Waters
THE SCIENCE OF WHAT'S POSSIBLE.®

Empower Cloud Compliance FAQ

1. **Do regulatory bodies (FDA, MHRA, TGA or CFDA) approve of the Cloud? Are there any regulations? What are the regulatory bodies?**
   There are no specific regulators for Cloud and the same regulators who take care of manufacturers today will still want to inspect in the same way as they do for non-cloud hosted solutions.

   Health Authority regulators do not approve or disapprove any technology. They need to see that regulated companies are applying risk management to any platform or technology that they are using. However, all regulators recognize that Cloud Infrastructure is simply a means of providing computing infrastructure:

   This is from the Draft Guidance from FDA on Data Integrity:
   "*Computer or related systems* can refer to computer hardware, software, peripheral devices, networks, cloud infrastructure, operators and associated documents (e.g. user manual and standard operating procedures)".

   AWS provided feedback to this Draft guidance as they found this was the first mention of 'cloud' in an FDA document.

   The OECD GLP guidance includes Cloud Services as an examples of a third party that should be evaluated and have written agreements (contracts) written "outlining responsibilities as of the supplier as well as clear statements about data ownership" and goes on to specifically describe how Hosted Services should be treated like any other supplier service (point 39)
   MHRA has a specific section on Cloud providers in their draft GXP Guidance (Point 20) where specific attention is directed at "ownership, retrieval, retention and security of data" as well as the "physical location where the data is held, including any laws applicable to that geographical location."

   From all this it is very clear that the regulators are acknowledging and including cloud services and hosted services in their view of computerized systems.

   Here is some additional information you will want to become familiar with:
   Lachman Consultants: Navigating through the Cloud(s) in Life Sciences,
   FDA: Data Integrity and Compliance with CGMP Compliance Guidance for Industry,
   OECD Application of GLP principles to Computerised Systems,
   MHRA GxP Draft guidance for Data Integrity,

Waters
THE SCIENCE OF WHAT'S POSSIBLE.®

2. **How secure is the data? How secure is AWS? Is it more secure than in-house servers? Is the AWS Cloud secure and compliant-ready for our regulated customers?**
   YES the AWS Cloud offers a level of redundancy and security which far surpasses any security that might be available from an "on premise" data center. This confidence in the security allows customers to deploy applications which require compliance.

   AWS hold many different certifications relating to the security of their cloud infrastructure which provide evidence that auditors have found the expected specific security controls are in pace and operating as intended.
   More information can be found here: AWS Compliance certifications

   Regulated companies need to work with AWS to determine how to leverage this security and redundancy, as well as manage the "location of data" which they may need to meet their own business needs. Unlike a typical on premise data center, it is unlikely that recognizable GxP procedures will be in place at AWS data centers and adoption of such things is not practical. The key is to understand what it is that AWS offers to a customer (e.g. for change control) and leverage that in the most effective way.

   Here is some additional information you will want to become familiar with: Amazon Web Services: GxP Cloud, Amazon Web Services: Considerations for Using AWS Products in GxP Systems, Amazon Web Services: Compliance Resources

3. **Does Cloud introduce additional compliance risks?**
   The use of cloud changes the landscape of risks around infrastructure, but in many ways reduces the risks associated with traditional physical infrastructure by simple standardization and automation of deployment with validated tools, eliminating manual processes and physical variation, increasing security and offering sophisticated monitoring tools no possible with physical infrastructure.

4. **Where does the data live?**
   The data may live in one or any of the AWS data centers. The service agreement with AWS can specify the location of data (region and availability zone) if they have any business concerns about who may request access to data if it resides in specific geological locations.

