JULY 2017

REDUCE RISK IN A DATA INTEGRITY WORLD: APPROACHES TO ENSURE COMPLIANCE

Sponsored by

Agilent Technologies

Presented in partnership with

LCGC

UBM

LCGC®

485F US Highway One South, Suite 210,
Iselin, NJ 08830
(732) 596-0276

LCGC North America (ISSN 1527-5949 print) (ISSN 1939-1889 digital) is published monthly by UBM Life Sciences, 131 West First Street, Duluth, MN 55802-2065. *LCGC Europe* (ISSN 1471-6577) and *LCGC Asia Pacific* (ISSN 1754-2715) are published monthly by UBM EMEA, Hinderton Point, Lloyd Drive, Cheshire Oaks, Cheshire CH65 9HQ, UK. Issues are distributed free of charge to users and specifiers of chromatographic equipment.

To subscribe, call toll-free 888-527-7008. Outside the U.S. call 218-740-6477.

INTRODUCTION

With the release of the long-awaited *Data Integrity and Compliance with CGMP Guidance for Industry* in 2016, the US Food and Drug Administration revealed a change in its current thinking: if an activity happened, it must be documented. For instance, if an injection is started—and the resulting data are unexpected for the sample—it must be recorded.

This principle places additional emphasis on the importance of data integrity in computerized systems and validation, especially as it relates to cGMP regulations. *LCGC*'s new eBook, *Reduce Risk in a Data Integrity World: Approaches to Ensure Compliance* (sponsored by Agilent Technologies), offers important insight about how laboratories can ensure their data are secure and their systems comply with FDA guidelines.

The first article, "Demystifying Software Validation," summarizes the key points from a recent *LCGC* webcast, highlighting the differences between software qualification and validation, the kinds of systems that require validation, when revalidation is necessary, and how one knows when enough validation work has been completed. The accompanying frequently asked questions (page 10) offer detailed information to clarify confusing issues related to software validation.

Next, R.D. McDowell, editor of the "Questions of Quality" *LCGC Europe* column, director of R.D. McDowall Ltd., and *LCGC Europe* editorial advisory board member, shows that a hybrid top-down/bottom-up approach to validation is beneficial for ensuring data integrity. He stresses that data integrity requires a multidisciplinary approach to avoid vulnerabilities.

Last, McDowell teams up with Paul Smith of Agilent Technologies to explore a life cycle risk assessment of high performance liquid chromatography instruments, specifically focusing on what can go wrong with a qualified liquid chromatograph during the operational phase. They also discuss how system suitability tests and their link to design qualification and operational qualification can mitigate some instrument problems.

While data integrity and the validation of software and computerized systems can be daunting, if staff members are well informed about points of confusion and the validation process is approached logically, one can achieve compliance in a less stressful manner.

Demystifying Software Validation:

What is It Really and When Do I Need to Do It?

All attendees will receive a FREE executive summary of the webinar!

ON-DEMAND WEBINAR

View for free at www.chromatographyonline.com/lcgc/validation

EVENT OVERVIEW:

The term "software validation" can trigger many responses, including dread and confusion. What is the difference between *qualification* and *validation*? What systems need to be validated? When do systems need to be revalidated? How much validation work is enough? In addition to answering these questions, this webinar will provide a foundation for thinking critically (and correctly) about system definitions, software validation, including discussions on the differences between qualification and validation, risk-based validation, and revalidation. You'll learn from Loren Smith, Agilent's software compliance expert and a University of California Berkeley instructor with nearly three decades of regulated software experience.

Who should attend:

- Lab managers
- Scientists
- Technical specialists

Webinar participants will learn about:

- Regulatory requirements and standards for software validation
- Applying critical thinking skills to what you hear or read regarding software validation
- Evaluating the validated state of your current laboratory software and associated processes
- Taking a practical approach to maintaining systems in a validated state
- When to and when not to rely on your vendors to support your validation

Presenter:

Software Compliance Program Manager
Agilent Technologies

Moderator:

Kate Mosford
Managing Editor
LGGC Europe

Sponsored by

Agilent Technologies

Presented by

LC|GC

For questions contact Kristen Moore at kristen.moore@ubm.com

TOC
Table of contents

REDUCE RISK IN A DATA INTEGRITY WORLD: APPROACHES TO ENSURE COMPLIANCE

LCGC

UBM

DEMYSTIFYING SOFTWARE VALIDATION

Learn what software validation means for you and your lab.

Introduction

The term "software validation" can trigger many responses, including confusion and even anxiety. What is the difference between qualification and validation? Which systems need to be validated? When do systems need to be revalidated? How much validation work is enough? This article provides a foundation for thinking critically about system definitions and software validation, including discussions on the differences between qualification and validation, risk-based validation, and revalidation.

Definitions: Data Integrity, Qualification, Validation?

Labs often have questions about software validation. A good place to start gaining clarity on this topic is to define three terms that are often confusing: data integrity, qualification, and validation.

Data integrity. Robert D. McDowall, PhD, provided a useful definition of data integrity in a 2013 article (1). He stated, "In the context of laboratory data integrity within a GMP environment, this can be defined as: generating, transforming, maintaining and assuring the accuracy, completeness and consistency of data over its entire life cycle in compliance with applicable regulations."

When using a computerized system to generate and maintain regulated records, the system and its validation are the foundation for all other related data integrity activities.

Qualification. One can consult FDA's *Glossary of Computer System Software Development Terminology* for a detailed definition of *qualification*, specifically installation qualification (IQ) and operational qualification (OQ). IQ is simply determining that a system was properly installed and configured, while OQ establishes that systems are consistently operating within established limits and tolerances.

Software validation. According to the same FDA document, *software validation* determines the correctness of the software with respect to the user's needs and requirements and is accomplished by verifying each stage of the software development life cycle (2).

A system may be correctly installed and its operations may be qualified, but these actions alone do not ensure correct results

for every process run on the system. Rather, each individual process must be validated to determine that the system generates predictable, repeatable results, whether it is drug manufacturing or another activity such as quality control.

It is important to understand that qualification and validation are interrelated (see **Figure 1**). IQ/OQ are necessary, but are not sufficient for system validation on their own. Likewise, system validation is necessary, but it cannot validate the process alone. While each piece is a required element of the software validation process, individual items are not sufficient in and of themselves to meet the complete regulatory requirements.

What Are the Regulatory Requirements for Software Validation?

In April 2016, FDA released its latest (and long-awaited) thinking on data integrity in computerized systems as it relates to cGMP regulations (3).

FDA evaluated the regulatory requirements and developed relevant questions with answers about the agency's thinking on several subjects. One question asks, "*Does each workflow on our computer system need to be validated?*"

The short answer is yes. The guidance explains that if one does not validate the computer system for its intended use, it is impossible to know if the workflow runs correctly. This underscores that system validation is important to, but not the same as, process validation.

FDA references supporting regulations for this thinking. In 21 *CFR* Parts 211.63 and 211.68, the FDA talks about the system's intended use and that the degree of verification should be based on the system's complexity. FDA also cites 21 *CFR* Part 211.110, which discusses process evaluation based on the degree to which it can affect a drug product.

Also in its 2016 guidance, FDA recommends certain controls to manage risks to computerized systems, and the agency's top three priorities when it considers "risk" are patient safety, product quality, and data integrity (3).

In terms of controls or processes that are appropriate for system validation, FDA returned to an old concept in its 2016 document (3): a system is more than just software and hardware. A system also includes the people, processes, and the documentation associated with it. Thus, when FDA uses the term "system" and discusses system validation, one must consider the much larger context of validating the entire process.

When Does My System Need to Be Revalidated?

Often, if not always, the concept of revalidation causes anxiety, perhaps because these projects can be large, long, expensive, and labor intensive.

FDA's *General Principles of Software Validation* discusses revalidation, suggesting that when systems are altered, those changes must be studied not just for the nature of the change itself, but also for any potential impact and unintended

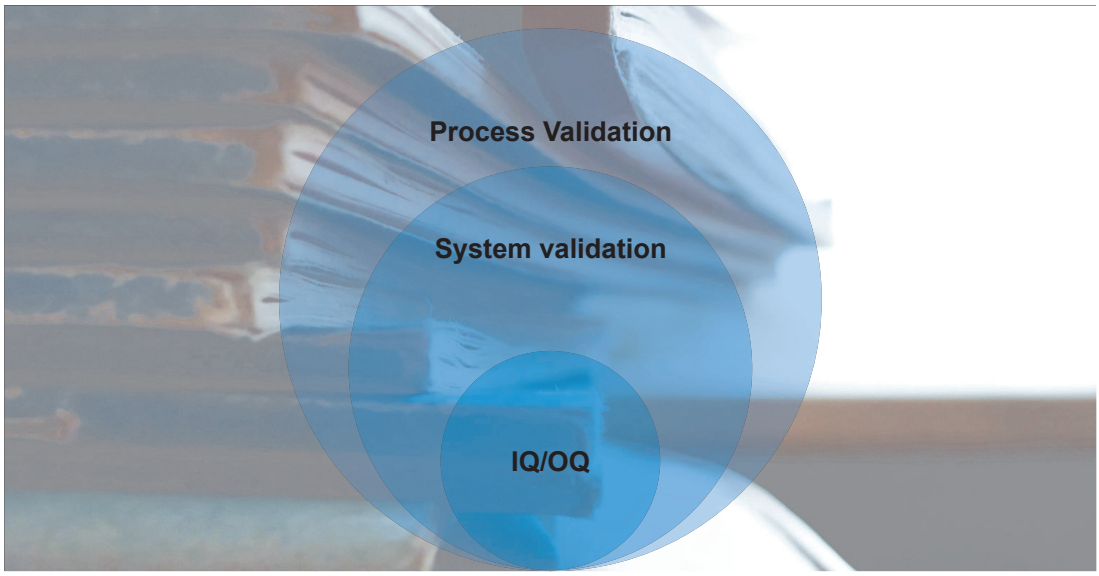


Figure 1: How qualification and validation are related.

consequences the change may introduce across the whole system (4). In a validated environment, such an evaluation normally includes regression testing.

