Cloud Framework, Audit Activities

phuse.global

Contents

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).

Purpose for Audits: As a part of purchasing process, the Cloud Service Customer must ensure that selection of a Cloud Service Provider or Cloud Service Broker fits with their ability to supply services in accordance with the requirements of the Cloud Service Customer.

Cloud service providers need to be assessed for quality, security, and compliance periodically. The need for an audit should be based on a risk assessment. The assessment or audit could be conducted on a cadence of about e.g., every two to three years, or more often, depending on risk. Additionally, these periodic audits/assessments will support the Cloud Service Customer to verify the Cloud Service Provider's readiness to support regulatory inspections of the customer.

To be clear, the regulatory burden resides with the Cloud Service Customer, as the company seeking authorisation for a new drug or medical device from the regulatory agencies, and ultimately the data and process owner. The regulatory requirements do not directly apply to Cloud Service Providers. However, since they in turn provide services that may impact regulated products and/or services, they carry an associated responsibility.

1.1 Regulatory Requirements for Auditing

Multiple regulatory authorities list requirements for election, evaluation and re-evaluation of suppliers, and requirements for collaboration between parties associated in the delivery and use of cloud services. Below follows a summary list of legal requirements with relevance to Cloud Services, and supplier assessment/audits.

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: [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.
EU GMP ref [2]	
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.
EMA Q&A: Good clinical practice (GCP) *https://www.ema.europa.eu/en/human-regulatory/research-development/compliance/good-clinical-practice/qa-good-clinical-practice-gcp* ***"...." Indicates, that text is taken out of a larger document. Please clarify with the link to the full text.***	
8. What are the pitfalls to be aware of regarding contractual arrangements with vendors for electronic systems in connection with clinical trials? Rev. April 2020	Audits and inspections It is sometimes not stated that the sponsor should have access to conduct audits at the vendor site and that the vendor site could be subject to inspections (by national and international authorities) and shall accept these. In addition, it needs to be specified that vendors shall provide necessary documentation (e.g., qualification documentation prepared by the vendor in relation to the system) when requested during a GCP audit/inspection process. Qualification and validation particulars That sponsor pre-qualification audits or other on-site pre-qualification activities and later audits of the IT vendor can take place. It should also be ensured that these audits and/or other on-site pre-qualification activities are performed with a sufficient amount of time and that sufficiently in-depth review of the vendor qualification documentation is performed in order to establish the qualification and validation status of a system.
9. What is the level of validation/ qualification needed to be performed by a sponsor when using an electronic system previously qualified by a provider? What documentation is required to be available for inspections? Rev. April 2020	The sponsor is ultimately responsible for the validation of the clinical trial processes, which is supported by electronic systems and for providing sufficiently documented evidence to GCP inspectors on the validation process and the qualification of the electronic systems. The conditions for a sponsor to use the vendor's qualification documentation include, but are not limited to, the following: • an assessment/audit has been performed by qualified staff, with sufficient time spent on the activities and with cooperation from the vendor; • an assessment/audit has gone sufficiently deep into the activities and that a suitable number of examples for relevant activities have been looked at (and documented);

2. 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 activities performed for the Cloud Service are appropriate and sufficient, so it is reliable for Cloud Service Customers to use the provided Cloud Service.

The Cloud Service Customer, Cloud Service Broker, and the Cloud Service Provider can perform audits in the Cloud Supply Chain, e.g., a SaaS provider might audit an IaaS provider. 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.

Certifications held by the party to be audited can be used as references and sometimes replace an in-depth assessment of topics already covered by a certification report.

The table below lists examples of possibly available external reports and/or certifications.

