WHITE PAPER

Understanding Cloud Computing for GxP Monitoring Environments: Risky or Rewarding?

we prove it.

SWISS QUALITY

Dr. Philipp Osl | ELPRO-BUCHS AG, Buchs SG (Switzerland)
Bob Lucchesi | USDM Life Sciences, Santa Barbara (USA)

In order to comply with the GxP-requirements, environmental conditions need to be monitored and documented along the entire supply chain of pharmaceutical products. Since we see more cloud solutions being used for this purpose, the question comes up if this approach is the right one. This whitepaper discussed different cloud models and their risks and benefits. In addition it provides a checklist for the use of cloud-monitoring in GxP-applications.

Over the last couple of years, acceptance for cloud computing and cloud hosting has rapidly grown for business applications across different industries. This is due to obvious advantages, such as:

- scalability (both for processing as well as storage capacities)
- built-in backup and recovery functionalities
- reduced maintenance efforts
- easy access for geographically distributed teams
- cost efficiency, thanks to reduced IT investments or required know-how

Yet today some concerns remain around lock-in effects and resulting dependencies on the solution provider, security concerns or delegation of control.

When you add GxP compliance to the list of concerns, you have a unique situation with unique data environments. As pharmaceutical and life science industries also move to the cloud, for the above-mentioned advantages, it's important to consider how it affects this specialized industry. Are cloud-based infrastructure, platforms and software in the cloud compliant and in line with data integrity requirements? This article will provide the answers, with a special focus on environmental monitoring solutions for the pharmaceutical, life science, biotech and health care industries.

Why is this important to you?

GxP regulated companies have a long list of global requirements for using, storing and communicating data. FDA 21 CFR Part 11, EU General Data Protection Regulation (GDPR), Data Integrity regulations from many countries… just to name a few. To stay within the regulatory lines, it's important you understand the pros and cons of cloud solutions for your pharmaceutical business. This article will lay out all the facts related to cloud services in a GxP monitoring environment and corresponding measures to ensure compliance. Plus, there is a checklist at the end of the article that your team can use to take next steps.

What is the Cloud?

Before we start the discussion of specific considerations regarding cloud-based GxP-compliant environmental monitoring solutions, let's briefly clarify different models of cloud services. Usually, three cloud models are differentiated, which differ from traditional on-premises hosting by the parts that are outsourced:

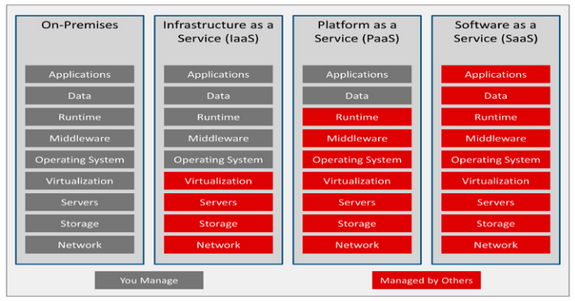

Illustration 1: Differences in cloud models [1].

Infrastructire as a Service **(IaaS)** is the cloud model where the client takes most responsibility: he runs the applications and database on his own operating system and middleware which operate o virtualized servers from the cloud provider. IaaS is beneficial for large organizations that wish to have complete control over their applications and software infrastructures, but are fine with having the hardware operated by a specialized provider or are looking to only purchase what is actually consumed or needed (e.g. they want to benefit from dynamic assignment of processing power or storage for applications with varying requirements over the time). A good example could be a life-science company who wants to host semi-critical applications on an IaaS: benefit from the outsourcing but still keeping tight control.

Platform as a Service **(PaaS)** gives more responsibility to the cloud provider since the virtualized servers also include the operating system as well as middleware. PaaS can provide great speed and flexibility to the entire process for companies who want to run their own application on a "turn-key environment". A good example could be a pharmaceutical company operating their own office application on a PaaS of a large cloud provider like Amazon Web Service or Microsoft Azure.

Software as a Service **(SaaS),** also known as cloud application services, represents the largest cloud market. SaaS delivers (business) applications that are typically accessed directly via the web browser and do not require any downloads or installations on the client side.

Besides the different cloud models described above, varying by the components that are outsourced, there are also different models of how those outsourced cloud resources are deployed:

> **Public Cloud** refers to the cloud computing model with which the IT services are delivered across the Internet. The cloud vendor is responsible for developing, managing and maintaining the pool of resources shared between multiple tenants from across the network. A sub-type of the public cloud is the so called **Community Cloud** which is also commonly used by various organizations. However, the access is not public but only accessible for a defined group of users with joint requirements. Common interest could for example be the compliance to audit regulations or common performance requirements for fast reaction times [2].