Many individuals try to avoid changes (including software updates) to computerized systems to avoid the need for revalidation. At some point, however, system fixes or improvements will become important enough to warrant an update and any required revalidation effort. The longer one waits to update a system, however, the larger the scope of changes and the greater the validation effort required. Thus, it is important to consider keeping systems current. If a system has been in use for a year and updates are implemented, the validation effort will probably not be as significant as if five years' worth of updates were installed all at once.

How Much Validation Work Is Enough?

Many firms want to know how much validation work is sufficient and whether they can use IQ/OQ vendor packages.

Vendors like Agilent often offer such packages to help customers qualify their systems. IQ/OQ activities are designed to ensure systems are installed and configured correctly and operate as intended. Is running an IQ/OQ package sufficient for system validation?

Monica Cahilly, a consultant and trainer for FDA who has worked extensively with the agency on data integrity, stated at a 2015 workshop that companies cannot abdicate their responsibility for validation to a vendor (5). For one thing, the IQ/OQ activities are limited. As represented in **Figure 1**, IQ/OQ is necessary, but not sufficient, to establish validation of the system or the process.

Figure 2: A model for vendor audit.

The next question often raised is: How can the validated state of current laboratory software and associated processes be evaluated?

Considering current FDA discussions about computerized system validation in the context of process validation, one should start by making an inventory of processes happening in the laboratory. Standard operating procedures can be used to review various types of testing, chemical analyses, instrumental analyses, and methodologies that occur.

Then, develop a list of instruments, software, data management systems, and laboratory information management systems (LIMS). Systems shared by multiple processes may have some overlap, so it may be possible to conduct a core validation for the LIMS, for instance, and expand upon any unique details for a particular process.

After the inventory step is completed, plan and prioritize the work based on risk in terms of patient safety, product quality, and data integrity, though not all systems will have the same degree of risk in these areas. For example, one may have a system for administering staff training, which is lower risk than a manufacturing execution system that would directly influence product quality. Clearly, higher-risk processes merit more validation work than lower-risk processes.

Finally, get the work done with the understanding that the longer firms wait to update their systems, the more work will be required later on and the greater

the chance of missed vendors' defect corrections and functional software enhancements.

How Can My Vendor Support My Validation?

FDA's *General Principles of Software Validation* suggests that manufacturers and laboratories can use vendor audit information as the starting point for their required validation documentation (4).

Ideally, audits should occur before companies acquire their systems or at least before validation begins to fully understand the vendor's process.

How are vendor audits conducted? In a 2006 technical article, IT quality and compliance expert Jacques Mourrain, PhD, introduced a model for vendor audit that is more effective and time efficient than the checklist method (see **Figure 2**) (6).

The model evaluates and scores six areas, starting with procedures and quality management systems, then branching out to testing, software development, infrastructure, and training/personnel. Mourrain's systematic approach allows companies to plan for and execute the vendor audit in an objective and organized manner.

Vendors are scored, and the results are then used to determine vendor-related risks or validation work. The model can be used to conduct a side-by-side comparison of multiple vendors and make a decision about which vendor's process works best for a given situation.

Summary

Systems changes are bound to happen, and when they do, firms must study those changes and revalidate systems, ensuring that the risk to patient safety, product quality, and data integrity are considered in that order. A systematic vendor audit is a helpful tool in this process. Waiting to complete software updates and revalidation is problematic; the longer changes are postponed, the more complex and burdensome the updates and the revalidation process will be.

Finally, qualification is not validation. Qualification, while necessary, deals with proper system installation and operation. Validation goes further to include the FDA's current focus on the context of the process.

References

(1) R.D. McDowall, "FDA's Focus on Laboratory Data Integrity: Part 1," Scientific Computing (Sept. 2013). http://www.scientificcomputing.com/article/2013/09/fda%E2%80%99s-focus-laboratory-data-integrity-%E2%80%93-part-1

(2) FDA, *Glossary of Computer System Software Development Terminology,* https://www.fda.gov/iceci/inspections/inspectionguides/ucm074875.htm

(3) FDA, *Data Integrity and Compliance with CGMP Guidance for Industry*, https://www.fda.gov/downloads/drugs/guidances/ucm495891.pdf

(4) FDA, *General Principles of Software Validation; Final Guidance for Industry and FDA Staff,* https://www.fda.gov/RegulatoryInformation/Guidances/ucm085281.htm

(5) M. Cahilly, Workshop on Data Integrity and Industry Practice, Peking University, Beijing, June 22–23, 2015.

(6) J. Mourrain, "Apples and Oranges: Comparing Computer Systems Audits," *Ther. Innov. Regul. Sci.* **40** (2), 177–183 (2006).

SOFTWARE VALIDATION: ANSWERS TO FREQUENTLY ASKED QUESTIONS

Question: How is change control used to keep software validated?
Answer: It is normal that any system needs to be changed over time because of changes in business needs and software updates. The objective is to make sure that those changes are described properly, that the impact and risk of that change is well understood, and that there is documentation to support that assessment of the impact and the risk. A determination is then made regarding the degree of testing or revalidation work that would be required to re-establish that the system is still behaving according to its intended use in the process where it's going to be used.

Question: How much validation effort is appropriate for custom reports?
Answer: According to the International Society for Pharmaceutical Engineering (ISPE) Good Automated Manufacturing Practices (GAMP) guidance, custom reports are category 5; being unique to a particular lab, they are of the highest level of configurability or customization. Thus, custom reports require fairly extensive validation to ensure that any custom calculations are working properly. Negative boundary and stress testing should be used to make sure that the report and the reporting environment would reject values that don't make sense—for example, characters instead of numbers.

Question: Once a vendor has been audited, is there a recommended time within which the vendor should be re-audited?
Answer: No. The frequency of re-auditing a vendor is based on many factors such as how well the vendor performed in the last audit; the relative risk of that system to patient safety, product quality, and data integrity; and any kind of problems that you may have had with that system.

If the vendor performed relatively well in the last audit, you can justify lengthening

the amount of time before the next audit. If the system has been relatively stable with relatively few problems, you may be able to justify going as long as three years before you do another audit. Two years is a common rule of thumb, and labs can shorten or lengthen that time depending on the factors described here.

If you plan a software update that adds a significant amount of new functionality, it would also be a good time re-audit the vendor.

Question: If there is an update for my software available and I choose not to install the update because my system is validated and I don't want to revalidate it now, will the FDA write me up for not updating my system?

Answer: Not directly. The FDA does not require keeping systems on the very latest version of software. However, if the FDA finds an issue that is related to and addressed by an update that they are aware is available, you can probably expect to hear from them.

Question: How do I audit the software validation status of a contract manufacturer?

Answer: Auditing the validation status of a contract manufacturer is no different from auditing the systems within your own organization. You would review their infrastructure and how they are defining and validating their computer systems within their particular environment for their intended uses. This process includes how they do their own internal audits for their systems and for their suppliers. It is not generally necessary to do a second- or a third-level audit of your contract manufacturers' suppliers. That audit would be their job and you would expect them to have their own audit programs.

The level of detail needed should be based on your contractual relationship with the vendor and the degree to which regulatory obligations have been transferred to your contract manufacturer. For example, the vendor may be doing manufacturing for you but using your computer systems, which presumably you would have already audited. In that case, there would be less need to audit their computer systems.

If the vendor is using its own systems, it is important to pay attention to data transfers from its systems to your systems because those data transfers are vulnerable to data transfer failures, missing data, and other data integrity concerns.

Question: Does the FDA recognize the use of electronic validation records and electronic signatures?

Answer: Yes, since 1997. The FDA does establish that any electronic records including validation records can be considered the equivalent of paper records, and any signatures on those electronic documents can be considered the equivalent of handwritten signatures.

It is common for validation work to be done at one facility, with the quality oversight of that work done at a physically

different facility using electronic transfer or review of validation documentation.

Question: How would you recommend executing the validation of a software product? Does it depend on the software's intended use?
Answer: Validation is best executed by the staff that will be using the system regularly. They best understand the use of the system in the context of the lab's process, and will be able to pay attention to details that an IT or validation organization might miss. It is also an effective way for lab staff (as opposed to IT) to take ownership of the system.

