Retrospective Validation of a Chromatography Data System

Per Johansson, Bengt Wikenstedt, Astra Hässle AB, Mölndal, Sweden,
and R.D. McDowall, McDowall Consulting, Bromley, Kent, UK.

This article presents the phases of the retrospective validation of a chromatography data system in a case-history format. It assesses current documentation and the quality of each item by identifying missing paperwork and discussing the approach to bridge this gap. The authors also discuss their approach to testing and qualifying the system, training the personnel involved and reporting the entire validation effort.

The purpose of this article is to describe work performed to validate a large, multiuser chromatography data system retrospectively. The first section outlines the overall process, and this is followed by a description of the development of the testing strategy in more detail and the documentary evidence that demonstrates the life-cycle validation of the system. This discussion is an extension of earlier work by Moore and co-workers (1) in which liquid chromatography–mass spectrometry software was validated for compliance with good laboratory practice (GLP).

The regulations for computerized systems in the pharmaceutical industry are either guidelines specific to those systems or the interpretation of existing regulations to equate computerized systems with instruments and other equipment. In the second approach, computerized systems should be fit for their purpose, have adequate capacity and have the same data integrity, accuracy and security as manual procedures as outlined by Lepore (2). However, in the first approach, regulatory authorities — such as the Organization for Economic Cooperation and Development (OECD) (3), Japan Ministry of Health and Welfare (4), and UK Department of Health (5) — have issued GLP principles and guidelines for computerized systems. The European Union good manufacturing practice (GMP) guidelines have a specific section (Annex 11) that covers computerized systems (6).

Increasingly, the pharmaceutical industry is taking the initiative to produce guidelines rather than be regulated. An example of this movement is the good automated manufacturing practice (GAMP) guidelines (7).

All these regulations and guidelines state that the manager of the operating laboratory is responsible for validating its computerized systems. The individual who has the operational responsibility for the department or organizational unit is the person who is responsible for the integrity and accuracy of the data produced by the laboratory's computerized system. This person is usually called the system owner.

In general, validation is concerned with generating the documented evidence to demonstrate that a computerized system was purchased or developed based on quality standards, was accurate when qualified and continues to be so during its operational life, and was operated with sufficient evidence of management awareness and control. The documented evidence must be logical, scientifically lucid, structured and audit friendly, and it must reflect the way you use the application. The last point is most important because it is senseless to validate a system function that you never use.

Because most regulatory affairs experts agree that full validation of a computer system is impossible (8), companies should keep laboratory managers and users foremost in mind when developing a computer validation process, followed by internal quality auditors and, finally, external inspectors or assessors. The reason for such a priority ranking is clear: Validation primarily serves laboratory managers and users and not inspectors and assessors, who perform laboratory audits only periodically. Managers and users operate these systems daily and must, above all others, have confidence in them, otherwise the investment in validation will be wasted.

A Case Study

In our work, we validated a chromatography data system operating in the analytical chemistry division of Astra Hässle (Mölndal, Sweden). The chromatography data system has 52 analogue-to-digital channels and uses Millennium 2020 version 2.13 (Waters Corp., Milford, Massachusetts, USA) software running on a VAX–VMS Alpha server (Digital Equipment Corp., Maynard, Massachusetts, USA).

The tasks performed by the division include the

- analysis of raw materials
- analysis of new drug formulations to aid their development to the final market image
- analysis of finished and packaged drug formulations for use in drug development
- determination of the stability of finished products.

The chromatography data system is involved in all stages of this work, and therefore it provides critical input to final product quality.

Facilities management — such as back-up, support and maintenance — and operation of the hardware platforms are currently performed within the division. As part of the audit, we investigated the possibility of having the internal information technology department perform this work.

Qualification Terminology

The processes of equipment qualification and computerized system validation both use the terms installation qualification, operational qualification, and performance qualification. However, these terms can be confusing because they have different meanings in each context (see Table 1).

Notwithstanding the minor differences in phrasing, the installation qualification definitions are equivalent. The equipment qualification definition for operational qualification is split into two phases for computerized system validation (the operational qualification and the performance qualification phases). The computerized system validation mechanism ensures that the system continues to perform in the specified way for a period review or performance monitoring exercise. This mechanism relates to the equipment qualification definition of performance qualification.

In the definitions outlined in Table 1, major differences exist in the meaning of the same terms.

For consistency within the analytical laboratory, the terminology used in this article was the same as that for the equipment qualification; that is, we performed the installation qualification and operational qualification (user acceptance testing) before writing the validation summary report and operational release. Afterwards, performance qualification was used to demonstrate ongoing system performance.

Scope of the Work

Figure 1 shows the work flow for the retrospective validation tasks for our system. The following are the main tasks:

- determine which validation documents are missing and decide the overall approach — gap and plan
- write missing documents
- qualify the system
- audit suppliers
- write standard operating procedures.
- establish the current system configuration
- write the validation report.

We will discuss each of these tasks in more detail in the following sections of this article.

The literature provides little guidance for retrospective validation beyond overviews; for example, Huber (9) outlines the approaches for retrospective evaluation of computerized analytical instruments. Although some of the approaches outlined by Huber — collect documention, describe and define the system, qualify the system and update documentation — and those used in this article are similar in some instances, some differences exist as well. For example, this case encompasses a larger element of software and the testing effort is greater than that for A/D units that have undergone periodic calibration with a traceable signal generator since purchase and installation of the system.

