STARLIMS™

COMPLIANCE AND VALIDATION BEST PRACTICES FOR COMPLEX LABS OF THE FUTURE

Former U.S. Deputy Attorney, General Paul McNulty said it best *"If you think compliance is expensive, try non-compliance"*. For regulated industries operating to GMP or other GxP guidelines, software validation is essential. FDA dictates that to satisfy regulatory compliance it is necessary to validate all software used for the design, manufacture, packaging, labeling, storage and servicing of all finished devices or products intended for human use. However, it's not enough just to show that each piece of software reliably carries out its expected function. Validation should consider the software infrastructure, and how one piece of software might interact with and be instructed by or control other systems, at every stage in a workflow. Only then is it possible to determine whether an individual software system satisfies regulatory standards for its intended use. Given that a software landscape may encompass programs developed in house, interfaced with out-of-the-box platforms or bolt-ons, and tailored solutions from multiple third parties, it becomes evident that validation is a complex undertaking.

In effect, software validation should demonstrate via objective evidence – and provide a high degree of assurance – that a specific process will consistently produce the expected result. As FDA notes in its late 2018 guidance document, Data Integrity and Compliance with Drug cGMP: Questions and Answers Guidance for Industry[1], (the data integrity guidance), *"If you validate the computer system but you do not validate it for its intended use, you cannot know if your workflow runs correctly."*

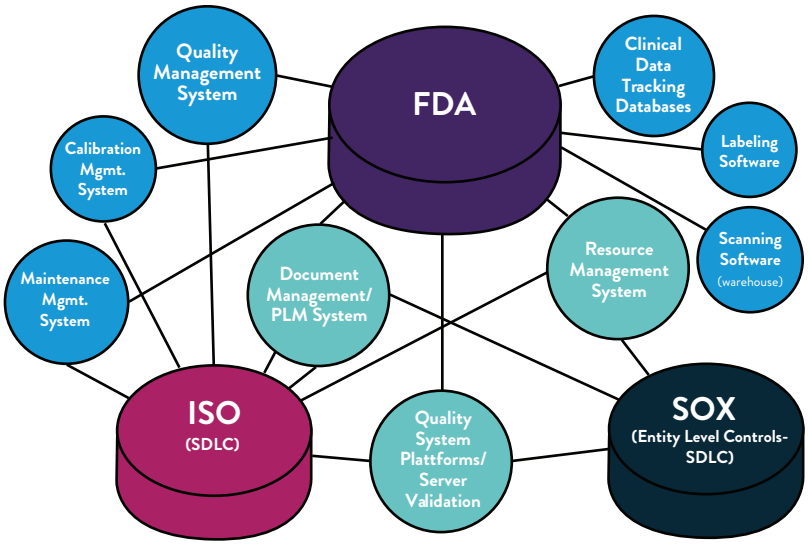

Fig.1: Manufacturing and Quality System Software Validation

Recent trends indicate that industries are moving towards the goal of paperless data handling and management to demonstrate data integrity. All records required under cGMP are subject to FDA inspection, which means that all software that generates or interacts with GMP data must be validated. "This applies to records generated and maintained on computerized systems, including electronic communications that support cGMP activities[1]." The agency recommends that organizations should implement "meaningful and effective strategies" to manage the risks of data integrity, based on their process understanding and knowledge management of technologies and business models. In effect, "meaningful and effective strategies should consider the design, operation, and monitoring of systems and controls based on risk to patient, process, and product[1]."

This paper discusses some of the intricacies of software validation and provides insight into why LIMS customers should be wary of vendors promoting 'pre-validated' solutions in this complex environment.

BENEFITS OF SOFTWARE VALIDATION

The benefits of validation are broad and varied. Software validation can increase the usability and reliability of the end product, potentially resulting in decreased failure rates, fewer recalls and corrective actions, and so less risk to patients and consumers. Software validation can also reduce long-term costs, FDA notes in its General Principles of Software Validation; Final Guidance for Industry and FDA Staff, "by making it easier and less costly to reliably modify software and revalidate software changes[2]." And as software maintenance can represent a major portion of the overall cost of software over its life cycle, FDA notes, "an established comprehensive software validation process helps to reduce the long-term cost of software by reducing the cost of validation for each subsequent release of the software[2]."

