# Cloud Framework, Audit Activities

phuse.eu

# Contents



Last Update: 2019-Apr-24

This document has been developed by the Pharmaceutical User Software Exchange (PHUSE) Working Group on Cloud Adoption and is subject to ongoing consultation and feedback from all relevant stakeholders.

You may submit comments and suggestions regarding this document to *avid@nnit.com* (Anders Vidstrup, NNIT A/S).

phuse

# 1. Scope

In adopting cloud-based solutions for GxP workloads, understanding the essential characteristics of cloud services and solutions is important for determining the applicability of GxP requirements to specific Cloud Service Providers and/ or cloud-based solution models.

*This document provides guidance in preparing and conducting Cloud Service Provider audits. It is one of three supplements to the "Cloud Services – Pre-Amble" ref [5] which all together form the "Framework for Adoption of Cloud Services in the Regulated Life Science Industry" from the Pharmaceutical User Software Exchange (PHUSE).*

# 2. Audits of Cloud Service Provider or /–Broker in general

Looking at good engineering practices, the Cloud Service Customer as a part of purchasing process must ensure that selection of a Cloud Service Provider or Cloud Service Broker fits to their ability to supply service in accordance with the Cloud Service Customers requirement.

## 2.1. Regulatory Requirements for Auditing

Different regulations from authorities do list requirements for election, evaluation and re-evaluation of suppliers, and requirements for collaboration between parties. Below follows a list of legal requirements with relevance for Cloud Services, and supplier assessment/-audit.

| FDA 21 CFR 820 ref [3] | |
|---|---|
| 820.50 Purchasing controls (a) | Evaluation of suppliers, contractors, and consultants. Each manufacturer shall establish and maintain the requirements, including quality requirements that must be met by suppliers, contractors, and consultants. Each manufacturer shall:<br>[1] Evaluate and select potential suppliers, contractors, and consultants on the basis of their ability to meet specified requirements, including quality requirements. The evaluation shall be documented. |
| 820.50, preamble #99 ref [4] | Where audits are not practical, this may be done through, among other means, reviewing historical data, monitoring and trending, and inspection and testing. |

| EU GMP ref [2] | |
|---|---|
| Chapter 7, §7.5 | Prior to outsourcing activities, the Contract Giver is responsible for assessing the legality, suitability and the competence of the Contract Acceptor to carry out successfully the outsourced activities. |
| Chapter 7, §7.6 (collaboration) | The Contract Giver should provide the Contract Acceptor with all the information and knowledge necessary to carry out the contracted operations correctly in accordance with regulations in force, and the Marketing Authorisation for the product concerned. The Contract Giver should ensure that the Contract Acceptor is fully aware of any problems associated with the product or the work which might pose a hazard to his premises, equipment, personnel, other materials or other products. |
| Chapter 7, §7.7 (collaboration) | The Contract Giver should monitor and review the performance of the Contract Acceptor and the identification and implementation of any needed improvement. |
| Chapter 7, §7.9 | The Contract Acceptor must be able to carry out satisfactorily the work ordered by the Contract Giver such as having adequate premises, equipment, knowledge, experience, and competent personnel. |
| Chapter 7, §7.11 | The Contract Acceptor should not subcontract to a third party any of the work entrusted to him under the Contract without the Contract Giver's prior evaluation and approval of the arrangements. |
| Annex 11, §3.1 (collaboration) | When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous. |
| Annex 11, §3.2 | The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment. |
| Annex 11, §3.4 (collaboration) | Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request. |
| Annex 11, §4.5 | The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately. |

# 3. General Audit Activities in the Cloud Supply Chain

Where possible and depending upon the risk involved, the Cloud Service Customers should consider auditing the Cloud Service providers/-brokers design and development methodologies used in the construction of the Cloud Service including operation and maintenance and should assess the development and validation documentation generated for the Cloud Service. Such audits can be conducted by the Cloud Service Customers or by a third party. The audit should demonstrate that the Cloud Service providers/-brokers procedures for and results of the verification and validation activities performed for the Cloud Service are

appropriate and sufficient for the safety and effectiveness requirements of the Cloud Service Customers to be using that Cloud Service.

The Cloud Service Customer, Cloud Service Broker, and the Cloud Service Provider can perform audits in the Cloud Supply Chain. Although the term 'Audit' is uniformly utilized to describe this activity, the term 'assessment' may better convey the type of activity required. A reputable and mature third party could also do these assessments.

