Agaram TECHNOLOGIES

GxP Data Integrity for Cloud Apps

White Paper

Part - 2

V. Raghavan

Agaram Technologies Private Limited

22 – Feb - 2021

TABLE OF CONTENTS

GXP REQUIREMENTS IN CLOUD ENVIRONMENT 3

Implications of Cloud Apps in regulated environment 3

1. Data Integrity 4
2. Data Confidentiality 5
3. Data Availability 9
4. Data Privacy 10

Risk Mitigations of Cloud Apps in GxP compliant regulated environment 12

1. Due Diligence and Audit 13
2. Risk Assessment 13
3. Agreement Considerations 14

Computerised system validation of Cloud Apps in GxP compliant regulated environment 16

Go-Live and After-go-live strategies 18

Checklist for Cloud service implementation for GxP compliance 19

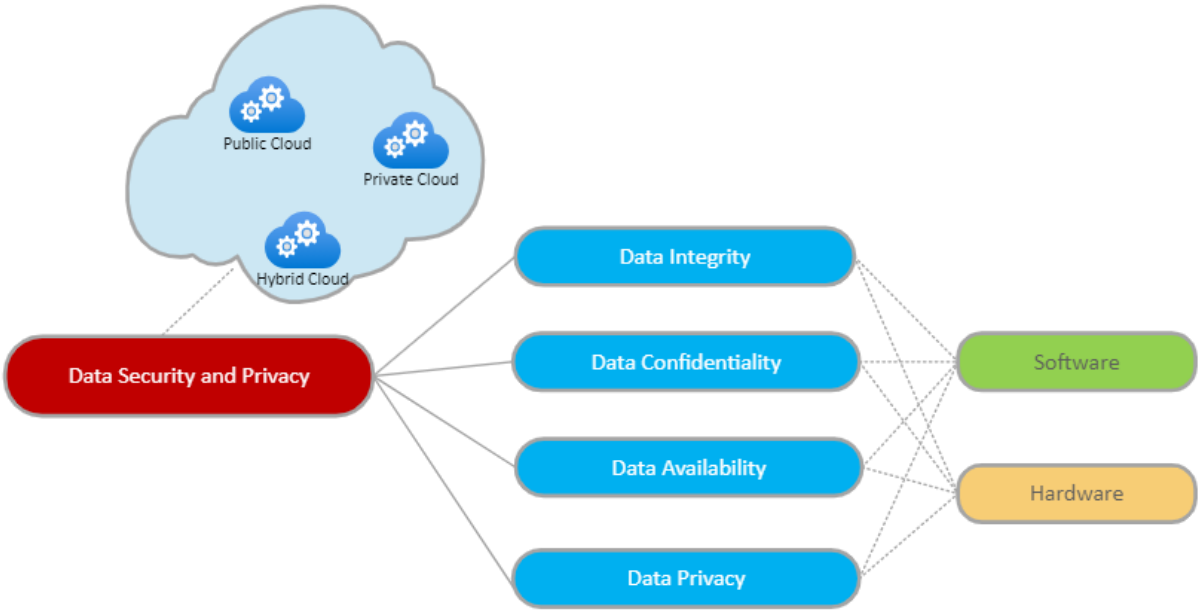
CONCLUSION 20

REFERENCES 21

ABOUT AGARAM TECHNOLOGIES PRIVATE LIMITED 21

GXP REQUIREMENTS IN CLOUD ENVIRONMENT

Implications of Cloud Apps in regulated environment



Cloud computing brings a number of attributes that require major attention when it comes to trusting the system. There are three major potential threats in cloud computing, namely, security, privacy, and trust.

Security plays a critical role in the current era of long dreamed vision of computing as a utility. It can be divided into four subcategories: safety mechanisms, cloud server monitoring or tracing, data confidentiality, and avoiding malicious insiders' illegal operations and service hijacking.

Security is the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of unauthorized withholding of information.

The trust of the entire system depends on the data protection and prevention techniques used in it. The major issues in the cloud computing include resource security, resource management, and resource monitoring.

