Demystifying Software Validation: Learn What Software Validation Means for You and Your Lab

Whitepaper

Introduction

The term “software validation” can trigger many responses, including confusion and even anxiety. This article provides a foundation for thinking about software validation based on expert articles and U.S. Food and Drug Administration (FDA) resources and consultants. The following validation-related topics are covered:

- What is the definition of data integrity?
- What is the difference between qualification and validation?
- What are the regulatory requirements for software validation?
- When do systems need to be revalidated?
- How much validation work is enough?
- How can vendor audits support my validation?

Agilent Technologies

Definitions: Data Integrity, Qualification, Validation

A good first step toward understanding software validation is to clearly define the terms that cause the most confusion: data integrity, qualification, and validation.

In his 2013 Scientific Computing article *FDA's Focus on Laboratory Data Integrity–Part 1*, Robert D. McDowall, Ph.D., defines data integrity in the context of laboratory data within a GMP environment as "generating, transforming, maintaining, and assuring the accuracy, completeness and consistency of data over its entire life cycle in compliance with applicable regulations."[1]

A computerized system that supports data integrity ensures that the data is human-attributable, legible, time-attributable (contemporaneous), not easily duplicated or modified (original), and accurate. The computerized system used to generate and maintain regulated records and its validation thus becomes the focal point for all other related data integrity activities.

The FDA's *Glossary of Computer System Software Development Terminology* provides a detailed definition of qualification, specifically installation qualification (IQ) and operational qualification (OQ).[2] Simply put, IQ determines that a system is properly installed and configured. OQ determines that a system is consistently operating within established limits and tolerances. In the same document, the FDA states that software validation is the process of determining the correctness of the software with respect to the user's needs and requirements. Software validation is accomplished by verifying each stage of the software development lifecycle.[2]

Though a system may be correctly installed and its operations may be qualified, these actions alone do not ensure correct results for every process run on the system. Rather, each individual process must be validated to determine that the system generates predictable, repeatable results, whether it is drug manufacturing or another activity such as quality control. This step is known as process validation.

Qualification, software validation, and process validation are interrelated as shown in Figure 1. IQ/OQ are necessary, but these alone are not sufficient for system validation. Likewise, system validation is necessary, but it alone cannot validate the process. While each is a required element of the overall validation process, they are not sufficient by themselves to meet the complete regulatory requirement.

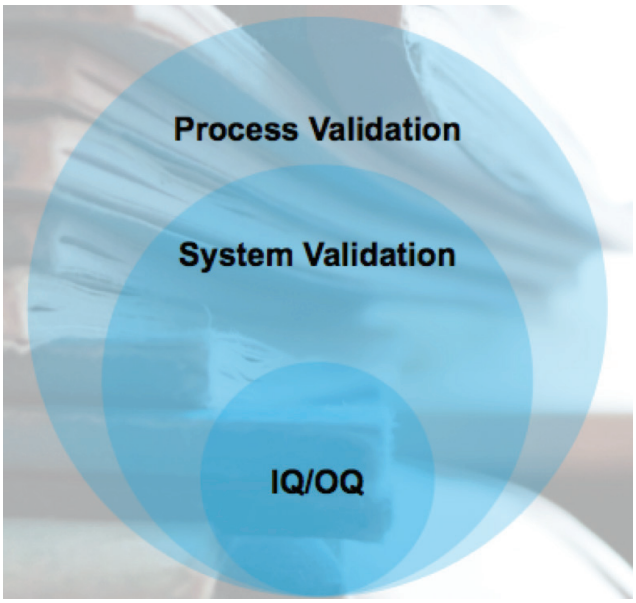

Figure 1. Relationship between IQ/OQ, system validation, and process validation.

Software Validation: Regulatory Requirements

In April 2016, the FDA released its latest and long-awaited guidance on data integrity in computerized systems as it relates to cGMP regulations, *Data: Integrity and Compliance with CGMP Guidance for Industry*.[3] To develop the guidance, the FDA evaluated their regulatory requirements in light of their experiences with inspections and regulatory enforcement, and developed relevant questions and answers covering several important topics. For example, one question asks, ""Does each workflow on our computer system need to be validated?" The answer is yes. The FDA guidance explains that if a computer system is not validated for its intended use, it is impossible to know if the workflow runs correctly. This underscores the idea that system validation is important to, but not the same as, process validation.

The FDA regulations that support its 2016 guidance include:

- 21 CFR Part 211.63, which discusses the concept of intended use of systems
- 21 CFR Part 211.68, which states that the degree of validation needed is based on system complexity
- 21 CFR Part 211.110, which discusses evaluating processes based on the degree to which they can impact a drug product

The FDA also recommends controls to manage risks to computerized systems. The agency's top three priorities for risk management are risks to patient safety, product quality, and data integrity.[3]

In terms of the controls or processes that are appropriate for system validation, the FDA concludes that a system is more than just software and hardware. A system also includes the people, processes, and documentation associated with it.[3] Thus, when the FDA uses the term "system" and discusses system validation, labs must consider the much larger context of validating their entire process.

