An Executive Summary

Addressing the Paradigm Shift in Regulatory Inspections

Humera Khaja
Software Compliance Program Manager
Agilent Technologies

Understanding the paradigm shift in a regulatory audit and what it means from an electronic system perspective.

Introduction

The term "FDA audit" can trigger many responses, including dread and panic, and can raise many questions. But, what triggers a regulatory audit? How has the FDA changed its auditing strategy and what are they focused on today? This paper explores what the paradigm shift in regulatory audits means for analytical laboratories, the FDA's goals during an inspection, systems that could be subject to inspection, mechanisms to ensure data integrity in analytical laboratories, and the type of documented evidence required to prove that software application systems have been validated.

Understanding the Paradigm Shift in Regulatory Audits

Although the focus on data integrity is not new, several factors have prompted a significant paradigm shift in regulatory audits. The factors include the evolution of globalized business models and documentation practices, a complex and interdependent supply chain, and increased availability and usability of data.

Figure 1 illustrates this new regulatory paradigm. In the past, formulation, testing, and manufacturing were typically carried out within the same country. More recently, product development has shifted overseas as companies outsource formulation, manufacturing, and quality control testing, and then ship products back to the United States for distribution and sale. Because of this changing business model, regulators no longer limit inspections to companies or firms located within the United States; they now also inspect foreign processing and manufacturing sites for products that are shipped to the United States. Drug and vaccine manufacturers, blood banks, food processing facilities, dairy farms, animal feed processors, and compounding pharmacies are all subject to regulatory inspections.

Figure 2 highlights the change in focus of the data review process. Since we have evolved from an industrial economy to a knowledge-based economy, the FDA is now more interested and focused on *data integrity* and *critical thinking* than ever before. This paradigm shift has put the focus on data integrity, which directly affects safety and product quality from the patient and consumer perspective.

SPONSORED BY

Agilent Technologies

LC GC north america

Figure 1: Regulatory paradigm shift.

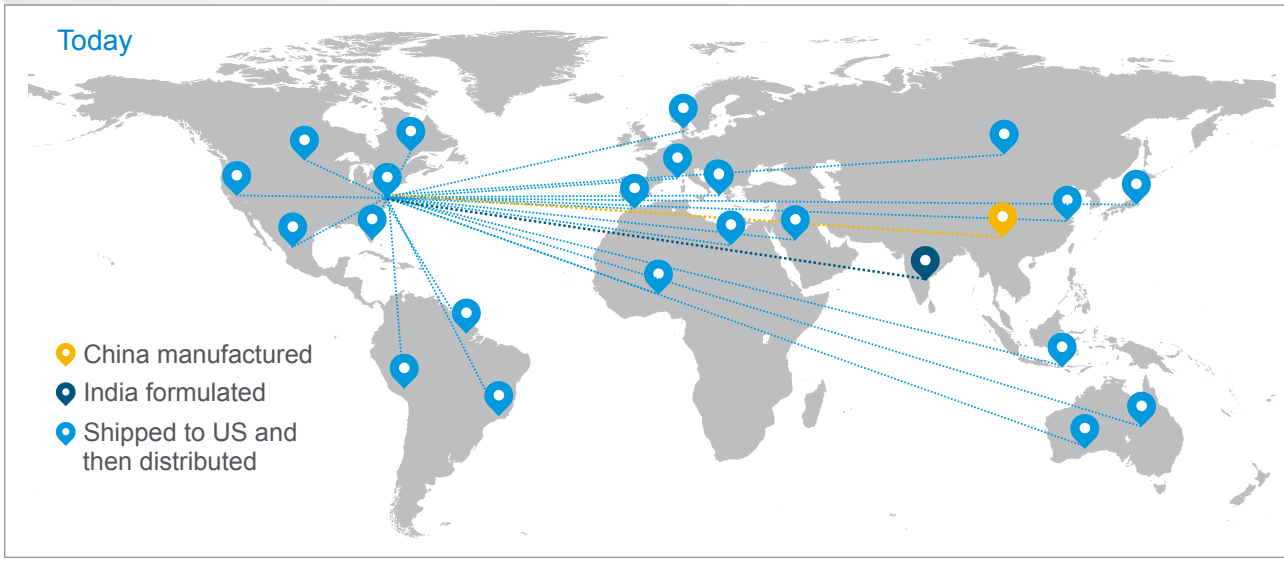


Figure 2: Regulatory paradigm shift.