> **Private Cloud** refers to the cloud solution dedicated for use by a single organization. The computing resources are isolated and not shared with other customers. Compared to the Public Cloud, the Private Cloud is significantly more expensive since the resources need to be multiplied with each new customer.

> **Hybrid Cloud** refers to the cloud infrastructure environment that is a mix of public and private cloud solutions. The resources are typically orchestrated as an integrated infrastructure environment. Apps and data workloads can share the resources between public and private cloud deployment based on organizational business and technical policies. Hybrid Cloud takes "the best of both worlds" but is more complex to overlook and manage.

Today, cloud computing is a major trend and revenues are exploding. Interesting enough, financial services/banking/insurance, industrial manufacturing and telecommunication services belong to those industries with the greatest number of cloud applications per business function [3]. This illustrates nicely, that today also (or even predominantly) industries with high requirement levels in regards to compliance and safety are using cloud computing services.

What is the right cloud set-up for a GxP compliant application?

Knowing the different types and resources of cloud computing, the following section elaborates the right set-up for a GxP monitoring solution's specific requirements:

The monitoring solution including the database must be validated. A computerized system validation (CSV) is the documented process of assuring that a computerized system does exactly what it is designed to do in a consistent and reproducible manner.

It basically means, that requirements must be documented, validation and test plans written, risks evaluated in a written risk assessment, functionalities tested and documented according to the test plan and finally a validation report issued summarizing all validation efforts. An IaaS or PaaS solution could be the right approach for users who are fine with validating the cloud infrastructure provider and managing software installation and maintenance by themselves. For users who do not want to deal with those issues or do not have an experienced IT department at hand, a SaaS approach could be the right solution: providing the additional advantage of only having one cloud solution provider instead of having to deal with the software vendor and the cloud infrastructure provider.

Mainly cost are relevant for the decision between the options Public, Private or Hybrid Cloud: how many organizations are carrying the various cost blocks?

> Independent from the cloud-model, each organization must carry their own cost for the data collection hardware like data loggers and sensors.

> At a public cloud set-up, all cost connected to the monitoring software are shared between all users. Typically the cloud provider invoices a fixed price per used measurement point and thereby carries the financial risk. The user benefits from distributing the cost on many shoulders and has a low entry barrier since no investment into the development, validation and operation of a monitoring software.

> With a private cloud, the cloud resources are not shared with other organizations. Therefore the fixed cost for the isolated infrastructure (e.g. servers, licenses for application and operating system, etc.) must be covered by one customer. On the other hand, while fixed cost is covered, variable cost get smaller.

> When consider a hybrid cloud, the distribution of the public versus the private cloud resources is relevant. In this scenario, we assume that customer specific development cost as well as cost for validation of the distributed architecture is covered directly by the user. In addition also the infrastructure cost for the private part of the hybrid solution must be directly covered by the customer. The public part of the infrastructure can thereby be covered by many users and included in a variable price per monitoring point.

The following picture shows the various cost blocks in the various cloud models as a schematic illustration. It shows nicely, that mainly small installations benefit from the public cloud model since the user benefits from the lack of fixed cost blocks. This cost benefit is reduced with larger installations of several hundred or thousand measuring points.

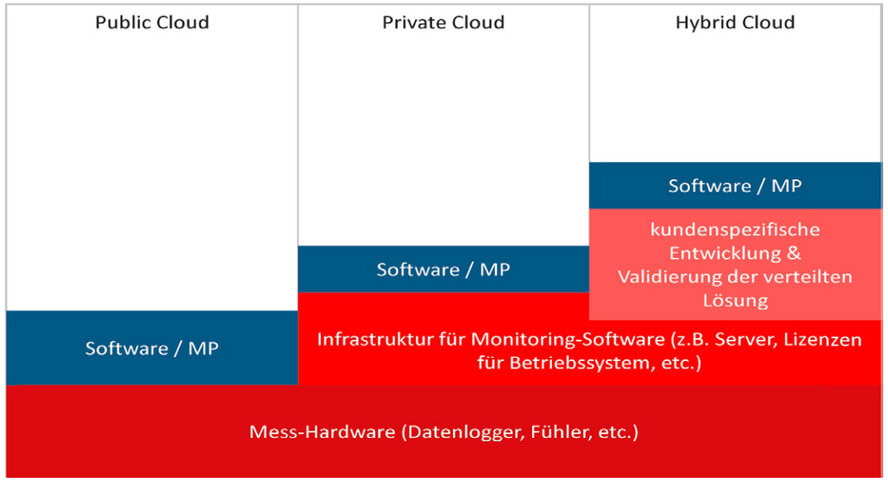

Illustration 2: Cost blocks in different cloud models (schematic illustration)