Data privacy is traditionally accompanied with data security. Comparative studies on data security and privacy can help to enhance the user's trust by securing data in the cloud computing environment.

1. Data Integrity

Data integrity is one of the most critical elements in any information system. As we have already seen and aware that data integrity means protecting data from unauthorized deletion, modification, or tampering. Managing organization's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated, lost or stolen.

Data integrity in the cloud system must be such that the data should not be lost or modified by unauthorized users. Besides storage of large-scaled data, cloud computing environment usually provides data processing service. Data integrity can be obtained by techniques such as RAID-like strategies and digital signature.

Due to the large quantity of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities or users can access data. By avoiding the unauthorized access, organizations can achieve greater confidence in data integrity. The monitoring mechanisms offer the greater visibility into determining who or what may have altered data or system information, potentially affecting their integrity. Cloud computing providers are trusted to maintain data integrity and accuracy. However, it is necessary to build the third-party supervision mechanism besides users and cloud service providers.

Data integrity in the cloud system must be such that the data should not be lost or modified by unauthorized users. Besides storage of large-scaled data, cloud computing environment usually provides data processing service. Data integrity can be obtained by techniques such as RAID-like strategies and digital signature.

Due to the large quantity of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities or users can access data. By avoiding the unauthorized access, organizations can achieve greater confidence in

data integrity. The monitoring mechanisms offer the greater visibility into determining who or what may have altered data or system information, potentially affecting their integrity. Cloud computing providers are trusted to maintain data integrity and accuracy. However, it is necessary to build the third-party supervision mechanism besides users and cloud service providers.

Few Techniques that can be suggested are:

- ✓ A proof of Retrievability (POR) is a compact proof by a file system (prover) to a client (verifier) that a target file F is intact, in the sense that the client can fully recover it. As PORs incur lower communication complexity than transmission of F itself, they are an attractive building block for high-assurance remote storage systems. The HAIL system uses POR mechanism to check the storage of data in different clouds, and it can ensure the redundancy of different copies and realize the availability and integrity checking.

- ✓ Trusted Platform Module (TPM, also known as ISO/IEC 11889) is an international standard for a secure crypto-processor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.

2. Data Confidentiality

Data confidentiality is very critical to store organization's private or confidential data in the cloud. Ensuring the data confidentiality by authentication and access control strategies in cloud computing will improve the cloud reliability and trustworthiness.

It is often felt that it is virtually impossible for the cloud storage service providers to eliminate potential insider threat, it is very dangerous for organization's users to store their sensitive data in cloud storage directly. Simple encryption is faced with the key management problem and cannot support complex requirements such as query, parallel modification, and fine-grained authorization. Some of encryption strategies are as follows:

2.1 Homomorphic Encryption

It ensures that the cipher text algebraic operation results are consistent with the clear operation after encryption results; besides, the whole process does not need to decrypt the data. The implementation of this technique could well solve the confidentiality of data and data operations in the cloud. However, the encryption system involves very complicated calculation, and the cost of computing and storage is very high. This leads to the fact that the fully homomorphic encryption is still far from real applications.

A cryptographic algorithm named Diffie-Hellman is proposed for secure communication which is different from the key distribution management mechanism.

For more flexibility and enhanced security, a hybrid technique that combines multiple encryption algorithms such as RSA, 3DES, and random number generator has been proposed. RSA is useful for establishing secure communication connection through digital signature-based authentication while 3DES is particularly useful for encryption of block data.

2.2 Encrypted Search and Database

These are light-weight mechanism for database encryption such as trans-position, substitution, folding, and shifting (TSFS) algorithm. However, as the numbers of keys are increased, the number of computations and processing also increases.

In-Memory Database encryption technique is proposed for the privacy and security of sensitive data in untrusted cloud environment. A synchronizer exists between the owner and the client for seeking access to the data. Client would require a key from the synchronizer to decrypt the encrypted shared data it receives from the owner. The synchronizer is utilized to store the correlated shared data and the keys separately. A disadvantage of this process is that the delays occur due to the additional communication with the central synchronizer. However, this limitation can be mitigated by adopting group encryption and through minimizing communication between nodes and synchronizer.