Gap-and-plan phase: The gap-and-plan phase is an essential stage in the retrospective validation of any computerized system. *Gap* refers to missing validation documents. Figure 2 shows the process in more detail.

The driving forces in this phase were the corporate validation guidelines and policies and the current interpretation of the computerized system regulations.

The first step in this stage is collecting all existing documentation about the system. These documents will include items such as

- validation plans
- user requirement specifications
- selection process documentation
- purchase orders and packing lists

F1

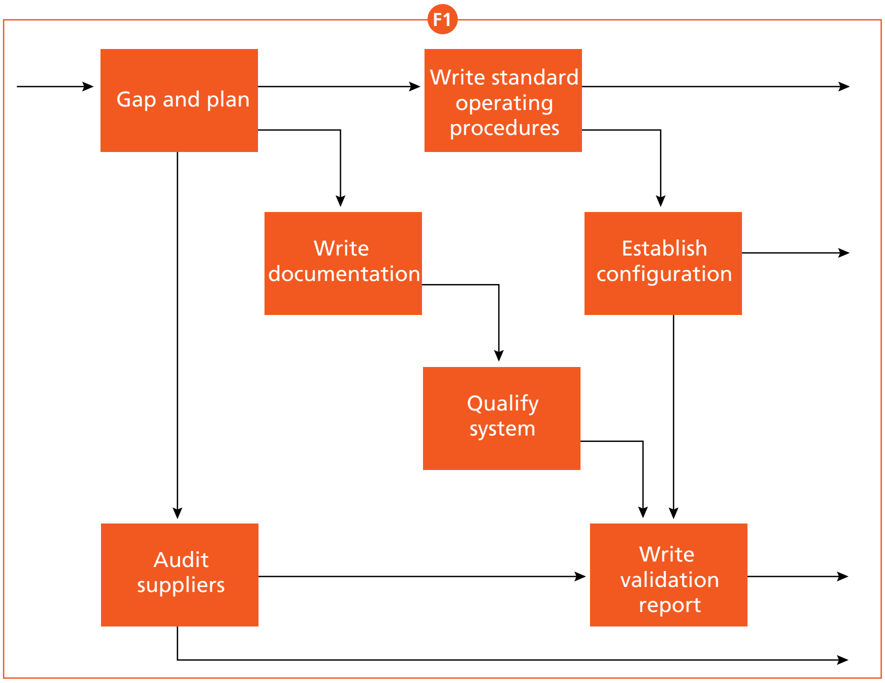

Figure 1: *Overall approach to the retrospective validation of the chromatography data system.*

T1

Table 1: Definitions of Qualification Procedures as they Pertain to Equipment Qualification and Computerized System Validation.

Validation Process Term	Definitions		
	Installation Qualification	**Operational Qualification**	**Performance Qualification**
Equipment qualification (14)	Assurance that the intended equipment is received from the manufacturer as designed and specified	Confirmation that the equipment functions as specified and operates correctly	Confirmation that the equipment consistently continues to perform as required
Computerized system validation (15)	Documented evidence that all key aspects of hardware and software installation adhere to appropriate codes and the computerized system specification	Documented evidence that the system or subsystem operates as intended in the computerized system specifications throughout representative or anticipated operating ranges	Documented evidence that the integrated computerized system performs as intended in its normal operation environment

- qualification tests and documentation
- user acceptance tests
- training materials
- in-house and vendors' operating manuals
- standard operating procedures.

Our system was relatively new, and we were able to retrieve most of the available documentation easily because it was held within the division. Furthermore, the personnel operating the system had been involved with the project from the start. With older systems the documentation may be non-existent and personnel may have left the company.

After collecting all documentation, we made a list to compare against a list of stated or inferred regulations or industry guidelines and the corporate validation policy. This comparison generated a list of missing documents and defined the gap to be filled.

Next, we reviewed the existing documentation to see that each item was of suitable quality, coverage and fitness for purpose. The mere existence of a document does not mean that its quality and coverage are good. Poor documents must be completed or otherwise discarded and replaced by new ones that meet the current compliance requirements.

For example, is a current user requirement specification specific enough to allow the construction of qualification tests? If the user requirement specification comprises one or two pages of general statements for a data system — such as "the data system performance must be fast" and "user-friendly operation" — then the document has no firm requirement to allow the construction of a meaningful test.

Furthermore, was every regulatory document approved by management and were they reviewed by quality-assurance personnel? This assessment of documents may result in more documents being added to the gap list.

After defining the gap, we had to decide whether to write the key documents and fill the gap or to let management take the business risk of not writing them, if they were unavailable. Worker time and resources must be included in this plan. The authorized list of documents to be written is the output of the gap-and-plan phase.

The gap-and-plan phase identified several key missing documents:

- a validation plan
- a work-flow analysis
- a user requirement specification
- a test plan for the system qualification
- user test scripts (operational qualification)
- a change control and configuration management standard operating procedure
- a system description.

Write the key missing documents: We considered the following documents to be crucial to the success of the retrospective validation: the validation plan, work-flow analysis, user requirement specification, test plan and test scripts. We wrote them as part of the project.

Validation plan: The validation plan, based on the system development life cycle, was required and written as an overall controlling document for the project. In overview, this document describes

- the roles and responsibilities of all who are involved with the project, including users, management, quality-assurance personnel and external consultants
- activities that must be performed to qualify the system
- a definition of the required documented evidence
- time scales of the validation effort.

