Welcome
Cloud Computing –
New Challenges in
Data Integrity and
Security
13 November 2014

Panel

• Tracy Lampula, Associate Director of GIS
  Compliance, Vertex Pharmaceuticals
• William Sanborn, Director of Information
  Technology, LFB-USA
• Robert Streit, Sr. Manager, Q&C Architecture and
  Design for IT Systems, J&J
• Robert J. Wherry, MSc, MS, CPGP, CQA, CPIP-
  Principal Consultant, Strategic Compliance
  Services, PAREXEL International Corporation
How Did We Get to The Cloud?

Why Cloud?

- Agility
- Scalability
- Redundancy
- Elasticity
- Cost effective?
Control Considerations

• Know your data
  – Data Classification
  – Risk Assessment

• Encryption
  – Transmission
  – At rest

• DevOps and DevOps tools
  – Chef
  – Puppet
  – Jenkins

Strong Procurement & Vendor Management Policies & Practices

• External – The Vendor
  – Be sure they can meet your needs (Security & Privacy)
  – Know how to get your data back
  – Establish appropriate controls (e.g. Change & Access Control) and regular oversight
  – SLAs

• Internal – Your users
  – Avoid Shadow IT
  – Know the implications of Commercial Cloud Use – e.g. Google Docs
Cloud computing?

“Cloud” based computing – Interesting facts:
• The popularization of the term can be traced to 2006 when Amazon.com introduced the Elastic Compute
• Cloud computing is the result of evolution and adoption of existing technologies and paradigms.
• The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them.
• The cloud aims to cut costs, and help the users focus on their core business instead of being impeded by IT obstacles

[Source - Wikipedia]

Cloud – technology stack

1. Application layer
2. Platform layer
3. Infrastructure layer

[Source - Wikipedia]
Software as a Service

SaaS – Software as a Service

– is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted
– It is sometimes referred to as "on-demand software".
– SaaS is typically accessed by users using a thin client via a web browser. SaaS has become a common delivery model for many business applications

[*Source - Wikipedia]*

Platform as a Service

PaaS – Platform as a Service

– In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server.
– Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers.
– With some PaaS offers like Microsoft Azure and Google App Engine, the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually.

[*Source - Wikipedia]*
Infrastructure as a Service

IaaS – Infrastructure as a Service
– providers of IaaS offer computers – physical or (more often) virtual machines – and other resources. (A hypervisor, such as Xen, Oracle VirtualBox, KVM, VMware ESX/ESXi, or Hyper-V runs the virtual machines as guests.
– Pools of hypervisors within the cloud operational support-system can support large numbers of virtual machines and the ability to scale services up and down according to customers’ varying requirements.)
– IaaS clouds often offer additional resources such as a virtual-machine disk image library, raw block storage, and file or object storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles.

[Source - Wikipedia]

Typical Systems that are hosted

• SaaS Solutions
  – NetSuite (ERP), Salesforce.com (CRM), ADP (Payroll / benefits)
• PaaS Solutions
  – Amazon, Google, Microsoft
• IaaS Solutions
  – Amazon – AWS and EC2, AT&T Synaptic Cloud, Rackspace
Basic Premise

• Annex 11

The application should be validated; IT infrastructure should be qualified

Key Question

If you build a virtual environment in your own data center, FDA expects validation and qualification of the system.....

How does this expectation change by putting that system in somebody else’s building?
Cloud Provider Responsibilities

• Auditing
• Data Integrity and Security
• Procedures
• Training
• Managing multiple clients
• Quality Agreements
• SLAs

Cloud Provider Certifications

• ISO 27000, 27001
• ISO 9000
• SSAE-16 & ISAE 3402
• FedRamp
• PCI DSS
Malware Hosting

• In Q3 2014, U.S. percentage of global malware hosting increased from 56% to 63% (*proportional to the overall number of hosted websites*).