There is also an asymmetric encryption mechanism for databases in the cloud. In this, the commutative encryption is applied on data more than once and the order of public/private key used for encryption/decryption does not matter. Re-

encryption mechanism is also used in the proposed scheme which shows that the cipher-text data is encrypted once again for duality. Such schemes are very useful in the cloud applications where privacy is a key concern.
A privacy-preserving multi-keyword ranked search approach over encrypted cloud data can also be worth trying as it can search the encrypted cloud data and rank the search results without leakage of the user's privacy.

2.3 Distributive Storage

To ensure the data integrity, one option is to store data in multiple clouds or cloud databases. The data to be protected from internal or external unauthorized access are divided into chunks using secret algorithm to generate a polynomial function against each chunk.

There is another technique called security-as-a-service in which the data is divided into chunks which are then encrypted and stored in separated databases. As each segment of data is encrypted and separately distributed in databases over cloud, this provides enhanced security against different types of attacks.

The tailored measurement technique is based on the network design and the specific routes for the incoming and outgoing traffic and gradually changing the resources according to the user needs.

Another method called Tailored Measurement Technique is based on the network design and the specific routes for the incoming and outgoing traffic and gradually changing the resources according to the user needs. This method depends on the computing resources and storage resources. Due to the variable nature of networks, the allocation of resources at a particular time based on the tailored active method does not remain optimal. The resources may increase or decrease, so the system has to optimize changes in the user requirement either offline or on-line and the resource connectivity.

2.4 Hybrid Techniques

A hybrid technique uses both key-sharing and authentication methods. The connectivity between the user and the cloud service provider can be made more secure by utilizing powerful key sharing and authentication processes. RSA public key algorithm can be used for secure distribution of the keys between the user and cloud service providers.

A three-layered data security technique is proposed: the first layer is used for authenticity of the cloud user either by one factor or by two factor authentications; the second layer encrypts the user's data for ensuring protection and privacy; and the third layer does fast recovery of data through a speedy decryption process.

2.5 Data Concealment

Data concealment may also be used to keep the data confidentiality in the cloud. It merges real data with the visual fake data to falsify the real data's volume. However, authorized users can easily differentiate and separate the fake data from the real data. Data concealment techniques increase the overall volume of real data but provide enhanced security for the private data. The objective of data concealment is to make the real data safe and secure from malicious users and attackers. Water-marking method can serve as a key for the real data. Only the authorized users have key of watermarking, so the authentication of users is the key to ensure the true data to be accessible for right users.

2.6 Deletion Confirmation

Deletion confirmation means that data cannot be recovered when users delete their data after the deletion confirmation. The problem is very serious, because more than one copy exists in the cloud for the security and convenience of data recovery. When users delete their data with confirmation, all the copies of data should be deleted at the same time. However, there are some data recovery technologies that could recover the data deleted by users from the hard disks. So the cloud storage providers should ensure that the deleted data of users could not be recovered and used by other unauthenticated users.

To avoid the data be recovered and unauthenticated used, a possible approach is to encrypt the data before uploading to the cloud storage space. FADE system is

based on technologies such as Ephemerizer. In the system, data are encrypted before they are uploaded to the cloud storage. When users decide to delete their data, the system just to apply the specific strategy to all the storage space could be covered with new data for replacing the deletion operation.

3. Data Availability

Data availability means the following: when accidents such as hard disk damage, IDC fire, and network failures occur, the extent that user's data can be used or recovered and how the users verify their data by techniques rather than depending on the credit guarantee by the cloud service provider alone.

The issue of storing data over the trans-border servers is a serious concern of clients because the cloud vendors are governed by the local laws and, therefore, the cloud clients should be cognizant of those laws. Moreover, the cloud service provider should ensure the data security, particularly data confidentiality and integrity. The cloud provider should share all such concerns with the client and build trust relationship in this connection. The cloud vendor should provide guarantees of data safety and explain jurisdiction of local laws to the clients. The main focus of the paper is on those data issues and challenges which are associated with data storage location and its relocation, cost, availability, and security.

