IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY | an informa business
Unlimited Validation Knowledge Awaits...
Published on *IVT Network* (http://www.ivtnetwork.com)

Establishing a Validation Process for Cloud Hosted Software

By **Laurent Saugrin Aug 22, 2018 4:52 pm EDT**

ABSTRACT

This article introduces the process of selecting a suitable cloud provider. It also discusses the different procedures, or other supporting documentation, that must be in place to define responsibilities and commitments between the service provider and the client. In addition, this article goes over the applicable validation activities necessary to ensure that GxP data is secured and that the cloud hosted application is successfully qualified and in a validated state for the entire duration of its life cycle, and in compliance with the regulating bodies. Whether you look for a Software as a Service (SaaS), a Platform as a Service (PaaS) and/or an Infrastructure as a Service (IaaS) provider, the process of selection shall be very similar. Since SaaS is a commonly offered service, this article focuses on it.

INTRODUCTION

Typically, companies in the pharmaceutical, biotechnology or medical devices industries host on premise in-house developed software or highly configurable off-the-shelf applications used for their GxP regulated activities. Hosting on premise applications offer total responsibility of control over the security and integrity of the GxP company data that the application creates and manages, in which the infrastructure stores and generally IT SMEs maintain.

However, in an era where the business approach is to reduce overall operating expenses, on premise environments have become less viable as the cost associated with infrastructure maintenance, data storage and backup, and personnel represent a substantial expense. SaaS, IaaS are nowadays the most widely adopted alternative solutions to on premise hosting.

DISCUSSION

1. CLOUD PROVIDER SELECTION PROCESS

The selection process of your future SaaS or IaaS provider is generally performed in three consecutive steps:

Stage 1: Review of the provider websites. What you are looking for is information about their customers and their knowledge of GxP regulations. Questions to ask include, but are not limited to: Does the provider have any regulated life science related customers? Is their infrastructure qualified, and can they provide a GxP-compliant service?

If the answers are no, no further action is required. If the answers are yes, you have narrowed down to few (not more than 5) potential cloud hosts, then move to stage 2 of the process.

Stage 2: Assessments and Audit. The remaining candidates are then sent a detailed questionnaire that asks questions about their accreditation schemes and their Quality Management System (QMS) such as quality manual, procedures, infrastructure qualification, and staff training. Look at the services offered by the company within the QMS and how these are documented.

You also need to focus on questions around backup and recovery, change control, configuration and incident management in the questionnaire to check that these processes and activities are carried out in a compliant way.

Other questions concern the security management of the facility and of data within the cloud based infrastructure itself: Data Storage Infrastructure (e.g. Where do the servers, processes, and data physically reside?), Physical Datacenter Security (e.g. building access as well as server room and physical host access; information on procedures for granting, periodic review, and

revocation of physical access), Encryption & Key Management (e.g. Do you encrypt data in storage and in transit? What encryption technologies are used?)

Review thoroughly the responses to your questionnaire. At this time, you should have narrowed down the candidates to not more than two acceptable cloud providers. The final decision for the selected suitable provider is commonly taken by the business as it is financially driven for the most part.

Stage 3: Generate a Service Level Agreement (SLA), or equivalent. This is the most critical document that exists between the service provider and you.

A SLA is a commitment between the service provider and you, the client or service user. It is your contract with the service provider and sets expectations for the relationship. It needs to be written to protect your cloud service(s) according to the level of risk you are prepared to accept. The SLA is a living agreement though and as services change, it should be reassessed.

Points to cover in a typical SLA (but not limited to):

- Provision of Services

o Customer Responsibilities

o Service Provider Responsibilities

o Data Backup and Restore (procedure, period)

o Support and Maintenance

o Service warranty

- Validation Activities (If Applicable)
- Invoicing and Payment
- Terms and Termination
- Limitations on Warranties and Liability
- Confidential Information

2. PROCEDURES AND DOCUMENTATION

Per the responsibilities defined in the SLA, the service provider is responsible for the management of the hosting environment, its security and its maintenance. As such, he shall be prepared to provide the service user/client with the procedures and other documentation that govern these activities. In fact, I highly recommend that the service user/client obtains a copy of each document and file it internally for reference. Procedures and documentation include:

2.1. Security Policy (or equivalent).

The security policy should, at least, cover the points discussed in the security questionnaire:

o Shared Security Responsibilities between the provider and the client

o Data Center Access Security

o Physical and Environmental Security

o Infrastructure Security (e.g. firewall)

o Network Security

o Data Access Security Features (e.g. credentials and authentication, encryption and key management, data stored on shared server)

o Employees Training

2.2. Business Continuity Plan

The Business Continuity Plan describes responsibilities, processes, and activities that ensure sustained execution of the

business continuity to the environment and its infrastructure operations and IT controls in the event of a disaster.