System Revalidation: Timing

Often the thought of revalidation causes anxiety, because the revalidation process can be complex, long, expensive, and labor-intensive. The FDA's General Principles of Software Validation discusses revalidation, suggesting that when systems are altered, those changes must be studied not just regarding the individual change, but also regarding any potential impacts and unintended consequences the change may introduce to the entire system.[4] In a validated environment, such an evaluation normally includes regression testing.

Many labs delay changes to their computerized systems, for example software updates, to avoid the need for revalidation. At some point however, system fixes and improvements will become important enough to warrant an update and any subsequent required revalidation effort. The longer a lab waits to update a system, the wider the scope of changes and hence the greater the validation effort required. For this reason, it is important to keep systems current. If a system has been in use for a year and updates are implemented, the validation effort will probably not be as great as if five years' worth of updates were to be installed all at once.

System Validation: Needs and Risks

Many labs want to know how much validation work is sufficient and whether they can use vendors' IQ/OQ packages to sufficiently validate their own system or process. Most vendors, including Agilent, offer such packages to help customers qualify their systems by ensuring they are installed and configured correctly, and operate as intended.

Monica Cahilly, an FDA consultant and trainer who has worked extensively with the agency on data integrity, has unequivocally stated that labs cannot abdicate to their vendors their own responsibility for validation.[5] IQ/OQ activities are limited to qualifying installation, configuration, and function as designed. As shown in Figure 1, IQ/OQ is necessary, but alone not sufficient to establish validation of the system or the process.

The next question labs often ask is: "How can the validated state of current laboratory software and associated processes be evaluated?" Considering FDA assertions that computerized system validation should occur in the context of process validation, labs should start by making an inventory of their processes. Standard operating procedures are useful in reviewing the various types of testing, chemical analyses, instrumental analyses, and methodologies that occur in the lab.

Once the processes are inventoried, the systems used in those processes can be likewise identified. The process inventory will provide the lab with a list of instruments, software, data management systems, and laboratory information management systems (LIMS). Multiple processes may share certain systems, such that it may be possible to conduct a core validation of the shared systems, for example a LIMS. Then the validation can be expanded to address any details unique to a particular process.

After the inventory of process and systems is completed, labs can plan and prioritize the validation work needed based on risk to patient safety, product quality, and data integrity. Not all systems will present the same degree of risk. For example, a system for administering staff training is likely of lower risk than a manufacturing execution system that directly influences product quality. Clearly, higher-risk processes merit more thorough validation work than lower-risk processes.

Value of Vendor Audits

The FDA's General Principles of Software Validation suggest that manufacturers and laboratories can use vendor audit information as the starting point for their required validation documentation.(4) Thus, a thorough vendor audit may justify less onsite validation. Ideally, vendor audits should occur before systems are acquired, or at least before the validation effort begins, to allow full understanding of the vendor's design and development methods.

How should labs conduct vendor audits? In his 2006 article Apples and Oranges: Comparing Computer Systems Audits, IT quality and compliance expert Jacques Mourrain, PhD, introduces a vendor audit model that is more effective and time efficient than checklist-based methods.(6) The model evaluates and scores six areas:

- **Procedures**: coverage, maintenance, reviews, and currency
- **Training and personnel:** evidence of training, and independence of quality assurance (QA)
- **Infrastructure**: operation, maintenance, disaster planning, and security (often irrelevant unless the vendor is housing your GxP data)
- **Software development**: systems development life cycle (SDLC), documentation, and reviews
- **Testing**: occurs throughout SDLC, completeness, robustness, and traceability
- **Quality management systems**: configuration management, change control, problem tracking, anomaly analysis, and corrective and protective action (CAPA)

The vendor should be able to provide documented job and training requirements—including training on the appropriate SOPs—and records of completed training. The vendor QA organization should also have sufficient independence from the development organization.

Vendor IT infrastructure—the server room, how backups are done, and disaster recovery—is important to audit in situations where the vendor is holding the labs' regulated data. However, in cases where computerized system vendors are not holding the lab's regulated data, spending time auditing vendor server rooms and backup procedures is probably of limited value.

Auditing the vendor's software development is much more obviously useful. In this case, labs review the vendor's software development life cycle, the documentation created during that development process, coding processes and standards, the kind of reviews performed, and testing practices. Design documentation enables vendor engineers to understand the design of the product in case they need to make changes or make corrections later.

Testing should occur all the way through product development, and should be robust, traceable to product requirements, and complete. Testing instructions and automated test designs should be clearly documented. Testing should also be summarized and documented so the vendor can show release criteria and how decisions have been made to approve the software for release. The amount of validation work needed is influenced by how well a vendor has tested their product.