Locating data can help users to increase their trust on the cloud. Cloud storage provides the transparent storage service for users, which can decrease the complexity of cloud, but it also decreases the controllability on data storage of users. There are proofs of geographic replication that have succeeded in locating the data stored in Amazon cloud.

The most common abnormal behaviour of untrusted storage is that the cloud service providers may discard part of the user's update data, which is hard to be checked by only depending on the simple data encryption. Additionally, a good storage agreement needs to support concurrent modification by multiple users.

Depot Cloud Storage system can guarantee Fork-Join-Causal-Consistency and eventual consistency. It can effectively resist attacks such as discarding and it can support the implementation of other safety protections in the trusted cloud storage environment (such as Amazon S3).

SPORC Framework system can implement the safe and reliable real-time interaction and collaboration for multiple users with the help of the trusted cloud environment, and untrusted cloud servers can only access the encrypted data.
However, operation types supported by reliable storage protocol support are limited, and most of the calculations can only occur in the client.

4. Data Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal them selectively. In the cloud, the privacy means when users visit the sensitive data, the cloud services can prevent potential adversary from inferring the user's behaviour by the user's visit model (not direct data leakage). Researchers have focused on Oblivious RAM (ORAM) technology. ORAM technology visits several copies of data to hide the real visiting aims of users. ORAM has been widely used in software protection and has been used in protecting the privacy in the cloud as a promising technology.
The privacy issues differ according to different cloud scenarios and can be divided into four subcategories as follows:

- ✓ how to enable users to have control over their data when the data are stored and processed in cloud and avoid theft, nefarious use, and unauthorized resale,
- ✓ how to guarantee data replications in a jurisdiction and consistent state, where replicating user data to multiple suitable locations is a usual choice, and avoid data loss, leakage, and unauthorized modification or fabrication,
- ✓ which party is responsible for ensuring legal requirements for personal information,
- ✓ to what extent cloud subcontractors are involved in processing which can be properly identified, checked, and ascertained.

4.1 Service Abuse

Service abuse means that attackers can abuse the cloud service and acquire extra data or destroy the interests of other users. User data may be abused by other users. Deduplication technology has been widely used in the cloud storage, which means that the same data often were stored once but shared by multiple different users. This will reduce the storage space and cut down the cost of cloud service providers, but attackers can access the data by knowing the hash code of the stored files. Then, it is possible to leak the sensitive data in the cloud. Hence proof of ownership approach has been proposed to check the authentication of cloud users.

Attackers may lead to the cost increase of cloud service. Fraudulent resource consumption is a kind of attack on the payment for cloud service. Attackers can consume the specific data to increase the cost for cloud service payment.

4.2 Averting Attacks

The cloud computing facilitates huge number of shared resources on the Internet. Cloud systems should be capable of averting Denial of Service (DoS) attacks.

It is suggested to integrate cloud services for trusted computing platform (TCP) and trusted platform support services (TSS). The trusted model should bear characteristics of confidentiality, dynamically building trust domains and dynamic of the services. Cloud infrastructures require that user transfers their data into cloud merely based on trust. Security of data and trust in cloud computing is the key point for its broader adoption.

Identity management, data recovery and management, security in cloud confidentiality, trust, visibility, and application architecture are the key points for ensuring security in cloud computing.

4.3. Identity Management

Cloud computing provides a podium to use wide range of Internet-based services. But besides its advantages, it also increases the security threat when a trusted third party is involved. By involving a trusted third party, there is a chance of

heterogeneity of users which affects security in the cloud. A possible solution to this problem could be to use a trusted third-party independent approach for Identity Management to use identity data on untrusted hosts.

There are problems of data leakage and loss of privacy in cloud computing. Different levels of protections can be used to prevent data leakage and privacy loss in the cloud. Cloud computing provides new business services that are based on demand. Cloud networks have been built through dynamic virtualization of hardware, software, and datasets. Cloud security infrastructure and the trust reputation management play a vital role to upgrade the cloud services. The Internet access security, server access security, program access security, and database security are the main security issues in the cloud.