In a GxP-environment, **data must be immutable**. Again the main concern is data integrity (assuring that data is attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring and available over its entire life-cycle [4,5]) and ultimately patient safety. Translated to a (cloud) monitoring solution, this means:

> In whatever infrastructure we work, we need a multi-layer application where data is safe and cannot be manipulated. You may ask yourself, whether in your opinion your IT can run an internal data center more professional than the global cloud providers like Amazon Web Services, Microsoft Azure, or Google Cloud Platform etc., that all are, by the way, aware of specific GxP requirements and provide comprehensive documentation materials for solution providers that want to run critical applications in their infrastructure.

> Furthermore, you may ask whether you at any point could be better aware of any data integrity risks than the monitoring solution provider that has the utmost knowledge of all of the system's interconnected components. Hence, we see again a Public Cloud SaaS an excellent choice for installations of any size, in particular for smaller installations given the cost advantages, while a Private Cloud SaaS is a charming alternative for larger installations, as this set-up - in comparison with the Public Cloud SaaS - may give you more room to manage software updates in accordance with your organization's qualification requirements, as the monitoring solution instance is only used by you and not shared between different tenants.

Conclusion: *Given the argumentation outlined above, it is hardly surprising that we see more and more monitoring solutions for GxP-critical applications offered as* ***SaaS in a Public Cloud****. This choice offers maximum quality (minimal risks) and at the same time minimal cost to achieve those targets. Many suppliers will offer single-tenant* ***SaaS in a Private Cloud*** *as an alternative at significantly higher costs. The following chapters will therefore focus on these two options to deliver a GxP-compliant monitoring solution via the Cloud.*

Risks and Mitigations Related to GxP-compliant Monitoring Solutions Provided as SaaS in the Cloud

In this section we will elaborate on the risks of the chosen set-up (Public Cloud SaaS (shared instance for several tenants) or Private Cloud SaaS (single-tenant instance exclusively for one organization)) related to a GxP-compliant monitoring solution and meaningful mitigation strategies that you should require your service provider to guarantee.

> In a SaaS set-up, the supplier defines **the physical location of data storage**. Data may be stored on different continents, regions and countries even having different laws in regards to data protection and privacy. If private data is included (such as names, addresses, phone numbers or credit cards) this data may also underlie different legislations and rules (e.g. EU GDPR as Europe's data privacy regulation). The service provider therefore must make sure (and state in the service level agreement) that:
- Appropriate safety measures are undertaken to protect the data (from unauthorized access).
- Appropriate back-up measures are in place to secure the data (from deletion or loss).
- Data privacy is guaranteed (and the solution supports compliance with GDPR).

> Every GxP-compliant solution must be **validated**. For a SaaS service, either offered as a Public or Private Cloud solution, this specifically means that the service provider must:
- Deliver the proof that all components of the monitoring solution were developed according to GAMP 5 – including validation plan, risk analysis and validation reports of all hard- and software components.
- Provide IQ-documentation of the cloud software.
- Provide efficient tools for the qualification of the customer-specific hardware components and the configuration by the client: IQ (Installation Qualification = "what measurement hardware has been installed?") and OQ (Operational Qualification = "does the measure ment hardware and software configuration work together as planned (e.g. issue alarms in case of deviation)?").

> One of the biggest advantages of SaaS is that the provider takes care of **Patches and Updates**. How can the client's GxP-compliance be safeguarded? If an auditor wants to see the validation and qualification efforts of the monitoring solution but the software is constantly upgraded, how should this go together? This is where we see the biggest differences between a shared instance in the Public Cloud and a single-tenant instance offered as a Private Cloud SaaS. Either way, the service provider must:
- Clearly define his 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.

> A major concern is **Business Continuity** – in particular in a SaaS set-up where the client has no control whatsoever on the operation of the solution. 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.