Additionally, labs operating in a GxP (including GMP) environment should not take for granted that what is marketed as a pre-validated LIMS will satisfy all the qualifications for validation. The entire informatics infrastructure, including software feeding into the LIMS and into which the LIMS exports data, needs to be validated alongside an individual software platform. This means establishing a quality management setup that outlines the complete validation approach. Each piece of software must be identified, and a risk assessment and 21 CFR Part 11 assessment carried out on all software that may interact with GxP operations such as security assessments or audit reviews.

While it is important to have a master plan in place, and to make sure that key personnel have a full understanding of the validation process, it can also be invaluable to encompass some level of third-party oversight, which can help to provide an extra layer of verification for the auditor.

Vendor packages should be built around best practices, so that the solution offers features to support compliance in regulated markets.

What is involved in a complete software validation approach? It's worth taking a step back and thinking about the complexity of validating even the most basic software. Software can carry out different commands – effectively performing different functions or operations – dependent upon the information, or instructions, that it receives. This capacity for workflow branching – and so changes to how one software instruction can alter or determine the function of one or multiple connected software systems – contributes to the complexity of any software package, FDA points out. It means that standalone testing in a single situation will not verify the completeness and correctness of software, which must be validated for every possible function and interaction.

And unlike hardware, which is typically built to carry out a set operation repeatedly over its lifespan, software can be adapted and updated. "... software is not a physical entity and does not wear out," the FDA software validation guidance continues[2]. "In fact, software may improve with age, as latent defects are discovered and removed. However, as software is constantly updated and changed, such improvements are sometimes countered by new defects introduced into the software during the change[2]."

Software validation is thus a complex undertaking, FDA suggests. "Software verification and validation are difficult because a developer cannot test forever, and it is hard to know how much evidence is enough[2]." In large measure, software validation is a matter of developing a "level of confidence that the device meets all requirements and user expectations for the software automated functions and features of the device[2]." It is commonly believed that because software can easily and swiftly be modified, software problems can also be corrected easily and swiftly. But this is a face value assumption. "Combined with a lack of understanding of software, it can lead managers to

believe that tightly controlled engineering is not needed as much for software as it is for hardware. In fact the opposite is true[2]," FDA notes. Correcting one aspect of software operation may impact on downstream functions that will necessitate revalidation each time an update or upgrade is made.

This is just part of the reason why it is critical that LIMS customers partner with a vendor who offers a solution that has been designed and developed using a quality-focused strategy that will continue to support regulatory needs. Given the requisite for robust, seamless software validation for purpose, STARLIMS has developed the STARLIMS Automated Validation Framework and Testing Kit to help laboratories meet this obligation.

Fig. 2: Benefits of Automated Testing

The STARLIMS Automated Validation Framework and Testing Kit is a comprehensive testing suite that is used to verify the STARLIMS core software functionalities for each setting and deployment. This essentially provides the LIMS customer with a set of tools that can be used for various aspects within their validation process. Firstly, the customer is equipped with a knowledgebase of STARLIMS' core functionalities, use cases, and overall intended use. This knowledgebase acts as a baseline for a fully functional deployment of STARLIMS. Subsequently, any changes that are made to the software, its environment, or its peripheral interfaces, can be compared against the working baseline to verify that core software functionalities and workflows were not affected by newly introduced changes.

Secondly, the STARLIMS Automated Validation Framework and Testing Kit allows for tremendous flexibility by providing the customer with a set of distinct testing scenarios for a given STARLIMS application or workflow. This allows the customer to exclude any functionality or testing cases that are not in use and focus on the applications and functionalities that represent intended use and are therefore at a higher risk based upon any software changes. Such a focused effort would reduce risk and lead to time and costs savings.

The STARLIMS Automated Validation Framework and Testing Kit may also be used as an input to perform Operational Qualification of the STARLIMS software within the deployed environment. Operational Qualification, another requisite to almost all validation efforts, is a testing process that ensures the software is operating correctly under its specified limits. Given that the Verification Kit contains a set of testing scenarios, such scenarios can be reused or repurposed to create an OQ that's specific to the deployment of the software.

But customers should also remember that while STARLIMS services and products provide the bulk of the collateral and expertise, validation will still be very much a collaborative effort. Project validation should not be isolated but should be carried out in alignment with an overarching quality system (QS). STARLIMS also recommends this process encompasses third party oversight and validation expertise.