Question: How often should a system be requalified by performing IQ/OQ? Some vendors state the qualification should be performed early.
Answer: The timing of the requalification should be based on when changes—such as installing new software or updates to the operating system—are being made. The nature of the change and the severity of problems with the system since it was last qualified also determine the timing of requalification. Some companies perform annual IQ/OQ to address minor periodic system changes pushed through by IT, such as Microsoft security patches. Requalification rationale, timing, and procedure should be documented so the FDA can understand how you made your decisions based on your organization's needs.

Question: Is product and process specification validation equal to analytical method validation plus qualification of liquid chromatography (LC) systems and software?
Answer: They are similar, but not equal. Method validation validates the science behind the analytical testing process for a particular product. Method validation is concerned with either confirming the identity, quantity, and strength of a particular compound, or looking for impurities in a sample.

A computerized system will likely be used for data acquisition and data analysis so method validation alone is not a replacement for the system validation. However, the method and system validation are related because the LC system and software validation occur in the context of the methods used.

Question: Is process validation relevant to industries outside the pharmaceutical industry?
Answer: Yes. The concept and practices of validation translate across industries. Whether it's pharmaceutical or food quality testing, food safety testing, forensic testing, or environmental testing, you want to be sure that the results produced by your system are consistent, repeatable, and trustworthy.

Food safety and environmental testing can directly impact human health and thus warrant validation concerns similar to pharmaceutical testing. Across all industries, consumers expect consistent,

reliable, and safe products. For example, in the case of fuel production, consumers expect consistent fuel quality for their automobiles.

Question: Please provide an example of how process validation covers an area that systems-level validation would not.

Answer: A chromatography data system (CDS) provides a good example. In the most basic sense, a CDS is designed to acquire, analyze, and report on data from an instrument such as a liquid or gas chromatography system. In a generic sense, if that functionality has been validated, you could say that the system has been validated. However, that does not validate the process for analysis of a particular product, including steps such as sample preparation. Process validation requires confirmation that the CDS works properly within the context of the testing of a particular drug product.

Question: Are there any major changes in the new 21 *CFR* Part 11?

Answer: The regulation itself has not changed since it was originally issued in 1997, however, in the draft guidance released in April of 2016, there were changes evident in the FDA's thinking. Previously, the FDA had conveyed that if an activity was not documented, it never happened. The FDA is a document-centric organization and thus when they do inspections, they appropriately want to look at documentation.

In the past, the FDA has explicitly stated, "For computerized systems, the record of that computerized system existed when that record was committed to durable media," meaning when that record was printed or saved to disk. In the 2016 guidance, the FDA now states, "The record exists when the data is generated," an important shift. The reason why the FDA made this change is that many labs around the world use real-time data previews as instruments generate data. If the operator sees unexpected data generated, they may interrupt that run and thus, under the previous guideline, those data would have never existed because they had not been captured or saved to disk. The FDA intent is to ensure that if "it happened," then it must be recorded. If an injection was started—even if the operator sees that the data coming off of the instrument is not what they are expecting for a particular sample—that injection still happened and that injection still needs to be recorded.

Companies may be fearful of recording data associated with a product problem. However, finding problems is an important purpose of labs. It could also indicate a sample preparation or instrumentation problem that should be addressed.

WELCOME TO THE BRAVE NEW WORLD OF CSV?

R.D. McDowall

Data integrity issues are changing the way that we should be undertaking computerized system validation (CSV) of our chromatography data systems. Do you understand what is required in the brave new world of CSV?

"Our CDS is validated" is a common statement I hear when training or consulting. Past articles have discussed different aspects of the validation of chromatography data systems (CDSs) and featured some case-study examples of validation from quality control or bioanalytical laboratories (1,2). The aim of articles such as these is to help readers understand that computerized system validation (CSV) is not rocket science or brain surgery, but the application of good software engineering practice principles in the context of a regulated chromatography laboratory. CSV is not a typical skill for a chromatographer, but the principles are not difficult to comprehend and can be easily understood over the course of a validation project. However, the CSV world is changing—let us see how.

The Way it is Now

Traditionally, CSV in a regulated context uses a rather old-fashioned life cycle V model to explain how to perform a CDS validation; this is presented in **Figure 1** and has been adapted for a laboratory system such as a CDS. In overview, the validation plan and validation summary report are the controlling documents that define the work life cycle phases to be undertaken and report what was actually performed. In more detail, the validation plan will define the tasks to be performed in each phase together with the documented evidence required to support the claim that the system is validated. The people involved with the validation are listed along with their responsibilities. The report should mirror the plan and describe the actual work performed plus explain any differences from the validation plan.

On the left-hand side of the figure, the specification of the system is contained in a user requirements specification (URS), in addition to how the CDS application will be configured in a document strangely called the *configuration specification.*

Together, the two documents define the intended purpose of the system as required by the regulations (3,4). The underlying computer platform and operating system, followed by the installation of the various components of the CDS are installed, qualified, and integrated into a basic unconfigured system shown at the bottom of the V in Figure 1. Next, the CDS software is configured as defined in the configuration specification; for example, by turning on or off functions in the software to change the business process to match the laboratory requirements; the use of electronic signatures; defining the user types and the corresponding access privileges; functions to protect electronic records, etc. Finally, the configured CDS is tested against the requirements in the URS. As shown, there is symmetry of the V model with an activity on the left-hand side that is matched by a corresponding activity on the right. This is similar to a chemical reaction—validation does not work unless the two sides of the equation (or V) are balanced.

And now, hey presto, the system is validated! Or, it would be if you have performed tasks like process redesign; traceability of requirements; writing procedures to use the system; writing procedural controls to plug regulatory compliance gaps (workarounds); IT support agreements; training users; implementing custom calculations; and designing custom reports; however, the bulk of the work is outlined in Figure 1 (5).

What a V model does not describe is how the application should be introduced into a laboratory.

Process, Process, Process

One of the items not covered in Figure 1 is the understanding of the chromatographic process and how it can be redesigned using the introduction of a new version of an existing CDS or a new CDS to make the process more efficient. Typically, this would be done so that electronic signatures and electronic working can be used, with the elimination (or perhaps extermination would be a better word) of all those horrible spreadsheets that slow down the process. This never ceases to amaze me. An organization spends millions on a shiny CDS that is capable of amazing things only for those in the laboratory to print out piles of paper and then enter data manually into a spreadsheet and carefully check the entries. Perhaps if Dante were to rewrite his *Inferno* and set it in modern times, this would be his vision of chromatographic hell. Endless manual data entry and transcription error checks performed forever in an ocean of paper. This would be coupled with the devils from Hell's QA department poking those miscreants who did not spot a transcription error with sharpened poles. Perhaps this is a description of your laboratory?

In an ideal world, we would be working electronically. The way that this would be achieved is to redesign the process, as shown in **Figure 2**. The CDS application would then be configured to match

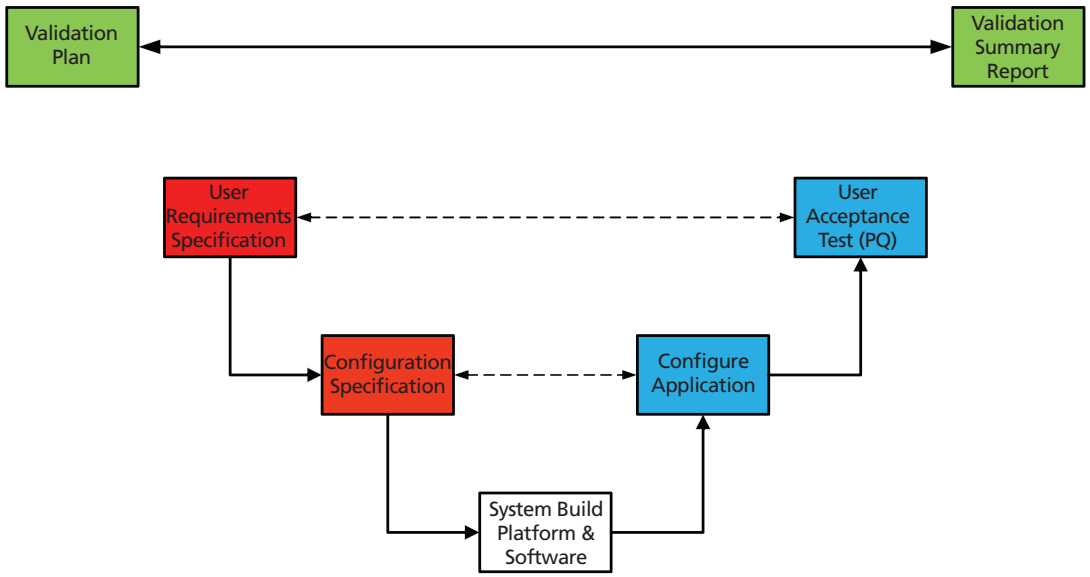


Figure 1: Typical life cycle model for a chromatography data system.

the resigned process. The focus is on a top-down approach aimed at the process efficiency.

