Regulatory Risk Reduction in the Cloud: Why Cloud Systems Are Safer Than On-Premise Systems

USDM Life Sciences

www.usdm.com

About **Our SME**

David Blewitt

VP of Cloud Compliance

USDM Life Sciences

David Blewitt is the Vice President of Cloud Compliance at USDM Life Sciences. He is an accomplished life sciences regulatory and IS compliance professional with more than 25 years of experience in the pharmaceutical, medical device, biotech, and blood management industries, specifically in the fields of computer systems validation, risk management, quality assurance, software development, product life cycle management, and compliance roadmap development.

Executive **Summary**

2020 will be a big year for the cloud in the life sciences industry. With the large number of companies across all areas — including medical device, pharmaceutical, and biotech — beginning to leverage the power of the cloud, coupled with the upcoming release of the FDA's Computer Software Assurance (CSA) guidance, there has never been a better time to dive into the rapidly calming waters the cloud offers.

The current Part 11 guidance and medical device cGMP quality system regulations were derived before the inception of the cloud and lacked clear direction on computer system validation (CSV) and its necessary documentation. Further, these now dated regulations had many unintended consequences due to manufacturers misinterpreting the regulations that led to the over-validatation of computer systems and testing every aspect of their software, deeming it a necessary checkbox in their CSV and manufacturing processes.

This belief created a heavy documentation burden in the CSV process, which resulted in manufacturers rejecting the use of automated systems and new technologies, assuming it would further increase their validation burden and cost. Traditionally, regulated companies also struggled to understand the root cause of issues to improve product quality as their focus was on compliance and validation – not critical thinking about the system impact on patient safety, product quality, or quality system integrity.

This confusion around non-product computer system requirements has created a significant barrier for both the FDA and for life sciences companies to embrace new technologies like cloud, artificial intelligence, or automated testing, that can help drive innovation and deliver improved safety and quality. Non-product software is defined as any software that is not directly used in a medical device, medical device as a service, or end-product (i.e., QMS, ERP, LIMS, LMS, and eDMS applications as well as software tools). It includes all the software used in manufacturing, operations, and quality system activities, which would follow the 21 CFR Part 820.70(i) guidance.

The goal of this white paper is to dispel the ingrained beliefs that on-premise systems are safer, and help regulated companies understand the inherent benefit and decreased burden of risk with today's cloud systems.

Direct Correlation between

“Risk to End-User” and “System Distance to End-Product”

The FDA believes the use of automation, information technology, and data solutions in non-product software can provide significant benefits to drive enhanced safety and quality, thereby reducing patient risk. By clarifying their stance on the validation of the ancillary systems used to develop, manufacture, and distribute medical device products, the FDA has also illuminated the potential of getting these products to market much faster, with less associated cost. Further, other industries utilizing automation have shown a substantial benefit in significantly enhancing product safety and quality, thereby reducing risk when compared to manual processes.

A crucial part of this new guidance, the so-called ***paradigm shift***, is utilizing critical thinking to determine the risk to patient safety and product quality associated with ***indirect systems versus direct systems*** to enable acceptable approaches to validation. Indirect Systems are tools used in your CSV process like bug tracking systems or load testing and lifecycle management tools that do not directly impact the product and require less documentation.

Direct systems like Electronic Device History or Adverse Event (MDR) Reporting, have an impact on the product and will require adequate testing based on risk. In other words, the risker a system impact is to the end-product, and to the safety of the patient, the more testing and documentation will be required.

Using a “risk-based approach” is nothing new, and global regulatory agencies and GAMP® have been advocating this for two decades. What is new, is the clarity on the stance and methodology used for the determination of

what is high-risk and what is not to minimize the misinterpretation manufacturers have been making for many years. The clarification in the CSA approach flips the paradigm to focus first on critical thinking (risk-based), then assurance needs, testing activities, and finally, documentation.

If you think of the 80/20 rule, currently, many manufacturers spend 80% of their time documenting and only 20% of their time testing. The FDA wants to flip this to be 80% of a manufacturer’s time spent critically thinking and applying the right level testing for higher-risk activities, and only 20% of the time documenting.

