Validation of Spectrometry Software

Part III — Vendor Audit, System Purchase, and Preparation for Installation

R.D. McDowall

R.D. McDowall is a visiting senior lecturer in the Department of Chemistry at the University of Surrey, principal of McDowall Consulting (Bromley, UK), and "Questions of Quality" column editor for *LCGC Europe*, *Spectroscopy*'s sister magazine. Address correspondence to him at 73 Murray Avenue, Bromley, Kent, BR1 3DJ, UK.

Let's take a step backward before looking at vendor audits and the purchase of your system.

Since the publication of the first two articles in this series (1, 2) the U.S. Food and Drug Administration (FDA) issued a draft guidance for industry on electronic records and electronic signatures (*21 CFR 11*) validation in September 2001 (3). Before we continue down the system development life cycle, it is worth reflecting on what I wrote in the last two parts of this series to check against this draft guidance to reinforce my points.

FDA Draft *21 CFR 11* Validation Guidance

Some of the key points from this draft guidance document are quoted and discussed below.

Write a validation plan. A validation plan is a required document — according to the FDA, a "strategic document that should state what is to be done, the scope of approach, the schedule of validation activities, and tasks to be performed.

"The plan should also state who is responsible for performing each validation activity. The plan should be reviewed and approved by designated management."

Although all of these items need to be part of a validation, I disagree that the schedule needs to be part of the validation plan; time scales invariably slip and I would recommend, from a practical perspective, that the schedule or project plan be separate from the validation plan.

Specify your requirements. The FDA draft guidance discusses the main points in the life cycle of a computerized system and makes the point that a systems requirements specification (SRS) is required. Earlier in this series of articles, I used the term user requirements specification (URS), but these terms are equivalent.

Regardless of whether or not the spectrometry software is purchased off-the-shelf with or without in-house modifications such as macros, custom calculations, or routines for spectral manipulation, establishing documented end user requirements is extremely important for computer systems validation.

In the FDA's view, "Without first establishing end user needs and intended uses, we believe it is virtually impossible to confirm that the system can consistently meet them." Put in the bluntest way: Without a requirements specification, you can't validate your spectrometer and its computerized system.

> "Once you have established the end user's needs and intended uses, you should obtain evidence that the computer system implements those needs correctly and that they are traceable to system design requirements and specifications. It is important that your end user requirements specifications take into account:
>
> • predicate rules (the Good Laboratory Practice [GLP] or Good Management Practice [GMP] regulations to which you normally work),
>
> • part 11, and
>
> • other needs unique to your system that relate to ensuring record authenticity, integrity, signer nonrepudiation, and, when appropriate, confidentiality."

In relation to some of the part 11 controls you should consider in the SRS, we discussed the controls required for security and access to the system in the last article (2).

Just in case you think that by buying commercial, off-the-shelf software, you can get away with doing little or nothing, you're wrong:

> • "Commercial software used in electronic record-keeping systems subject to part 11 needs to be validated, just as programs written by end users need to be validated. See 62

Federal Register 13430 at 13444–13445 (March 20, 1997).

• We do not consider commercial marketing alone to be sufficient proof of a program's performance suitability.

• The end user is responsible for a program's suitability as used in the regulatory environment.

• However, the end user's validation approach for off-the-shelf software is somewhat different from what the developer does because the source code and development documentation are not usually available to the end user.

• End users should validate any program macros and other customizations that they prepare. End users should also be able to validate off-the-shelf software by performing all of the following:

End user requirements specifications. End users should document their requirements specifications relative to part 11 requirements and other factors, as discussed above. The end user's requirements specifications may be different from the developer's specifications. If possible, the end user should obtain a copy of the developer's requirements specifications for comparison.

Software structural integrity. Where source code is not available for examination, end users should infer the adequacy of software structural integrity by doing all of the following:

Conducting research into the program's use history. This research should include:

(1) Identifying known program limitations;

(2) evaluating other end user experiences;

(3) identifying known software problems and their resolution; and

(4) evaluating the supplier's software development activities to determine its conformance to contemporary standards. The evaluation should preferably be derived from a reliable audit of the software developer, performed by the end user's organization or a trusted and competent third party. [This evaluation is otherwise known as a vendor audit. We'll cover approaches to this in more detail later in this installment.]

Functional testing of software. End users should conduct functional testing of software that covers all functions of the program that the end user will use."