The validation of a CDS therefore couples the life cycle tasks outlined in Figure 1 with the process redesign shown in Figure 2. Now the system is validated! We can now relax, safe in the knowledge that things are under control.

Data Integrity and Potential Problems

The above has been the way most validation work has been performed. However, there are three potential problems that may arise in this approach (Figure 2):

1. *Process level*: A problem arises if the system is used as a hybrid and paper is defined as the raw data. Oh dear! The FDA shot this argument down in flames in 2010 with a Level 2 guidance where they stated that paper was neither a true copy nor an exact and complete copy of the underlying electronic records (6). I have discussed this in detail when looking at complete data for a CDS (7,8).

2. *Application level:* The CDS configuration settings are not documented or the settings do not protect the electronic records, for example, the audit trail functions have not been enabled. This is unwise because inspectors have been trained to request this documentation. Hence, one should understand the ramifications contained in Figure 1.

3. *Record level:* Protection of electronic records created and managed by the application. We will discuss this issue in more detail later. However, if

your electronic records are stored in directories in the operating system—be afraid, be very afraid.

Beneath the application in Figure 2 are the data and metadata produced from the analyses performed in the laboratory. Burgess and McDowall offered a more detailed discussion of the records that constitute a primary analytical record in a 2015 *LCGC Europe* article (9). Let us look at these records in more detail.

With a CDS there are two options for storing the data: either in directories in the operating system file structure or in a database. McDowall and Burgess published a trilogy of papers in four parts in *LCGC North America* that looks at the ideal chromatography data system for a regulated laboratory (10–13), in the paper on system architecture we recommended that standalone workstations are not fit for purpose and that a CDS must store the data and contextual metadata in a database (11). Records stored in directories are too vulnerable to deletion and unrestricted access to the system clock can enable time travelling on a standalone workstation. A user can access the system clock and put the clock back in time, delete failed records, repeat the work, pass the batch, and no-one is the wiser! To be secure, data must be stored on a fault tolerant network drive where the clock source is a time server linked to a trusted time source, with effective and regular backup performed by the IT department.

Please note that data integrity is not a simple, single discipline issue solely in the chromatographic domain. Rather, it is a multidisciplinary function that requires a mix of people who have between them IT, regulatory compliance, software engineering, and business knowledge skills. People with cross-disciplinary skills are invaluable here (14).

Validated System with Vulnerable Records?!

Let us consider the following situation: We have a CDS (standalone or networked) where the electronic records generated by the system are stored in directories within the operating system. If we have validated the system taking the approaches outlined in Figure 1 and Figure 2, there is still a possibility that the records can be inadvertently deleted or manipulated. Where does our validation stand now? Application under control but records potentially vulnerable? Not the best situation to be in, is it? What should we do—apart from panic or ensure our CVs are current?

Note that this discussion is CDS specific, but the principles outlined here are also applicable to other standalone laboratory systems and PC instrument controllers.

Back to the Future?

To go forward, let us go back in time. In 2005, the GAMP Forum (Good Automated Manufacturing Practice) published a Good Practice Guide (GPG) on Compliant Part 11 Electronic Records and Signatures (15). The approach was rather different to the way I have described

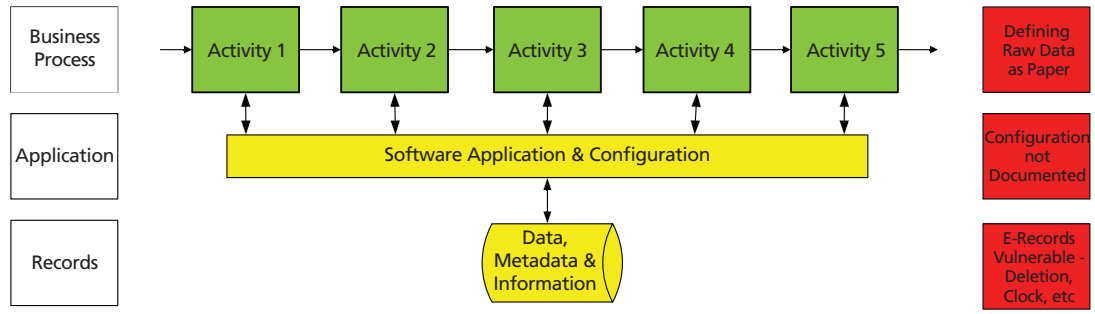


Figure 2: Traditional computer validation focuses on the process.

validation above. Instead of the top-down validation approach, they took a bottom-up approach and focused on the electronic records and signatures created and used within the system. In overview, the process was to identify the records created in the system, evaluate their regulatory impact, and, as a result, determine the controls that were necessary to control and protect them. What happened? The validation world listened with deaf ears and saw with blind eyes.

I believe the problem is that this approach does not create process efficiencies that the top-down approach does; a focus on records creates protected records but you can still have an inefficient process. However, it is time to reconsider the bottom-up approach.

Brave New CSV World?

I would suggest a hybrid of both approaches to get the best of both worlds and to ensure the integrity of our electronic records. With little additional effort but with great compliance benefit, the vulnerability of the electronic records should be managed by controls specifically implemented, which are based on the record's regulatory impact. This is shown in **Figure 3** and would proceed in a number of stages:

1. The start of the project would be a focus on process improvement and efficiency gains.
2. As the selected application was prototyped and configuration settings of the CDS examined, all applicable electronic records generated in the course of analysis (data and metadata including audit trail entries) would be identified.
3. The regulatory impact of the records would be assessed depending on their function; for example, method development, method validation batch release or protocol analysis, stability testing, and so forth.
4. The vulnerability of the electronic records would be assessed and

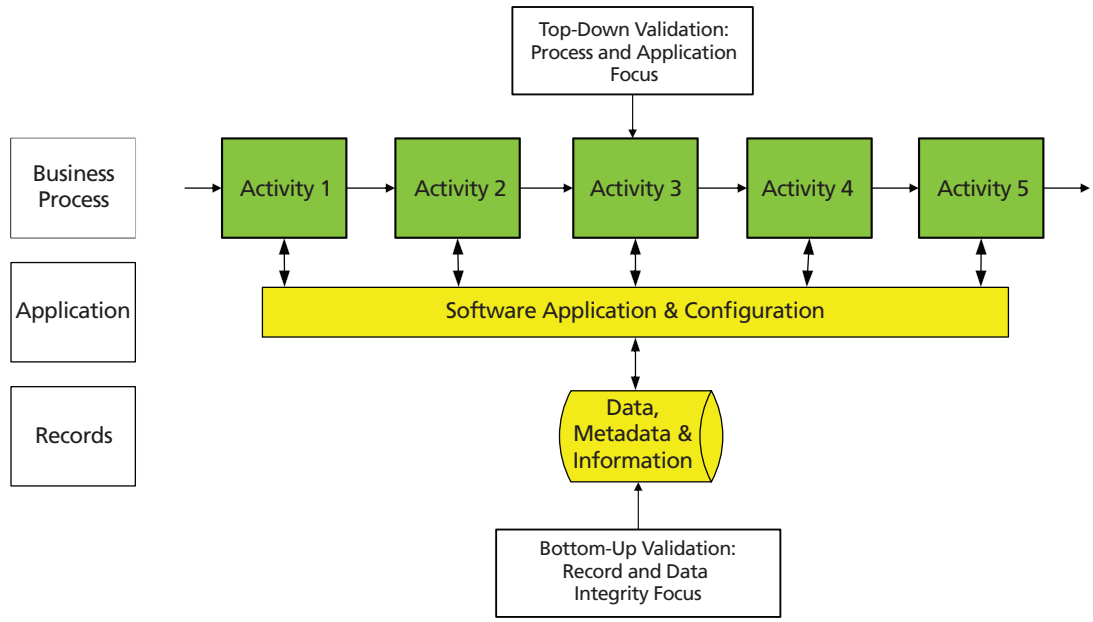


Figure 3: Computerized system validation using a combination of top-down and bottom-up approaches.

appropriate controls to protect these records would be added to the specification documents for implementation in the later stages of the validation project

5. As the system is being built, controls for the electronic records and signatures would be implemented at the same time as application configuration. These controls can be either technical or procedural.
6. During the performance qualification (PQ) or user acceptance testing (UAT) phase of the validation the additional controls for the records and signature would be integrated into the overall testing of the intended use of the CDS application.

Turning Principles into Practice

That may be the principles, but you may be thinking that a few fancy diagrams do not give sufficient detail to the approach. Let us take the principles and turn them into practice here.

We join the validation of a new CDS at the prototyping phase where the application is being configured and the Part 11 controls are being evaluated. The CDS is being installed in a regulated quality control laboratory undertaking verification of compendial methods, and analysis of active ingredients, in-process materials, and finished goods. Stability testing is also performed. The project team decides that electronic signatures and the 21 *CFR* 11 controls offered by the application will be implemented.