This critical thinking and rigor should be focused on three questions: Does this software impact patient safety? Does this software impact product quality, and how does the software impact your quality system integrity? And just as important – to what realistic extent is the risk likely to occur and how many levels of infrastructure lay between the system and the end-user or patient? In other words, how many downstream checks and balances exist before the product is shipped?

Direct and **Indirect Systems**

In this instance, I define risk as it relates to the development, manufacturing, and distribution of medicines and medical devices. There are three main areas of risk to consider:

1. The risk to the patient (most important)
2. The risk to product quality or data integrity
3. The risk to company financials or reputation

Indeed, we could slice these three areas in several ways based on their downstream impacts and upstream corrections (e.g., a risk to the product could impact both the patient's safety and the company's financials), but the point is that it always comes down to these three elements. When considering the risk a system poses, it is necessary to derive the system distance from the end-product. In other words, is the cloud system in question a ***direct system*** or an ***indirect system*** to the product?

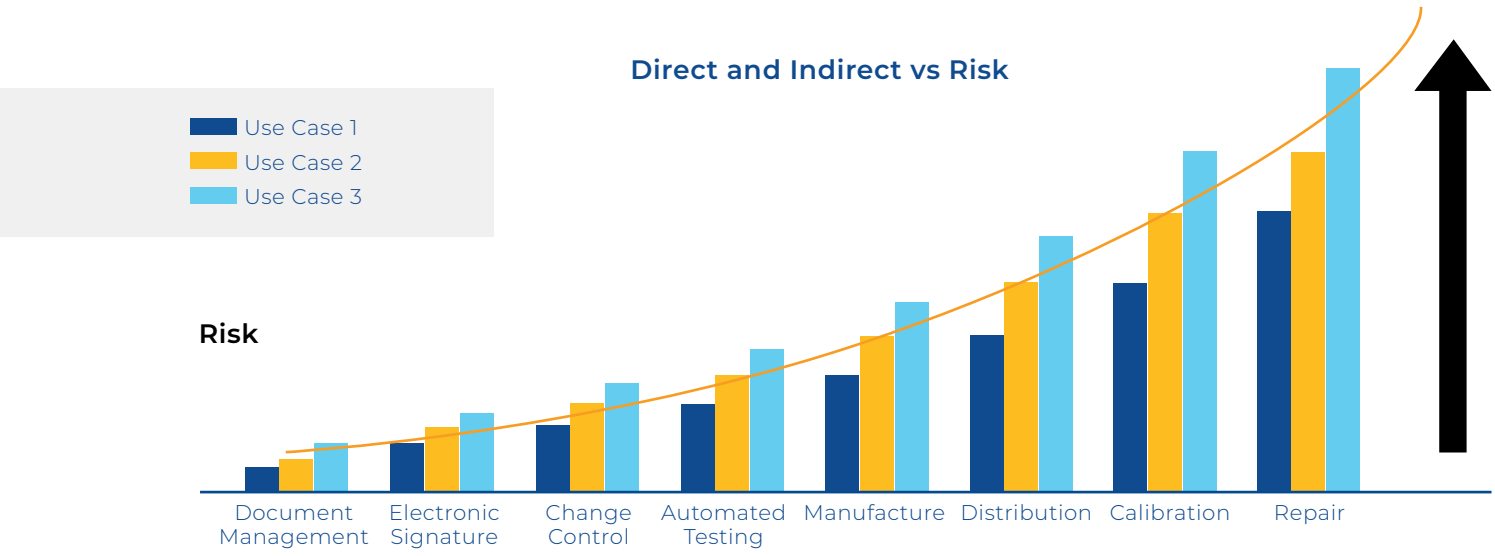
A direct system would be one that touches the product in some way. These systems include:

- Manufacturing
- Repair
- Calibration
- Distribution

An indirect system is one that is used for ancillary management of those direct systems, for example:

- Document Management
- Electronic Signature
- Complaint Handling
- Change Control
- Automated Testing

The graph below depicts indirect systems to the left and direct systems to the right. The closer a system or application is to the end-product, the higher the risk.



