ESTABLISH GxP COMPLIANT CLOUD SOFTWARE VALIDATION PROCEDURES

APRIL 27, 2018

PRESENTED BY: LAURENT SAUGRIN
Computer Validation Specialist IV, IT Compliance
Laurent.saugrin@dexcom.com

Dexcom
One Step Ahead

19TH ANNUAL
Computer and Software Validation

AGENDA

CHAPTER 1: CLOUD PROVIDER SELECTION PROCESS

1.1. Overview

1.2. Survey Questionnaire (or Assessment): QMS

1.3. Mail Audit: Security Inspection (Interactive Exercise)

1.4. Service Level Agreement (SLA)

AGENDA

CHAPTER 2: CLOUD PROVIDER PROCEDURES AND DOCUMENTATION

2.1. Security Policy

2.2. Business Continuity Plan

2.3. Backup and Restore Procedure

2.4. Change Management Procedure

AGENDA

CHAPTER 3: VALIDATION

3.1 Validation Deliverables

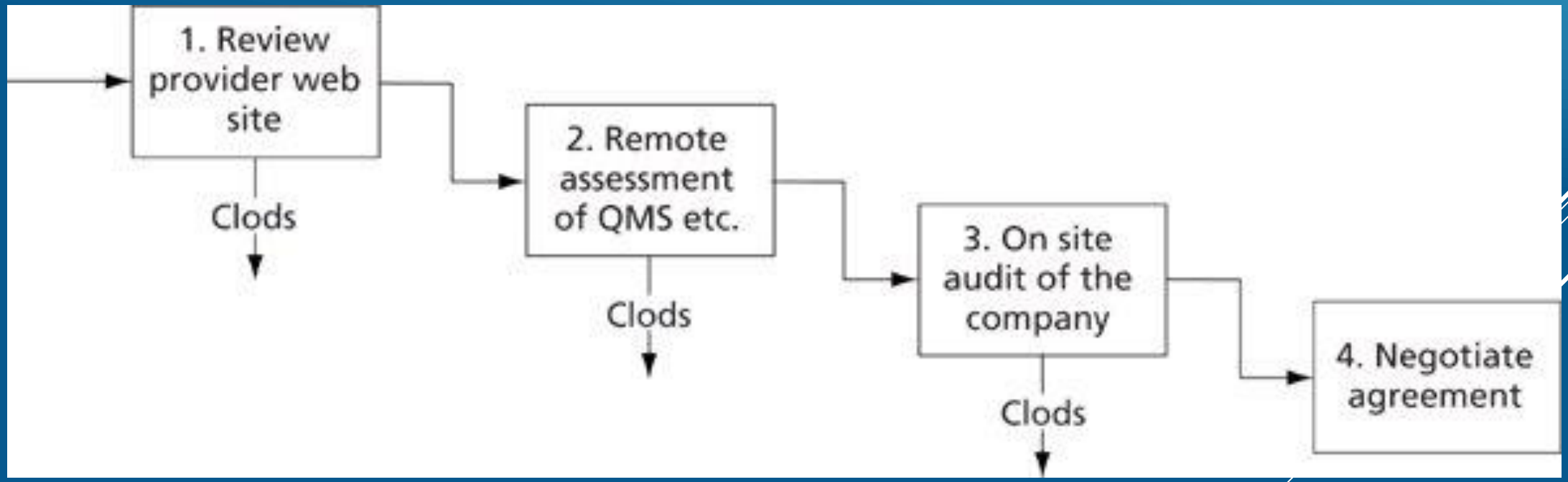
3.2 Validation Testing

INTERACTIVE EXERCISE

Design a mail-in security inspection questionnaire that ensures data security at the cloud provider data center.

CHAPTER 1: CLOUD PROVIDER SELECTION PROCESS

1.1. Overview



1.2. Survey Questionnaire (or Assessment): QMS

Questions about:

- Accreditations (e.g. ISO, NIST, ASTM, etc…)
- Compliance to GxP regulations, HIPA (if the SaaS will manage Protect Health information)
- QMS such as quality manual, procedures, change control, incident/risk management
- Staff Training
- Infrastructure Qualification, Backup and Recovery, Business Continuity

1.3. Mail Audit: Security Inspection (Interactive Exercise)

Within the scope of Computer System Validation, Data Security is best defined as the act of protecting data against unauthorized access or corruption.

Typically, not enough controls around computerized systems is the root cause of data security issues.

This questionnaire also assesses the service provider QMS (see section 1.2)

1.4. Service Level Agreement (SLA)

- **A service-level agreement (SLA) is a commitment between the service provider and you, the client/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**
- **Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service user.**
- **The SLA is a living agreement though and as services change, the SLA should be reassessed.**

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

- **PROVISION OF SERVICES**
  - **Additional Users and/or Additional Service.**
  - **Customer Responsibilities**
  - **Service Provider Responsibilities**
  - **Data Backup and Restore (procedure, period)**
  - **Support and Maintenance**
  - **Service warranty**

- VALIDATION ACTIVITIES (If Applicable)
- INVOICING AND PAYMENT
- TERM AND TERMINATION
- LIMITATIONS ON WARRANTIES AND LIABILITY
- CONFIDENTIAL INFORMATION

CHAPTER 2: CLOUD PROVIDER PROCEDURES AND DOCUMENTATION

2.1. Security Policy

The service provider carries a security policy (or equivalent) and the customer shall obtain a copy.

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

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

- Shared Security Responsibilities between the provider and the client
- Data Center Access Security
- Physical and Environmental Security
- Infrastructure Security (e.g. firewall)
- Network Security
- Data Access Security Features (e.g. credentials and authentication, encryption and key management, data stored on shared server…)
- 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**
  - Identification / Declaration of disaster
  - Internal Communication
  - Communication to Customer
  - Restoration Activities
  - Disaster Analysis
  - Communication to Customer
  - Declare Closure of Disaster

2.3. Backup and Restore Procedure

The backup and restore procedure describes responsibilities and activities to ensure that the (customer) data in the environment is securely backed up, stored, restored and tested to enable 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**
  - Schedule Backup: identify the data to backup as per the schedule
  - Perform Backup: define responsibilities and process
  - Monitor Backup
  - Review for Data Backup Failures (as Applicable)
  - 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 have his 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:

Cloud Provider

- **Responsibilities / Accountabilities / Authorities**
- **Identify Type of Change:** E.g. OS update, security patch, software installation on hardware, defect/issue fix, enhancements, etc…
- **Identify Level of Change:** E.g. 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)**

Cloud Provider:

- Initiate change control
- Communicate the changes in scope to the customer: e.g. Release Notes

Customer:

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

- 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
- Obtain internal authorization to implement the change
- Communicate to the cloud provider to implement the change in Qual environment
- Testing (as applicable)
  - Pre-requisite validation deliverables
  - Perform and document validation testing
  - Issue Validation Summary Report

- Communicate to the cloud provider to implement the change in Prod environment
- Testing (as applicable)
  - IQ in Prod
- Customer closes his change request
- Cloud Provider closes his change control

CHAPTER 3: VALIDATION

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

3.1. Validation Deliverables

- Validation Plan
- Requirements Documents: URS, FRS, Config Specs…
- Qualification Testing Documents (including Trace Matrix)
- Validation Summary Report

3.2. Validation Testing

Special Consideration: Web-access system: Open or Close systems (per Part 11 definition)?

Ultimately, you decide: Is the 3rd party considered as an extension to your company (Close) or a different entity (Open)?

- Same testing as for a Close system, plus
- Verify data encryption: At rest and in transit (i.e. Open system part 11 requirement)

QUESTIONS