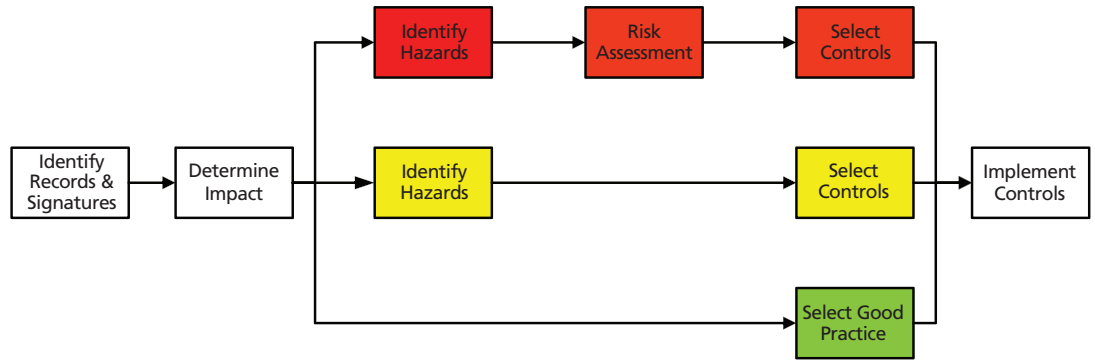


Figure 4: Identification of controls for high, medium, and low Impact regulatory records (see reference 16).

Table 1: Classification of high, medium, and low impact regulatory records (see reference 16).

Record Category	Regulatory Impact
High	Direct impact: • Product quality (batch release) • Patient safety (pharmacovigilance) • Electronic signatures • Records submitted to a regulatory agency; for example, PLA or NDA • Records required by predicate rule; for example, master schedule, GLP, or GCP study protocols
Medium	Indirect impact: • Records used to support product quality; for example, CSV and method validation and calibration records • SOPs • Training records
Low	Negligible impact: • Calibration and maintenance plans • Project plans

Although the application is networked, all data are stored in directories in the operating system and not in a database. Snatching defeat from the jaws of victory for the selection team!

The process for bottom-up or records-based validation is outlined in **Figure 4** and each stage is described below:.

- The first task is to identify the electronic records and signatures generated and maintained in the system (9).
- Next, the regulatory impact of the identified records or signatures needs to be assessed. The GAMP Part 11 GPG classifies records into high, medium, and low impact categories as shown in Table 1. From the descriptions of the use of the system and the table, the CDS records fall into the high impact category because they are involved in product release.
- The identification of any hazards that the records face is now performed followed by a risk assessment (all

documented). To expedite the process, we will assume that this has been done. At the highest risk are the records on the server hard drive in the operating system directories because they can be deleted outside of the application, without leaving any evidence of their deletion.

- Controls need to be selected to protect these high risk records; for example, records can only be accessed by authorized users via the application, restricting access to directories by a shell program, hiding the drive on the network, monitoring access to the drive via the operating system, restricting copy of CDS records. These controls need to be documented in the specification(s) for the CDS.
- TAs the validation progresses the controls will be implemented and later tested as part of the user acceptance tests for the system.

Summary

This short example gives you a better idea to of how to ensure that both a top-down and bottom-up approach to validation, as shown in Figure 3, provides business benefits while at the same time implements controls that will help ensure data integrity. Data integrity is not just the domain of the laboratory but requires a multi-disciplinary team to assess record vulnerability and to incorporate the controls within a CDS validation.

Acknowledgement

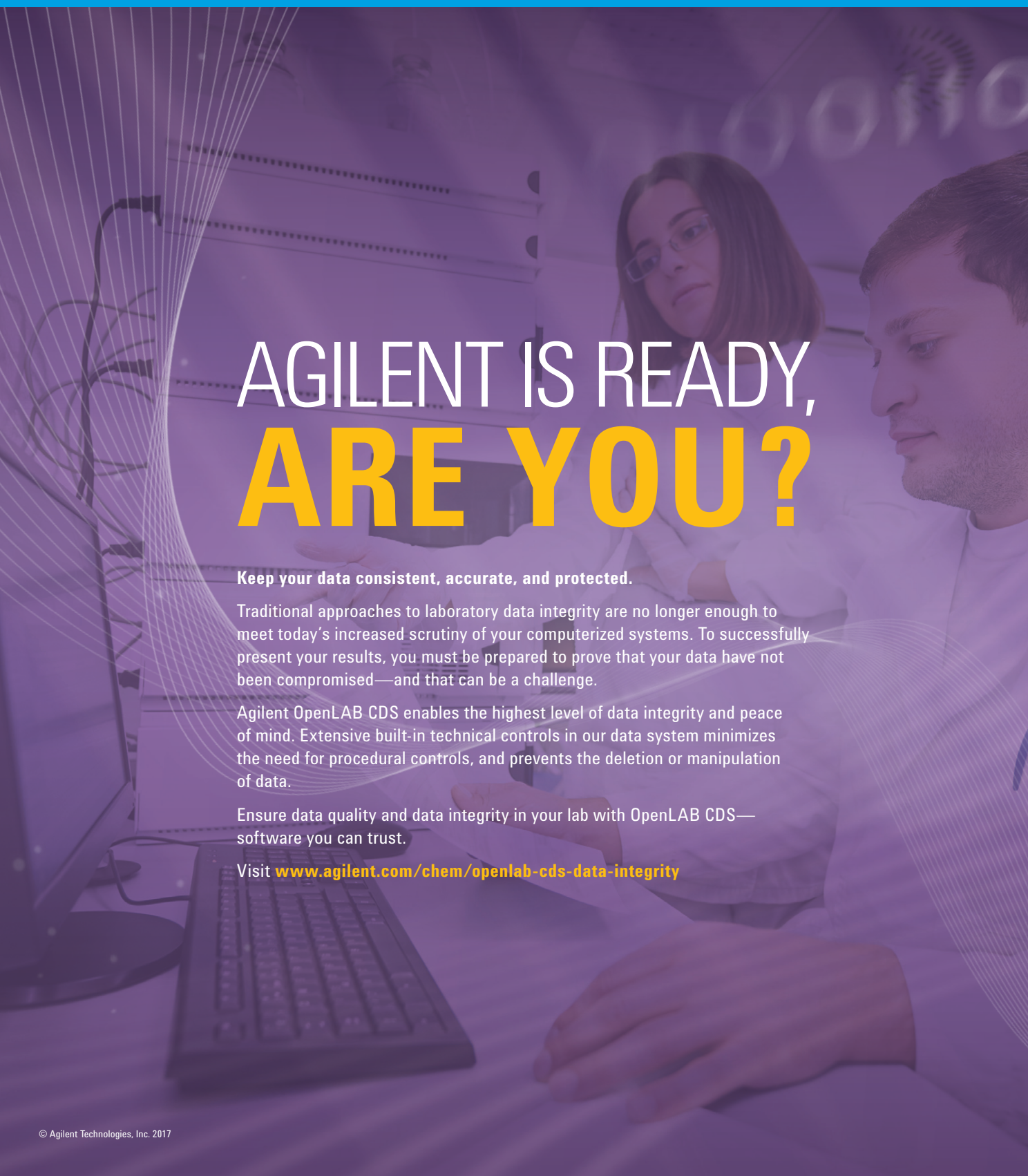
I would like to thank Mark Newton for his comments in preparing this column.

References

(1) J. Donath and R.D. McDowall, *LCGC Europe* **18**(9), 453–464 (2005).
(2) T.D. Thompson, D. Browne, D. Mole, and R.D. McDowall, *LCGC Europe* **14**(11) 687–692 (2001).
(3) Current Good Manufacturing Practice for Finished Pharmaceutical Products, 21 *CFR* 211.63 (2008).
(4) EU GMP Annex 11 computerized systems (2011).
(5) R.D. McDowall, *Spectroscopy* **21**(4), (2006).
(6) Questions and Answers on Current Good Manufacturing Practices, Good Guidance Practices, Level 2 Guidance: Records and Reports, http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm124787.htm
(7) R.D. McDowall, *LCGC Europe* **26**(6), 338–343 (2013).
(8) R.D. McDowall, *LCGC Europe* **26**(7), 389–392 (2013).
(9) C. Burgess and R.D. McDowall, *LCGC Europe* **28**(11), 621–625 (2015).
(10) R.D. McDowall and C. Burgess, *LCGC North America* **33**(8), 554–557 (2015).
(11) R.D. McDowall and C. Burgess, *LCGC North America* **33**(10), 782–785 (2015).
(12) R.D. McDowall and C. Burgess, LCGC North America **33**(12), 914–917 (2015).
(13) R.D. McDowall and C. Burgess, *LCGC North America,* February 2016.
(14) M.E. Newton, personal communication.
(15) Good Automated Manufacturing Practice (GAMP) Good Practice Guide, Compliant Part 11 Electronic Records and Signatures, ISPE, Tampa, Florida, USA, (2005).

"Questions of Quality" editor **Bob McDowall** is Director at R.D. McDowall Ltd, Bromley, Kent, UK. He is also a member of *LCGC Europe*'s editorial advisory board. Correspondence about this article should be addressed to the editor-in-chief, Alasdair Matheson, at alasdair.matheson@ubm.com

This article first appeared in *LCGC Europe* **29**(2), 93–96 (2016).



AGILENT IS READY, ARE YOU?

Keep your data consistent, accurate, and protected.