- FDA's focus on critical thinking
- Expectation from regulatory agencies to move to electronic systems (traceability and transparency)
- Data integrity as a holistic risk-based approach of data in the data life cycle, through data governance program

Consequence
How severe would the outcomes be if the risk event occurred?

Likelihood
What's the chance of the risk occuring?

	1 insignificant	2 minor	3 significant	4 Major	5 severe
5 almost certain	5 medium	10 high	15 very high	20 extreme	25 extreme
4 likely	4 medium	8 medium	12 high	16 very high	20 extreme
3 moderate	3 low	6 medium	9 medium	12 high	15 very high
2 unlikely	2 very low	4 low	6 medium	8 medium	10 high
1 rare	1 very low	2 very low	3 low	4 medium	5 medium

What is critical thinking? The concept of critical thinking is explained in *International Conference on Harmonization* (*ICH*) Q8, Q9, Q10, and Q12.

- *ICH* Q8 discusses data by design, critical thinking, and process understanding for knowledge sharing.
- *ICH* Q9 describes quality risk management.
- *ICH* Q10 covers quality systems management governance.
- *ICH* Q12 focuses on feedback from consumers.

Once a product is released to the market, it will be used by consumers with different demographics, different geographies, and different genetic makeups. Adverse effects are unpredictable and can be very different from the data that was collected during the clinical trials. Thus, regulators expect drug companies to have a mechanism in place to easily gather and monitor consumer and patient feedback (e.g., adverse effects and complaints) after products have been released to the market. Hence, accountability now is different than before. It's all about engaging and improving on consumer feedback.

The Medicines and Healthcare products Regulatory Agency (MHRA) expects companies to move from paper-based systems (or even paper–electronic hybrid systems) to fully electronic systems that allow for traceability and transparency. While the FDA wants companies to choose the system that

best suits their organization, the agency has become impatient with companies that still use paper-based systems. In fact, it has been more than 20 years since the release of the 21 *CFR* Part 11 electronic records and signatures guidance and yet not all companies have transitioned to electronic-based systems.

Regulators are also expecting companies to take a holistic risk-based approach to data throughout its life cycle as part of a strong data governance program. For example, the sponsor company and CMOs are handling, analyzing, and trending data at different points in the data life cycle. Companies might have thousands of data points for one manufactured product. Among the questions that must be asked are:

- Is there a proper risk analysis in place?
- Is a proper risk analysis being performed that identifies the critical data points and focuses more on them?

One interesting result of the increased focus on data integrity has been the creation of Chief Data Officer positions within companies. The goal of the Chief Data Officer is to ensure risks about data is addressed.

Predicate Rule

Regulators stress that data must meet all the predicate rules and 21 *CFR* Part 11 requirements. The predicate rules are the degree to which data is **Attributable, Legible, Contemporaneous, Original, Accurate (ALCOA):**

- **Attributable.** In the context of paper records, *attributable* means having initials and handwritten signatures. In electronic systems, *attributable* includes logins, user IDs, and electronic signatures.
- **Legible.** In the context of paper records, *legible* means indelible inks must be used, and changes must be made with a single-line cross out that are initialed, dated, and justified with a reason for the change. In electronic systems, *legible* means enforcing saving, no overwriting of data, and no deletion of data. Furthermore, voided records must be visible, their changes captured in detail, and there must be a clear backup and archival mechanism for operational business continuity and disaster recovery.
- **Contemporaneous.** With paper records, *contemporaneous* means recording the date and time of the activity, no backdating, and no pre-completion of records. *Contemporaneous*, as it applies to electronic records, means records must be saved immediately after the data is entered, and there must be controlled access to the time and date stamps on network systems, servers, stand-alone systems, and workstations. In terms of the operating system, access to the server time must be controlled. All time and date stamps must be synchronized to certified time source.
- **Original.** *Original*, as it applies to electronic data, means that the data captured at the source system must be complete with its associated metadata, and the original records must be reviewed at the source.

Accurate. *Accurate* means data is correct, truthful, complete, valid and reliable.

Meeting Regulatory Requirements

What are regulators focusing on when they examine a company's data review process? What has changed from years ago?

The data generated in the 1980s and 1990s actually followed the predicate rule better than the data generated between 2000 and 2018. In the past, the original data was recorded in paper format and the predicate rules applied to huge stacks of data, results, reports, and related metadata. There was a direct comparison and review of data to the original source.

Currently, most companies follow an approval process that only includes the review of audit trails and reports, which is inadequate and incomplete. By limiting the approval process to audit trails and reports, many companies are failing regulatory audits. Regulators expect companies to review every log and audit trail that affects the quality of the results set. So, what should a company's data review process include to meet regulatory requirements?