Risk Mitigations of Cloud Apps in GxP compliant regulated environment

The auditors inspecting the GxP controlled environment will focus on the following aspects in SaaS solutions for managing their core business processes:

- ✓ Integrity of data is assured
- ✓ Risks clearly identified & mitigated
- ✓ Formal agreements/contracts between organization and Cloud Service Provider
- ✓ Quality systems of Cloud Service Provider
- ✓ Applicable SOPs, Validation process, change control Process, Training
- ✓ Cyber Security
- ✓ Data backup and recovery procedures as well evidences
- ✓ Supplier audit(s)

The organization in the regulated environment can be made GxP compliant by selection, control and management of Cloud Service Provider by following the steps as below:

Step 1: Due Diligence and Audit

Step 2: Risk assessment for potential impact of using the service (regulatory, security and business risks)

Step 3: Mutually verified and managed agreement and metrics to ensure Service Provider meets Performance and ensures regulatory compliance

Let us briefly understand these steps:

1. Due Diligence and Audit

During this process, the following are verified and recorded.

- ✓ How long the Service Provider has been in the business of Cloud Service and what are the major customers?
- ✓ Has the provider had any experience with Cloud Security Alliance?
- ✓ Has the Provider been able to ensure the security processes followed are of international standard?
- ✓ Has the Provider provided evidences that tried and tested methodology has been followed (set and achieved KPIs and other performance metrics)?
- ✓ Has extensive experience with compliance needs of the pharma and life sciences industry, and uses tools to ensure that compliance is achieved efficiently.
- ✓ Can provide qualification documentation of appropriate quality that allows leveraging, using a risk-based approach to reduce your validation effort.
- ✓ Is able to explain complex technology environments so they can understand the operation and design elements.
- ✓ Has been audited by similar organizations in terms of intended use and compliance needs.
- ✓ Operates a robust and suitable QMS that mat ches life sciences industry expectations.
- ✓ Employs adequate Subject Matter Experts (SMEs) that cover IT from a technical and compliance perspective.

2. Risk Assessment

ISPE's GAMP® 5 (Good Automated Manufacturing Practices) provides a pragmatic and practical approach to achieve compliant computerized systems, fit for intended use in an

efficient manner. It addresses the entire lifecycle of an automated system and its applicability to a wide range of information systems, lab equipment, integrated manufacturing systems, and IT infrastructures. It's regarded as the definitive industry guidance and is referenced by regulators worldwide, including the FDA and EMA.

This risk-based approach has the following stages:

Step 1: Perform an initial risk assessment and determine the system impact
Step 2: Identify the functions that may impact on very critical elements (Example: patient safety, product quality and data integrity)
Step 3: Perform Functional Risk assessment and identify controls
Step 4: Implement and verify appropriate controls
Step 5: Review risks and monitor controls

3. Agreement Considerations

The following need to be considered to arrive at an agreement with the Service Provider. Whether the Service Provider has

- ✓ Delivered the proof that all components of the monitoring solution have been developed according to GAMP 5 – including validation plan, risk analysis and validation reports of all hard- and software components.
- ✓ Provided Installation Qualification-documentation of the cloud software.
- ✓ Provided efficient tools for the qualification of the customer-specific hardware components and the configuration by the client: IQ ("what measurement hardware has been installed?") and OQ (Operational Qualification = "does the measurement hardware and software configuration work together as planned (e.g. issue alarms in case of deviation)?")

The service provider must:

- ✓ Clearly define the policies regarding notification, documentation and qualification in the service level agreement (for a Private Cloud SaaS there might be room to negotiate these policies in order to align them with your organization's needs regarding upfront notifications, testing and qualification options prior to installing any Patches or Updates)
- ✓ Provide change management notifications and documentation (Patches are minor changes and must at least be documented; Upgrades must be announced in

advance and rated minor or major and documented appropriately). As a good practice, each document should clearly state, if the client should take action (or not) (this is only good practice, as the responsibility to ensure GxP-compliance always remains with the organization using the software).

- ✓ All of the above listed must be available for to the client at any time, including during an audit (ideally online as part of the Cloud service).