This point is an important one that should be remembered for the requirements specifications: Functions not used do not need to be validated and can be excluded in the SRS; however, this means that the users must be vigi-

lant and not use unvalidated functions for regulatory work. We'll be discussing this aspect of validation in the next article in this series.

Overall, the contents of the first two articles in this series stand up well to the draft validation guidance document and specific areas such as the need for an SRS or URS given added emphasis. Okay, now back to the plot . . .

Vendor Certificates and Vendor Audits

Many spectrometry vendors will be certified to ISO 9000 of some description and may offer you a certificate that the software is validated. This is fine, but please note, as mentioned earlier, that you are responsible for validation, and the certificate only covers the part of the life cycle (design, build, and test) that the vendor is responsible for. Note also that no requirement exists for product quality in any ISO 9000 schedule, and, if you look at the warranty of any software product, there is no guarantee that the software is either fit for purpose or error free. The certificates are fine, but if the system is critical to your operation, then a vendor audit looms large, as outlined in the validation guidance.

The vendor audit should take place once the system and vendor have been selected but before you have placed the order. The purpose is simply to see if a quality system exists and is applied effectively to the design, build, and maintenance of the software. The evaluation and audit process is a very important part of the life cycle because it ensures the design, build, and testing stages (which are under the vendor's control) have quality built into the software. The audit should be planned and should cover items such as the design and programming, product testing and release, and documentation and support phases. After the visit, a report of the audit should be written and will be part of the validation documentation.

The process, running in parallel with the definition and selection of the vendor, is to:

- Define the scope and boundaries of the system or application.
- Assess the business and regulatory risk of the system.
- Make a decision — if business and regulatory risk is high, then a vendor audit is required; if low, then no further action is required.
- Notify the selected vendor of your intention to audit; if they refuse, then select another supplier.
- Agree on a date and send the audit checklist.
- Conduct the audit and report the results.
- Decide if the vendor is acceptable and purchase the system; if not, either select another vendor or start a process of supplier management.

Your overall purpose in a vendor audit is to determine the quality of software development and what you, as a user, should do to ensure that the sys-

tem selected and the company that supplies it are suitable. The overall philosophy that I would like to present is that the software vendor should become an extension to the laboratory and a business partner; however, it is a two-way street: what the vendor should do for the purchaser should be reciprocated by the purchaser to the vendor.

What Is an Audit?

This question presents a good starting point for discussion. An audit is essentially an independent check of a service or a product (here, a product can be defined either as a unit of work or as a finished product). There are three types of audits: first-, second-, and third-party.

If the audit is done from inside an organization, it is called a first-party audit. Normally this audit is achieved through either a separate quality assurance group specifically established for the role or by using part-time staff from other areas that are independent of the audited area. The focus will be either on the quality of work or to see if written procedures have been followed, or possibly both.

A customer, or somebody on their behalf who will assess the vendor and their ability to design, produce, and maintain a product or service, performs a second-party audit. We will spend most of the time discussing this class of audits in this installment. Audits on behalf of customers can be applied to suppliers of raw materials, components, or software — practically anything where the quality of the product can affect the operation or output of the customer. Obviously, in this article we will only examine the spectrometry software.

A third-party audit occurs through an independent accreditation body using guidelines published by the International Standards Organization (ISO) or its equivalent. This results in the vendor being certified under a particular quality scheme; furthermore, this type of audit is ongoing, with surveillance visits every 6–12 months and reassessment visits every 3–4 years, depending on the quality scheme.

Obviously, the further removed an audit party is from the organization that did the work, the more objective the result will be; however, the intimate knowledge of the individuals and the processes involved is much less. Therefore, when considering a vendor audit, we are looking at a second-party audit by yourselves or your representatives, such as a consultancy that specializes in this work. The use of third-party audits through accreditation bodies and their agents may back this process.

The principles I would like to discuss are: how far can you take work on trust — especially if you work in a regulated industry — and how much do you have to verify through an audit? The short answer is that you have to use your best judgement — see the draft FDA guidance presented earlier and the discussion following.

When Do I Audit?

The short answer is "before you purchase." In the honeymoon period between selecting a system and placing an order, the vendor can be very helpful. This attitude may change after the application or system is delivered. Therefore, if any corrective actions require money being held back to ensure that those actions are completed, it is best to get them onto the table as early in the process as possible because it is difficult to recover from a poor bargaining position as it will invariably involve more time for discussions or legal action.