For starters, the electronic data generated at the source system must be reviewed in conjunction with the associated metadata and audit trails. Regulators also expect that companies review their *Server activity logs, Operating system-specific activity logs, Application-specific activity logs, Instrument error logs,* and *IT tickets* to check backend database changes for modified or deleted data. The main takeaway is to not limit the review and approval process to results and audit trails (see **Figure 3**).

Inspection Goals and Targeted Systems

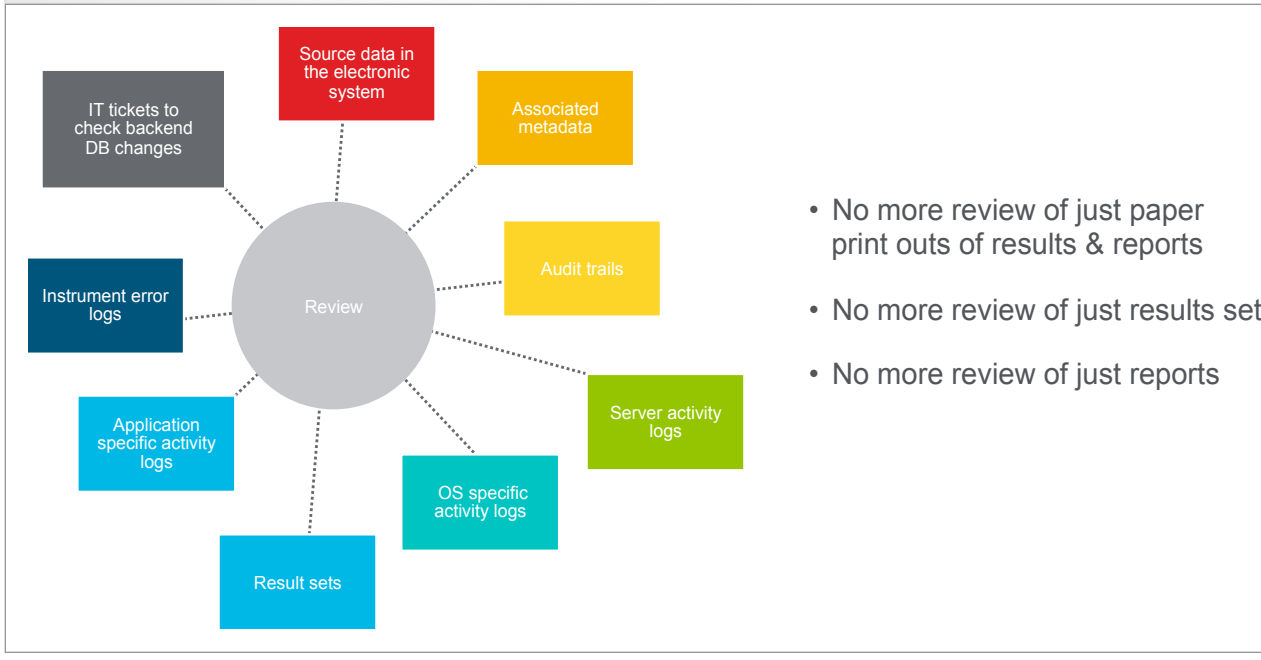
A surveillance audit can be triggered when the FDA has concerns about the company's CGMP compliance, which is often based on a previous inspection. Other triggers include:

- Patient or consumer complaints
- A whistle blower contacting the FDA
- New potential for cross-contamination arising from changes in the process or product line, the introduction of new technology, or the addition of new equipment or new facility that requires updates to the SOPs and additional training of personnel.

Compliance inspections are triggered as a follow-up to a previous surveillance inspection once the company has stated that they have addressed certain observations. These can be either "For cause" inspections (which require a full inspection approach) or a follow-up from previous regulatory actions (e.g., recalls and warning letters).

During an inspection, regulators have several goals. They want to determine if inspected companies are operating in compliance with applicable CGMP requirements and to provide input to companies during inspections to improve their compliance with respect to regulations and data integrity. They want to reduce the risk of adulterated products from reaching the marketplace and to increase the communication and transparency between the industry and the agency while

Figure 3: Change in focus of data review process.



providing regular feedback on the continual improvement and status of the company's CGMP compliance.