Traditional approaches to laboratory data integrity are no longer enough to meet today's increased scrutiny of your computerized systems. To successfully present your results, you must be prepared to prove that your data have not been compromised—and that can be a challenge.

Agilent OpenLAB CDS enables the highest level of data integrity and peace of mind. Extensive built-in technical controls in our data system minimizes the need for procedural controls, and prevents the deletion or manipulation of data.

Ensure data quality and data integrity in your lab with OpenLAB CDS—software you can trust.

Visit **www.agilent.com/chem/openlab-cds-data-integrity**

Agilent Technologies

LIFE CYCLE RISK ASSESSMENT OF HPLC INSTRUMENTS

Paul Smith and R.D. McDowall

What does risk assessment in the context of the life cycle of a high performance liquid chromatography (HPLC) instrument really mean? This article looks at problems with an operational liquid chromatograph to see if they can be picked up in the performance qualification (PQ) or prevented in the operational qualification (OQ). The relationship between PQ and OQ and the design qualification (DQ) phases of the life cycle are also explored.

Regulated GxP laboratories must qualify their chromatographs to demonstrate that they are fit for purpose. A qualification process based on the 4Qs model is typically used to qualify liquid chromatographs. The 4Qs model, enshrined in *United States Pharmacopoeia* (USP) <1058> (1) consists of four interlinked phases: design qualification (DQ), installation qualification (IQ), operational qualification (OQ), and performance qualification (PQ). We will discuss life cycle risk assessment of high performance liquid chromatography (HPLC) instruments in the context of the 4Qs model. In this discussion, we will not consider chromatography data systems (CDS), but there is the underlying assumption that the instrument is controlled by this software.

We will look at life cycle risk assessment of HPLC instruments from the perspective of what can go wrong with a qualified liquid chromatograph during the operational phase (PQ phase). How can identification of problems here be used to help us manage and mitigate risk in other phases? From this perspective, we will look at how system suitability tests and their linkage between DQ and OQ can mitigate some, but not all, the instrument problems.

Perceptions of Risk Assessment

Over the past decade, risk management and risk assessment have become part of the pharmaceutical lexicon; they are the subject of an ICH Q9 paper on quality risk management (2). However, what does this mean for regulators and the industry?

From the regulator's perspective, industry should undertake risk assessments to identify the most critical parts of an activity or process and focus

Table 1: Possible LC instrument failures and the ability to detect them in operational qualification (OQ) or performance qualification (PQ).

Module	Possible Failure	OQ	PQ		
			SST	Instrument	Extra SST
Pump	Wrong flow rate	✓	✓ 1		✓
	Variable flow rate	✓	✓ 1		✓
	Gradient error	✓	✓ 1		
	Instrument leak			✓	
Injector	High temperature	✓			✓
	Low temperature	✓			✓
	Carryover	✓	✓ 2		
	Poor injection precision	✓	✓		
	Poor injection linearity	✓			
Column Oven	Wrong temperature	✓			✓
	Variable temperature	✓	✓ 3		✓
Detector	Poor detector response	✓	✓ 4		
	Wrong wavelength	✓		✓ 7	
	Low energy		✓ 5	✓ 8	✓ 9
	Poor signal-to-noise	✓	✓ 6		
System (Holistic) Test	Integrated test of all system components	✓	✓		

The numbers shown in the table above against various failures are discussed below:

1. Variable flow rate would affect the precision of peak retention time and a significant flow rate or gradient error might give peaks outside of expected retention windows.
2. Carryover would only be detected if a blank injection is included in a system suitability test (see the lean sigma vs. scientifically sound SST discussion).
3. Variable temperature of the column oven would give variable chromatography or retention times.
4. How different would the detector response need to be so that it can be "detected"?
5. If lamp energy is checked as part of a PQ that is not just focused on a SST.
6. Needs a blank injection or a suitable area in a chromatogram where S/N can be determined.
7. This depends on the instrument and how it is used. Many instruments now include a diagnostic wavelength test using the deuterium emission lines when turned on.
8. Some instruments may warn if the lamp energy falls below a certain level.
9. Manual check of detector lamp energy is required.

mitigation efforts there. It is a means of putting scarce resources where they are most needed and of identifying improvements in quality risk management (3). Generally, from the industry's perspective it can be a means to justify doing less. We will explore some of these points in this article.

What Can Go Wrong?

Features that can go wrong with an operational HPLC system is the starting point for our discussion. This is illustrated in **Figure 1** where a liquid chromatograph consists of four modules: pump, injector (autosampler), column oven, and the detector. We have omitted the column from the figure as our aim is to look at an LC instrument's qualification rather than method performance. Underneath each module are listed the main failures that could occur. Note that this list is not exhaustive and some of the failures could be broken down further. However, to keep the discussion simple we have decided to look at this problem from a high level perspective. Some failures may not happen if the instrument in your laboratory does not have a particular feature, for example, for an isocratic pump there will not be gradient errors.

Now that we have listed the main failures, we need to consider the circumstances under which these might be detected in a OQ or PQ, as shown in **Table 1**. The PQ is broken down into three areas: system suitability test (SST), an instrument detecting the problem, and a group called *extra SST* where parameters can be measured if the SST is designed to include them.

What Is An Instrument Performance Qualification—Part 1?

As our discussion is focused on the operational phase of an instrument life cycle, we also need to consider the PQ. One of the current ambiguities associated with *USP* <1058> relates to OQ and PQ. Specifically, what they should contain and who has responsibility for them? Historically, before *USP* <1058> was first implemented in 2008, the 1987 US Food and Drug Administration (FDA) guidance for process validation (4) was adapted and applied to analytical instrument qualification. This guidance was interpreted in divergent ways by laboratories and service providers. This divergence is recognized in <1058>, which states in the information under Table 1 (1):

> *Performing the activity is far more important than the phase under which the activity is performed.*

And elsewhere:

> *When an instrument undergoes major repairs or modifications, relevant OQ and/or PQ tests should be repeated [so, in this context, OQ and PQ might be considered interchangeable].*

However, *USP* <1058> also provides the following definitions of OQ and PQ:

> *Operational qualification is the documented collection of activities necessary to demonstrate that an instrument will function according to its operational specification in the selected environment.*
>
> *Performance qualification is the documented collection of activities necessary to demonstrate that an instrument consistently performs*

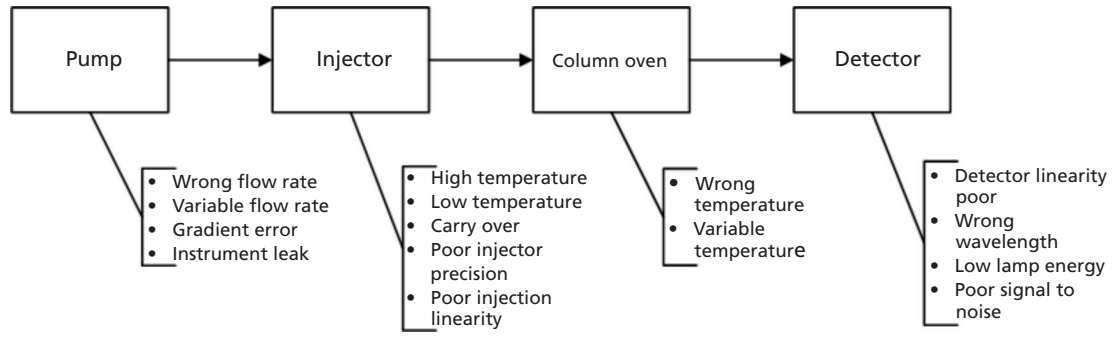


Figure 1: HPLC instrument showing the possible failures for each module.

according to the specifications defined by the user, and is appropriate for the intended use.

Therefore, although there is ambiguity (and from the experience of the authors quite a lot of uncertainty in laboratories), an OQ and a PQ serve completely different functions.

- The OQ is related to testing the instrument under standardized conditions so that the correct operation of the instrument in the laboratory versus the DQ can be confirmed.
- The PQ addresses the suitability of the instrument under actual conditions of use in between repetition of the OQ.

The potential role of SST in PQ has been discussed previously (5). Part of the choice that some laboratories may make relates to the conditions under which an OQ or a PQ may be required to be repeated. In the opinion of the authors, an OQ and a PQ must be performed on any "new" instrument before it is used to generate GxP data. With instrumentation purchased for GxP use, the suitability of the instrument for the work it will be documented initially in the DQ. This will define the intended use of the instrument and when the OQ is performed will show why the instrument is fit for purpose.

A Different View of the 4Qs Model

Typically, the instrument qualification life cycle is depicted or implied as a linear model, especially in *USP* <1058> (1) where it is presented in a table. However, to fully understand the 4Qs model it is better if the first three phases are presented in the form of a V, as shown in **Figure 2**.

In this simplified V model, it is much easier to see the relationship between the stages of the 4Qs. The OQ verifies the specification as outlined in the definition of OQ in *USP* <1058> (1)—provided whoever performs the OQ knows the content of the DQ or that the DQ has actually been written.

There is also an ongoing, dynamic, requirement to manage the DQ.

