Published by *FierceMarkets*

GxP in the AWS cloud:

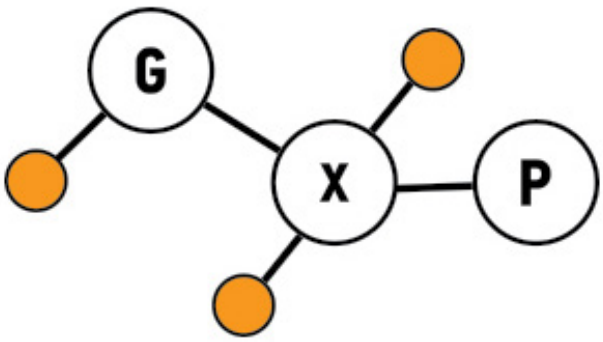
The compliance and efficiency benefits of rethinking regulated workloads

amazon web services

Highly-regulated corners of the biopharma industry were initially wary of the cloud. Faced with a lack of regulatory clarity and possessing understandable caution, companies stuck with systems they knew. That is no longer the case. Now, companies know the Amazon Web Services (AWS) cloud meets their needs and those of regulators. This shift has unleashed a model that is enabling companies to achieve more control with less effort by fundamentally transforming compliance practices.

The initial reticence of companies to run regulated workloads in the cloud reflects the importance and scrutiny of these tasks. Errors in a system handling unregulated workloads affect the internal operation of the company. The fallout from such disruption, while undesirable, is typically isolated. Errors in a system handling regulated workloads affect the regulatory status of the company and potentially patient safety. These are the sorts of issues that have major, long-term consequences.

Companies commit considerable time and resources to avoiding such issues. Compliance with the good laboratory, clinical and manufacturing practices (GxP) regulators enforce to protect patient safety is central to these efforts. GxP ensures the integrity, reproducibility and traceability of data companies generate while developing, testing and producing drugs.



Each set of good practices is built on a core concept: If it isn't documented it didn't happen.

Following this maxim necessitates the validation—and accompanying documentation—of computer systems to ensure they are accurate, reliable and consistently perform as intended. The validation must also show if records have been altered or are otherwise invalid.

HOW THE CLOUD IMPROVES COMPLIANCE

Today's on-premise GxP systems operate in the physical realm. Data comes into receiving docks, is unpacked and moved on to data centers. Companies can audit the sites and servers they use to show compliance with GxP.

These manual compliance checks happen at distinct points in time. This allows a company to show auditors its system was compliant at a particular time on a certain day. However, the company cannot show compliance after that point. A void in the company's knowledge of the status of the system begins once the validation is performed. The void only ends after another manual compliance check is performed. In the time between checks, systems can drift away from their compliant states unnoticed.

The problem is compounded by the level of effort required to manually validate systems. This is a labor-intensive task. The upshot is increasing the frequency of point-in-time checks to shorten the drift window would require more resources.

Cloud GxP systems can fix some of these problems. The cloud is a virtual, software-defined realm. Code is the infrastructure. In this realm, companies can automate and script checks and controls rather than task employees with periodically validating and monitoring their systems. The result is a move from

manual point-in-time validation to automated near-continuous compliance.

This means the voids in compliance knowledge inherent in the old model are truncated. Cloud users can say with far more confidence that their systems are compliant right now. Furthermore, they can present documentation to auditors to support such confidence.

Companies running GxP workloads in the cloud achieve this level of traceability while reducing the effort involved. Once created, automated services deliver consistent assessments of the system with minimal input and oversight. To simplify matters further, many of the services are based on pre-built cloud services.

MOVING GxP WORKLOADS TO THE CLOUD

Merck is among the companies to use pre-built cloud services to help move GxP workloads into the cloud. The Big Pharma started using the cloud for some of its unregulated workloads around five years ago but only started applying the model to parts of its business covered by GxPs two years ago. Merck has increased its use of the cloud to run GxP workloads gradually as it has become more comfortable with the model and more aware of its benefits.

The process followed by Merck shows how biopharma companies can move to the cloud and the benefits they can realize. Merck began by creating a security framework. This was the bedrock of Merck's plan. The systems had to be secure.

As an AWS user, Merck shared responsibility for security with its vendor. AWS handled the security and quality of the cloud itself, as it does for all customers under its Shared Responsibility Model. Merck took responsibility for the security and quality of what happened in the cloud, exactly as it had when using an on-site datacenter.

In addressing its security responsibilities, Merck adopted a safety-first, hands-on approach that mandated manual checks of whether services were enabled and policies met expectations.