We considered the early and active involvement of the quality assurance group to be essential in the acceptance and rapid approval of this work.

Work-flow analysis: We conducted a work-flow analysis to gather information about how the system is currently used and to keep the testing at an acceptable level (10). Our rationale was that users cannot test everything, so we decided to follow a reasonable methodology to define the necessary areas to test and to identify the functions and features to leave untested.

The basis of work-flow analysis is to plot the steps performed by the users. Figure 3 shows the overall work flow for our chromatography data system. As the flow chart in the figure demonstrates, the laboratory information management system (LIMS) link is introduced when the system becomes operational, and it therefore was excluded from this qualification.

Further analysis of each data system area, along with input from the user requirements specification, provide information about the system functions used in day-to-day work and the size of the analysed batches. Figure 4 shows an

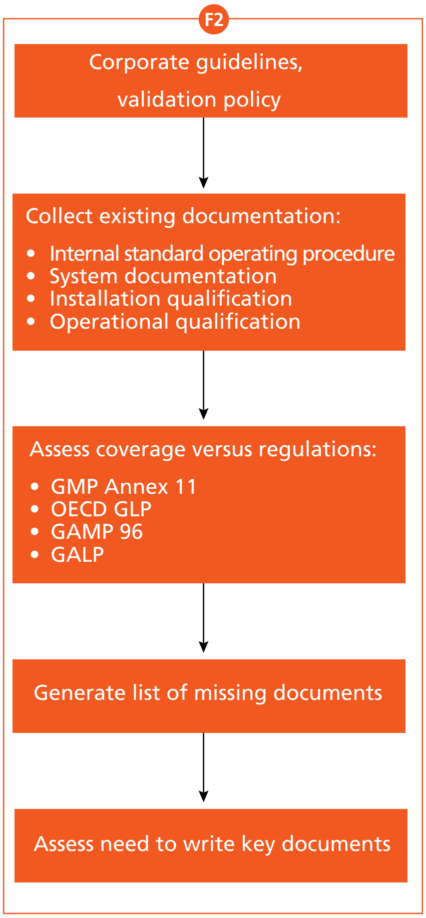
F2
Corporate guidelines, validation policy
Collect existing documentation:
• Internal standard operating procedure
• System documentation
• Installation qualification
• Operational qualification
Assess coverage versus regulations:
• GMP Annex 11
• OECD GLP
• GAMP 96
• GALP
Generate list of missing documents
Assess need to write key documents

Figure 2: *The outline of the gap-and-plan phase.*

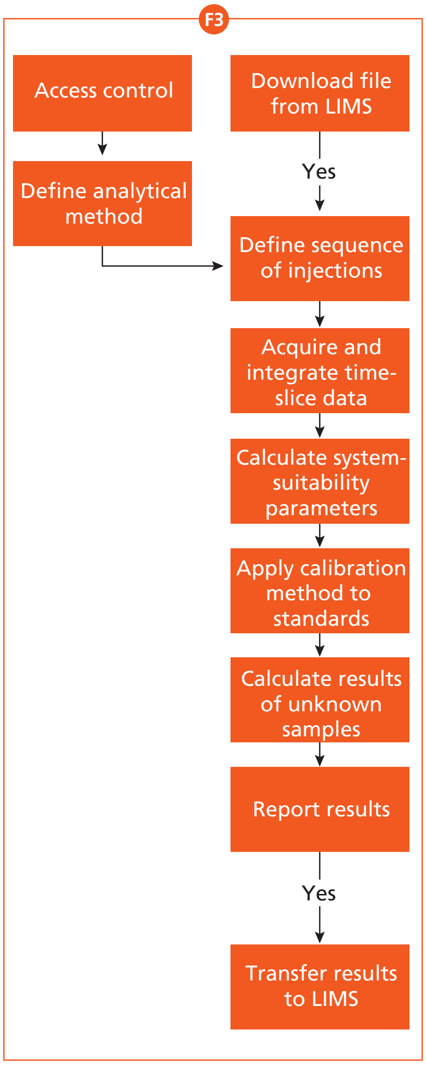
F3
Access control
Define analytical method
Download file from LIMS
Yes
Define sequence of injections
Acquire and integrate time-slice data
Calculate system-suitability parameters
Apply calibration method to standards
Calculate results of unknown samples
Report results
Yes
Transfer results to LIMS

Figure 3: *Work flow of the chromatography data system.*

example of a detailed flow diagram that can be used in work-flow analysis.

This approach is advantageous for various reasons. First, it defines the scope and boundaries of the system and, hence, the extent of qualification activities. Second, it explicitly identifies the functions used in the operation of the system. Third, it implicitly identifies functions not used by the system. Fourth, it identifies batch sizes and capacities of critical functions.

User requirement specification: After completing the work-flow analyses, we found that the initial user requirement specification had poor coverage and was not specific. We wrote a new user requirement specification because the currently accepted definition of validation requires "a predefined specification" (11). The user requirement specification is the predetermined specification; without it, the system is not validated.

We found that the current user requirement specification was insufficient because it lacked enough detail to define user-acceptance or performance-qualification tests to validate the system. The new retrospective user requirement specification was written based on the laboratory work flow and how the system was used in the laboratory. The document focused on the following main topics of a chromatography data system:

- methods
- sequence file–run list
- data acquisition, including A/D conversion and buffering capacity
- data interpretation, including data file integrity, peak detection, printing and plotting, and chromatogram overlay
- calibration, including models used for calculation, calibration points and statistical calculations
- reporting and collation of results.