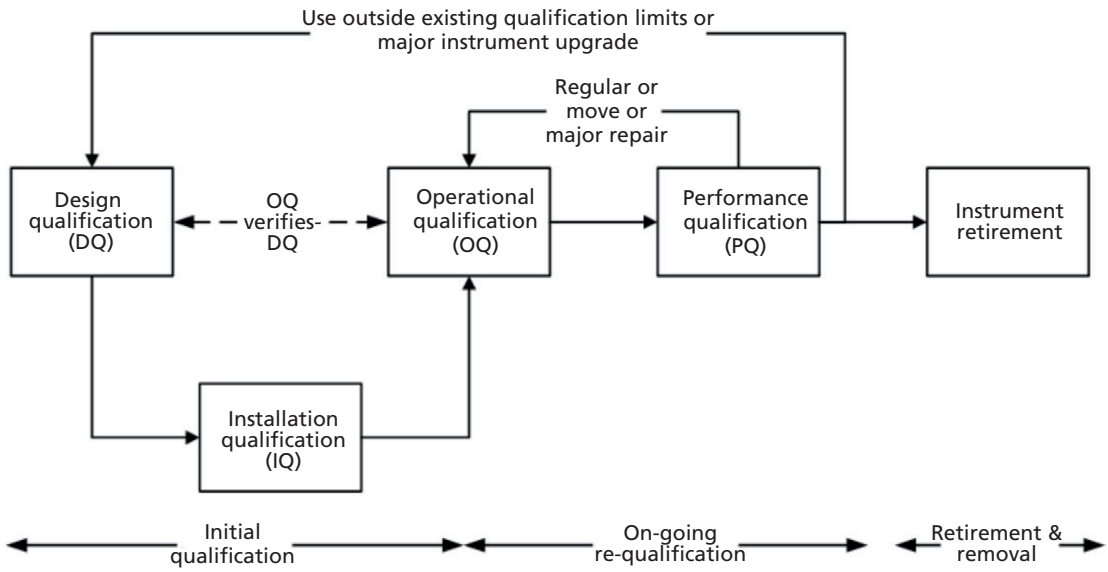


Figure 2: Depiction of the 4Qs model as a V.

This is in part dependent on how the DQ is defined (for example, if this references a very specific pharmacopeial requirement or chapter then each time the pharmacopeia is updated the DQ for the instrument will need to be reviewed). Instead, it is more efficient to address any high level compliance in the procedures that support the DQ and to limit the DQ requirements to instrument usage (remember that we are focusing only on the instrument).

This diagram also highlights that where an instrument has a major upgrade (because there is a wide divergence of opinion this is left to an individual laboratory to define) or is used with new methods not previously considered, there is a need to review the DQ for suitability. Without this feedback loop, there is a risk the instrument is not suitable for a new application. In addition, because of the relationship between the DQ and OQ, it will also highlight if different set points need to be included in the OQ to test the range of use. In terms of our discussion of risk the OQ can cover:

- Qualification of a new instrument;
- Requalification of an existing instrument following a defined time period typically linked with a preventative maintenance service;
- Requalification following a major repair;
- Extending the operating range of a qualified instrument because of an upgrade or new application that operates

outside of the existing range;
- Significant move of a qualified instrument with the justification for the extent of OQ testing documented in a risk assessment.

The OQ is intended to demonstrate that at a fixed time point the instrument operates to the specifications in the DQ and can therefore demonstrate that it meets the intended purpose. At this point it is worth repeating the statement from *USP* <1058> that routine analytical tests do not constitute OQ testing (1).

What Is An Instrument Performance Qualification—Part 2?

Let us return to the OQ versus PQ discussion. The different roles of OQ and PQ need to be fulfilled and supported on an ongoing basis during the lifetime of the instrument and there are options for how this can be achieved. Summarizing from *USP* <1058> (1) for an HPLC instrument, PQ tests should:
- Define user specifications for PQ tests to demonstrate trouble-free instrument operation for the intended applications.
- Verify the acceptable performance of the instrument for its intended use (parameters listed in Table 1 under Extra SST).
- Be typically based on the applications of the instrument in your laboratory.
- Be based on good science and reflect the general intended use of the instrument.
- Be performed concurrently with the test samples (SST) to demonstrate that the instrument is performing suitably.

There is a direct relationship between the DQ and PQ because the latter needs to demonstrate that the ongoing instrument operation is consistent with the intended use requirements in the former.

One of the OQ versus PQ uncertainties relates to defining how often qualification functions should be performed during the life cycle of the instrument and what triggers qualification requirements. In the absence of black and white guidance (in *USP* <1058> [1], GAMP [6], or other), generally for HPLC systems, annual requalification is often performed, and this ties the instrument maintenance to the qualification work. One consequence of this tie-in is the potential perception that an instrument may have a fault corrected during maintenance that was not previously detected, but because of the maintenance, this fault is corrected and therefore not evaluated in the subsequent qualification testing or detected.

In some instances, this has resulted in a discussion of "as-found" measurement (testing an instrument parameter before any adjustments are made), particularly where a laboratory may use the word calibration as a descriptive label for the qualification work. This question is at the heart of this paper and the consideration of how an instrument might fail and if that failure is detected. But, before considering this further, it is fundamental that any regulated laboratory understands the planned maintenance work performed and exactly what was done.

Most HPLC maintenance work is associated with wear related to usage and therefore the maintenance procedure defines replacement of consumable parts such as pump seals. Any other part replaced (such as pump pistons following a visual inspection) are listed in the service report (typically, because they are chargeable but this depends on the contract). Firmware upgrades must be pre-approved before installation and a risk assessment carried out using the available information from the manufacturer or service agent to determine the level and extent of requalification. In addition, any testing performed during preventative maintenance (PM) and visibility of any test failure should be included in the PM report and the laboratory should act on this information. Typical tests might include leak tests or temperature tests but this can be dependent on the instrument manufacturer or service provider. Always ensure that the work performed during a planned maintenance or instrument repair is fully documented and understood before being signed off.

With this in mind, the risk that any PM activity will correct a failure before it is detected is usually small. Therefore, requests for an as-found test for an instrument as complex as an HPLC system are meaningless because there is visibility of what work is performed, what tests are done, and the outcome of those. In fact, the only way to provide a 100% check would be to perform a pre-PM OQ, then a PM, then a post-PM OQ, which is not the smartest way to work!

Lean Sigma Versus Scientifically Sound SSTs

It is always good to challenge a business process but to do it without full knowledge of the regulations is foolhardy. Sometimes this is where risk management falls into the Clint Eastwood category of "I'm feeling lucky." A facilitator will challenge what is done and will typically ask "Where does it say that in the regulations?" Sometimes this can verge on an interrogation and failure to identify a regulatory requirement can result in a task being discarded.

Take an assay where each injection takes 30 min and the system suitability test includes five replicate standard injections and a blank sample: Where does it explicitly say in either the GMP regulations or the pharmacopoeias that you need a blank? Nowhere. The result is that the blank injection can end up being discarded, saving a vital 30 min. High fives all around!

BUT…Have you read the regulations? US GMP (21 *CFR* 211.160[a]) requires that all activities be scientifically sound (7); *USP* <1058> (1) requires a PQ test to be based on good science, as noted above. Is a blank injection of any value? More importantly, is it scientifically sound? A blank injection can determine the baseline flatness and noise level and if there is any carryover from the autosampler (see Table 1). Yes, you can

drop the blank injection, but if problems were found before the samples were committed this would save much time later in laboratory investigations — but only if you have a blank sample in the SST.

Let us be clear here, if you are going to redesign the process it is important to understand the risks that you will carry when eliminating tasks. Saving 30 min for a single injection (which in all probability is minimal as most of the LC injections occur overnight) needs to be weighed against the time spent on laboratory investigations looking for an assignable cause after the run if the run fails. Similar considerations need to be made for the inclusion of an approved and well characterized control sample, particularly for impurity characterization (11). It is not uncommon in a post-lean laboratory for chromatographic methods not to include a standard to serve as a comparison for the run. Given the fact that chromatography is a comparative analytical technique, this could be seen as stupidity on stilts. The choice and the risks you carry or mitigate are yours. Are you feeling lucky?

Assessment of Ongoing Instrument Performance

Designed to satisfy pharmacopeia requirements such as *USP* <621> (8), SSTs play a pivotal role in documenting the performance of the chromatography system (at the analytical run level). A natural evolution of this is to consider how SSTs can support ongoing PQ requirements (after the initial PQ to move the instrument into the operational phase). Previous consideration of this (5) identified that additional tests need to be added to those routinely defined in *USP* <621> (8). This requirement has not changed, but consideration of the ways an instrument might fail adds a different perspective. This can potentially be quite a painful process, because the implication is that in the post lean laboratory there may be some failures that are not currently detected. At the heart of this document is the question—*how might an instrument fail; and would that failure be detected in your laboratory?*

In practice, this approach means that laboratories have to review the information shown in Table 1 (how an instrument might fail) against the SSTs they currently include in their chromatographic methods (for example at the SSTs defined in each of their analytical methods). One of the core strengths of this fundamental approach is that it evolves the thinking within the laboratory management away from lean and back towards scientifically sound. In particular, in an era where regulators such as the FDA are considering data integrity from a fraudulent practices perspective—your approach should be defendable from both a scientific soundness and data integrity perspective. This thought process helps laboratories to identify potential gaps in their regulatory defence. So, instead of thinking purely from a

theoretical perspective: "What would happen if," make the situation real: "If this happened, what would the potential performance impact be and how would we defend it in an audit?"