Regulators are interested in evaluating different systems as part of any inspection, including Quality systems, Facilities, Equipment systems, Production systems, Packaging and Labeling system, and Laboratory control system. At minimum, two systems will be evaluated, with one being a Quality system.

Laboratory control systems that consist of a software-based system and an Information management system are frequently targeted in inspections. This is one of the most critical systems in the product workflow. An example is the Agilent OpenLab CDS and MassHunter.

Ensuring Laboratory Data Integrity

To ensure data integrity in an analytical laboratory, regulators want to see if a company has proper prevention mechanisms in place, including strong quality agreements with their Contract manufacturing organization (CMOs) and a control environment for implementing changes in laboratory operations. Any changes made to the functionality of the application should be captured by a change control process with proper review and approval procedures in place. Regulators will also want to confirm the role of Quality Assurance (QA) and their involvement in the overall process.

System configurations should be validated against well-defined Configuration Specifications based on a business process and any new functional changes should be validated in the control environment (e.g., development, test and validation environments). Many companies are focused on validating user and functional requirements and not on configuration verifications. Identifying the required configurations to enable specific technical controls is the key to any system validation (e.g., enabling audit trails, version controls, and system logs).

Suggested Mechanisms to Ensure Data Integrity in Analytical Laboratories

From the perspective of prevention, regulators want to see what mechanisms are in place to ensure that analysts follow the approved procedures, starting with validation or verification of analytical methods. Every firm should have a policy on method validation, and method validation packages that are consistent with *ICH* and FDA guidelines. There should also be a policy in place to allow for the verification of any *USP* methods that may be in use. Control mechanisms should also be in place to track samples and to ensure that the required testing is performed on each sample.

Controls should also be in place to ensure that the laboratory analysis is captured in enough detail to confirm all steps have been followed and that there is a documented investigation of any unexpected discrepancies. QA must be involved in these investigations and regulators will want to know that the level of QA review is adequate and timely. They also want to make sure that the result data is traceable back to the raw data with no evidence that data is not being used because of an atypical or failing result and that there are controls in place to prevent detection, deletion, or overriding of raw data.

Regulators will also want to make sure that there is adherence to out-of-specification procedures, including timely completion of any investigations. The investigation process needs tp be consistent with any retesting performed and

backed up by statistics (e.g., outlier testing) where appropriate. Modern systems like OpenLab CDS have the ability to flag out-of-spec records, and thus the FDA and MHRA are pushing for modernized electronic systems.

Additional control mechanisms also need to be in place to support stability programs and analytical methods used for stability analyses. Mechanisms should be in place to trend, monitor and review the stability data and failed result data is reported within a few days of detection.

Finally, a detection mechanism must be in place to make sure that SOPs are reviewed and updated (when necessary) in a timely manner and that users are properly trained and the training is documented. Data in the source system and associated meta data needs to be reviewed prior to each batch release. Instrument error logs should be reviewed. Regulators also want to make sure that the following items are in place:

- a recipe or a method management system as well as data monitoring mechanisms that flag anomalies
- an instrument error alarm mechanism that will notify the appropriate user groups.

Documenting Evidence of System Validation

Having addressed detection and prevention mechanisms, the next step in the process is providing documented evidence of system validation. Validation is nothing more than making sure that the system performs according to its intended use and per pre-defined specifications, from the beginning of the project through completion. Validation is a dynamic inter-related process starting from the planning stages through the maintenance and operation phases, and companies must consider all the documentation that flows throughout the entire process to ensure that the system is maintained in a validated, traceable state over its lifetime.

Figure 4 lists many of the documents that must be drafted and approved by appropriate stakeholders to support system validation. A sound validation process includes risk assessment and validation plans as well as a data migration plan, if applicable. Supporting documents can be divided into two types: Specifications and Qualifications, all starting with a risk analysis that is based on the well-defined SOP. The most important document in this process is the validation summary report, which auditors typically request first because it provides a complete insightful picture of the validation efforts. The key objective is to maintain the system in the validated state for the entire period of its use and to maintain the quality and assurance of the validation documents through traceability using a traceability matrix.

FDA 483 Observations

An FDA 483 Observation is issued to firms at the conclusion of an inspection when the investigators have observed conditions that in the auditor's judgment may constitute as violations to the Food Drug and Cosmetic (FD&C) Act and related Acts. One of the most common 483 observations are related to CMOs not reporting failing results to sponsor companies.

FDA investigators are trained to ensure that each observation noted on the FDA Form 483 is clear, specific, and significant. Observations are listed in the order of importance within each system. Where repeated or similar observations are made, they are consolidated under a unified observation.

