The Wisdom of Clouds
Where are we?

- Single Computer
- Mainframes with terminals
- Client/Server Computing
- Network Computing
- Cloud Computing

Time:
- 1960
- 1970
- 1990
- 2000
- 2010

Complexity:
- Centralized
- Distributed

Back to mainframes? 😊
Beware of Cloud Washing

Not everything is really a “Cloud” something

Image source: http://infreemation.net/cloud-computing-linear-utility-or-complex-ecosystem
Actually, it’s Hosting Evolved

ISP 1.0
Provided access to the Internet (dial-up, ISDN, T1, T3)

ISP 2.0
Access to servers at the Internet access point

Colo (ISP 3.0)
Racks for your equipment at the Internet access point

ASP (ISP 4.0)
Hosted (traditionally designed) applications on servers at the Internet access point

Cloud (ISP 5.0)
Dynamic, Internet-optimized infrastructure for hosting your applications

SaaS
Internet-based applications and services

Source: Forrester Research, Inc.
# The Promise of Clouds

<table>
<thead>
<tr>
<th>The classical problem</th>
<th>The promise:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Under-utilized server resources waste computing power (and energy)</td>
<td>• Server resources are delivered on-demand as usage-metered compute utilities</td>
</tr>
<tr>
<td>• Over-utilized servers cause interruption or degradation of service levels</td>
<td>• Cloud-user does not need to forecast demand</td>
</tr>
<tr>
<td>• Turn fixed costs into variable costs</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The emerging problems</th>
<th>The promise:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Highly dynamic scalability demands</td>
<td>• Reduced provision lead times</td>
</tr>
<tr>
<td>• Time to market</td>
<td>• Scalability</td>
</tr>
<tr>
<td>• Sophisticated infrastructure is available as Services</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Leveraging the modern Web</th>
<th>The promise:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Evolution of Desktop apps to Software-as-a-Service</td>
<td>• A stable, reliable platform to develop, test and deploy network-centric end-user applications</td>
</tr>
<tr>
<td>• Programmable Web</td>
<td></td>
</tr>
</tbody>
</table>
Applications in the Cloud

Security Requirements

HIGH

LOW

Cloud

Routine Applications

Analytics and Reporting

Mail and Collaboration

Software Development/Test

On Premises (traditional)

Business Applications

Document Management

Financials and Planning

DR

Mission Critical/OLTP

Critical Applications

Conventional business applications with:

• Patient Data
• Employee Information
• Financial Information
• Customer Information
• Government

Source: UNISYS
Applications in the Secure Cloud

Cloud

Secure Cloud

Traditional

HIGH

Security Requirements

LOW

Mail and Collaboration

Analytics and Reporting

Web

Software Development/Test

Conventional business applications with:
- Patient Data
- Employee Information
- Financial Information
- Customer Information
- Government

Document Management

DR

Financials and Planning

Mission Critical/OLTP

Routine Applications

Business Applications

Critical Applications

Source: UNISYS
# Cloud Computing Services

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| **IaaS** | Infrastructure as a Service  
Renting use of computing power or storage over the Internet (e.g., Amazon’s EC2 & S3) |
| **PaaS** | Platform as a Service  
Renting use of an application environment over the Internet (e.g., Google App Engine) |
| **SaaS** | Software as a Service  
Renting execution of software solutions over the Internet (e.g., salesforce.com) |
**Special Government Considerations**

### Federal Government Considerations for Cloud Computing

<table>
<thead>
<tr>
<th>Cloud Computing Services</th>
<th>Security &amp; Data Privacy</th>
<th>Delivery &amp; Operations</th>
<th>Interoperability &amp; Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software as a Service (SaaS)</strong></td>
<td>Offer different levels of security and data privacy based on the application and nature of the services provided.</td>
<td>Enable adoption of Cloud Computing services in different Cloud models including Public, Private, Hybrid and Community models.</td>
<td>Develop interoperability standards in conjunction with the industry to provide interoperability at the data infrastructure, platform and application levels.</td>
</tr>
<tr>
<td></td>
<td>Potentially standardize Low, Med and High categories for Simplicity.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Platform as a Service (PaaS)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Infrastructure as a Service (IaaS)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Source:** GSA
NIST Cloud Models

Cloud Sourcing Models

Outsourced

Government

High

Trust (Security and Data Privacy)

Low

Private Commercially Hosted Cloud

Dedicated Government Network (VPN, TIC)

Private Government Cloud

Public Cloud

Public Internet (TIC)

Multi-agency Community Cloud

Hybrid Government Cloud

Source: NIST
Where Hype meets Reality

- What happens when the Network fails?
- Does it make economic sense?
- How will we handle legal matters?
- Once we’re in, how do we get out? (portability)
- How will we handle security and compliance?
- Will there be a “big switch”? (portability)
- How do we interoperate with our existing “stuff”?
- Is computing really like electricity?
- Will it perform well?
- Who’s blamed when I get hacked?
- Reliability?
- Maturity?
- Stability?
Combined Federal & Commercial Architecture (Carpathia)

- Role based Users
- Compliant Portal
- Orchestration
- FSI Cloud (XenServer)
- Multi-tenant (XenServer)
- Reserved Servers
- Shared Servers
- Encrypted Datastore
- Reserved Storage
- Template, ISO, backup storage
- Enterprise Portal
- Orchestration
- Cont. Scanning
- RSA Auth
- SSL VPN
- Parascale (Parallel NFS Object store)
- Template, ISO, backup storage
NIST’s view of Cloud IA, C&A

Notional Government Wide Security Authorization Process for Cloud Systems

Government Wide Collaboration (Data Owners)
- Identify FIPS 199 Level (using NIST SP 800-60)
- Derive the initial baseline NIST SP 800-53 controls
- Tailor NIST SP 800-53 controls for cloud type and document additional security requirements
- Create system security specification and vet within government
- Publish AO approved consensus cloud security specification

Executed once for each cloud type

Cloud Providers (Information System Owners)
- Cloud provider produces authorization package
- Independent 3rd party performs assessment
- Implement and document relevant security controls
- Develops security plan and possibly negotiates modifications to the specification

Executed once for each cloud system

Government Wide Authorizing Official(s)
- Reviews authorization package and identify remaining risks and security gaps
- Potentially require additional risk mitigations (compensating controls, documentation, or testing)
- Authorizing Official(s) sign the authorization and accept the residual risk

Executed once for each cloud system
Conclusion
Questions & Answers, Discussion