Test plan: The test plan established the required functionality areas of testing for the chromatography data system as defined in the user requirement specification. This document is based on the Institute of Electronic and Electrical Engineers (IEEE) standard 829–1983 (12). Writing the test plan was an iterative process; we wrote an initial draft of the test plan and then updated it in parallel with the test scripts. This parallel process is necessary because the knowledge gained about assumptions, exclusions and limitations during the writing of the test scripts was incorporated in the test plan.

The test plan for the system included the following topics:

- a definition of the different components and modules that make up the overall system environment
- a definition of the scope of the system to be tested
- functions of the system that require testing
- functions of the system that require no testing
- a list of assumptions, exclusions and limitations of the test approach taken for this system.

The last item is a critical element of the validation effort because it allows the validation team to write contemporaneous notes about the intellectual processes that formulated the testing strategy. This process includes rationales for both the functions to be tested and those functions not to be tested.

Because the test scripts are written for operational qualification, further assumptions, exclusions and limitations emerge. For this reason, we built feedback into this section of the test plan (shown in Figure 5). Therefore, the test plan usually remains unfinalized until the test scripts have been drafted and initially reviewed.

Test scripts: A total of 18 test scripts were required for operational qualification based on the laboratory work flow for the system, the user requirement specification and test plan drafts. These scripts provided adequate coverage for all important critical functions and the components discovered in the work flow and user requirement specification.

We wrote each test script according to a common format based on the IEEE standard 829–1983 (See Table 2) (12). All scripts had sections for the test script (instructions for the tester to follow), space for notes made while performing tests, a log to record any software errors, definitions of the individual pass-or-fail criteria and an overall pass-or-fail statement for the test script.

We designed the tests to demonstrate adequate capacity of the system, the handling of common problems and out-of-range entries that were designed to fail.

The test scripts were divided into two groups. The first group included tests to be performed by the system managers; they addressed concerns such as security, access control and Year 2000 compliance. The second group of tests covered user functions such as autosampler continuity, validation of calibration functions used by the division and system-suitability test calculations.

F4

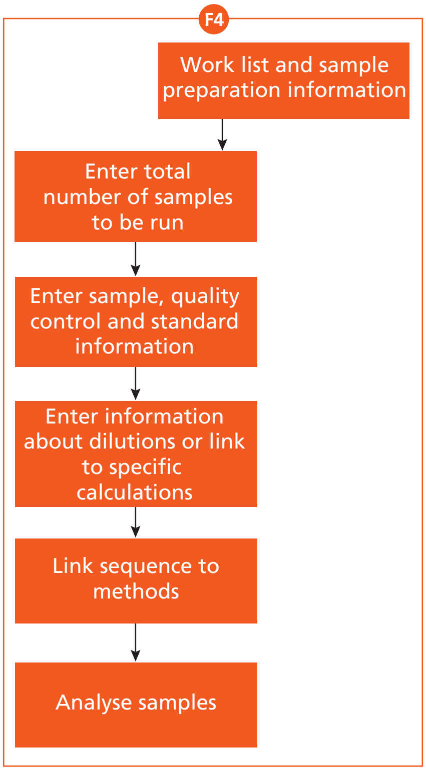
Work list and sample preparation information
Enter total number of samples to be run
Enter sample, quality control and standard information
Enter information about dilutions or link to specific calculations
Link sequence to methods
Analyse samples

Figure 4: *Detailed work flow of the sequence of injections.*

F5

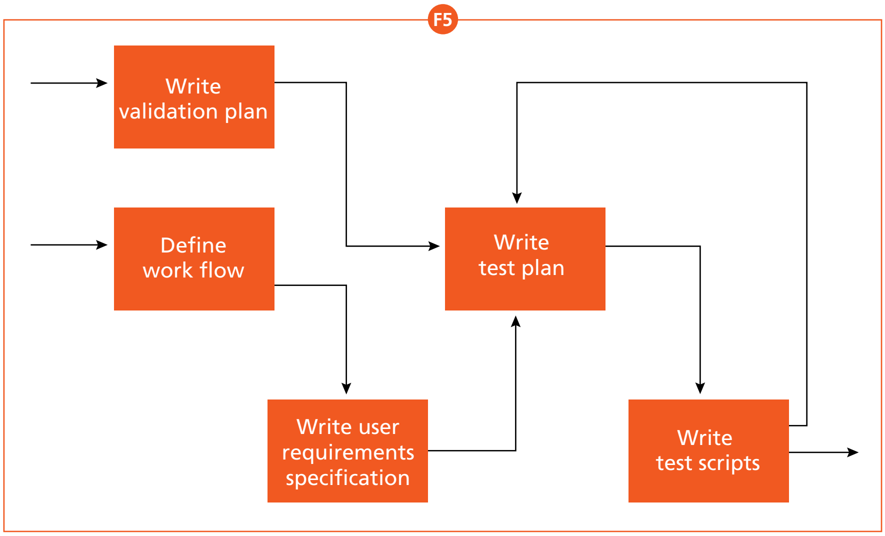

Figure 5: *Plan for writing the key missing documentation.*

Audit the suppliers: OECD GLP guidelines expect that suppliers should be audited (3). In our situation, we had the option of auditing two suppliers: the supplier of the chromatography data system software and the internal information technology department, which could supply future system support service.

