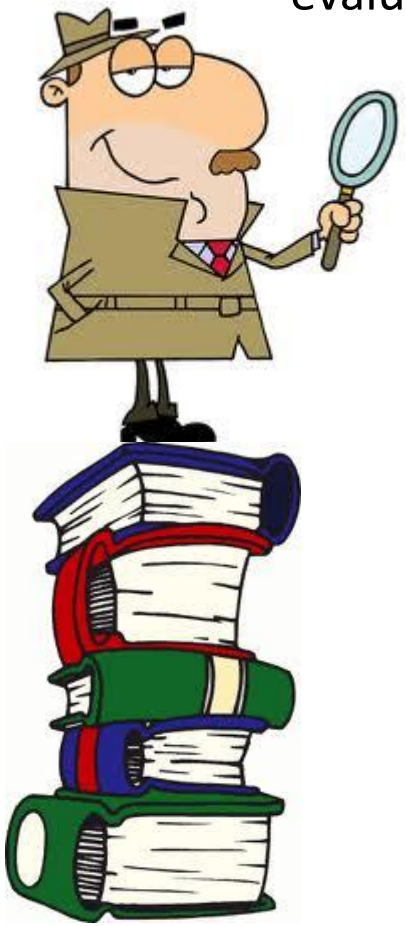
- **Back-up for the Back-up**
- **Data Access / FOIA / e-discovery**
- **Incident Response**

7. Intellectual Property

- Protect government and set boundaries for vendor
- How will infringing material be handled?
- Level of indemnity provided by vendor or government? (Consider ADA)
- Access to vendor IP (especially for IG investigations and audits)?

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

Cloud Computing:

What to negotiate?*

*** EVERYTHING!**

Cloud Contracts and Service Level Agreements

Have the right people at the table…

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

And remember, 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?