The assessment reference could be many, but mainly based on external assessments such as:

- SOC 1 Report: Description of the Service Organization Controls.
  - **Note:** *as part of this review, the Cloud Provider (and/or Broker) should also review and document their explanation of their the Complementary User Entity Controls (i.e. how Cloud Provider has implemented complimentary controls from their side that need to work in concert with the Cloud Provider's controls.)*
  - **Note:** *SOC 1 is normally covering financial institutes, but gives good indications on general controls.*
- SOC 2 Report: Service Organization Controls Type 2 Report. Report on Management's Description of System Controls Relevant to Security and Availability. A SOC 2 report is a restricted use report, and includes substantial detail related to which controls are in place at the cloud provider. It is normally only shared with customers and prospective customers.
- SOC 3 Report: Service Organization Controls Type 3 Report. Report on Management's Description of Controls Relevant to Security and Availability. Compared to a SOC 2 report, this report is brief and contains little detail. It is intended for general use and may be publicized, for example on the cloud provider organization's webpage.
- ISO 27001 certification report: Specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization.
- ISO 9001 certification report: Sets out the criteria for a quality management system

**Note:** *there is a difference between a quality approach and security. ISO 27001 defiantly also delivers quality into IT deliverables from a security point of view. But from a quality perspective ISO 9001 and 27001 have different scope. The following clauses from ISO 9001:2015 are not covered by ISO27001:2013 or there are no similar clauses in ISO 27001.*

- Quality management principle (Introduction, clause 0.2)
- Process approach (Introduction, clause 0.3)
- Customer focus (Leadership, clause 5.1.2)
- People (Support, clause 7.1.2)
- Infrastructure (Support, clause 7.1.3)
- Environment for the operation of processes (Support, clause 7.1.4)
- Monitoring and measuring resources (Support, clause 7.1.5)
- Organizational knowledge (Support, clause 7.1.6)
- Release of products and services (Operation, clause 8.6)
- Control of nonconforming outputs (Operation, clause 8.7)

### 3.1 Auditing topics to be covered by role

Below are general auditing topics to be covered by role:

| | IaaS | PaaS | SaaS |
|---|---|---|---|
| Cloud Service Customer | • Quality and Security Management review<br>• Internal Audit's<br>• Process for selecting and monitoring supplier's<br>• Risk Management program in LoB<br>• Configuration- and Change Management<br>• Business Continuity, disaster and recovery plans<br>• Manages privileged accounts and/or service accounts<br>• Additional qualification of infrastructure according to intended use | • Quality and Security Management review<br>• Internal Audit's<br>• Process for selecting and monitoring supplier's<br>• Risk Management program in LoB<br>• Configuration- and Change Management<br>• Business Continuity, disaster and recovery plans<br>• Manages privileged accounts and/or service accounts<br>• Workflow supporting application needs<br>• Additional qualification of infrastructure- and platform according to intended use | • Quality and Security Management review<br>• Internal Audit's<br>• Process for selecting and monitoring supplier's<br>• Risk Management program in LoB<br>• Configuration- and Change Management<br>• Business Continuity, disaster and recovery plans<br>• Manages user accounts and roles<br>• Workflow supporting application needs<br>• Validation of applications according to intended use |
| Cloud Service Broker | • Quality and Security Management review<br>• Internal Audits<br>• Process for selecting and monitoring supplier's and selecting Cloud Service Provider on behalf of or together with the Cloud Service Customer.<br>• Risk Management program in LoB<br>• Configuration- and Change Management<br>• Business Continuity, disaster and recovery plans<br>• Manages privileged accounts and/or service accounts<br>• Additional qualification of infrastructure according to intended use<br>• Service requirements based on the approved service business case and the service risk assessment. | • Quality and Security Management review<br>• Internal Audits<br>• Process for selecting and monitoring supplier's<br>• Risk Management program in LoB<br>• Configuration- and Change Management<br>• Business Continuity, disaster and recovery plans<br>• Manages privileged accounts and/or service accounts<br>• Workflow supporting application needs<br>• Additional qualification of infrastructure- and platform according to intended use and the process for evaluating the need for standards for the service on behalf of or together with the Cloud Service Customer.<br>• Service, including service level options.<br>• Process for defining cloud service provider KPIs. | • Quality and Security Management review<br>• Internal Audits<br>• Process for selecting and monitoring supplier's<br>• Risk Management program in LoB<br>• Configuration- and Change Management<br>• Business Continuity, disaster and recovery plans<br>• Manages privileged accounts and/or service accounts<br>• Workflow supporting application needs<br>• Process for Ensuring implementation of services by the Cloud Service Providers according to the defined service requirements and agreed service levels.<br>• Process for releases service. |