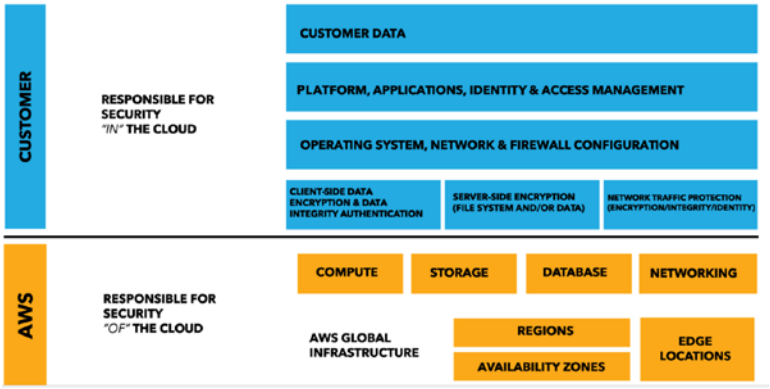
5. **Who has access to the data?**
   Excluding any regional regulatory access rules, all access to data is defined by the application supplemented by security and access in the other layers of the cloud services. AWS don't have access to any client's data.

6. **Who owns the data?**
   The regulated company.

7. **What exactly are AWS responsible for?**
   This is probably the most critical question to understand when thinking about GxP compliance, validation and Data Integrity, and will vary depending on the Service that Waters and our customers are leveraging.

   In Infrastructure as a Service, the regulated company remains responsible for the overwhelming majority of compliance and validation

   The models of Shared Responsibility can be found on this link on Amazon's Website
   [AWS shared-responsibility-model]



   This diagram clearly outlines that while AWS is responsible for the security OF the cloud, the regulated company remains responsible for the security IN the cloud.

8. **Can someone hack into a customer AWS account? Who is liable if this happens?**
   Any online account can be hacked, given enough time, skill, and motivation. However, Amazon has a reputation to preserve, and their AWS services are a key aspect of that. Even though the public uses Amazon accounts for many low-risk activities, AWS services rely on the security they offer.

   However, remember that much of the firewall/VPN and application security is still the responsibility of the regulated company, just as it is for non-hosted deployments.

Waters
THE SCIENCE OF WHAT'S POSSIBLE.®

9. **Are you still able to be compliant and meet data integrity requirements?**
   The compliance of any computerized system and the integrity of the data held in there is very heavily dependent on the application itself (in the blue layers); the technical controls in the application the configuration, documentation and validation of the application, the completeness and adherence to the SOPs written for that application and the review of the data created by that system. Almost every Data Integrity consideration is concerned with the application and its use by the human analysts rather than the means of providing hardware or computing power to host that application. Therefore, the Data Integrity challenges, while a little different in a hosted situation are likely to be less of an issue with a cloud based solution.

10. **What added benefits does Cloud bring to tracking data integrity?**
    For customers who outsource to other laboratories and partners, they will be able to provide Empower access via Empower Cloud to the contract laboratories and partners. This ensures that data acquired by the contract laboratory uses the exact same compliance ready applications as the regulated company, configured and validated by them. It also permits the regulated company to have complete access to the data at any time, and allows for regular quality and data integrity assessment of the data,

11. **How will your audits change? What should you expect in an Audit? Can you or regulators audit AWS?**
    AWS will offer certain kinds of audit on their services, but this is unlikely to resemble the same kind of audit that a regulated company is used to performing for a physical data center. Specifically, it is very unlikely that AWS will allow any Quality auditors (or regulators) to make an onsite visit to any of their data centers.

    On the flip side, visiting any specific AWS data center also loses its meaning if there are no physical resources assigned to a specific company, so companies using cloud in GxP environments are much more likely to audit the control objectives / process controls they need to see put in place by AWS.

    This link will help customers learn about auditing AWS
    AWS_Auditing_Security_Checklist
    It is important to note that AWS use the term 'auditing' to mean a much wider kind of audit than Life Science companies typical mean. They also provide many additional services for auditing the AWS deployment tools and security at a much higher level than would ever be seen in an on-premise data center.

    AWS also offer some on demand "compliance reports" for customers though their management console which may be seen a useful.