The client must be able to trust the service provider that Data Integrity is always secured. The service provider must:

- ✓ Ensure that raw data (measurement values) cannot be changed at all.
- ✓ Implement an audit trail keeping track of every change.
- ✓ State in the service level agreement that he takes care of the maintenance and assurance of the accuracy, consistency and completeness of data over its entire life-cycle.

As part of Business continuity plan, the service provider must:

- ✓ Define and guarantee the performance and availability of the solution in his service level agreement.
- ✓ Make sure that the system and data is backed up regularly and recoveries are exercised and documented regularly.
- ✓ Monitor the availability and performance of the solution and provide reports thereof to the client.

In nutshell the agreement must typically cover the following:

- ✓ Topics to formally agree on with your CSP would concern:
- ✓ Backup and restore.
- ✓ Patch management.
- ✓ System security.
- ✓ Availability and capacity management.
- ✓ Incident management.
- ✓ Configuration and change management.
- ✓ Regulatory compliance

The terms contract contents must be comprehensive, because what is not defined in writing has to be re-negotiated later (and likely paid extra). For example, by using a SaaS

product the implementing organization will become highly dependent on the Software supplier for providing input during possible audits. Therefore, it is necessary to ensure that audit cooperation must be included in the agreement to be able to answer questions on topics such as configuration management, qualification of infrastructure, disaster recovery, and training records.

Another example of what is seen in daily business is that things tend to get more complex if the SaaS provider uses separate IaaS providers for infrastructure and hosting. In that case, focus on examining if and how your SaaS provider has audited and qualified this third party. If it's an unacceptable risk that your company's critical data resides with your supplier's supplier, be sure to extend your contract and/or Quality Agreement with statements that formally disallow your CSP to deploy such models.

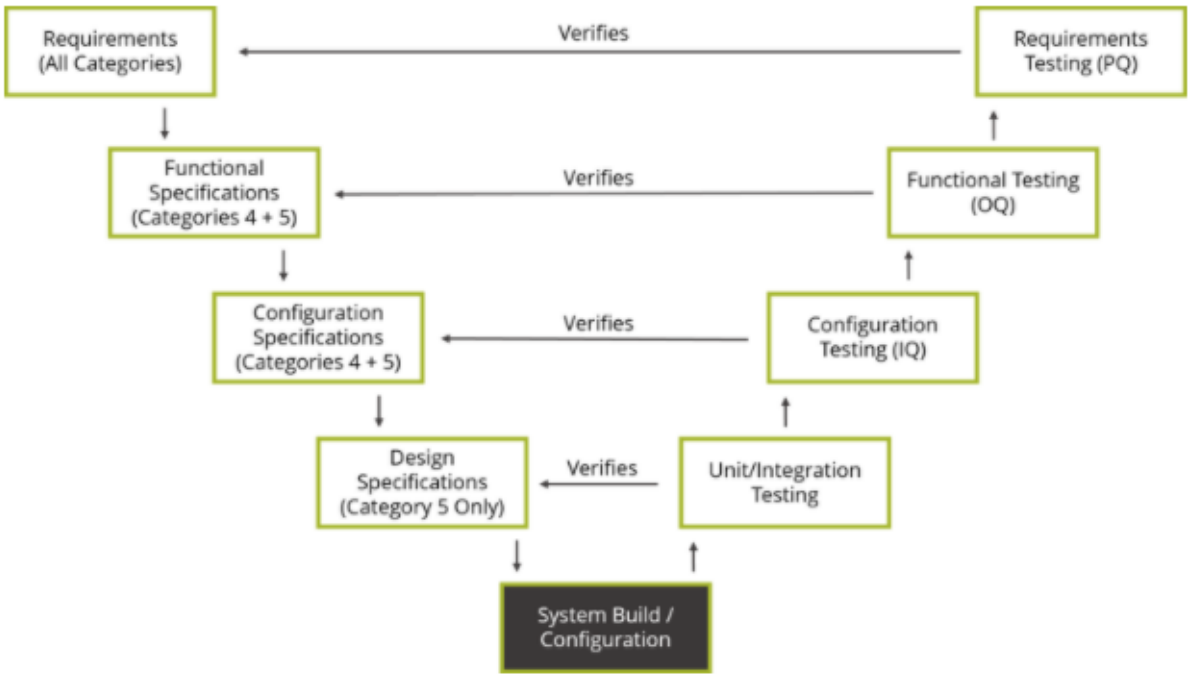
Computerised system validation of Cloud Apps in GxP compliant regulated environment