VALIDATION & REGULATORY REQUIREMENTS

Regulatory requirements mandate that companies validate their LIMS systems for intended use. However, it is still the LIMS customer's responsibility to validate per intended use and to verify their configuration, business workflows, and static data. LIMS system validation should be integrated into the organization's overall quality management system, to certify that the system is documented, and to support the organization during quality audits. To underpin this process, the organization should follow their system life cycle (SLC)/validation methodologies, policies and procedures and demonstrate that the system is in a validated state per intended use.

What documentation is required for regulatory validation?

Auditors may expect to see a comprehensive set of documentation to support a quality system validation:

Software validation protocol (validation plan)

This document outlines the overall validation strategy, project deliverables and defines responsibilities. LIMS validation shouldn't be considered a stand-alone activity. Rather, it should be integrated with the customer's quality system – including a comprehensive risk analysis for all software used in GxP environments – and with methods and instrument validation, operator training/security, audit review, and other essential activities.

Network diagram

This required document provides a visual layout of how the system is configured on the network. It should demonstrate and ensure that everyone understands how the system is configured for the specified implementation. In practice, this diagram may be included as an attachment to the software requirements specification.

Software requirements specification

User and software requirements will be founded on safety analysis and 21 CFR Part 11 compliance analysis, and feed into the verification protocol, test cases and requirements traceability matrix. Ultimately, this software verification protocol and parallel business process procedures should be combined to draft a complete software verification and validation report. The requirements specification should encompass physical hardware requirements on top of the software requirements, and span training requirements, integration with other systems and user and business requirements and procedures.

Risk assessment

Risk assessment is a critical and complex component of any GxP environment and requires input from resources at all levels of the organization. It is also an inspection area on which FDA is becoming increasingly focused. Identifying and mitigating potential harm during the validation process will help to minimize the likelihood that an inspection will find deficits that require subsequent corrective actions, or the need for preventive actions (CAPA) when in production.

21 CFR Part 11 compliance analysis

Part 11 compliance is as important to a LIMS as it is to the organization. Vendor and validation documentation should provide a complete evaluation of system adherence to and requirements for the use of electronic signatures and audit trails as required by FDA in 21 CFR, Part 11.

Design specification (only f or s ystems o r a reas o f t he system which contain custom code)

A design specification is typically not required for a purchased configurable business quality system. However, a design specification document may be warranted if there is to be major integration or customization carried out as part of the project.

Verification protocol/ test plan

This is a critical document that outlines the testing plan and how testing will be carried out, as well as defining any measures that are in place to deal with test anomalies and deviations, and their procedures and schedules.

Test specifications/test cases

The test specification/test cases document should outline system-level test cases, which have been designed according to the requirements specification. If these are separate or maintained as an attachment to the verification protocol it makes it easier to add modules or new phases to the validation package, while limiting revision time.

Final validation report

All documentation and activities associated with software validation should be summarized as part of the final validation report, which will also detail any deviations, and encompass instructions for user training, the extent of software support, backup and change management. The final validation brings together and connects all the activities and documentation associated with the software validation process.

Summary and conclusions

As a LIMS provider, STARLIMS strives to provide as much out-of-the-box functionality as possible, while remaining flexible to each LIMS customer's current and projected future needs. Our QMS provides thorough testing to ensure quality products are released from the outset. The STARLIMS quality system includes SOPs, validation plans, completed test documentation, and validation summaries. Our implementation process

follows industry standard guidelines to provide necessary assessments, testing, and documentation to deliver and support quality solutions. The STARLIMS methodology for implementation is founded on industry best practices, to include identification/tracking of requirements, continuous communication, and change management. Additionally, we can provide the expertise, experience, documentation templates, and toolsets such as the STARLIMS Automated Validation Framework and Testing Kit to educate and enable LIMS customers to undertake a full end-to-end validation.

