XAAS GOVERNANCE MODEL:
Managing the role of vendors and service providers
Kosal Keo
Guest Presenter
April 2018

XaaS Governance Model 5 Key Concepts

1. Accountable vs Responsible
2. Auditing to Standards
3. Vendor Management
4. SLA/Quality Agreements
5. Computer System Lifecycle Management
Accountable vs Responsible

- There is very little difference in the lifecycle management (deliverables) of on-premise vs hosted solution. The most important concept in this space is the issue of **accountable vs responsible**.
- Both models should follow the same lifecycle management with some small exceptions: emphasis on Vendor management, SLA’s and Quality Agreements (for service provided solutions).
- The real difference is the understanding that your organization is always accountable for its own data; with “as-a-service” model we’ve just shifted responsibility for various quality and operational elements to the service provider.

Accountable vs Responsible Continued…

1. SaaS Governance Policy
   a. Identifying 5 Key Concepts and the procedures ensuring compliance to the key concepts
   b. Executive Approach and Responsibility

2. IT Compliance Manual:
   a. IT-centric approach
   b. Topics IT-related
   c. Roles and Responsibility of the IT group and functions within IT
Audit to Standards

- Once we’ve defined the issue of accountable vs responsible, you are now responsible to audit and qualify that the vendor meets your organization’s minimal compliance standards.
- Create a group of “standards” that contain key concepts of critical GxP processes (i.e. System Admin SOPs, change control, incident management, vendor management ....etc.) within your organization.
- This serves as a reference for auditors to audit service providers against and also to set structure around internal SOPs as well.

Audit to Standards continued...

Audit Management:
1. How to conduct audits (the W’s)
2. Vendor Criticality based on the system or service being provided
3. Types of audits and when to conduct them
   a. Remote / Postal / Questionnaire
   b. Full audits onsite / remote
4. Vendor Test Rating
   a. TR1
   b. TR2
   c. TR3
Service Provider Management

• Once a vendor has been qualified, the next major concept is Vendor Management.
• Once you’ve shifted responsibility to the vendor for certain quality and operation aspects, it is now your responsibility to ensure that the service provider operates in a manner that is analogous to your internal processes and procedures.
• Thus, a strategy of service provider management needs to be implemented.

Service Provider Management (Continued…)

• The recommendation of how to manage vendors is based on the criticality of the service which is being provided.
• GxP Assessment should contain service-related items and how to quantify their criticality. This criticality will help to dictate the frequency at which we will monitor or review a service provider’s documentation that they are meeting their own process and procedures (which we have qualified via the audit).
Service Provider Management (Continued…)

Vendor Management:
• What is the frequency of audits or re-evaluation
• Monitoring process
• Involvement in service providers Quality Operations (i.e. Change / Incident / CAPA management

SLA’s and Quality Agreements
• Since it is your responsibility to manage and verify that the service provider is in compliance to their own processes, you have to ensure that you are able to review on an on-going basis activities that that the service procedure is now responsible for.
• The concept of SLA’s and Quality Agreement is very crucial in setting expectations and the understanding of how your organization plans on approaching the process of managing service providers.
  • For example, if the service provider is providing a critical function (assessed by GxP assessment), your organization should dictate that they are either reviewers or approvers of critical change controls (as opposed to major or minor).
  • This is added resource time to the vendor and therefore should be accounted for in the Quality agreement.
• Verify that the supplier’s change management procedure contains an adequate process for impact assessment (this element of change control should be defined in the Change Management Standard).
SLA’s and Quality Agreements Continued

SLA and Quality Agreement Management:
• Based on the criticality of the system or service
• Define and specify communication process
• Quality Dashboards
• Define Vendor Management

ICE & Computer Systems Lifecycle Management

Integrated:
• To give or cause to give equal opportunity and consideration to regulatory impact, business impact and complexity

Compliance:
• The act of conforming, acquiescing, or meeting regulatory obligations.

Ecosystem:
• A system, or a group of interconnected elements, for med by the integration of our methodology.
CSLM Overview

- Based on a scoring system
- Yes/No Questions
- Quantitative over Qualitative

Deliverables Matrix

<table>
<thead>
<tr>
<th>Deliverables</th>
<th>Regulated Applications</th>
<th>Nonregulated Applications</th>
<th>Infrastructure Systems</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Need Assessment</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>System Regulatory Applicability and Criticality Assessment (this document)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Audit</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post Audit</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Audit Required</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>FMEAS Compliance Assessment</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initiation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Requirements Specification</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SLA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality Agreement of Safety, Reliability, or Fault Tolerance</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation Plan</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LEADS</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>URS Criticality Classification</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GAMP 5: Functional Specifications, Design Specifications / Code review / Design Qualification</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scope Matrix (Trace URS to FRS to Test Scripts)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Configuration Specifications</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Connecting Pharmaceutical Knowledge ispe.org
User req. criticality classification (UCC)
Each requirement is assessed for criticality
Based on 3 questions
Result: all requirements gets a rating
This will help to determine what will be tested

• Leverage the experts work (Vendor testing)
• Priority on Vendor audit process
• For a really good vendors (TR1) you only test High criticality requirements that is assigned as part of the UCC
• TR2 – you are less confident on the vendor so more due diligence is required. You would test high and medium criticality requirements
• TR3-Poor vendor but business requirements dictate use this vendor. Test everything.
CSLM Overview

- Concept phase
  - High Level Requirements
    - High Criticality
      - RAC
      - Low Criticality
    - User Requirements
      - High
      - Medium
      - Minor
  - vendors audit/assessment
    - determines testing effort:
      - TR1 - test critical reqs
      - TR2 - Test critical & Major reqs
      - TR3 - Test all reqs

- Initiation phase
  - UCC
    - High
    - Medium
    - Minor

- Project phase
  - ERES
  - Execute the Project based on RAC and test based on UCC/VA

- Operational Phase
  - CHANGE CONTROL

- Retirement Phase
  - Data Migration and archiving
  - Decommissioning

Connecting Pharmaceutical Knowledge
ispe.org
Summary
1. Create Standards documents for Key critical GxP and Operational processes
2. Include concept of Accountable vs Responsible for Lifecycle management and Vendor Management SOPs
3. Create frequency and vendor management chart in Lifecycle Management SOP
4. Include ICE concepts in the Lifecycle Management SOPs
5. Include SLA’s and Quality Agreements in the Deliverables matrix (should also create a Standard for Quality Agreements)

THANK YOU!

Kosal Keo
CEO, Boston Technology Research
kkeo@bostontr.com