Reference	Main purpose	Why look into this
SOC 1 Report: Description of the Service Organization Controls	Covers financial institutions, however, it provides good indications of general controls. Assures that the party fosters a culture of security awareness and compliance within the organization. High level of trust to assure the security of client data.	A SOC 1 report can offer these benefits: • Verification that there are appropriate internal controls to deliver high-quality services. • Ensure that policies and business processes can support the organization's operations. • Information about risk management and the strategic allocation of cybersecurity resources. • Overcome blind spots and uncover vulnerabilities overlooked by internal personnel. • Strengthen your cybersecurity posture and minimize the risk of data breaches. • Gain a competitive advantage by showing a commitment to information security.
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 the controls in place by the cloud provider. It is normally only shared with customers and prospective customers.	• Provides a user organization an assessment of the sensitive data and critical systems used to provide the outsourced services. • Examines IT and Operational controls associated with any or all of security, privacy, availability, confidentiality, and processing integrity. • May also include criteria pertaining to HIPAA and HITRUST.
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	Same as above in short version
ISO 27001 certification report	International Security Standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization.	In general, failure to have achieved this certification will be a barrier to adoption by most user organizations, especially internationally
ISO 9001 certification report	International Standard focused on Quality Management Systems	• Outlines the framework of how an organization consistently provides products and services that meet customer expectations. • Provides an indication that senior management considers quality and integral part of the business
The Federal Risk and Authorization Management Program (FedRAMP)	Provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by U.S. federal agencies.	Goal is to ensure that federal data and information is consistently subject to a high level of protection.
HITRUST (Health Information Trust Alliance)	Established to simplify the harmonization of multiple compliance frameworks. Combines HIPAA, ISO 27001, NIST 800-53, GDPR, and PCI DSS.	Although used by multiple industries, the HITRUST CSF (Common Security Framework) is becoming the choice for healthcare organizations to manage regulatory risk.

NOTE: SOC reports can be either Type 1 or Type 2. A Type 1 report is limited to the design of controls and of little value for the purpose described in this document. A Type 2 report looks at the operating effectiveness of controls over a period of time. The Type 2 report is more applicable to this process.

Note: there is a difference between a quality approach and security. ISO 27001 infuses quality into IT deliverables from a security point of view. But from a quality perspective, ISO 9001 and 27001 have a 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)*

2.1 General Auditing Topics

Below are general auditing topics to be covered by role illustrating, what is expected for e.g., a Cloud Service Customer to look after during an audit for IaaS, PaaS and SaaS solutions. For example, in the far downright square are these topics for when a Cloud service provider audits a SaaS provider/solution.

	IaaS	PaaS	SaaS
Cloud Service Customer	• Quality and Security Management review • Internal Audit's • Process for selecting and monitoring supplier's • Risk Management program in Line of Business • Configuration- and Change Management • Business Continuity, disaster and recovery plans • Manages privileged accounts and/or service accounts • Additional qualification of infrastructure according to intended use	• Quality and Security Management review • Internal Audit's • Process for selecting and monitoring supplier's • Risk Management program in Line of Business • Configuration- and Change Management • Business Continuity, disaster and recovery plans • Manages privileged accounts and/or service accounts • Workflow supporting application needs • Additional qualification of infrastructure- and platform according to intended use	• Quality and Security Management review • Internal Audit's • Process for selecting and monitoring supplier's • Risk Management program in Line of Business • Configuration- and Change Management • Business Continuity, disaster and recovery plans • Manages user accounts and roles • Workflow supporting application needs • Validation of applications according to intended use
Cloud Service Broker	• Quality and Security Management review • Internal Audits • Process for selecting and monitoring supplier's and selecting Cloud Service Provider on behalf of or together with the Cloud Service Customer. • Risk Management program in Line of Business • Configuration- and Change Management • Business Continuity, disaster and recovery plans • Manages privileged accounts and/or service accounts • Additional qualification of infrastructure according to intended use • Service requirements based on the approved service business case and the service risk assessment.	• Quality and Security Management review • Internal Audits • Process for selecting and monitoring supplier's • Risk Management program in Line of Business • Configuration- and Change Management • Business Continuity, disaster and recovery plans • Manages privileged accounts and/or service accounts • Workflow supporting application needs • 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. • Service, including service level options. • Process for defining cloud service provider KPIs.	• Quality and Security Management review • Internal Audits • Process for selecting and monitoring supplier's • Risk Management program in Line of Business • Configuration- and Change Management • Business Continuity, disaster and recovery plans • Manages privileged accounts and/or service accounts • Workflow supporting application needs • Process for Ensuring implementation of services by the Cloud Service Providers according to the defined service requirements and agreed service levels. • Process for releases service.
Cloud Service Provider	• Quality and Security Management review • Internal Audit's • Process for selecting and monitoring suppliers • Risk Management program in Line of Business • Configuration- and Change Management • Business Continuity, disaster and recovery plans • Manages privileged accounts and/or service accounts • Based on good engineering Practice verify that infrastructure service is in control and compliance e.g., with software development methodology/SDLC similar to commissioning and qualification activities • Process for provisions and manages the physical resources, builds and maintains the resource abstraction and control layer. • Customer Support. • Provides handling of security and risk identifications and controls.	• Quality and Security Management review • Internal Audit's • Process for selecting and monitoring suppliers • Risk Management program in Line of Business • Configuration- and Change Management • Business Continuity, disaster and recovery plans • Manages privileged accounts and/or service accounts • Process for Implements and/or deploys services according to the defined service requirements and agreed service levels. • Operates services. • Provides Customer Support. • Provides handling of security and risk identifications and controls. • Based on good engineering Practice verify that Infrastructure- and Platform services is in control and compliance e.g., with software development methodology/SDLC similar to commissioning and qualification activities	• Quality and Security Management review • Internal Audit's • Process for selecting and monitoring suppliers • Risk Management program in Line of Business • Configuration- and Change Management • Business Continuity, disaster and recovery plans • Manages privileged accounts and/or service accounts • Activities related to SDLC (Software Development Lifecycle) • Process for Implementation or deployment services according to the defined service requirements and agreed service levels. • Operates services. • Provides Customer Support. • Provides handling of security and risk identifications and controls. • Validates generic functionality in application • Release Management