On-Premise Systems **versus Cloud Systems**

As service providers, we still must convince life sciences organizations of the benefits of cloud-based systems. The history of compliance and technology has decades of ingrained fears of 483 observations and warning letters, cybersecurity hacks, and cultural behaviors that create barriers to innovation. Nothing should be done because of fear of regulatory observations but because it drives better product quality. Too much work is done because of fear of regulatory punishment instead of fear of putting a poor-quality product on the market.

Traditional methods of risk management, for on-premise and even some cloud systems, is to determine the potential risk and apply an equivalent level of verification activity, test everything, and document everything to ensure no negative impact. This is the traditional approach defined by GAMP® and other regulations, and it requires manual intervention and subjective thinking for risk determination.

Testing is often carried out in the end-user testing environments, which was perceived to be better because the release gets tested first in a testing environment and then goes into a production environment. *However, the test environments need to be maintained as substantially equivalent copies of the production environments, which is nearly impossible with distinct data differentials, integrations, and user interactions*.

Further, attempting to maintain a test environment that is equal to the production environment creates more opportunity for error. Have you ever had an issue in your production environment even after it was supposedly checked using all the prior testing, analysis and risk assessment? We've all been there. By far, the biggest problem of this dated approach is that when these inevitable issues get into the production environment, they are not always evident, and they can take days or even weeks to detect. The issues that sneak into production can pose a very high risk. Maintaining two testing environments has been the perceived best approach for more than 20 years, and until recent cloud advances, it was the best approach.

The advantages of cloud-based systems are more broadly understood today. Certainly, the cost argument has been in favor of cloud systems since there are no hefty upfront hardware costs, no infrastructure to maintain, and less overhead required. The cloud also offers continually released new functionality, and when utilized and developed correctly, can keep pace with innovation. Mobility and access anywhere, the ability to connect devices anytime, and operations on-the-go are additional advantages. Cloud vendors are now

performing much of the upfront groundwork for their customers when it comes to qualification and validation, making it easier to onboard new applications and leverage the vendor's validation activities.

Yet even with all these advantages, many life sciences companies still resist moving to the cloud. Some of the concerns we continue to hear from our customers include:

- If I am not in control of the infrastructure, how do I know my system is maintained appropriately?
- How do I know my data is secure?
- Will the continuous updates affect my system integrity?
- How do I manage the updates and stay compliant?
- How do I decommission a system and know I have all my data back?
- How can I ensure I am not locked into using the system forever?

The answers? Vendor selection is a critical aspect of your overall risk reduction strategy. The right vendors will provide not only stable infrastructure, platforms, and applications, but also the evidence to demonstrate that stability. Maintenance can be built into a vendor's responsibilities as well. Third-party release analysis and regression testing can be leveraged to ensure a stable environment persists.

The right vendors will provide not only **stable infrastructure, platforms, and applications**, but also the **evidence to demonstrate that stability.**

Additionally, data retrieval and your accompanying exit strategy, along with considerations for vendor lock-in (proprietary lock-in which makes a customer dependent on a vendor for products and services, unable to use another vendor without substantial switching costs) of applications need to be strategically considered when selecting vendors and should be integral to cloud adoption and usage strategies.

Whether you are leveraging your vendor's activities or utilizing your internal CSV tools, it is now acceptable (and encouraged) to use process controls and automated assurance activities to mitigate risk in the cloud.

Automated Testing **in the Ever-Changing Cloud**

Undoubtedly, development and validation must be done utilizing separate environments, and we realize these environments should persist with regular configuration and code mirroring to keep pace with the production environment. Further, these environments should always be used to test new code and new integrations. This is another highly leverageable area to take advantage of, namely, vendor testing and third-party verification. Vendors should have well established SDLCs in place to ensure appropriate testing is always conducted before any release to either test environments or production environments, for new features.

As discussed, *testing* in an environment which is *like* your production environment is standard but flawed. Minor product changes, bug fixes, and everyday maintenance move far too fast to be constrained by the inherent limits of human intervention, analysis, and risk-based testing. A change to a platform or application can – if done correctly and with the proper testing and procedures in place – be performed directly into the production system.