The cloud provider shall train its employees to face any eventualities and work out alternate methods to restore the organization business and infrastructure needs thereby minimizing business impact in the event of any disaster.

Points to cover in a typical business continuity plan:

- Responsibilities / Accountabilities / Authorities
- Business Continuity Plan Test Frequency and Process
- Overall Process:

o Identification / Declaration of disaster

o Internal Communication

o Communication to Customer

o Restoration Activities

o Disaster Analysis

o Communication to Customer

o Declare Closure of Disaster

2.3. Backup and Restore Procedure

The backup and restore procedure describes responsibilities and activities to ensure that your data in the cloud hosted environment is securely backed up, stored and/or restored, all these activities tested as scheduled to ensure business continuity.

Points to cover in a typical backup and restore procedure:

- Responsibilities / Accountabilities / Authorities
- Backup and Restore Verification Test Frequency and Process
- Overall Process:

o Schedule Backup: identify the data to backup as per the schedule

o Perform Backup: define responsibilities and process

o Monitor Backup

o Review for Data Backup Failures (as Applicable)

o Restore Data Process

2.4. Change Management Procedure

The Change Management (or Change Control) procedure describes responsibilities and activities to ensure complete control of the lifecycle of all the changes in software requirements, IT infrastructure and application environment, and controlled documents based on continual improvement and process improvement.

Important: the cloud provider shall follow his own change control process but ultimately changes are still managed in accordance with your change control process.

Points to cover in a typical Change Management procedure:

- Responsibilities / Accountabilities / Authorities
- Identify Type of Change: For example, an OS update, security patch, software installation on hardware, defect/issue fix, or enhancements.

- Identify Level of Change: For example at system level or functional level

• Impact and Risk Analysis: to the system environment, potential downtime of the system

• Test the change and document testing: Integration and/or validation test in cloud provider environment.

• Overall Process (once all of the above is completed) with responsibilities shared between the cloud provider and the customer:

(Cloud Provider)

o Initiate change control

o Communicate the changes in scope to the customer: This can be accomplished by releasing notes, for instance.

(Customer)

o Review the cloud provider scheduled changes and all his documentation. If acceptable,

o Initiate and document change control

? Description of the change

? Impact and Risk Analysis: Regulatory and Business

? Implementation plan and test plan (as applicable)

? Recovery plan

o Initiate Change Request

? Description of the change

? Impact and Risk Analysis: Regulatory, Business and validation deliverables

? Implementation plan and test plan (as applicable)

? Recovery plan

o Obtain internal authorization to implement the change

o Communicate to the cloud provider to implement the change in Quality environment

o Testing (as applicable)

? Pre-requisite validation deliverables (e.g. requirement documents)

? Perform and document validation testing

? Issue a Validation Summary Report

o Communicate to the cloud provider to deploy the change in Prod environment

o Customer closes his change control

o Cloud provider closes his change control

3. VALIDATION

The validation responsibilities, process, and approach for a cloud hosted system are the same as a system installed and maintained on premise.

3.1. Validation Deliverables

o Validation Plan

o Requirements Documents: ADS(1), URS, FRS, Config Specs…

o Qualification Testing Documents (including Trace Matrix)

o Validation Summary Report

(1) The Architectural Design Specifications (ADS) document should be tailored towards cloud environment: Firewall, infrastructure diagram, hardware (e.g. application server) and software specifications, connectivity, and encryption protocol.

3.2. Validation Testing

As usual, validation testing will ensure that all pre-defined requirements and specifications are successfully challenged and met, and that testing is properly documented.

Because a cloud hosted application predominantly has a web-access, it is considered as an Open system per the 21 CFR Part 11 definition. Thus, special testing consideration shall be given to ensure that the data is encrypted at rest and in transit as well.

CONCLUSION

This article presented a roadmap to obtain evidence that an application hosted in the cloud an offered as a Software as a Service is successfully validated in accordance with the GxP regulations. The road map starts with the process of selecting the right cloud provider, continuing with the identification of the required procedures and other supporting documentation, until the execution of the applicable validation activities.

REFERENCES

Oral presentations:

1. L. Saugrin, IVT 19th Annual Computer and Software Validation Conference (Philadelphia, PA, 2018).

Government publications:

2. Code of Federal Regulations, Title 21, Food and Drugs, Part 11.