GAMP 5's approach can be summed up by the V-model diagram. The V-model proposes the specifications of a system are validated. The types of specifications associated with a system are tied to its degree of complexity. For example, for a configured product (Category 4), requirements, functional and configuration testing is conducted to verify the requirements, functional and configuration specifications. However, functional and configuration specifications are not required when using commercial off-the-shelf software (Category 3). As a result, the extent of the testing performed would also be reduced.

The aim of conducting verifications is to demonstrate that the system functions as intended. This is accomplished by using the requirements and specifications as an objective standard to which the system is tested. The test scripts are traced to the requirements and specifications they verify. If the test passes, the executed test script serves as documented evidence that the associated requirements and specifications are met.

Depending on the nature and configurability of the system, qualification by your CSP can even include performing a configuration verification to ensure that the configured

Computerised system meets organization's specific requirements, and functional verification to challenge the system both positively and negatively. The latter activity would be typically executed as a joint effort by organization and Cloud Service Provider (CSP).



Once such qualification phases are done, it is time to validate. Whether on-premise or cloud, GAMP 5 is still the preferred framework to approach validation of your applications and can be used to do as much or as little as you deem appropriate. From a GAMP 5 perspective, the CSP has covered the bottom part of the so-called V model.

Validation needs on this level are specific to intended use of the Computerised system and the uniqueness of the system configuration. This activity cannot be performed by CSP, because the system needs to be validated in the context of how it supports organizations operations, practices, and requirements. Obviously, this implies that at least a user requirements specification or similar document is in place, and that you have determined risk-based what your validation focal points should be. It is important to take a business process-oriented approach in case of cloud Computerised systems, and not to be tempted to merely view this validation phase as a technical exercise. The end-result should not just be an auditable set of documents, but hopefully a computerised software solution that does what it is meant to do.

Go-Live and After-go-live strategies

If GAMP 5 for the validation has been carried out for cloud computerised system, it will be released for entering the operational phase based on successful validation of a specific version of that system. Once live in an on-premise situation, at some point in time the decision will have to be made on whether or not to upgrade system to newer versions whenever these become available. An important feature of SaaS, however, is that the supplier frequently pushes new versions to improve performance and user experience. Such upgrades are mandatory and apply for all of their customers, usually without a possibility to opt- out. This of course is an advantage from many perspectives, but introduces significant challenges for regulated users as each new version requires validation (or: revalidation).

The necessity of change management, impact assessment, and verification testing adds to the work burden and short-term costs for CSP. This aspect is one that not all providers will be used to, and is therefore crucial to carefully examine in auditing stages of the implementation project.

In case the CSP performs a change to their infrastructure, platform or the Computerised system that you are using, and does not inform you accordingly. This would compromise the validated state of your system directly.

Following the approach propagated by GAMP 5, it is preferred to execute the (re)validation of hotfixes or version upgrades following a risk-based process. It should be a relatively short process that simply focuses on new functionality and checks any potential impact on functionality from the previous version. If the computerised system is offered in a three-system landscape (e.g., development/ test/production), it is common practice that CSPs introduce the new version or hotfix in the development and/or testing environment first, prior to releasing it in the production environment. This allows the organization to prepare for the upcoming change, assess and mitigate the associated risks, and execute (re)validation activities accordingly.

It must always be kept in mind the timeframe maintained by CSP between releasing the upgrade in the test environment and production environment. If the upgrade is carried out in production environment one week after the testing environment, it is unlikely that the

organization will be able to manage this change from a quality and compliance perspective. Depending on organization's internal procedures and the criticality of the system, even a timeframe of one month would in most cases be a challenge.

In addition to the time-frame between upgrade of the different environments, the frequency at which upgrades are introduced is also an important factor to take into account. What is the frequency in which CSP push upgrades: monthly, quarterly, or yearly? Will the organization be able to cope with this frequency in combination with the timeframe mentioned earlier? These are the vital questions.