> **Archiving** is not clearly defined in GxP regulations and left open for everybody's own interpretation. Often heard during audits are archiving periods of 10 years, sometimes 15 years. It is easy to store electronic flies and data over many years but a huge problem is the availability of software for analysis. Many people have the romantic idea, that when data is archived, it should be available forever in the same way as it is generated (same software, same interface). Wikipedia says: "Data archiving is the process of moving data that is no longer actively used to a separate storage device for long-term retention. Archive data consists of older data that is still important to the organization and may be needed for future reference, as well as data that must be retained for regulatory compliance." So, by definition "archive data" has a different form than "process data":

> **Process Data** is "fresh data" which is used for taking business decisions (e.g. of a product, MKT calculation of a stability study). For **two years**, the service provider must ensure that Process Data
- is available electronically for visualizations (e.g. zoom, overlay)
- it must be possible to draw statistics easily (e.g. calculate MKT),
- it must be possible to add comments in the system and generate reports (e.g. release decision),
- it must be possible to export the data (e.g. to higher batch management system).

> After the first two years, the data is not needed any more in business processes and typically changes its location and form to become Archive Data. The service provider must ensure that Archive Data is available for at least 10 years and fulfils the following requirements:
- clearly labeled (e.g. monthly report per sensor)
- in a "human readable" form as a record (e.g. PDF/A report)
- in a secure archive (e.g. in a drive that is backed up regularly to a different physical location)

> When choosing a GxP-monitoring provider, the client is **locked-in** with this provider. How can we make sure data is still available in case the provider goes out of business or the solution is no longer offered?
- Make sure to keep a copy of the data (e.g. a monthly sensor report) in a human readable format (e.g. PDF/A) at the client's premises (e.g. automated monthly email to in-house mail-account).
- The service level agreement must define that the client remains owner of the data and that data is available for download before service ends.
- The service level agreement must define a meaningful notice period prior to service termination.

> Besides a Service Level Agreement defining all of the above mentioned measures, the service provider must also **accept on-site audits** by his customers. As part of these audits, clients must be able to
- Access detailed GAMP 5 documentation to verify the provider's validation certificate
- Review relevant account management guidelines, e.g. for accounts on the Cloud servers (Who from the service provider's side has access to the cloud infrastructure? How are these people instructed/trained?)
- Review account management guidelines for customer accounts (Who from the service provider's side has access to which data of the customer? How are these people instructed/trained?) Review contracts / service level agreements with 3rd party Cloud infrastructure providers (like e.g. Amazon Web Services, Microsoft Azure etc.), if used
- Review "service organization control (SOC) 2[1] " reportsfor the data center or Cloud infrastructure provider used

Conclusion

If done right, cloud-based monitoring solutions allow for benefits like cost efficiency, scalability, convenience (no hardware and software maintenance), highly professional backup and recovery strategies etc. for companies that need to comply with GxP regulations. Regarding validation and qualification needs, the same requirements applies to cloud services as to self-operated systems. This means that documentation is king and shared responsibilities regarding documentation needs to be clearly defined in the service level agreement. Also, critical processes like change management process, data backup and retention to ensure business continuity or long-term archiving must be defined as part of the service level agreement.
In addition, we recommend that you require your service provider to accept on-site audits by his customers, where you will be granted access to further, more detailed documentation. Having all this defined and the comprehensive but manageable set of documents made available by the service provider 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 partnership between the cloud service provider and the customer. A strong partnership is probably the most important success factor to achieve the required level of compliance and "audit fitness" for the client, who always remains responsible for the safety of his patients.

[1] The SOC 2 report focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system, as opposed to SOC 1/SSAE 18 which is focused on the financial reporting controls [8].

Checklist for Using the Cloud in a GxP Monitoring Environment

1. Is the service available as "Software-as-a-Service" (SaaS)?
2. Is the service available as private or public cloud?
   <100 Measurement points: Public Cloud available?
   >100 Measurement points: Private Cloud available?
3. Does the supplier perform a computerized system validation (CSV)?
4. Does the supplier guarantee that data is immutable?
5. Is an audit trail available tracking each login, event and action?
6. Is data protected from unauthorized access?
7. Is the data backed-up regularly at a secure place (protected from deletion or loss)?
8. Are data recoveries exercised and documented regularly?
9. Is data privacy guaranteed (& solution supports compliance with GDPR)?
10. Does the SaaS provider guarantee GAMP 5 compliance?
11. Are Validation Plan, Risk Analysis & Validation Report available?
12. Are Qualification templates available for IQ and OQ
13. Are there clear policies regarding notification, documentation and qualification?
14. Does the supplier provide comprehensive change management notifications and documentation?
15. Are clear performance and availability levels of the solution defined?
16. Are performance and availability reports made available to clients regularly?
17. Is process data available for as long as they are needed in the business processes?
18. After this period, can data be archived for minimum 10 years in a human readable format?
19. Does the client remain the owner of the data?
20. Does the Service provider accept on-site audits by the client?
21. Is a service level agreement in place covering all above points?

