



Computer System Validation at LabHQ

LabHQ LIMS has been developed and tested using the company's Computer System Validation Process (CSVP). Below is a description of computer system validation, why we do it, what is involved and how we apply this in LabHQ Limited.

What is Validation?

In its basic form, validation is a documented process of demonstrating that a product or process is doing the right thing and doing it right. The US Food and Drug Administration (FDA) in 1987 defined validation as *"Establishing documented evidence that provides a high degree of assurance that a specific process will consistently produce a product meeting its pre-determined specifications and quality attributes"*. This definition was originally applied to the drug manufacturing processes, but has since been expanded to include associated drug-related activities including analytical methods and computer systems used in regulated processes.

There is an expectation that validation should allow quality to be built into all stages of a regulated system's life cycle, in order to minimise system errors, problems and the risk of a system not maintaining its validated state, any of which may a) prove expensive to fix and b) more importantly, may be responsible for causing harm to a patient. The latter is the single key driving force behind the regulatory necessity for validation. In order to achieve this we use the concept of a validation lifecycle, which sits alongside a product's life cycle (in this case the product being a computer system). In this context, a computer system is any system used to perform a business function, and includes computer hardware, software, procedures *and people*.

The LabHQ Computer System Validation Process

CSVP includes a number of phases that mirror the system life cycle. These are:

- Planning
- Design and Build
- Installation
- Testing
- Reporting and Release
- Use/Support
- Retirement

Planning

This occurs right from the start of the system project concept. It usually starts with developing a set of **Business Requirements**, which are a relatively high level description of what the system needs to do. Business requirements should be developed for any computer system, irrespective of whether it needs to be regulated.



The next step is to determine if validation is actually required. This is usually done by considering the business requirements and the business processes involved and assessing these for regulated activity and data. This typically involves a formal **GxP** risk assessment of the system, even though at this stage it is still a concept. This decision is documented in a **Compliance Determination**.

Once the decision has been made that a system requires validation, it is a good idea to plan what is needed, how much, in what order, what standards and procedures will be used etc. This is not a project plan, but a **Validation Plan**. It acts as the guide for all validation activity that must be done, at least up to the system being released for operational use. It will include the rationales as to why things are done (and why some things will not) and generally describe the validation approach for this particular system. It should also describe the governance procedures that will be used, such as management of documentation, changes, incidents, configuration and project training.

Design and Build

A **Design Specification** is usually created to define the proposed design (or configuration) and how this will meet the requirements. For bespoke development there may also be detailed **Unit Specifications** for individual functions. **Hardware Design Specifications** detail what computer hardware is required and how it fits together. Where the system needs specific configuration this will be documented in a **Package Configuration Specification**.

When the design documentation is available, a **Design Review** will take place, to check that all requirements are in place and that the proposed design documents demonstrate that the requirements and quality attributes can be met. At this point a traceability process is initiated. This is designed to show the explicit links between the requirements, design attributes and (eventually) the test steps, demonstrating that each requirement has design attributes and has been tested. This process of **Requirements Traceability** is often managed using a spreadsheet which shows links and this is maintained throughout the life of the system. It is especially useful when changes are proposed as it can be used to show what testing needs to be performed or modified, and any hitherto unrecognised impacts of making a change can be identified.

When bespoke software is being developed (and this may be necessary even for COTS systems e.g. bespoke reports), then there must be a process in place to develop the code specific standards, documented in a **Programming Standards** document. The coding process will also include some level of source code review to check that the code meets the programming standards, resulting in a **Source Code Review Report**. **Unit testing** is also likely to occur when individual functional blocks are being developed as a means of detecting faults as early as possible.

Installation

The installation of both software and hardware is documented in one or more **Technical Installation Plans or TIPs**. These define exactly what needs to be installed for each environment and for each component, and what evidence is to be collected to demonstrate that the plan was followed. The completion of each TIP will result in a **Technical Installation Report or TIR**. If data is required for testing or to be migrated from a legacy system, a Data Migration Plan is developed



to describe how this will take place and the checks performed which demonstrate that data integrity is maintained.

Testing

System Testing takes place to demonstrate that the system as a whole can meet the System Requirements. **User Acceptance Testing** is performed to demonstrate that the Business Requirements have been met. The rationale and extent of the testing for a particular system and how and when it will be performed is documented in a **Test Plan**. The test plan will also include the standards and conventions that must be adopted for that level of testing. The testing itself is documented in **Test Cases**. These are preapproved documents and may include a number of test objectives covering the testing of specific areas of functionality. Each test objective is written as a series of steps, each of which defines what should be done, what should happen, expected results and what evidence must be collected. Each test step includes space for observations and results to be documented by the tester and whether that step passed or failed any stated success criteria. When completed test cases are independently reviewed and approved. A **Test Report** summarises the degree of success of carrying out the test plan at that stage.

Reporting and Release

When all testing is complete then a **Validation Report** will be created to summarise all of the validation activities and outcomes, which should mirror the Validation Plan. The key aim of the Validation Report is to state the validation status of the system and its suitability for release as a live system. It will include a list of all the validation deliverables that have been produced. As a result this is a key document when regulatory inspectors take an interest in a specific computer system. A separate **System Release Notification** is used as a means of signalling that the system can be made available for live or production use.

Note: User Acceptance Testing may occur, at least in part, only after the system has been released. This may be necessary to further test the system in full production use and at normal performance levels. This is often referred to as Performance Qualification (PQ). The initial Validation report may therefore be an interim report which is subsequently updated when all PQ activity is concluded.

Use/Support

Before a system is made available for live use, there will usually be a number of deliverables developed that define how the system will be used and supported. The **System Access Plan** is used to define the process for gaining access to the system (though this may be also documented in a user SOP). The **Support Quality Plan** will define how the process for how the system will be supported and describe what quality attributes will be controlled, how and when. This may include references to backup/restore processes, disaster recovery plans and business continuity plans. Typically, before the validation is complete, system **SOPs** and/or **User Manuals** will be developed and **Service Level Agreements (SLAs)** with all service providers will be agreed.



Validation must periodically be reviewed to determine if the validated state has been maintained and to review the cumulative impact of any system changes that have taken place. This will take the form of a **Periodic Compliance Review** and its frequency will be determined according to the business criticality and GxP risks associated with the system (minimum every three years).

Retirement

When a system is to be taken out of service, it must be done so in a controlled and planned way. This is especially important when system data must be retained to comply with data retention policies or regulations, or is to be migrated to a replacement system. **A Decommissioning Plan** will document the process for removing the system from service.