# Breaking Down Computer Systems Validation in a Regulated Environment

- Quality & Regulatory

Jun 9, 2021
by
Ray Roggero, Medvacon Life Sciences

A computer system operating in a company regulated by the U.S. Food and Drug Administration (FDA) does not solely consist of computer hardware and software. It may also include any equipment and instruments connected to the system, as well as the users who operate the system or equipment following standard operating procedures (SOPs) and manuals.

Computer Systems Validation (CSV) is a documented process that is required by regulatory agencies around the world to verify that a computerized system does exactly what it is designed to do in a consistent and reproducible manner. The FDA defines software validation as:

*Confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled.* **(1)**

In other words, computer systems need to be examined to confirm that the system will work in *all* situations, and all validation activities and test results must be documented. The FDA and other global regulatory agencies require CSV processes to confirm the accuracy and integrity of data in computerized systems in order to ensure product safety and effectiveness. Whether you are configuring a new system or making a change in a validated system (e.g., upgrades, patches, extensions), CSV processes are based on applicable regulations and guidance, best practices for the industry, and the characteristics of the system being validated.

CSV ensures that both new and existing computer systems consistently fulfill their intended purpose, produce accurate and reliable results that are regulatory-compliant, meet user requirements, and provide the ability to discern invalid and/or altered

records. CSV uses both static and dynamic testing activities throughout the software development lifecycle—from system implementation to retirement.

All computerized systems used in a regulated pharmaceutical environment should be documented with system inventory and assessment to determine *which* systems need to be validated. User requirement specifications, along with operational (regulatory) constraints, clearly define *what* the system should do. Functional requirement specifications clearly define *how* the system will look and *how* it will function to achieve the user requirements.

# Putting Computer Systems Validation into Practice

A validation plan is needed to define the objectives of the validation and an approach for maintaining the validation status. A validation risk assessment, an analysis of failure scenarios and regulatory impact, is conducted to determine the scope of validation efforts. A requirements traceability matrix cross-references the user and functional requirements and verifies that everything has been tested.

Network and infrastructure qualification documentation shows that the network and infrastructure hardware and software supporting the application system being validated has been installed correctly and is functioning as intended. Installation qualification tests check that the system has been installed correctly in the user environment, and operational qualification tests check that the system does what it is intended to do in the user environment.

Performance qualification testing is for checking that the system does what it is intended to do by trained people following SOPs in the production environment. The validation report reviews all activities against the validation plan and protocols; it documents that the validation activities are complete, and the system is ready for its intended use.

One of the biggest mistakes a company can make when starting a CSV project is not performing the strategic planning necessary to ensure success. The first step in any informatics validation project should always be conducting a thorough workflow and business analysis. This process allows the development of clear and precise functional and user requirements tailored to your unique operating environment with a high degree of specificity and defined at a level that can be addressed through the software. Without clear and precise requirements, CSV will not adequately verify that the system is functioning as intended.

*"Efficient and effective CSV processes ensure that projects are delivered on time and within budget"*

CSV can take a lot of time and IT resources to accomplish, so following a flexible *Good Automated Manufacturing Practice (GAMP) 5* approach that utilizes a risk-based assessment of the system to determine the required test cases and optimal level of testing would be wise **(2)**. CSV efforts should concentrate on what is identified in the risk assessment for the critical elements of the system that affect quality assurance and regulatory compliance. The benefits of taking this risk-based approach to CSV include reduced cost, reduced business risk, and reduced duration of validation efforts. Like any technical endeavor, CSV processes should be guided by a good plan that is created before the project starts. This plan will define the objectives of the validation, determine the approach for maintaining validation status over the full software development lifecycle, and satisfy all regulatory policies and industry best practices (e.g., GAMP 5). The validation plan will be created by people who are knowledgeable about CSV requirements and the technology involved, thus minimize the impact of the project on day-to-day processes.

The validation plan should detail the scope of the project, outlining the parts of the system that will be validated, and chart the deliverables and documentation required for the project. Validation activities are only applied to the aspects of the system that will be utilized by the company, an approach that must be justified in the risk assessment. The validation plan should define the types of data that will be used for testing, along with the kinds of scenarios that will be tested. The plan should list the members of the validation team, along with their roles and responsibilities in the validation process. Finally, the plan needs to define the requirements that need to be satisfied, or the acceptance criteria, before the system is considered suitable for use in regulated activities.

# More Than Hardware and Software

The project team should have CSV experience and knowledge of regulatory guidelines and compliance expectations, validation procedures, processes, and the technology being validated (e.g., informatics software, laboratory devices, instruments). The CSV team should include a sufficient number of members, so individuals are not stretched too thin during the project.

The company needs to develop clear and precise test scripts related to the functional and user requirements and specifications to confirm the system is fulfilling its intended use. Vendor-provided test scripts typically only validate the base system requirements and will not be sufficient to ensure regulatory compliance. Performance qualification must also be conducted to test the system in its normal operating environment, operated by trained users following approved SOPs.

CSV processes and results need to be clearly documented over the full software development lifecycle to the extent that the documents are sufficient to pass an audit by regulatory agencies. A good policy to follow is: If it is not documented, then it was

not done. Having project team members with a thorough understanding of regulatory guidelines is an important part of creating the necessary documentation.

In addition to performing CSV on internal systems, a regulated company needs to be prepared to audit its third-party service providers (e.g., contract research organizations), as well as vendors of critical applications and cloud-based software services. The manufacturer of an FDA-regulated product is ultimately responsible for the integrity of the data that supports that product's efficacy and safety. So, if third-party vendors or service providers are used, the manufacturer must take the appropriate steps to ensure those providers are operating under standards that would hold up under an inspection by a regulatory body.

A risk-based assessment should be conducted to determine if an audit is necessary. At the minimum, the manufacturer should establish formal agreements, clearly detailing responsibilities, with any third parties it uses to provide, install, configure, integrate, validate, maintain, or modify a computerized system.

Effective, risk-based validation of computerized systems is an important part of maintaining regulatory compliance and product quality. Efficient and effective CSV processes ensure that projects are delivered on time and within budget.

# References

1.  U.S. Food and Drug Administration. *General Principles of Software Validation; Final Guidance for Industry and FDA Staff*; U.S. Department of Health and Human Services: Rockville, Md., 2002. Available at **https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-principles-software-validation**.

2.  International Society for Pharmaceutical Engineering. *GAMP 5 Guide: Compliant GxP Computerized Systems*; ISPE: Tampa, Fla., 2008.

## ABOUT THE AUTHOR

**Ray Roggero** is a Managing Partner and the Chief Operations Officer for Medvacon Life Sciences, LLC. He serves on the External Advisory Board of the Pharmaceutical Manufacturing Engineering (PME) Graduate Program at Stevens Institute of Technology. In addition to being a member of PDA, Ray serves on the Board of Directors for the New Jersey Chapter of the International Society of Pharmaceutical Engineers (ISPE).