Review of the vendor quality management system—including change control, problem tracking and analysis, corrective action and prevention—is also valuable. Is the vendor aware of the reasons for their product defects? Are they making corrections to their processes to minimize the introduction of defects? In addition to product changes, is the vendor also paying attention to managing changes to the systems that support their product development and testing activities?

Mourrain's systematic approach allows labs to plan for and execute the vendor audit in an objective and organized manner. Vendors can be scored, and the scores used to determine vendor-related risks and additional validation work. The model can also be used to conduct a side-by-side comparison of vendors and to decide which vendor's processes work best for a given situation.

Summary

System changes are bound to occur. When they do, labs must study those changes and revalidate their systems to the extent appropriate, based on the scope of the changes and the risk to patient safety, product quality, and data integrity. Waiting to complete software updates and revalidation is problematic. The longer changes are postponed, the more complex and burdensome the revalidation process will be, and there is a greater chance of missing critical defect corrections and functional software enhancements.

Qualification (IQ/OQ) is not validation. Qualification, while necessary, deals only with proper system installation and operation, but not a user's specific processes. Thus vendor IQ/OQ packages are helpful, but not enough. Similarly, it is not sufficient to establish validation of the system outside the context of the overall process. The FDA's focus goes far beyond system validation as a standalone activity and instead views validation within the processes where the system is used.

A systematic vendor audit can provide valuable information to inform a risk-driven validation strategy. When vendors can demonstrate well-managed product development process, labs can justify doing less validation work.

Frequently Asked Questions

Question: How is change control used to keep software validated?:

Answer: It is normal that any system needs to be changed over time because of changes in business needs and software updates. The objective is to make sure that those changes are described properly, that the impact and risk of that change is well understood, and that there's documentation to support that assessment of the impact and the risk. A determination is then made regarding the degree of testing or revalidation work that would be required to re-establish that the system is still behaving according to its intended use in the process where it's going to be used.

Question: How much validation effort is appropriate for custom reports?

Answer: According to the International Society for Pharmaceutical Engineering (ISPE) Good Automated Manufacturing Practices (GAMP) guidance, custom reports are category 5; meaning that being unique to a particular lab they are of the highest level of configurability or customization. Thus custom reports require fairly extensive validation to ensure that any custom calculations are working properly. Negative boundary and stress testing should be used to make sure that the report and the reporting environment would reject values that don't make sense--for example characters instead of numbers.

Question: Once a vendor has been audited, is there a recommended time within which the vendor should be re-audited?

Answer: No. The frequency of re-auditing a vendor is based on many factors such as how well the vendor performed in their last audit; the relative risk of that system to patient safety, product quality, and data integrity; and any kind of problems that you may have had with that system.

If the vendor performed relatively well in their last audit, you can justify lengthening the amount of time before the next audit. If the system has been relatively stable with relatively few problems, you may be able to justify going as long as three years before you do another audit. Two years is a common rule of thumb, and labs can shorten or lengthen that time depending on the factors described here.

If you plan a software update that adds a significant amount of new functionality, it would also be a good time re-audit the vendor.

Question: If there is an update for my software available and I choose not to install the update because my system is validated and I don't want to revalidate it now, will the FDA write me up for not updating my system?

Answer: Not directly. However, if the FDA finds an issue that is related to and addressed by an update that they are aware is available, you can probably expect to hear from them. The FDA does not require keeping systems on the very latest version of software.

Question: How do I audit the software validation status of a contract manufacturer?

Answer: Auditing the validation status of a contract manufacturer is no different from auditing the systems within your own organization. You would review their infrastructure and how they are defining and validating their computer systems within their particular environment for their intended uses. This process includes how they do their own internal audits for their systems and for their suppliers. It is not generally necessary to do a second- or a third-level audit of your contract manufacturers' suppliers. That audit would be their job and you would expect them to have their own audit programs.

The level of detail needed should be based on your contractual relationship with the vendor and the degree to which regulatory obligations have been transferred to your contract manufacturer. For example, the vendor may be doing manufacturing for you but using your computer systems, which presumably you would have already audited. Therefore there would be less need to audit their computer systems.

If the vendor is using their own systems, it is important to pay attention to data transfers from their systems to your systems because those data transfers are vulnerable to data transfer failures, missing data, and other data integrity concerns.

Question: Does the FDA recognize the use of electronic validation records and electronic signatures?

Answer: Yes, since 1997. The FDA does establish that any electronic records including validation records can be considered the equivalent of paper records, and any signatures on those electronic documents can be considered the equivalent of handwritten signatures.

It is common for validation work to be done at one facility, with the quality oversight of that work done at a physically different facility using electronic transfer or review of validation documentation.