A recent "Questions of Quality" column discussed vendor audits (13). The internal information technology department audit ensures that the validated status of a system is not compromised if a compliant system is operated by a third party.

Internal supplier: A future direction for the division was to have the internal information technology department take over and support the hardware platforms and network that support the chromatography data system software. In addition, the department would undertake all of the operational support such as back-up and recovery, storage and long-term archiving of data and disaster recovery.

The audit of the internal supplier was designed to ensure that the services supplied were compliant with the regulations.

External supplier: A vendor audit was considered for the supplier of the chromatography data system software. If the system to be validated was relatively old and would not be upgraded, then a vendor audit would have little benefit; one possible decision would be to take the business risk and ignore a vendor audit. In our case, however, the system was relatively new and the laboratory management was considering implementing a new version of the software.

We decided not to conduct a vendor audit of Waters in this qualification phase, because the main goal was getting the system into compliance. The rationale was that Waters was ISO 9001 compliant and TickIT certified (TickIT is a version of ISO 9001 with defined levels of quality), and the test plan for the qualification included assumptions and documentation that the system had been designed and developed in a quality manner.

However, we did perform a vendor audit of the next version of Millennium before implementing it. The format for the audit followed the approach outlined by McDowall (13, 19–20). The goals were to meet the requirements of the Astra Hässle corporate policy for computerized systems validation and specific requirements of European Union (EU) GMP requirements outlined in Annex 11 (6), namely

- Clause 5: "The user…should take all reasonable steps to ensure that [the software] has been produced in accordance with a system of Quality Assurance."
- Clause 18: "Where outside agencies are used to provide a computer service…[t]here should be a formal agreement including a clear statement of that outside agency (see Chapter 7)."

This process will be performed once during the system's lifetime with the assumption that ongoing certification will ensure ongoing product quality.

Write missing standard operating procedures and system description: The OECD GLP consensus document provides a minimum list of standard operating procedures required for the operation of a computerized system (3). We found the existing standard operating procedures to be acceptable except for a change control and configuration management standard operating procedure. We wrote this document as part of filling the gap.

Finally, both GMP and GLP regulations require a system description, which we also wrote as part of the process.

So far, we have outlined the initial phases of the retrospective validation of a chromatography data system. This validation process includes determining the extent and quality of existing documentation, identifying key missing documentation needed to support validation of the system, deciding whether to provide resources for writing the documents (or taking a regulatory risk) and then writing the documentation.

The following sections will examine subsequent steps in validating the chromatography data system, including qualifying the system, training the users, creating change control and configuration management, and writing the validation summary report. We will look in more detail at

- determining the functions of the system to be tested
- designing test scripts (see Table 2)
- executing the test scripts and training the users
- establishing change control and configuration management of the data system
- executing and reporting the vendor audit
- ensuring procedures are in place to guarantee the continued validation status of the system over its lifetime

Table 2: Elements of a Test Script.

- Purpose and features of the chromatography data system to be tested
- Referenced documents
- Special requirements (such as a calibrated peak output generator)
- Identification of the personnel executing and reviewing the test script
- Instructions for completing the test procedure with individual acceptance criteria for each test performed
- Documented evidence collected during testing
- Logs for recording any test incidents and software errors
- Summary of testing results
- Sign-off of the test script with an overall pass or fail statement

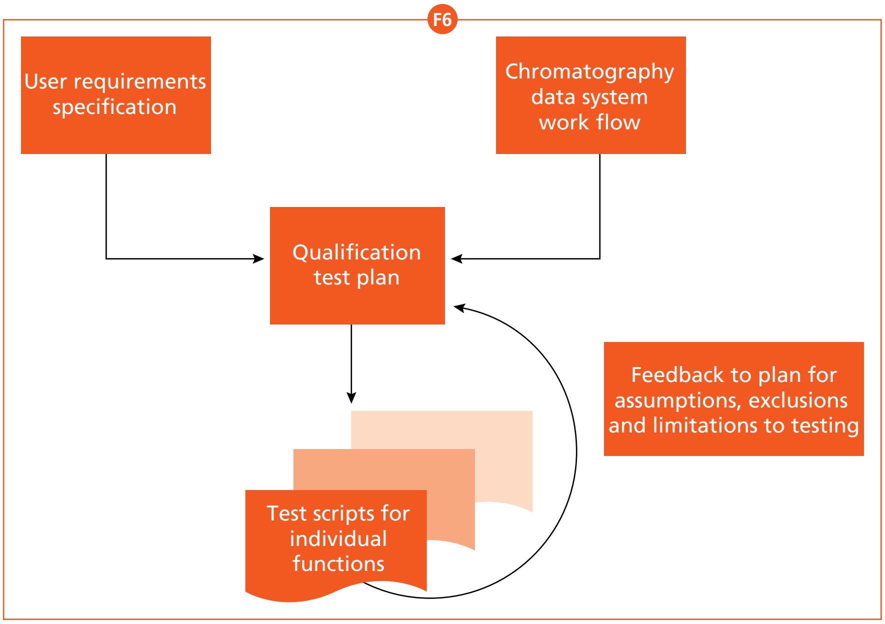
User requirements specification
Chromatography data system work flow
Qualification test plan
Feedback to plan for assumptions, exclusions and limitations to testing
Test scripts for individual functions

Figure 6: *Diagram showing the overall approach to defining functions to test in data systems qualification.*

- evaluating the quality of the system documentation provided by the vendor and standard procedures for system operation
- training the users
- writing the validation summary report.