Note: there is a difference between terminology related to IT in different sectors. The main purpose should be to evaluate whether processes are in control and reliable. It requires the auditor to be open-minded, i.e. willing to consider alternative ideas or points of view.

2.2 Specific SDLC topics to be audited

The Cloud Service Customer's Software Development Life Cycle (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, such as GxP, and company policies. Although it is beyond 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.

Areas to be audited:

Introduction to business processes focused on consistently meeting customer requirements and enhancing their satisfaction, e.g., implemented via a quality management system (QMS) or similar. This includes introduction to Cloud Services and the Framework for governance for role and responsibility	
Structure Policy's Periodic evaluation of Framework for governance Internal Audits Document Handling Handling of Deviations	
Life cycle activities for Services	**Supporting activities, e.g.**
Life cycle phases, documents, reviews and approvals of: • Requirements • Risk Assessment • Design • development/implementation • Testing • Releases	• Configuration management • Change management • Problem Management • Incident management • Identity and Access management • Back-up and restore • Business Continuity and Disaster Recovery • Training.

2.3 Specific Security topics to be audited

In the context of traditional computing, companies generally have a good understanding and handle on exactly where their data/host are and what resources, if any, they 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 risk management practices but have also stimulated a fresh evaluation of legal issues.

Topics to be audited (noncomprehensive list):
- Physical and personnel security
  - restricted and monitored access to critical assets.
  - isolation of dedicated infrastructure
- Identity and Access management
  - Described access management process.
  - Logical security architecture
  - Management of access credentials
- Data protection
  - logical (and physical?) segregation of customer data
  - Security of data in transit and data at rest
- 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. We recommend considering this framework when conducting audits, both internally and externally.

3 Data Integrity

Data Integrity is not a new concept. It has been around since paper and ink were the only ways of doing business, but Regulators have become increasingly prescriptive in their requirements.

Since 2015, the FDA [6], EMA [7], MHRA [8], WHO [9] , PIC/S [10] and other associations (PDA, ISPE) have been publishing Data Integrity guidelines to increase the industry's understanding of the expectations for compliance.

This white paper does not intend to repeat the requirements defined in the above guidelines and regulations. However, auditors of Cloud Service Providers should be familiar with the well-understood requirements for paper data integrity and how these may be translated to apply to electronic records and computer systems.

Generally, not following these principles may lead to data integrity issues for the Cloud Services Customer and consequently often leads to findings during regulatory inspections.

Data integrity principles exist across numerous industries. We would like to highlight the principles introduced by, and still used by the FDA, known as the ALCOA+ data integrity principles:

- Attributable; When creating a record, you must record the identity of the person or computer system that collected or generated the data. It's also important to record the date of the collection or generation.

- Legible; Ensuring data is legible is about more than being able to clearly read the data, although that is important in situations where manual data record-keeping takes place. Being able to make out the words is much less of a problem with electronic data, though.

- Contemporaneous; It's essential that individuals or systems make a record of an activity at the time it takes place. With electronic data, this is normal practice, so this is another point that has more relevance to manual record-keeping.