FDA now employs common language for findings to ensure consistency among various inspections. This common language also enables them to determine if events are repeated observations. Repeated observations are of particular interest to FDA as they may indicate the firm's inability to address its problem areas.

Figure 4: Validation documents.

	Specifications	Qualifications
Risk Assessment Plan (RS)	User Requirement Specification (URS)	Infrastructure: Installation Qualification (IQ)/ Operational Qualification (OQ)
Validation Plan (VP)	Functional Requirement Specification (FRS)	Application Installation Qualification (IQ)
Data Migration Plan (if applicable)	Design Specification	Operational Qualification (OQ)
	Sofware Design Specification (DS)	Performance Qualification (PQ)
	Software Architecture Overview	Requirement Traceability Matrix (RTM)
	Configuration Specification (CS)	Validation Summary Report* (Test results, Protocol variations & Bug summary)
		System Release Notification

Q&A from the Webcast

How often does FDA audit outside of the United States?
The number of applications that have foreign data are high for new drug submissions and latest statistics indicate it's about 60% or more.

To eliminate the time zone issues, regional language, and logistical issues, FDA has opened dedicated offices in India and China and many other foreign countries.

What criteria is included in an FDA audit for data management?
Regulators want to see that the information submitted in the form of "Results sets" and/or "Reports" match the electronic source data. In addition, they want to check if the active users have been trained on those SOPs, whether deviations from the SOPs were promptly and clearly documented, and whether the SOPs have been followed effectively. And finally, there are some questions that need to be addressed with respect to protocol, for instance.

How is the protocol followed? Was everything that was predefined in the protocol executed successfully? Were the deviations documented? And if the new software implementation was released with exceptions and known deviations, have they been documented with appropriate justifications prior to release?

How can data be validated if it's taken from a validated method?
You do not validate the data; you validate the method and review the data (result sets, reports, etc.) that was generated using the validated method.

Do GLP laboratories need to document every method development step?
You should document method development through its final version as well as the steps used to validate the method in the GLP environment. Adverse effects reported by consumers after the drug is on the market is different from the data collected during the clinical trials. If you want to backtrack after an adverse effect to see how your method has been tweaked, such documentation helps you know exactly which changes were made to which version of the method.

All the steps from the method development phase through method validation should be clearly documented in a GLP environment. This is important because the adverse effects reported by consumers after the drug is been released to the market can be very different from the data collected during the clinical trials. In these scenarios, it becomes necessary to investigate and retrace previous method versions to identify the root cause.

What are the main goals of an inspection?
One main goal of an inspection is to make sure that the company is operating in compliance with respect to data integrity, since this directly affects patient safety and product quality. A Form 483 can be a blessing in disguise, especially when you need improvements in your systems, workflows, and SOPs. Companies should view these inspections as a form of communication with the regulators for continual improvements.

How do you prove that you have properly reviewed audit trails, logs, system errors, and all the critical data?
It depends on the kind of system you have. Most modernized electronic data systems have the ability to review your audit trails and activity logs within the system itself. That data (result sets, chromatograms, audit trails, activity logs, etc.) along with the e-signatures can be exported into a report and submitted for final QA approval.

What is the data lifecycle?
The data lifecycle differs by context and workflows. For example, when you're trying to validate your application, the data lifecycle starts at the execution of your protocol and the data that has been collected during the execution of your test protocols.

Do regulators have right to copy the data from our software to their hardware or CD?
Yes, they have the right to copy the data and also analyze the data in whichever form they want to.

Is it mandatory to review the data for every batch before release?
Yes, it is, and the SOP should clearly state how the data should be reviewed before the batch release.

A company's response to the observation should be timely; typically within two weeks of receiving a 483. It is expected that the firm will consider addressing not only the specific observations, but also related systems that might be affected. It is expected that all commitments to address the observations are achieved by the company and that any significant changes to the commitments made are communicated back to the FDA in a timely manner.

Conclusion

Auditors want to see that prevention and detection mechanisms are in place; that the source electronic data is available in a secure and controlled environment, has been properly reviewed, contains the metadata and audit trails, and that systems have been properly validated for their intended use by both sponsors and any contract manufacturers involved. It is important that methods are validated by the sponsor and are re-validated by the contract manufacturers. Regulators want to see a holistic approach to data integrity that includes both sponsors and contract manufacturers. In addition, regulators expect companies to establish a Data Governance and Data Integrity Program that is supported by SOPs, training, a thorough data review process and validation of the data systems.