Defining the Functions to Test

Figure 6 diagrams the overall approach to defining the functions to test in data system qualification. The two main documentation procedures required in this process are the user requirements specification and the work-flow analysis of the system.

These documents define the functions of the data system, system capacities, calculations used and the limits of parameters. The information provided by this documentation identifies the critical areas to test as well as the areas of the system to leave untested.

Writing the Test Scripts

From our examination of the laboratory work flow for the system, the user requirements specification, and the draft of the test plan, we identified 18 test scripts that were required for the performance qualification. The authors agreed that this number of protocols would provide adequate coverage for all critical functions and components in the work flow and user requirements specification.

Tests performed in this validation effort were not designed to confirm the existence of known errors (which, along with other features, should be documented in the manufacturer's release notes for individual software applications), but rather to test how the system is used daily. Any errors and steps taken to resolve the errors can be recorded in the test scripts in the test execution log.

The test scripts were divided into two groups. The first group consisted of tests to be performed by the system managers and covered items such as security, access control and Year 2000 compliance. The second group of tests was designed to examine user functions such as autosampler continuity, validation of calibration functions, and system-suitability test calculations.

The system managers tested the following features:

- data acquisition
- cross-talk of the analogue-to-digital (A/D) converters (16)
- data archiving and retrieval
- data back-up and restoration
- data file integrity
- network availability
- Year 2000 compliance
- system security and access control.

Users were responsible for testing

- calibration methods
- analyte calculation
- data reporting
- sample continuity
- remote processing over the network
- system-suitability test parameters
- connection and data processing using a photodiode-array detector
- custom fields such as the mathematical functions embedded within the chromatography data system used to implement calculations on data
- the system's mean vial calculation program, which calculates the mean of the results from duplicate injections
- rounding of numbers
- dual-detector data acquisition.

Capacity tests, such as analysing the largest expected number of samples in a batch, were incorporated within some test scripts to demonstrate that the system was capable of analysing the actual sample volume that could be expected in the laboratory. This test is a specific response to the US GMP regulations that require the system to have "adequate size" (17). Furthermore, we designed tests to demonstrate the handling of common problems and out-of-range entries.

Equally important is the documentation of untested functions. This documentation was included in the test plan for the system qualification. Items such as the operating system were excluded from testing because using the application software implicitly tested them (7).

The assumptions, exclusions and limitations of the testing effort were recorded in the appropriate section of the qualification test plan to provide contemporaneous notes about particular approaches. This documentation is very useful in case of future inspection, because it serves as a reference for the testing rationale.

Examples of Detailed Test Design

Good test case design is a key success factor in the quality of validation efforts. To provide an overview of the approach to designing tests, we present two examples for test design. These examples are the logical security of the system and, as a very current topic, testing for Year 2000 compliance.

Logical security: Although logical security appears at first glance to be a very mundane subject, the inclusion of this topic as a test is very important for regulatory reasons. Moreover, it serves as a good example for test case design and is linked with good information technology practices (GITP), which are postvalidation documented activities — such as back-up, change control and antivirus monitoring — performed by supporting information technology personnel.

The test design consists of three basic components:

- a test sequence in which the incorrect account fails to gain access to the system
- a single test case in which the correct account and password gain access to the system
- a test sequence in which the correct account but minor modifications of the password fail to gain access to the software.

This test design carries two important considerations. First, successful test cases are designed both to pass and to fail. More than 75% of the test cases for logical security were designed to fail to demonstrate the effectiveness of this aspect of the system. Second, the test relies on GITP to ensure that users regularly change or are compelled to change their passwords and that the passwords are of reasonable length (minimum 6–8 characters).

Year 2000 conformity: The basis for the Year 2000 conformity test script is the British Standards Institute document PD2000-1, which states, "Year 2000 conformity shall mean that neither performance nor functionality is affected by dates prior to, during, and after the year 2000" (18).

In particular, a system must meet four rules for compliance:

- No value for the current date will cause any interruption in operation.
- Date-based functionality must behave consistently for dates before, during and after the year 2000.
- In all interfaces and data storage, the century in any date must be specified either explicitly or by unambiguous algorithms or inferencing rules.
- The year 2000 must be recognized as a leap year.

Using this basis, we wrote a test script that looked at the following test cases: data acquisition in 1999; rollover from 1999 to 2000; leap years for 2000, 2001 and 2004 (because 2001 is not a leap year, the first and last test cases were designed to pass, while the middle one was designed to fail); and retrieval of data acquired in 1999 during 2000.

The testing would be executed using Year 2000–compliant computers that would be subject to separate Year 2000 compliance tests.

Both the validation team and management approved this test procedure. However, in the course of writing the test script we learned from the vendor that some parts of the system were not fully functional after 1999. Consequently, we suspended this test script for the current version of the system. The vendor assured us that the next version of the chromatography data system (Millennium^{32} from Waters) would be Year 2000 compliant, so we decided to execute this test script as part of the validation of the new release of the software.

Test execution: Once the test scripts were written, the users and system managers executed them and found the following unexpected results:

- The sine function in the custom fields did not function as anticipated.
- The binary coded decimal transfer to the A/D converters was working only in the range 1–99.
- If a detector signal was outside the technical specifications of the A/D converter, no out-of-range notification occurred.