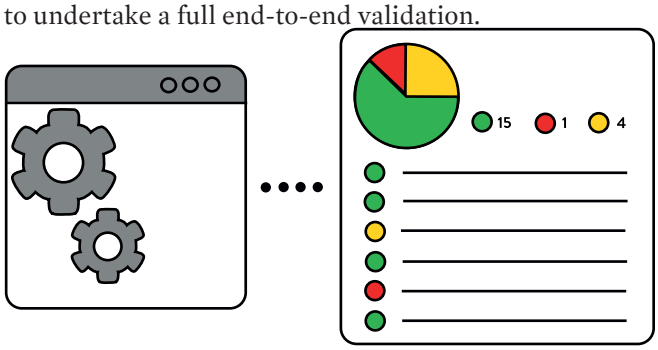

Fig. 3: Test Automation

STARLIMS also understands how empirical, time consuming, and generally all-encompassing an end-to-end validation is. Validation, even for the smallest of software changes, can be a costly effort involving many days and resources of testing. Depending on the type of change, it may even involve testing of peripheral systems and interfaces, thereby increasing the manpower and requisite knowledge needed to validate. One of the main problem statements that arises from performing a validation is simply this; Validation is expensive, lengthy, and can drop productivity in a business. Our mission is to help our customers scale their businesses, reach success, and be change agents in their industries. This is not only done by creating an innovative LIMS but by also providing a means to automate the deployment of the LIMS. At STARLIMS , we've taken our Automated Validation Framework and Testing Kit further towards automation to position our customers on a path that, not only makes them more productive, but makes them differentiators in the market.

Automating any portion in a lab's ecosystem during a validation effort can yield significant cost, time, and manpower savings. In one such example, an effort to fully execute test cases for the LIMS software, took upwards of 20 weeks, with a staffing cost of $60,000[3]. With the automated STARLIMS Automated Validation Framework and Testing Kit, the execution time dropped significantly to under 2 weeks with a staffing cost of $4,000[3]. This yielded a 90% reduction in cost and time needed to run the suite of test cases for the LIMS. More importantly, continuous human involvement was no longer needed and the likelihood of human-introduced error during testing dropped significantly.

When leveraging automation, a test scenario may be executed multiple times, with little-to-no interaction from a human, and without increasing execution time and cost. Given that an automated validation is highly expedited, it also means that validations can be ran more often and the testing scenarios can be broader; essentially increasing the quality and frequency of testing. With more robust tools for testing, such as the STARLIMS Automated Validation Framework and Testing Kit, our customers can achieve regulatory compliance in a more efficient and reliable way.

STARLIMS is confident that its platform represents a robust informatics solution that will meet scientific, business and regulatory requirements. However, regardless of our input, LIMS customers are ultimately responsible for validating their system per intended use, including their workflows and the configuration, and their business data. While STARLIMS services and products provide the bulk of the collateral and expertise, validation of the informatics solution is very much a collaborative effort and should be carried out in alignment with the client's overall quality system. A risk-based approach is recommended to simultaneously identify high-risk areas and minimize the validation burden. However, it is recommended that customers also engage a qualified third-party vendor to support them through the validation efforts as needed.

CONCLUSION

To recap this important caveat, auditors may be wary of what might be marketed as pre-validated or turnkey systems that involve a high degree of complexity, heavy configuration, and potential customization. Therefore, when choosing a LIMS vendor, it is important to take said vendor's QMS process, track record, and implementation support system into consideration before deciding. At STARLIMS, we are well positioned to assist customers with stringent regulatory processes.

We understand the need to achieve compliance, and so each of our solutions is designed as a complete package for GxP environments that can help to achieve regulatory accreditation and certification.

REFERENCES

1. Data Integrity and Compliance with Drug CGMP: Questions and Answers Guidance for Industry
https://www.fda.gov/media/119267/download

2. General Principles of Software Validation; Final Guidance for Industry and FDA Staff
https://www.fda.gov/media/73141/download

3. Based on internal STARLIMS staffing costs

starlims.com

STARLIMS
Tel: +1 954 964 8663
4000 Hollywood Blvd, Suite 333 South, Hollywood, FL 33021-6755 USA

UNITED KINGDOM
Tel: +44 161 711 0340

GERMANY
Tel: +49 2302 915 245

FRANCE
Tel: +33 1 61 37 02 00

SPAIN
Tel: +34 91 663 67 64

NETHERLANDS
Tel: +31 72 511 8100

ASIA PACIFIC
Tel: +852 2793 0699

LATIN AMERICA
Tel: +1 954 964 8663

CANADA
Tel: +1 888 455 5467

AUSTRALIA
Tel: +61 3 9670 0678