Checklist for Cloud service implementation for GxP compliance

1. Does the supplier perform a computerized system validation (CSV)? Does it include validation of backup and recovery and has that been tested?
2. Is an audit trail available tracking each login, event and action?
3. Is data protected from unauthorized access?
4. Is the data backed-up regularly at a secure place (protected from deletion or loss)?
5. Are data recoveries exercised and documented regularly?
6. Is data privacy guaranteed (& solution supports compliance with GDPR)?
7. Does the SaaS provider guarantee GAMP 5 compliance?
8. Are Validation Plan, Risk Analysis & Validation Report available?
9. Are Qualification templates available for IQ and OQ?
10. Are there clear policies regarding notification, documentation and qualification?
11. Does the supplier provide comprehensive change management notifications and documentation?
12. Are clear performance and availability levels of the solution defined?
13. Are performance and availability reports made available to clients regularly?
14. Is process data available for as long as they are needed in the business processes?
15. After this period, can data be archived for minimum required number of years in a human readable format?
16. Does the client remain the owner of the data?
17. Does the Service provider accept on-site audits by the client?
18. Is a service level agreement in place covering all above points?

CONCLUSION

Implementation of Cloud computing solutions ensure benefits like cost efficiency, scalability, convenience (no hardware and software maintenance), highly professional backup and recovery strategies etc. for organizations that need to comply with GxP regulations, provided they adopt and implement effective approach. With regard to qualification and validation of computerised systems, the same requirements apply to cloud services as to on-premise systems. Standardised documentation process must be set in place and must be clearly defined in the service level agreement. The critical processes like change management, data backup, restore, audit-trail and retention to ensure business continuity or long-term archiving must be documented, validation during implementation, signed-off and must be adopted after go-live.

In addition, it is highly recommended that service providers as well as any 3rd party consultants/Providers must be willing to accept on-site audits by the customer organizations. Clearly and comprehensively defined and manageable set of documents prepared by the organization in collaboration with CSPs will not only provide customers operating in a GxP environment with the required support and security, but will also help to frame and establish a strong and reliable working partnership between them. Such a partnership and working are the critical important success factors to achieve the required level of compliance and “audit fitness” for the customer organization who always remains responsible for the safety of his patients and end products/services.

In **Part 1,** we have understood the basic concepts of GxP requirements and Cloud implementation of computerised systems

In **Part 2**, we have understood the strategies to be adopted by Organisations implementing cloud systems to comply with GxP requirements

REFERENCES

1. “Data Security and Privacy in Cloud Computing” by Yunchuan Sun, Junsheng Zhang, Yondping Xiong and Guangyu Zhu.
2. “Understanding Cloud Computing for GxP Monitoring Environments: Risky or Rewarding?” By Dr. Philipp Osl and Bob Lucches
3. “Data Integrity in the Cloud” by Mark Stevens
4. "Advantages and challenges for the life sciences industry - Compliant in the Cloud" By Steven de Bruijn

ABOUT AGARAM TECHNOLOGIES PRIVATE LIMITED

Agaram Technologies has been stablished in 1998 with Headquarters in Chennai, India and has offices in USA, Europe and South Korea.

It is a leading provider of enterprise class Integrated Laboratory informatics software and solutions namely LIMS, QMS, ELN and SDMS.

Agaram provides integrated software solutions, consulting services, product support and training to laboratories in Pharmaceutical, Healthcare, Dairy, Food & Beverage, Chemical, Oil & Gas, Environmental, Contract Research Organization (CRO), Forensics, Agriculture and Bio-Banking Industry.

Agaram Technologies exclusively focuses on laboratory informatics products. It has earned a leadership position in this market by combining a world class customer experience with a powerful, yet simple and affordable suite of software products. These products have been organically built to seamlessly integrate all Laboratory related functions.

It is an ISO certified organization (ISO 9001:2015) in Design, Development, Implementation, Maintenance and Support of Laboratory Information and Analytical Instrumentation Software Products and Services.