It's natural to have a lot of questions when "outsourcing" your data. However, is it really outsourcing? Who owns the data yet? Does the SaaS provider back-up your data and ensure data recovery? Does the provider accept on-site audits? Download the complete Checklist and more to get started with Cloud. https://www.elpro.cloud/en/

About the Authors

Philipp Osl
Head of Product Management at ELPRO Global. He is an experienced Product Manager with a demonstrated history of working in the software as well as mechanical/industrial engineering industry in businesses and research institutes. Philipp's proven skills spread across Innovation Management, Business Process Management and Entrepreneurship. Philipp holds degrees in Economics and Computer Science from Vienna University of Technology, and a Doctorate in Business Innovation from University of St. Gallen.

Bob Lucchesi
Vice President of Global Regulatory Compliance, Quality Assurance and Auditing at USDM Life Sciences. His expertise extends to several USDM Life Sciences practice areas, including Enterprise Quality Management, Enterprise Content Management, Quality Management Systems, and Governance, Risk and Compliance.
Bob offers over 30 years of experience in quality assurance and regulatory compliance in pharmaceuticals, biotech, medical device, engineering and nuclear industries. Among his many accomplishments, Bob gives presentations on a variety of compliance and regulatory subjects worldwide, including the ASTM: E2500 model for validation and a variety of life science auditing topics spanning data integrity to GxP Compliance for IT.
Bob has led global audit teams for Quality, mock FDA, policies and procedures, Part 11, NIST, supplier-vendor (internal, external, sterile, non-sterile, manufacturing, logistics), mock recalls, IT Vendors, and major life sciences assessments. Bob is also an expert in risk-based validation methodologies, GAMP, enterprise content management, data and content migrations as well as overall pharmaceutical and medical device regulatory issues.
In his spare time, Bob loves sports and playing bass in a rock cover band on the East Coast, USA.

References and Sources

[1]SaaS vs PaaS vs IaaS: What's The Difference and How To Choose, by Stephen Watts, 22.Sep.2017,
https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/
[2]Community-Cloud, Margaret Rouse, last updated February 2012,
https://www.computerweekly.com/de/definition/Community-Cloud
[3]Differences in Cloud Adoption Across Global Industries, by TATA consultancy services, undatiert,
https://sites.tcs.com/cloudstudy/differences-in-cloud-adoption-across-global-industries
[4]Ensuring Data Integrity Through ALCOA, Grant South, 29.Apr.2016,
https://www.pharmout.net/data-integrity-alcoa/
[5]CSV Considerations Around Data Integrity, Kelly Jordan, 03.Mar.2016,
https://www.propharmagroup.com/blog/csv-considerations-around-data-integrity/
[6] Archivierung elektronischer Daten im GxP-Umfeld
https://www.apv-mainz.de/fileadmin/dateiablage/apv-mainz/Publikationen/1207-1215_Hornberger.pdf
[7] Data Archiving, Definition on TechTarget, last updated November 2018,
https://searchdatabackup.techtarget.com/definition/data-archiving
[8]SOC 2 (Service Organization Control 2), Margaret Rouse, last updated April 2012,
https://www.searchsecurity.de/definition/SOC-2-Service-Organization-Control-2
[9]The article was first published in the German magazine
https://www.elpro.com/fileadmin/elpro-com/lmn/blog_articles/Art_Technopharm_0649_Cloud_Solutions_for_Monitoring_web.pdf

Continue the conversation here

You may have noticed ELPRO is big on education.

As a trusted global leader in our industry for over 30 years, we continue to innovate and discover new ways to help you solve problems. We keep our ears to the ground and conversations going.

Join ELPRO's Leading Minds Network to receive our monthly newsletter, links to new white papers and invitations to relevant (free) industry events.

If environmental monitoring and data management is a concern in your pharmaceutical or healthcare laboratory, facility, or supply chain – stick with us – we have something to say.

Read on! leadingminds.elpro.com:

Examples of Data Integrity Violations in a GxP Laboratory

How Biotech Endocyte Uses Central Monitoring to Protect Critical R&D Assets

Maintaining Control and Compliance of Growing Healthcare Networks

Meet the ELPRO Cloud Solution- Wireless Monitoring with Limitless Possibilities

ELPRO Cloud is a compliant and scalable temperature monitoring solution that puts your data at your fingertips 24/7. Do-it-yourself set-up is quick and easy. Order today and begin monitoring in minutes.

- Easy to install
- Global IoT accss 24/7
- Wireless Sensors

elpro.cloud