Change Control and Configuration Management

The initial validation of a system is relatively simple. The major challenge is to maintain the validation status during operation. The validation team therefore established procedures for change control and configuration management to ensure that the validated status of the system could be maintained throughout its operational lifetime.

These procedures are important because they provide a mechanism to ensure that changes can be made in a defined and controlled manner (with the exception of emergency changes that the system managers can make under predefined situations). Change control and configuration management procedures establish recordkeeping protocols that enable users to reconstruct an exact configuration of a chromatography data system on any specified day. From a scientific and regulatory perspective, this information enables users to assess the duration and impacts of a configuration item on the system. A configuration item is the smallest piece of hardware or software — such as a client PC, hard disk drive or software package version — that will be monitored. These procedures also provide a record to demonstrate system stability.

Changes will occur throughout the lifetime of the system and can include upgrades of the chromatography data system software, upgrades of network and operating system software, changes to the hardware (such as additional memory and processor upgrades), and extension of the system for new users. From the installation of a system to its retirement, change control is a key validation component, and specific references to controlling change appear in both the Organisation for Economic Cooperation and Development consensus document (3) and EU GMP regulations (6).

Establish the initial configuration baseline: We established the configuration baseline by conducting an inventory of the whole system. This procedure resulted in a description of all the parts of the Millennium system, including hardware, software and documentation.

Implement change control: We implemented change control through a standard operating procedure that included a change form to request and assess change. This form requires information such as a description of the change as described by the individual submitting the form; the impact of the change, assessed by the system managers and then approved or rejected by management; and changes that were approved, implemented, tested and qualified before operational release.

We determined the degree of necessary revalidation work while conducting impact analysis. Changes that affected the configuration (hardware, software and documentation) were recorded in a configuration log maintained in Microsoft Excel (Microsoft Corp., Redmond, Washington, USA).

Evaluate System Documentation

A validation effort should include a review of the documentation of the system. However, this review should not be limited to items provided with the application. It should also include vendor-provided documentation and existing internal documentation such as user manuals, performance qualification test scripts, revalidation standard operating procedures, training records and *curriculum vitae*. Following is a discussion of the documentation review at Astra Hässle.

Vendor's documentation: The system documentation from Waters is well structured and easy to read. The coverage is sufficient for both users and the system administrator. Although some references cite Millennium 2010 rather than 2020, it is essentially the same software, and this reference has no impact upon the data integrity or data quality.

User manuals: Astra Hässle uses two manuals. The first manual includes a short introduction about the most basic use of the Millennium system, and the second manual outlines the minimum requirements for the printout of analytical results.

Test scripts: We developed a performance qualification test script to verify that the system remains qualified for operational use. This protocol should be performed after upgrades or at 12-month intervals and includes the following functions to be tested:

- A/D converter linearity and repeatability, tested with a calibrated peak generator
- data file integrity, checked with a Millennium system program that calculates the check sum for each installed file in the Millennium system
- remote processing over the network, conducted with a sample set that was generated in the operational qualification testing of the system.

Revalidation procedures: We established validation criteria and included them in the appropriate section of an internal revalidation standard operating procedure. This document states that a revalidation will be considered when the system configuration or operational procedures experience any change that may affect the validation status of the system. Some of the important elements of the computer system to be considered for revalidation in the event of change are the central processing unit, hard disk drives, the applications software, the operating system software and A/D converters.

The internal standard operating procedure should evaluate the need for revalidation after a change and the extent of testing required. For example, if a new acquisition client is added to the system, an installation qualification is performed with two or three performance qualification test scripts.

Training records and *curriculum vitae*: One key item for the validation effort is to ensure that all the personnel involved with the validation and qualification efforts are trained and that this training is documented appropriately. The personnel and the training records involved at our company's validation effort were

- *Vendor staff who were responsible for the installation and initial testing of the data system software:* These individuals provided copies of their training certificates listing the products they were trained to service, and these training certificates were checked to confirm they were current and covered the relevant products and then were included in the validation package.

- *System managers with vendor training in the use of the system and administration tasks:* This training was documented in the validation package. In addition, a consultant provided intensive training and technology transfer of validation skills to enable the system managers to undertake the validation effort, all of which was also documented.
- *Analytical chemists or technicians who were trained by Waters' staff to use the data system:* The consultant taught a short training course for the staff members responsible for completing the test scripts. At the conclusion of both types of training, the employees received certificates for completing the courses, and they used this documentation to update their training records appropriately by noting the date and type of training received.
- *Consultant who was involved in aiding this validation effort:* This person provided a *curriculum vitae* and a written summary of skills to include in the validation package for the system.

The Validation Summary Report

We reported the whole life cycle and the documentation resulting from these activities in a summary report, which should be concise and not detail-intensive. If additional detail is required, it can be cross-referenced within the report.

The format of the summary report is based on the Institute of Electronic and Electrical Engineers standard for software validation and verification plans (21). This document outlines the summary report as follows:

- *Introduction:* purpose, objective and scope of the validation effort
- *Validation activities:* evaluation of the requirements, implementation, integration, and validation phases; summary of anomalies and resolutions; and assessment of overall system quality
- *Recommendation from the validation team*.

In addition, a section at the beginning of the report should state that management authorizes the operational use of the system within a regulated environment.

