Computer System Validation
Best Practices

MEDVACON Life Sciences delivers leading Compliance and Computer System Validation services that are designed to help reduce the overall cost of compliance for Life Sciences organizations. We offer our clients comprehensive services, including leadership and a range of strategic solutions and tactical services that provide cost-effective and comprehensive compliance and validation. The MEDVACON Life Sciences team of highly-qualified consultants can deliver a broad suite of solutions in areas of computer systems validation, infrastructure qualification, IT Quality Management, and process improvement. Below is a discussion of best practives to ensure the success of your CSV project.

Computer system 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. These regulatory agencies require CSV processes to confirm the accuracy and integrity of data in computerized systems in order to ensure product safety and effectiveness. Computer system validation is required when configuring a new system or making a change in a validated system (upgrades, patches, extensions, etc.). CSV processes sare based on applicable regulations and guidance, best practices for the industry, and the characteristics of the system being validated. With regards to Computer system validation, a “computer system” in an FDA regulated company is not just computer hardware and software. A computer system can also include any equipment and/or instruments connected to the system, as well as users that operate the system and/or equipment using Standard Operating Procedures (SOPs) and manuals.

Computer system validation ensures that both new and existing computer systems consistently fulfill their intended purpose and produce accurate and reliable results that enable regulatory compliance, fulfillment of user requirements, and the ability to discern invalid and/or altered records. CSV utilizes both static and dynamic testing activities that are conducted throughout the software development lifecycle (SDLC) – from system implementation to retirement.

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.” Computer systems need to be examined to confirm that the system will work in all situations. Additionally, all validation activities and test results need to be documented.

All CSV activities should be documented with the following:

- **System inventory and assessment** – determination of which systems need to be validated
- **User requirement specifications** – clearly defines what the system should do, along with operational (regulatory) constraints
- **Functional requirement specifications** – clearly defines how the system will look and function for the user to be able to achieve the user requirements.
- **Validation Plan (VP)** – defines objectives of the validation and approach for maintaining validation status
- **Validation Risk assessments** – analysis of failure scenarios to determine scope of validation efforts
- **Requirements Traceability Matrix** – cross reference between user and functional requirements and verification that everything has been tested
- **Network and Infrastructure Qualification** – documentation showing that the network and infrastructure hardware/software supporting the application system being validated has been installed correctly and is functioning as intended
- **Installation Qualification (IQ)** – test cases for checking that system has been installed correctly in user environment
- **Operational Qualification (OQ)** – test cases for checking that system does what it is intended to do in user environment
- **Performance Qualification (PQ)** – test cases for checking that System does what it is intended to do with trained people following SOPs in the production environment even under worst case conditions
- **Validation Report** – a review of all activities and documents against the Validation Plan
- **System Release Documentation** – documents that validation activities are complete and the system is available for intended use.

Putting it all into practice: Best Practices for Computer System Validation

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

Perform risk-based CSV. CSV takes a lot of time and IT resources to accomplish, so it is wise to follow a flexible GAMP 5 approach that utilizes a risk-based assessment on the system to determine required test cases and the optimal level of testing for each. CSV efforts should concentrate on what is practical and achievable for the

critical elements of the system that affect quality assurance and regulatory compliance. Benefits of this risk-based approach to CSV include reduced cost, business risk, duration of the validation efforts.

Create a Good Validation Plan. 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, the approach for maintaining validation status over the full SDLC, and satisfy all regulatory policies and industry best practices (e.g., GAMP 5). The validation plan will be created by people who have a good knowledge of the technology involved (i.e., informatics systems, instruments, devices, etc.) and serve to minimize the impact of the project on day-to-day lab processes. The validation plan should detail the following:

- ***Project Scope*** – outlines the parts of the system that will be validated, along with deliverables/documentation for the project. Validation activities are only applied to aspects of the system that will be utilized by the company.
- ***Testing Approach*** – Defines the types of data that will be used for testing, along with the kind of scenarios that will be tested.
- ***Testing Team and Responsibilities*** – Lists the members of the validation team, along with their roles and responsibilities in the validation process.
- ***Acceptance Criteria*** – Defines the requirements that need to be satisfied before the system is considered suitable for use in regulated activities.

Create a Good Project Team. The project team should have CSV experience and knowledge of regulatory guidelines/compliance, validation procedures, processes, and the technology (e.g., informatics software, laboratory devices and instruments, etc.) being validated. It is important that the team is big enough so that members are not stretched too thin during the project.

Test all Requirements and Specifiactions. Develop clear and precise test scripts related to the functional and user requirements and specifiacitons to confirm the system is fulfilling its intended use. Note, vendor provided test scripts typically only validate the base system requirements and will not be sufficient to ensure regulatory compliance. A PQ must also be conducted to tes the system in its normal operating environemnt, operated by trained users folloing approved SOP's.

Create Good Documentation. CSV processes and results need to be clearly documented over the full SDLC to the extent that the documents are sufficient to pass an audit by regulatory agencies. Having project team members with good understanding of regulatory guidelines is an important part of creating the necessary documentation.

Audit third-party Providers. In addition to performing CSV on internal systems, an FDA-regulated company needs to be prepared to audit third-party service providers (e.g., CROs), along with vendors of critical applications and cloud-based services (SaaS). The manufacturer of an FDA-regulated product is ultimately responsible for the integrity of the data that supports the product's efficacy and safety, so if third-party

vendors or service providers are used, the manufacturer needs to take appropriate steps to ensure that they are operating under standards that would hold up under an FDA inspection. A **risk-based assessment** should be conducted to determine if an audit is necessary. At the minimum, formal agreements that clearly detail responsibilities must exist between the manufacturer and any third parties that are used 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 projects are delivered on time and within budget.

If you have additional questions about computer system validation, or would like to have an initial, no obligations consultation with an expert to discuss your validation project, please feel free to contact us.