An Executive Summary

Five Essentials for Surviving Your Next Laboratory Inspection: A Quality Control Example (Part 2)

Bob McDowall
Director
RD McDowall Ltd

Paul Smith
Global Compliance Specialist
Agilent Technologies

Josh Miller
OpenLab Software Marketing – eLearning Expert
Agilent Technologies

How to prepare for a regulatory inspection of your laboratory.

Overview

Even with robust quality systems governing your analytical laboratory and a strong data integrity (DI) program in place, you may still be nervous about preparing for a regulatory inspection. What will the inspectors want to know? What will they ask? Is your team prepared? This article, the second in a two-part series, describes what to expect during a regulatory inspection of a laboratory and provides insight into the following:

- How DI plays a role in the inspection
- How to understand and answer the inspector's questions
- How to understand the impact of poor analytical decisions
- How to use systems that can help demonstrate DI and regulatory compliance
- How to use technical controls to enforce operating procedures

Regulatory Expectations for Data Integrity

In preparation for a regulatory inspection, it is important for company management to provide guidance to employees on how to interact with the inspector. The most important message is to never lie to an inspector. Only answer the question that is asked. At the same time, take a proactive approach by anticipating what documentation may be requested as a follow up to the question. If the question is not clear, request that it be repeated or rephrased. If you do not know the answer, it is perfectly acceptable to pass the question to someone who does. Lastly, be aware that a good inspector assumes that non-compliance exists and is only looking to prove it.

Employees also should be familiar with the principles of DI. Part 1 of this article presented DI in terms of the three-level model shown in **Figure 1**. Part 2 of this article focuses on Level 3—the right analysis for the right reportable result. This depends on everything being in place that is represented by Level 1 (the foundation layer)—the right instrument and system for the job; and by Level 2—the right analytical procedure for the right job. Also, it is important to be aware that the whole analytical process, not just the computerized systems, is used to generate numbers and that effective risk management is essential.

SPONSORED BY

Agilent
Trusted Answers

LC GC north america

Figure 1: DI model.

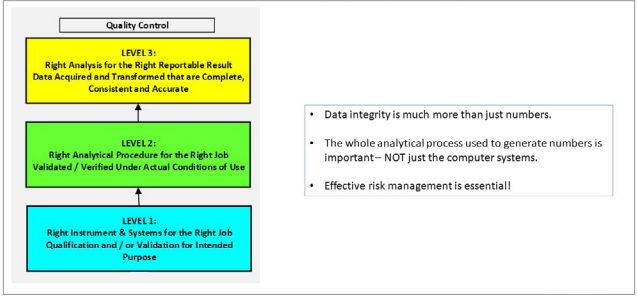


Figure 2: Examples of FDA action on blank forms and spreadsheets.

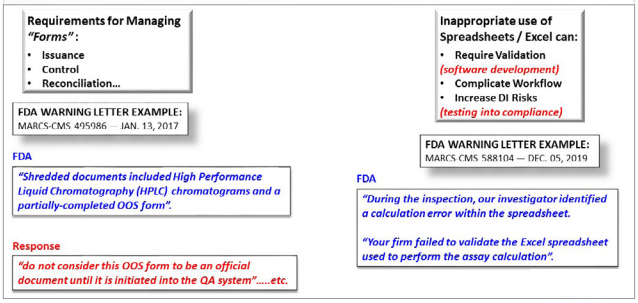


Figure 3: Peak integration.

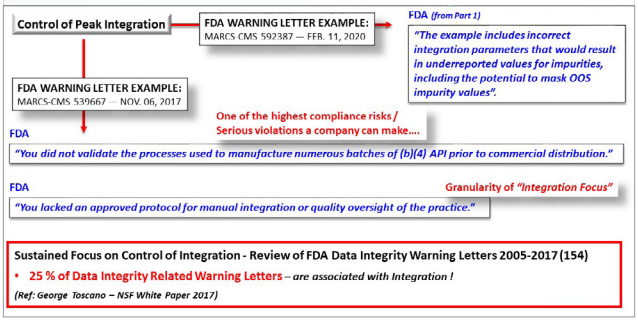
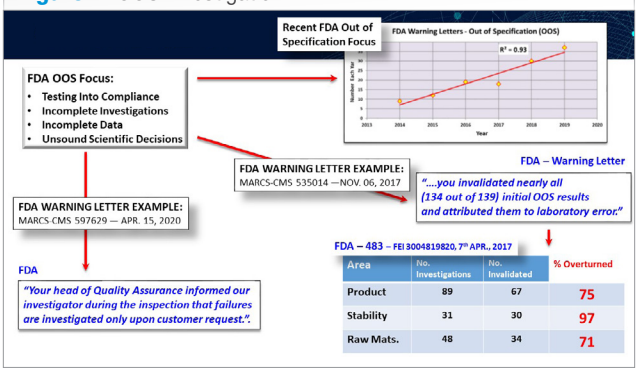


Figure 4: OOS investigation.