Waters
THE SCIENCE OF WHAT'S POSSIBLE.®

12. **How do Waters demonstrate/document they tested a Cloud deployment?**
    Just as we document in our SDLC documentation (including release notes) that we test Citrix deployments today, the AWS deployment simply becomes another deployment model that will be tested (on a risk-based approach) before an Empower release. Compared to other deployment testing, the Cloud deployment offers additional confidence as Waters test the cloud formations template (which includes Empower installation media and the deployment scripts). Servers are created in a fully automated way to assure equivalence to those we tested (noting that the Platform layer may have been updated since our testing (eg security updates etc). Waters have also tested the creation mechanism of AWS workspaces using Empower installation files from the automatically created server instance.

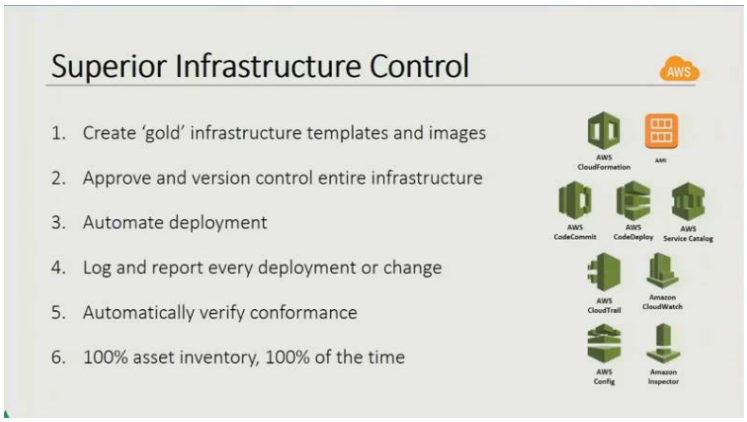
13. **Do validation policies change?**
    No, the need to validate any application as fit for purpose applies exactly the same for hosted as well as physical deployments.

14. **How can a regulated company perform IQ and OQ on the 'computing hardware' like they do for Servers and LAC/E's today?**
    Remember first that LAC/E boxes will remain physical and would be qualified in a hosted scenario just as they are qualified today, most likely using Waters SQT for Software, but with additional hardware testing IQ and OQ) that the customer my use, especially if they build their own boxes.

    For the AWS workspaces and servers, AWS may use a term called 'instantiation" rather than installation. This denotes an automated (and validated) procedure which 'creates' the virtual environment. This virtual infrastructure environment includes much of the network architecture as well as the computing 'platforms'.

    Customers may try to document this process like they used to for physical infrastructure (taking screen shots throughout the use of the management console) but others approve their cloud formation template as their protocol.

    AWS and other cloud providers can also perform 'continuous checks' on the workspaces and virtual platforms they provide, so compliance testing is no longer a onetime event and the automated and reproducibility of "deployment" increases robustness.



15. How are Amazon workspaces qualified? Are Waters Qualification Services still valid?

Just as Waters SQT for Software is used for IQ and OQ of Waters clients and LAC/Es, regardless of the hardware or virtual computers used, Waters SQT for software will work equally well for checking the Empower deployment on AWS workspaces.

Regulated companies may evaluate the degree of consistency between the platform supporting the AWS workspace which is considerably higher in hosted deployments than any physical platforms. Using a risk based approach to qualification it is likely that companies will apply a different statistical methodology to LAC/E qualification, physically deployed clients and AWS workspace clients, in the same way as they modified the schedule for Citrix qualification. This may result in similar or fewer required qualification activities.

16. How will Waters engineers have access to a cloud instance of Empower for either maintenance or qualification activities for instruments, LAC/E's or clients?

Waters Engineers should log into Empower with a unique, attributable user name.

As with a physical deployment, the engineer needs access to the client environment. They require a login for the physical client machine and OS, for a Citrix session, or in the case of Cloud, access to an existing user's AWS workspace or one of their own.

The customer needs to give the service engineer access to either a local Empower client or an AWS workspace (with a client installed) so the engineer can access their system.