Question: How would you recommend executing validation of a software product? Does it depend on the software's intended use?

Answer: Validation is best executed by the staff that will be using the system regularly. They best understand the use of the system in the context of the lab's process, and will be able to pay attention to details that an IT or validation organization might miss. It is also an effective way for lab staff (as opposed to IT) to take ownership of the system.

Question: How often should a system be requalified by performing IQ/OQ? Some vendors state the qualification should be performed yearly.

Answer: The timing of the requalification should be based on when changes—such as installing new software or updates to the operating system—are being made. The nature of the change and the severity of problems with the system since it was last qualified also determines the timing of requalification. Some companies perform annual IQ/OQ to address minor periodic system changes pushed through by IT, such as Microsoft security patches. Requalification rationale, timing, and procedure should be documented so the FDA can understand how you made your decisions based on your organization's needs.

Question: Is product and process specification validation equal to analytical method validation plus qualification of liquid chromatograph (LC) systems and software?

Answer: They are similar but not equal. Method validation validates the science behind the analytical testing process for a particular product. Method validation is either concerned with confirming the identity, quantity, and strength of a particular compound, or looking for impurities in a sample.

A computerized system will likely be used for data acquisition and data analysis so method validation alone is not a replacement for the system validation. However they are related because LC system and software validation occur in the context of the methods used.

Question: Is process validation relevant to industries outside the pharmaceutical industry?

Answer: Yes. The concept and practices of validation translate across industries. Whether its pharmaceutical, food quality, food safety, forensic, or environmental testing, you want to be sure that the results produced by your system are consistent, repeatable, and trustworthy.

Food safety and environmental testing can directly impact human health and thus warrant validation concerns similar to pharmaceutical testing. Across all industries, consumers expect consistent, reliable, and safe products. For example, in the case of fuel production, consumers expect consistent fuel quality for their automobiles.

Question: Please provide an example of how process validation covers an area that systems-level validation would not?

Answer: A chromatography data system (CDS) provides a good example. In the most basic sense, a CDS is designed to acquire, analyze, and report on data from an instrument such as and LC or gas chromatography (GC) system. In a generic sense, if that functionality were validated, you could say that the system is validated. However, that does not validate the process for analysis of a particular product, including steps such as sample preparation. Process validation requires confirmation that the chromatography data system works properly within the context of the testing of a particular drug product.

Question: Have there been any major changes in 21 CFR Part 11?

Answer: The regulation itself has not changed since it was originally issued in 1997, however, in the draft guidance released in April of 2016, there were changes evident in the FDA's thinking. The FDA had conveyed that if an activity was not documented, it never happened. The FDA is a document-centric organization and thus when they do inspections; they appropriately want to look at documentation.

In the past, the FDA has explicitly stated "For computerized systems, the record of that computerized system existed when that record was committed to durable media," meaning when that record was printed or saved to disk. In the 2016 guidance, the FDA now states; "The record exists when the data is generated," an important shift. The reason why the FDA made this change is that many labs around the world use real-time data previews as instruments generate data. If the operator sees unexpected data generated, they may interrupt that run and thus, under the previous guideline, that data would have never existed because it had not been captured or saved to disk. The FDA intent is to ensure that if "it happened," then it must be recorded. If an injection was started—even if the operator sees that the data coming off of the instrument is not what they are expecting for a particular sample—that injection still happened and that injection still needs to be recorded.

Companies may be fearful of recording data associated with a product problem. However, finding problems is an important purpose of labs. And it could also indicate a sample preparation or instrumentation problem that should be addressed.

References

1. R.D. McDowall, "FDA's Focus on Laboratory Data Integrity – Part 1," Scientific Computing (Sept 2013). http://www.scientificcomputing.com/article/2013/09/fda%E2%80%99s-focus-laboratory-data-integrity-%E2%80%93-part-1
2. FDA, Glossary of Computer System Software Development Terminology, https://www.fda.gov/iceci/inspections/inspectionguides/ucm074875.htm
3. FDA, Data Integrity and Compliance with CGMP Guidance for Industry, https://www.fda.gov/downloads/drugs/guidances/ucm495891.pdf
4. FDA, General Principles of Software Validation; Final Guidance for Industry and FDA Staff, https://www.fda.gov/RegulatoryInformation/Guidances/ucm085281.htm
5. M. Cahilly, Workshop on Data Integrity and Industry Practice, Peking University, Beijing, June 22–23, 2015.
6. J. Mourrain, "Apples and Oranges: Comparing Computer Systems Audits," Ther. Innov. Regul. Sci. 40 (2), 177–183 (2006).

To watch the On-Demand webinar of this article, visit:
http://www.agilent.com/en-us/video/demistifying-software-validation-2017

www.agilent.com/chem/OpenLAB

Published in the USA, June 20, 2017
5991-8176EN

Agilent Technologies