The review of significant FDA actions (i.e., warning letters and FDA Form 483 citations) on relevant topics is another useful step for preparing for a successful regulatory inspection by understanding the types of issues FDA focuses on (**Figures 2-4**). For example:

- On the management of forms, in a 2017 warning letter, FDA cited a company for shredding documents containing raw data. The response given was that the company did not consider these and similar documents to be official until initiated into the quality system. Clearly, this situation represents a lack of control over raw data documentation.
- On the use of spreadsheets, in a 2019 warning letter, FDA cited a company for using non-validated spreadsheets for decisions on compliance. All spreadsheets used for compliance decision-making must be validated against user requirements following a validation lifecycle. Some of the other complications associated with the use of spreadsheets are that they complicate the workflow, since they may involve transcribing data in and out of them, and that they increase DI risks, including testing into compliance.
- On process validation, in a 2017 warning letter, FDA cited a company for not validating the manufacturing processes used for numerous batches prior to commercial distribution.
- On peak integration methodology, in a 2020 warning letter, FDA cited the use of incorrect peak integration parameters that would result in underreported values for impurities, including the potential to mask out-of-specification (OOS) impurity values.
- On OOS investigations, in 2017 and 2020 warning letters, and in a 2017 FDA Form 483, FDA cited examples of incomplete failure investigations and inappropriate invalidation of test results (over 97% of results were overturned).

These examples demonstrate the types of issues and the level of granularity FDA gets to when assessing DI practices during laboratory inspections and are indicative of FDA's sustained focus on DI.

A review of all warning letters from 2005-2017 related to DI revealed that 25% were associated with peak integration. A common observation involves testing into compliance, or repeated re-integration of a peak by changing the integration parameters until passing results are obtained. Inspectors know that when manual integration is used to calculate peak areas, and when spreadsheets are used to automate calculations, there is a risk of testing into compliance.

The industry has become increasingly demanding and analysts are being driven to work long and repetitive days, so it is human nature for these types of scenarios to occur. Therefore, when either manual integration or spreadsheets are used, it is important to perform data process mapping to identify the parts of the process that are vulnerable, then to validate the parts of the process that are of high risk.

Figure 5: Technical controls – well defined roles.

Best Practices for Ensuring Compliance with 21 CFR Part 11 and Data Integrity

In addition to understanding the regulatory expectations from the point of view of an inspector, the prevalence of computerized systems means that preparing for a successful laboratory inspection requires the implementation of best practices and technical controls to ensure compliance with 21 *Code of Federal Regulations* (*CFR*) Part 11 FDA regulation for electronic signatures and electronic records. It is important to remember that software is not compliant out of the box. Compliance is a daily practice and is achieved through the proper application of procedures and specifications. Following are best practices to consider for ensuring DI, when implementing a chromatography data system (CDS) or other computerized system:

Audit trails. Audit trails are an essential part of record keeping, and every available audit trail should always be enabled. Electronic audit trails are indispensable, because they keep a contemporaneous record that is easy to review. Assuring that entries are descriptive by allowing user entry of comments, combined with effectively managed procedures, will help support thorough investigations. In addition, procedures for audit trail review should be in place that require a review of the audit trail as a part of any approval of results, to verify that the reported result is valid. Also, regular system-level reviews should be performed to assure systems are performing as expected.

Electronic signatures. Use of electronic signatures will speed up inspections and approvals. They are equivalent to physical signatures, but each user must have their own unique account that is never shared. Use multiple signature levels, control the access to the application of signatures, and make sure to enforce the order of signatures to support the documented workflow.

User access controls. 21 *CFR* Part 11 requires that user access to systems must be controlled. When setting up the system, it is important to grant permissions to users based on their job role and the specific workflow. Users should be given access only to those features required for them to complete their job, but no more. Daily users should not have administrative control of the system. The best practice is to establish group permissions that the system administrator can easily maintain and review. Periodic review of the configuration versus requirements specifications is mandatory to ensure continuous compliance.

Well-defined roles. It is important to clearly define and document the access privileges that your data system users have and to do it well. The goal is to prevent conflicts of interest. Start by defining each group of users and take your workflow into consideration to define actions each group of users should be able to perform based on their role. Use these definitions to configure system permissions and be ready to show that they are in sync with the documentation (**Figure 5**).

Analytical practices of interest. The inspector will be looking to see how the system is used in practice. Expect to be asked about any short or aborted runs in the system, as these indicate a problem with some analysis, and they want to see how you handle those problems. Consider what happens when a manual error is made, such as an incorrect number typed into a sample weight. Upon seeing this, an inspector will demand thorough documentation of how the issue was handled. They will want to confirm that electronic and paper records are contemporaneous and consistent with each other. Always make sure that OOS investigations are well-documented and scientifically sound to support your inspection.

> “Always make sure that OOS investigations are well-documented and scientifically sound to support your inspection”

Second person review of laboratory data. Finally, a second person review of laboratory data is essential to assuring compliance. The scope of the second person review should cover everything from the sampling to reporting of results. It is important that this is performed correctly and diligently by an experienced analyst. The reviewer should focus on sample preparation records and on manual data entered into the CDS sequence file (e.g., weights, purities, or dilutions, and should ensure that peak integration is correct, especially manual integration. The order of assessment of data files should be system suitability, standards, then samples. Lastly, the audit trail entries should be reviewed for GMP-relevant changes to data.