| | IaaS | PaaS | SaaS |
|---|---|---|---|
| Cloud Service Provider | • Quality and Security Management review<br>• Internal Audit's<br>• Process for selecting and monitoring supplier's<br>• Risk Management program in LoB<br>• Configuration- and Change Management<br>• Business Continuity, disaster and recovery plans<br>• Manages privileged accounts and/or service accounts<br>• Qualifies Infrastructure services.<br>• Process for provisions and manages the physical resources, builds and maintains the resource abstraction and control layer.<br>• Customer Support.<br>• Provides handling of security and risk identifications and controls. | • Quality and Security Management review<br>• Internal Audit's<br>• Process for selecting and monitoring supplier's<br>• Risk Management program in LoB<br>• Configuration- and Change Management<br>• Business Continuity, disaster and recovery plans<br>• Manages privileged accounts and/or service accounts<br>• Process for Implements and/or deploys services according to the defined service requirements and agreed service levels.<br>• Operates services.<br>• Provides Customer Support.<br>• Provides handling of security and risk identifications and controls.<br>• Qualifies Infrastructure- and Platform services | • Quality and Security Management review<br>• Internal Audit's<br>• Process for selecting and monitoring supplier's<br>• Risk Management program in LoB<br>• Configuration- and Change Management<br>• Business Continuity, disaster and recovery plans<br>• Manages privileged accounts and/or service accounts<br>• Process for Implements or deploys services according to the defined service requirements and agreed service levels.<br>• Operates services.<br>• Provides Customer Support.<br>• Provides handling of security and risk identifications and controls.<br>• Validates generic functionality in application |

### 3.2. Specific SDLC topics to be audited

The Cloud Service Customer's SDLC policy is the primary policy that defines, and sets forth, the requirements and procedures to implement and maintain a computerized system. This policy also ensures compliance with applicable laws, regulations, and company policies such as GxP.

Although it is beyond of the scope of this document to define an SDLC policy, the SDLC policy at a Cloud Service Customer defines an overall framework often made up of phases from project initiation and planning, thru requirements, design, build, test, install, operation and retirement.

| Introduction to Cloud Services and the Quality Management System (QMS) | |
|---|---|
| Structure<br>Policy's<br>Periodic evaluation of QMS<br>Internal Audits<br>Document Handling<br>Handling of Deviations | |
| **Life cycle activities for Services** | **Supporting activities, e.g.** |
| Life cycle phases, documents, reviews and approvals of:<br>• Requirements<br>• Risk Assessment<br>• Design<br>• Construction<br>• Testing<br>• Releases | • Configuration management<br>• Change management<br>• Problem Management<br>• Incident management<br>• Identity and Access management<br>• Back-up and restore<br>• Business Continuity and Disaster Recovery<br>• Training. |

### 3.3. Specific Security topics to be audited

In traditional IT you know exactly where your data/host is and what resources, if any, you share with others. Multitenancy is almost a given in cloud computing services. These differences give rise to a unique set of security and privacy issues that not only impact your risk management practices but have also stimulated a fresh evaluation of legal issues.

Topics to be audited (not comprehensive list):

- Physical and personnel security
  - There must be restricted and monitored access to critical assets.
  - How is dedicated infrastructure isolated?
- Identity management
  - Description of who have access to data must bed described.
  - Architecture must be reviewed
  - Management of access credentials
- Data protection;
  - Is data separated from other customers data?
  - Is it clear where data is stored?
  - Method of data transfer between cloud service Provider and you
- Vulnerability management
- Availability

The Cloud Controls Matrix Working Group [1] has made a framework providing organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry. This is recommended to look into, when conducting audit both internally and externally.

## 4. Observations given by regulators

The following observations given by FDA aren't reflected directly to Cloud Services, but could be applied in context to conducting supplier audits.

Warning Letter, 2015-FEB-13
Multimedical S.R.L., Italy

2. Failure to establish and maintain procedures to ensure that all purchased or otherwise received products and services conform to specified requirements, as required by 21 CFR 820.50. For example:
   a. Your firm's quality audit procedure requires an audit for critical suppliers be conducted at least once every three years. However, your firm's critical suppliers of raw materials and services have not been audited in more than three years

Warning Letter, 2018-FEB-20
Dexcowin Co., Ltd., Republic of Korea

5. Failure to establish and maintain data that clearly describe or reference the specified requirements, including quality requirements, for purchased or otherwise received product and services, as required by 21 CFR 820.50(b). For example, the approved supplier list documented grades of "(b)(4)", for each supplier; the CEO, Raymond Ryu, was not able to provide a justification behind the identical ratings and evaluation of each supplier.

Warning Letter, FLA-15-29, 2015-JUL-23
Stat Medical Devices, Inc., US

3. Failure to adequately establish procedures to ensure that all purchased or otherwise received product and services conform to specified requirements, as required by 21 CFR 820.50. For example:
   b. Your firm did not implement your "Qualification of Vendors and their Product or Service" procedure, SOP 7.4-3, Rev. No. 6.....

## 5. Glossary

See Glossary in PHUSE, Cloud Services - A Framework for Adoption in the Regulated Life Sciences Industry, Pre Amble, Edition 4, April, 2019

## 6. References


1. Cloud Security Alliance, Cloud Controls Matrix
2. EudraLex - Volume 4 - Good Manufacturing Practice (GMP) guidelines
3. US FDA, 21 CFR part 820, Medical Devices Quality System Regulation
4. US FDA, 21 CFR part 820, Medical Devices Quality System Regulation, preamble October 7, 1996
5. PHUSE, Cloud Services - A Framework for Adoption in the Regulated Life Sciences Industry, Pre Amble, doc ID WP-23, April, 2019