The OQ column of Table 1 shows that the OQ should be designed to evaluate and detect all these potential high level failure modes. However, in operational use, some of the failure modes may not be detected. It is in part dependent on how the laboratory is using the instrument (for example the instrument should initiate a wavelength diagnostic check when turned on, using well characterized lamp emission lines, so is the instrument turned off and on?). While others, such as those which might be detected by retention time differences (flow rate and temperature for example) are dependent on chromatography practices within the laboratory (for example, formalizing acceptance criteria associated with peak identification windows).

Ultimately, ongoing monitoring of SSTs, including any additional requirements identified to help detect failure modes listed in Table 1, must be integrated into the controlling CDS software, so that it can be performed and trended in a semi-automated manner. Periodic review of this SST data would then support compliance with the requirements of FDA draft guidance on method validation (9) and, in part, be analogous to periodic review required for software.

Another benefit of developing this approach is that it provides a risk framework that can be applied to support additional compliance decisions, such as moving from maintenance or qualification based on a fixed annual requirement, towards compliance models that could be based on usage. This has been successfully applied outside of the laboratory area (10), because the method-based risk assessment framework already considers failure modes and the detectability of potential failure.

Care also needs to be taken with injecting samples to evaluate the performance of a chromatograph because recent FDA guidance (11) wants to avoid using sample injections as a means of testing into compliance. Therefore all work needs to be included in documented procedures and the generated data reviewed (11).

What Do I Do When...?

When an instrument fault is detected, the instrument must be removed from service (to prevent use by another analyst) and the laboratory procedure for considering the potential impact of the instrument failure on previous analytical results initiated. Typically, the instrument is repaired and an appropriate level of requalification work must be performed before it is returned to use.

Depending on the service contract for an instrument, minor repairs could be performed by laboratory personnel (for example, change seals, check valves or lamp), while major repairs are taken on by the service agent. Regardless

of who does it, it is important that a consistent approach be applied to any requalification work done following repair and before the instrument is returned to use. Sometimes, minor repairs performed by the laboratory might have a different approval process to major repairs performed by the service agent and this represents a potential risk. Inconsistency is always an area of focus during an audit.

A qualification test matrix, either in the laboratory or service agents documentation, should be approved that defines and lists the instrument repairs performed and the requalification work required for the chromatograph. Without this, in principle, a laboratory might be expected to perform a full instrument requalification if the pump seals are replaced, when a pump flow test is all that is required. If any repair work is performed that is not detailed in the requalification test matrix (which essentially pre-approves the qualification work), then the service agent must agree the re-qualification work performed with the customer. For major repairs it can be more efficient from a decision-making and workflow perspective to perform a full requalification, because the time to discuss, agree, and justify anything less can extend the instrument downtime.

Operational Qualification

The definition of OQ from <1058> was presented earlier, and the opinion of the authors is that this definition does not require modification. The OQ phase provides a controlled way of testing the performance of the instrument and the intended use (for example, the "set points" needed to cover the intended range of use). For tests such as temperature and flow, these can be measured as metrology tests using an appropriately calibrated device, while other tests include the use of a reference material and are more holistic in their nature. Generally, wavelength is evaluated using a suitable reference material such as caffeine or holmium oxide in perchloric acid. This means that the wavelengths that can be evaluated are dependent on the availability of suitable reference materials, which can cause a problem for users of detectors who have to operate at 200 nm, 5 nm below the 205 nm peak of caffeine. Here, a justification is required, which the supplier or service provider may be able to help write.

The OQ tests the functional operation of the instrument under standard conditions, which should match the operational range of use. Some tests, such as injection precision, are included in the OQ, the PQ, and ongoing instrument performance evaluation (SST). There is an important distinction to be made here, because some tests, such as injection precision and carryover, are application specific. Therefore, the limits applied in the OQ are related to the standardized method used to measure this in the OQ, while any injection precision limits applied which are related to the analytical methods are best evaluated in

the PQ and ongoing SST related to the pharmacopeial requirements (8). Where a PQ is performed, the chromatography method used should be related to the methods and applications applied in the laboratory. Note that this would also be a feedback to the DQ.

Understanding the clear and distinct role of the OQ and PQ relative to the instrument use is fundamental to good compliance practice and robust instrument defence. Where a reference material is used, this should be traceable and appropriate for the intended use—there should be documented justification of the suitability; when a method that is new to the instrument is set up, this should be an automatic trigger to review the DQ to OQ link to decide if different set points are required.

Summary

Representing the life cycle process as a modified V model more clearly illustrates the relationship between the stages of the 4Qs model and makes it conceptually simpler to understand. In particular, that the laboratory defines the usage of the instrument in the DQ stage and that this is tested at the OQ stage using standardized methods which could potentially be independent of the make and model of the instrument. The methods and range of operation defines the set points that need to be considered so that the OQ tests the range of use. Therefore, if methods are changed or added, this becomes an automatic trigger to review the current DQ to OQ relationship—any different wavelengths, temperatures, or flow in the new methods trigger an update to the standardized qualification tests set points in the OQ, so that the OQ is not static but dynamically configured to satisfy the ongoing OQ requirements of the laboratory. The protocol approval process needs to be appropriately structured (application of Lean Sigma principles) to support a more dynamic and responsive approach.

The details of the risk assessment—considering how an instrument failure might be either detected and/or defended, has to be performed in the laboratory, against the actual SSTs and working practices currently used in the laboratory. On the face of it, this approach may seem like a lot of work with little benefit. However, once the work is done, the ongoing management of the risk-based matrix is much simpler and the benefits include the development of stronger compliance defence in the laboratory, both in terms of justification of the potential impact of an instrument failure on results and reduction of risks because the possibility of an undetected instrument failure has been significantly reduced. At a time when regulators across the globe are focusing on data integrity and exchanging audit risk information, this has to be a good thing.

Finally, by augmenting the SSTs defined in *USP* <621> (8), the SSTs can be used to support the demonstration of the

ongoing consistent performance of the instrument (PQ) rather than being used to test compliance (11).

References

(1) United States Pharmacopeia, <1058>, Analytical Instrument Qualification.
(2) ICH Q9 Quality Risk Management, step 4, 2005 (www.ich.org).
(3) Kevin O'Donnell *et al.*, *PDA J Pharm Sci and Tech* **66**, 243–261 (2012).
(4) *FDA Guidance for Industry — Guidelines on General Principals of Process Validation,* May 1987.
(5) Lukas Kaminski *et al.*, *LCGC Europe* **24**(8), 418–422 (2011).
(6) *GAMP Good Practice Guide, A Risk-Based Approach to GXP Compliant Laboratory Computerized Systems,* (Second Edition, ISPE Tampa, Florida, USA, 2012).
(7) Code of Federal Regulations, 21 *CFR* Part 211.160 (a).
(8) United States Pharmacopeia, <621>, Chromatography.
(9) FDA Draft Guidance for Industry — Analytical Procedures and Methods Validation for Drugs and Biologicals, Section VIII Life Cycle Management of Analytical Procedures, February 2014.
(10) I.H. Afefy, *Engineering* **2**, 863–873 (2010)
(11) Item 7, http://www.fda.gov/Drugs/GuidanceCompliance RegulatoryInformation/Guidances/ucm124787.htm

Paul Smith is Global Strategic Compliance Program Manager at Agilent Technologies. After initially specializing in spectroscopy and application of chemometrics to spectroscopic data, Paul developed his compliance expertise in a variety of quality and management roles within the 17 years he spent in the pharmaceutical industry. Paul worked as an independent consultant and university lecturer before moving into laboratory compliance consultancy and productivity roles. "Questions of Quality" editor **Bob McDowall** is Director at R.D. McDowall Ltd, Bromley, Kent, UK. He is also a member of *LCGC Europe's* editorial advisory board. Correspondence about this article should be addressed to the editor-in-chief, Alasdair Matheson, at alasdair.matheson@ubm.com

This article first appeared in *LCGC Europe* **28**(2), 110–117 (2015).

REVISED USP <1058> IS COMING
ARE YOU READY?

Let Agilent help you minimize your regulatory audit risk.

Pharmaceutical labs—or any lab producing results subject to regulatory requirements—must demonstrate and document the suitability of analytical instruments for their intended use.

To date, the United States Pharmacopeia is the only major Pharmacopoeia with a general chapter dedicated to analytical instrument qualification (AIQ): **USP <1058>**. The final version of USP <1058> will be effective starting August 2017—and is a key regulatory document with significant implications for your laboratory.

Agilent can help you implement qualification processes and align your SOPs to comply with new USP <1058> requirements—taking an integrated, lifecycle-based approach to AIQ.

To learn more, please visit us at **www.agilent.com/chem/qualification**

Agilent Technologies