Waters
THE SCIENCE OF WHAT'S POSSIBLE.®

17. **How will you track and manage change control of AWS machine images?**
    Once a customer has configured and created the custom server instances for DB and File share, the instance is never updated by Amazon. Therefore, as in a physical deployment, customers are responsible for applying, documenting, and managing changes to custom server instance.

    New AWS workspaces are created from a template or gold standard image. If the regulated company validates that template and the deployment process (or leverages the testing done by Waters), then all new workspaces are reliably reproduced.

    Unlike Citrix sessions, AWS workspaces persist between user sessions, and updates must be applied to these as they are to any physical client.

    You need to apply changes (upgrades, new drivers, and so on) to the gold image, and potentially push to all existing deployed workspaces with the tool of the customer's choosing (or using manual installations).

    It is the regulated company's responsibility to manage and document those changes. AWS can provide additional tools to document changes to machine images and workspaces.

18. **What kind of validation package does Waters offer?**
    Waters can offer the same software IQ and OQ qualification services that we offer today.

    Additionally, Waters Computer System Validation consultants could offer a customized validation suite of Professional Services to validate the Empower application and deployment, just as we do today.

    While there may be adaptation in the Risk Assessment portion of a validation plan due to the use of hosted services, if a laboratory already uses Empower in a regulated environment, and have a comprehensive validation suite they used for that deployment, everything they created then, could be leveraged in a new deployment hosted by AWS IaaS, with very little change.

19. **How are current or new backup procedures validated? Who is responsible for this? Who is responsible for the integrity of backups?**
    Backup and Restore SOPs will remain the responsibility of the regulated company and both validation and training on these still need to be considered.

    These critical procedures are not negated when the infrastructure is a service, nor is this delegated to AWS. AWS will offer a degree of redundancy /high availability and security to our customers, but this does not replace the need to regularly backup the database and data

Waters
THE SCIENCE OF WHAT'S POSSIBLE.®

20. **Are validators at Amazon trained and certified in GxP?**
    While it is evident that more and more staff at AWS and intimately involved in the GxP industry, and are GxP aware, there really is no role for AWS staff to perform validation under GxP for regulated companies

21. **Are Waters Developers and Field Engineers qualified to work in the AWS Cloud and with the associated templates?**
    Water's has put together a comprehensive training program with our partner AWS, for Waters staff supporting Cloud depending on their roles.

22. **Does Cloud impact the Quality escalation process?**
    As with other deployment models, the Waters escalation process needs to understand how Empower is deployed. For the majority of technical questions related to the application, the deployment should have no impact on how the application functions. When a call comes in from a customer using a hosted deployment, Waters staff attempts to replicate the issue in a regular deployment and escalate it in the standard fashion. If the reported incident can only be replicated in a cloud deployment Waters works with AWS to troubleshoot the Empower application's deployment for simple cloud or availability issues. The customer also has a direct escalation route to AWS through their service agreement.

23. **How do regulated companies leverage the additional monitoring services which cloud providers offer to help meet regulatory concerns about access to data and configuration changes?**
    Merck outlined in their whitepaper how the shift to cloud hosting offers considerable benefits to maintaining control and continuous monitoring of any hosted application. Part of their decision to forgo on-site audits of AWS facilities was that AWS could provide "continuous monitoring and alerts of the environment, daily verification of accounts and encryption of data". Additionally, the configuration and deployment processes, which are all automated, also create electronic logs of the deployment process, eliminating the traditional IQ procedures required with manual installations. These additional services provided by cloud vendors such as AWS, combined with Merck's own internal assessments of "Information Risk, IT Practices and Privacy", significantly add confidence that software installations are accurate and consistent and that "nothing changed" or "nobody accessed the system" without the need for detailed time point limited manual reviews of the installation or access at the OS/platform levels.

    Customer should be encouraged to talk to their AWS Lifescience representative about the kinds of monitoring and logging services which they can offer to provide confidence in the security, consistency and the Level 0/1 of their hosted Empower application.