The key to this is the critical thinking required to determine the risk. Which areas of your system are at risk, and which of those areas risk impacting your GxP requirements? *If you can answer these questions and focus a barrage of automated, always-on, always-monitored tests on these critical elements, then you can update your production system and know immediately if there is a problem*.

Test results can be used to show trends and incorporate artificial intelligence (AI) to predict potential downstream issues. And if issues or failures do occur, the identification is immediate, and the procedures in place for CAPA and system roll-back can be immediately enacted according to the level of the issue and risk presented.

It's worth reiterating that vendor selection is critical, along with leveraging the vendor's testing and SDLC. The vendor must have robust development and testing checks in place to provide a level of confidence that when issues occur, the disruption will be as minimal as possible and will be corrected as quickly as possible.

Indirect **Systems**

Automated testing tools are inherently indirect systems. However, depending on the system being tested, the level of risk could be only one level away from the end-product, or multiple levels from it. Assessment of the use case is the key to determine what level of testing is required. At USDM, we validate and monitor our automated testing systems with the anticipation that they are going to be only one level away, which allows us to utilize our automated tests across multiple system types regardless of distance from the end-product.

The benefits of this type of automated testing include:

- Better testing, less documentation, and paper
- Real value-added CSV (not just paper exercises)
- Less “subjectivity” in assessments by removing human error
- Higher quality systems
- Higher quality products
- Better, faster system delivery
- Not only safe, SAFER!

In **Conclusion**

As regulatory agencies evolve to meet technological advances, there are fewer and fewer reasons to keep on-premise systems. The FDA has publicly stated that they believe the use of automation, information technology, and data solutions throughout the system lifecycle can provide significant benefits to drive enhanced safety and quality, thereby reducing patient risk.

To utilize a less-burdensome CSV approach, leverage vendor activities, automate some of your testing efforts, or to improve the quality of your products and truly drive innovation, you must start by embracing cloud technologies and embrace digital transformation.

Technology is advancing faster than ever, and so are your competitors. You need rapid assurance that your systems are functioning as intended. Fully automated, always-on regression testing is, in fact, less risky than the older methods, because it is real-time and minimizes humor error. Knowing your system is functioning as intended, on the latest release, and that it is continuously compliant is a huge comfort and vital business assurance. USDM has been supporting the development and maintenance of these best-in-class cloud systems for several years, and we are here to help when you are ready to take the first step toward the cloud.

How **USDM Can Help**

The competitive advantages provided by cloud systems and a risk-based methodology are clear. The FDA has stated that while the Computer Software Assurance guidance will be released later this year, the principles and methodology can *and* should be applied today. USDM can help you take the first step by providing guidance on how to apply critical thinking by assessing your current CSV processes, and creating a small pilot program to show the value and encourage company buy-in.

- Improved quality and efficiency
- Over 50% less validation cost and time
- Up to 90% decrease in test script issues
- Siginifcant testing overhead reduction
- Utilize prior vendor assurance activities
- Maximized use of CSV and expert resources
- Capability to deliver value faster

USDM CSA Solutions:

CSA Education and Training – USDM can help teach and mentor your teams on CSA principles and how to apply critical thinking to your process to create a strawman to your approach.

CSA Assessments – USDM can assess your CSV process and recommend CSA changes based on your quality of documentation, testing, SOPs/WIs, testing, use of automation, performance on audits, etc.

CSA Methodology and Execution – From vendor selection to methodology development to end-user training, USDM can transform your CSV into a CSA approach and help drive adoption across your organization.

Cloud Assurance – USDM can manage your entire CSA process and deliver an end-to-end GxP compliant managed service, including the continuous maintenance of all your cloud vendor releases.

What are you waiting for?

Contact us at (888) 231-0816 or compliance@usdm.com

Contact Us

USDM Life Sciences
535 Chapala Street
Santa Barbara, CA 93101
+888-231-0816

USDM Europe GmbH
The Squaire 12 - Am Flughafen
60549 Franfurt am Main
Germany
+49 69-95932-5459

usdm@usdm.com
www.usdm.com

Published by USDM Life Sciences, February 2020

Any comments relating to the material contained in this document may be submitted to the contact info above.

#CA_WP008A

USDM
Life Sciences