Retrospective validation can also include a procedure or mechanism for situations in which the system produces incorrect data. This procedure should include information such as who should be informed and how to account for decisions made using poor data. Judging the risk of this occurrence to be low in our situation, we did not complete such a section because the system was neither unique nor built in-house. However, if we had done this work it would be discussed in the validation summary report as an assessment of anomalies and overall system quality.

Upon completion of the validation summary report, line managers released the system for operational use.

Future Expansion

Changes in the release date for the new version of the software necessitated system expansion with the addition of new A/D units for new chromatographs and additional client workstations for new users. To meet this need we developed a test plan specifically designed for network expansion. The plan describes how new A/D units and new client computers should be tested after adding them to the Millennium network.

It discusses the use of the installation qualification test scripts for the client computers and calls for running specific operational qualification test scripts to demonstrate that the client computers and the A/D units are operating correctly.

Before executing the test scripts under this plan, we would need to submit and receive approval for a change request, make the changes and test them with specified test scripts and write a validation summary report for the extension to ensure that the system remained in compliance.

Service level agreement: When companies outsource the support for the hardware platforms and network that interface the chromatography data system software with the internal information technology department, they must write a service level agreement. This agreement should cover procedures such as data back-up and recovery, data archiving and restoration, data storage and long-term data archiving, and disaster recovery. It should cover the minimum agreed-upon service levels along with measurable performance levels to enable effective monitoring of the service.

Summary

Retrospective validation of a chromatography data system usually involves more tasks than a prospective validation effort because missing documentation must usually be written after the system is already installed and operational. Furthermore, validation of a chromatography data system is more than just testing the system's A/D converters, as this article shows.

Documented evidence of activities is a mandatory requirement for validation. Some of the key documents are

- a user requirements specification that defines what is required of the system and facilitates the definition of qualification testing
- a validation plan that defines all activities required to get the system into compliance, defines the package of documented evidence and controls the system throughout its operating life
- an effective and efficient change control and configuration management system, which is the key to ensuring continued operational validation status of the system.

Validation is a team exercise involving participation of the vendor, the users, information technology personnel (where appropriate) and external expertise (also where appropriate). It is not a one-time exercise but an ongoing journey in which understanding and technology transfer of validation skills are prerequisites if users are subject to regulatory inspection.

References

(1) J. Moore, P. Solanki and R.D. McDowall, *Lab. Auto. Info. Mngmnt.*, **31**, 43–46 (1995).

(2) P.D. Lepore, *Lab. Info. Mngmnt.*, **17**, 283–286 (1992).

(3) *The Application of GLP Principles to Computerized Systems* (Organization for Economic Cooperation and Development, Paris, France, 1995).

(4) *Koseisho, Good Laboratory Practice Attachment: GLP Inspection of Computer System* (Japan Ministry of Health and Welfare, Pharmaceutical Affairs Bureau, Tokyo, Japan,1988) pp. 157–160.

(5) *United Kingdom Compliance Program: The Application of GLP Principles to Computer Systems* (UK Department of Health, Good Laboratory Practice, London, UK, Advisory Leaflet Number 1, 1989).

(6) *Good Manufacturing Practice for Medicinal Products in the European Community, Annex 11* (Commission of the European Communities, Brussels, Belgium, 1997).

(7) *Good Automated Manufacturing Practice Guidelines, Version 3*, March 1998.

(8) B. Boehm, "Some Information Processing Implications of Air Force Missions 1970–1980," Rand Corp. (Santa Monica, California, USA, 1970).

(9) L. Huber, *Validation of Computerized Analytical Systems* (Interpharm Press, Buffalo, Illinois, USA, 1995).

(10) R.D. McDowall, "The Use of Work Flow Analysis in the Validation of a Chromatography Data System," paper presented at Computers in Analysis meeting, London, UK, October 1997.

(11) *Process Validation Guidelines* (US Food and Drug Administration, Washington, District of Columbia, USA, May 1987).

(12) Software Test Documentation, IEEE Standard 829–1983 (Institute of Electronic and Electrical Engineers, Piscataway, New Jersey, USA,

Software Test Documentation, 1994).

(13) R.D. McDowall, *LC•GC Int.*, **10**(10) 648–654 (1998).

(14) M. Freeman et al., *Pharm. Technol. Eur.*, **7**(10), 40–46 (1995).

(15) "Validation of Computer-Related Systems, Parental Drug Association, Technical Report Number 18," *J. Paren. Drug Assoc.*, **49**(1), S1–S17 (1995).

(16) C. Burgess, D.G. Jones and R.D. McDowall, *LC•GC Int.*, **10**(12), 791–796 (1997).

(17) *U.S. Food and Drug Administration, Guidelines, Recommendations and Agreements*, 43 FR 45077 (Part 211, Section 211.63, Equipment Design, Size, and Location) (Government Printing Office, Washington, District of Columbia, USA, 29 September 1978).

(18) *A Definition of Year 2000 Conformity* (British Standards Institute, London, document number PD-2000-1, 1997).

(19) R.D. McDowall, *Sci. Data Mngmnt.*, **2**(1), 8–19 (1998).

(20) R.D. McDowall, *Sci. Data Mngmnt.*, **2**(2), 8–13 (1998).

(21) Software Validation and Verification Plans (Institute of Electronic and Electrical Engineers, Piscataway, New Jersey, Software Engineering Standards, IEEE Standard 1012-1986, 1994).