Merck then assessed what it needed to do to ensure it was prepared for a regulatory inspection. This entailed talking to colleagues working in quality, inspectional readiness, technical posts and other functions to formulate an overall systems assurance strategy. The result was a set of processes to ensure the Merck Managed Cloud meets GxP requirements and the needs of auditors.

These processes use AWS services. Every change to the system is logged using AWS CloudTrail. Auditors can view who, what, when and where from for every change. The low cost of cloud storage means companies can keep all logs indefinitely.

Other services cover different aspects of GxP compliance. AWS Config enables Merck to show what its environment was like on any given day in the past. Providing such information to auditors used to require reams of paper. Working in the cloud, users simply scroll back through time. This shows when files were added or removed from storage.

The historical oversight provided by Config is a major advance over what went before. Until now, compliance was a point-in-time activity. Companies could show compliance at discrete points in time but only assume compliance between these points. Config provides near-continuous compliance that is far more comprehensive than earlier systems.

AUTOMATING CLOUD MONITORING

Merck provided an onboarding document to help teams put apps into the cloud. Teams subsequently embraced the cloud. This validated the model but also created challenges. User growth outpaced capacity at the IT department. The manual checks implemented in the early days to ensure security became burdensome. A new, more automated way of working was needed.

Companies seeking to automate aspects of the management and oversight of cloud systems can use readymade services. IT teams can connect these off-the-shelf services to their systems, or link multiple services together and make minor modifications to create processes tailored to their needs.

The aforementioned CloudTrail traffic logger links to Amazon CloudWatch, a cloud monitoring service. IT teams can configure CloudWatch to send alerts via text or email when certain events happen. For example, the system could send an alert when someone tries to log in with superuser privileges. This allows IT to see whenever someone accesses—or tries to access—the system with powers that enable them to make major changes.

AWS Config Rules enables similarly proactive, automated oversight. This service, an extension of the aforementioned AWS Config, automates the enforcement of policy. When something unusual happens or is detected in an automated periodic assessment, the service triggers an action. The IT team defines what is unusual and what action is triggered. For highly-undesirable events, the service can automatically roll back the system to its status before the change happened.

Other services ensure the integrity of data. One way to achieve this is through encryption. If data integrity is compromised, the system will detect the problem during decryption. This automates control of one of the most common GxP problems. Backup and recovery controls allow IT teams to return the system to its former, uncompromised state.

Merck also used the building blocks provided by AWS services to create custom monitoring tools. One such creation automatically places restrictions on what new users can do and access. Another minor development checks each user against Merck's active directory when they try to access the cloud. If a user leaves Merck, they are automatically removed from the directory and therefore prohibited from accessing the cloud.

ACHIEVING CONTINUOUS COMPLIANCE

These automated services allowed Merck to support a fast-growing user base without expanding its IT team in lockstep. Merck and companies with similar setups control their systems and the users who interact

with them. As importantly, they generate extensive documentation on their GxP systems to demonstrate such control to auditors.

The next step is to automate the monitoring of the system itself. Such monitoring is needed to ensure the cloud services and processes are functioning properly.

To do this, Merck created a checker of continuous compliance. This checks if the right email addresses are used for alerts, confirms all AWS services are enabled, tests if Config is connected to the right source of logs and otherwise validates that the environment is consistent with Merck's requirements.

The checker runs periodically and on demand. Merck uses it to check each environment before it is released and each day thereafter. Errors trigger notifications. Each run generates an archive for historical auditing.

Merck has paired this automated checker with manual, periodic assessments of its cloud. As the cloud has no dedicated physical resources, Merck foregoes on-site audits in favor of other ways of checking the system. These include annual assessments of support tickets and performance issues. Merck also performs reviews of the AWS environment and checks its partner's industry certifications are up to date.

MAKING FURTHER IMPROVEMENTS

These tasks are part of a dwindling list of manual jobs involved in running GxP workloads in the cloud. As companies have become more comfortable with regulated workloads in the cloud, they have realized efficiency gains and compliance benefits by switching from manual to automated checks and controls.

This is an ongoing process. Merck is exploring whether the system can self-correct, rather than just informing people of a problem and letting them implement the fix. This would further reduce the need for active management of the cloud environment.

Companies will approach such new ways of working cautiously. But the experience of moving GxP workloads to the cloud so far suggests companies can quickly eliminate barriers to adoption.

The companies that engage with vendors and regulators to drive forward such advances and seize existing opportunities will be rewarded with systems that provide more control for less effort than ever before.