• Top ISPs Hosting Malware
  • GoDaddy 44% Q3 (+42% Q2)
  • Amazon 17% Q3 (+24% Q2)
  • Google 14% Q3 (+5% Q2)


Overlap

- Security
- Quality
- GxP

• Change Control
• Incident Mgmt
• Doc Mgmt
• Backup/Restore
• Training
• System Maintenance
IaaS Vendors – Not all the same

<table>
<thead>
<tr>
<th>Capability/Enabler</th>
<th>Life Sciences Targeted</th>
<th>Life Sciences Aware</th>
<th>Life Sciences Aware (Low)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualification Documents</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Specific Change Agreement</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qualification Assistance</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Permits Onsite Audit</td>
<td>✓</td>
<td>✓</td>
<td>(may charge a fee)</td>
</tr>
<tr>
<td>Enterprise Scale</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Service/Deployment Models</td>
<td>Private Cloud, IaaS, PaaS, some SaaS</td>
<td>IaaS, PaaS</td>
<td>IaaS, some PaaS</td>
</tr>
<tr>
<td>Cost Profile</td>
<td>$$$</td>
<td>$</td>
<td>$</td>
</tr>
</tbody>
</table>

Validation – Objectives

- Achieving a state of control over the computerized system
- Data must be accurate, reliable and maintain integrity
- Validation documentation is necessary to provide evidence of the above
  – The same as any other similar GxP system
cGMP Computers Needing Validation

- Inventory control & Management
- Laboratory Information Management
- Building/Warehouse/EM Management
- Documentation (SOPs, etc.)
- Bill of Materials & Materials Weigh-out
- eMPR/eBPR
- Process Supervision and Control
- Statistical Process Control
- Deviations/Investigations Management
- Product complaints Management
- Maintenance/calibration Management
- Change Control Management
- Labeling Control
- Recalls

Validation – Strategy

GAMP 5 Approach
- Life Cycle
- Risk-Based = QRM
- Effective Governance
- Supplier Good Practices

Qualify* & Validate:
- Architecture
- Software
- Configuration
- Functionality
- Archival/Retention

*Audit / Certify any supplier qualifications
GAMP 5 – Primary Responsibility

GAMP 5 – Risk-Based Approach

Step 1: Perform Initial Risk Assessment and Determine System Impact

Step 2: Identify Functions with Impact on Patient Safety, Product Quality, and Data Integrity

Step 3: Perform Functional Risk Assessments and Identify Controls

Step 4: Implement and Verify Appropriate Controls

Step 5: Review Risks and Monitor Controls

Source: Figure M3.1, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org
Validation – Realization

• A Cloud-based GxP computerized system requires the same validation documentation as any internal system:
  – Where the documentation resides may differ
  – Key aspect to validate:
    • Security and user access
    • Functionality and calculations
    • Audit Trails for Security & Data Changes
    • Back-up and Recovery

Validation – Other Considerations

• Maintaining the state of control
  – Does the cloud have sufficient environments (e.g., development, pre-test, validation, and Production) for change control?
  – SLA &/or Quality Agreement should have a defined list of types of HW/SW changes and the notification requirements for each type of change
  – Disaster Recovery (Supplier)
  – Business Continuity (you)
FDA Perspectives on Cloud

• FDA is already in the Cloud
  – Information Computing Technologies for the Twenty-First Century (ICT21 Initiative)
  – Cloud First policy: use cloud computing technologies by 2013 to:
    • Maximize data capacity
    • Reduce computing to a utility
    • Access simplified, rapid, on-demand resources.

Source: http://www.fda.gov/aboutfda/reportsmanualsforms/reports/ucm274442.htm

FDA Perspectives on Data Integrity

• Old issue with a renewed focus
• Focus area for recent inspections
• Application Integrity Policy
• BioResearch Monitoring (BIMO) Program
• Preapproval Inspections
• Stand-alone computers
• What this means for cloud-based systems...
FDA Perspectives on Data Integrity

Various Concerns Extracted From WLs
- Modified raw data
- Omissions in data
- Missing raw data or Deleted raw data files
- Lack of security & Lack of adequate controls
- Non-documentated testing
- Failure to maintain complete data