- Original; Records should be original rather than copies or transcriptions. Again, this applies mostly to manual record-keeping. Instead, the original recording of the data should be on the main record, whether that record is on paper or on a digital system.

- Accurate; All records should reflect the reality of what happened and should be error free. Also, there should be no editing of the original information that results in that information being lost. When recording data electronically, the system must have built-in accuracy checks and verification controls.

- Complete; All recorded data requires an audit trail to show nothing has been deleted or lost.

- Consistent; This primarily means ensuring data is chronological, i.e., has a date and time stamp that is in the expected sequence.

- Enduring; While this is touched on in a previous principle, this principle of ALCOA+ places specific emphasis on ensuring data is available long after it is recorded – decades in some situations.

- Available; This point follows on from the last point, i.e., data must not only exist, it must be accessible. The most efficient way of achieving this is normally by recording data electronically.

3.1 Risks With Cloud Computing

When leveraging cloud computing, Life Science companies must consider the overall associated risk vs. benefit balance. Today, cloud computing and all associated and related services are so prevalent that such services are likely already intertwined in a life sciences company's overall information systems and IT strategy and operation. Furthermore, cloud computing is not core business for life science companies, although it is for cloud services companies. It would be generally understood that cloud services companies, whose core business is delivering such services would be extremely well adept at providing these services to very high standards with high quality, security, and data integrity.

Outsourced cloud computing may present numerous benefits, including potential cost reductions coming from the providers' economies of scale, as well as solid operational capabilities tied to the fact that operational excellence is enabled by a strong focus on this very specific service – cloud.

That said, it is still clearly understood that the overall responsibility for data integrity and any associated regulatory burden clearly reside with the sponsors – the life sciences and pharmaceutical entities.

We are providing hereby several key aspects of data integrity, as they relate to cloud computing, which a sponsor would be responsible for regardless of the service being provided by a third party, and which the sponsor should include in their third-party vendor evaluations and audits.

3.1.1 Data Integrity Key Elements

Governance

- Existence of an established and codified governance structure guiding cloud operations
- Internal controls and evidence of internal evaluation of these controls on a recuring basis
- Change control procedures and process governing infrastructure and associated changes
- Corrective and preventive actions or similar processes
- Process for training and qualifications of all individuals associated with cloud operations

Security

- Shared responsibility over data security and clear responsibility matrix
- Information security team lead by a CISO
- Evidence of continuous awareness of best practices and infosec news
- Well, established and understood security architecture
- Privileged access to cloud consumer data
- Understanding of how security incidents may spill over to multiple cloud tenants
- Clear risk and severity assessment procedures with associated action plans
- Established actions and communications plans in case of a breach
- Clear understanding of data encryption, and architecture, for data at rest and in transit
- Attention to both cyber and physical security

Business Continuity

- Business continuity governance procedures (BCP)
- Disaster recovery (DR) plans and procedures
- Periodic testing, evaluation and exercising of DR and BCP
- Established and defined Service Level Agreements (SLAs) for system and data recovery
- Definition of Recovery Time Objective and Recovery Point Objective
- Understanding of differing government and industry regulations for data privacy and associated storage policies
- Established agreement on responsibilities and process for data retention
- Financial stability of the vendor
- Awareness of any risks to future business continuity of the vendor
- Contingency for access to data and applications that may be impacted by discontinuity of the business (e.g. escrow)

Legal and Compliance

- Vendor must be willing and ready to accommodate audits and to invest in necessary controls
- Contingency for migration of platform, software, or data to another cloud provider/environment
- Agreement and legal definitions supporting government access to data and adherence to local country specific requirements and regulations
- Adherence to privacy laws applicable to the residence of the data

4 Glossary

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

5 References

1. Cloud Security Alliance, Cloud Controls Matrix, v4, July 2021
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
6. US FDA - Data Integrity and Compliance With Drug CGMP Questions and Answers Guidance for Industry, April 2016
7. EMA - Guidance on good manufacturing practice and good distribution practice: Questions and answers, September 2016
8. MHRA - Guidance on GxP data integrity, March 2018 and September 2021 (GLP)
9. WHO - Guideline on data integrity (draft), June 2020
10. PIC/S - Good Practices for Data Management and Integrity In Regulated GMP/GDP Environments, PI041-1, July 2021