One exception to this rule is when you are undertaking a retrospective validation of a system. If the system is crucial to the operation of the laboratory and has a long lifetime, then a vendor audit is highly recommended. However, if the system will be replaced in the short to medium term, it would be better to put the resources into a more rigorous validation of the replacement system.

Parallel with the vendor audit, you should review the vendor's contract; as a result, you may also want to negotiate some terms in the contact. Combining

the two makes for good timing and good sense.

Assessment of Business, Regulatory, and Compliance Risk

Do you need to audit all vendors of spectrometry software packages? Look at the system you are purchasing and its function. What is the impact of the system on your organization?

- Is it an application that is only used for research with little impact on the organization, or is it used for product release or in-process testing with a greater impact in terms of time or money lost through production delays if the system is unreliable?
- Does the system hold data that are valuable for your organization?
- Does the system directly affect the quality, safety, or efficacy of a product?
- Does the system store or manipulate data or information that is used to support patent applications?

You should consider auditing the vendors of systems that have a major impact on your organization, not just from the perspective of the regulations but from good business sense.

For these critical software applications, the approach is taken on trust with verification of the process through a vendor audit. The phrase "trust but verify" comes from the disarmament process of nuclear weapons between the former USSR and the United States. During that process, the actual destruction of the nuclear weapons was open to inspection to the other side, either by on-site inspections or by using spy satellites.

ISO 9000: Saint or Sinner?

Many companies that could be audited will be ISO 9000 certified. Is it worth auditing these companies? They have a quality system in place and produce a quality product — don't they?

Much is made of ISO 9000 accreditation and certification, especially by vendors, because they promote a quality philosophy with an organization. The philosophy behind ISO 9000 is to document procedures and processes to ensure that they are adequately controlled and that output is consistent. This is similar in many ways to other quality schemes, such as GLP, GMP, and ISO Guide 25.

However, it is important to note that ISO 9000 does not guarantee product quality.

The underlying principle that ISO 9000 is based on is that organizations that follow documented practices and procedures in a consistent manner are more likely to create products that meet the customer's needs than those organizations that do not follow accepted practices and procedures.

A skeptical or alternative view of ISO 9000 is that it produces a poor product with bad processes that are well documented. You should never buy a software application, or any product for that matter, based only on ISO certifica-

The proposal says:

"Software products are designed to operate with standard computer hardware in the typical laboratory environment. Their design functionally integrates laboratory instruments and results in a unified information architecture that allows for more effective use and control of laboratory data. This enhances the value and utility of the data, especially when measured against regulatory compliance.

"Validating laboratory software is becoming more complex resulting in escalating costs and longer time scales. Because the company has achieved ISO 9001 and TickIT certification, while stressing a high level of commitment to open industry standards and software design, customer validation is made easier. ISO 9001 with TickIT certification can significantly reduce time on customer audits of vendor facilities as well as user functional validation."

The contract says:

"The company makes no warranties that errors have been completely eliminated from any licensed software. The company makes no other warranties, express or implied, including but not limited to fitness for a particular purpose or merchantability with respect to any licensed software."

tion of the company, as we will discover later in this installment — hence the importance of the SRS in defining the application you want, followed by time spent to evaluate and select vendors in the marketplace.

Let us explore in more detail the two key elements for ISO 9000. The first is the quality manual and the associated documented procedures it covers; the second is the scope of certification open to vendors.

The quality management system is universal to all ISO schemes and covers four overall areas:

- Quality policy statement
- Quality manual with overviews of areas such as organization, roles and responsibilities, training records, quality function, customer complaints, and so forth
- Written and authorized procedures detailing how the policy and manual will make the system effective
- Internal audits by the quality manager or representatives.

Flavors of ISO 9000

Regarding the second key element, three main types of ISO 9000 certification cover the whole or parts of a product or service life cycle:

- ISO 9001: quality assurance in design, development, production, installation, and servicing.

Conformance to specified requirements is to be assured by the supplier throughout the whole life cycle of a product or service (4).

- ISO 9002: quality assurance in production, installation, and servicing.

Conformance to specified requirements is to be assured during production, installation, and servicing (5). Note that research and development is not covered under this scheme.

- ISO 9003: quality assurance in final inspection and test (6).

Conformance is to be assured by a supplier only at the final inspection and test.

ISO 9001 and ISO 9000-3 Compared

ISO 9001 is not specific enough in the case of software, which resulted in the production of ISO 9000-3 guidelines specifically for software (7). The reason is that, with software, a need exists to coordinate the activities of both the purchaser and the supplier to ensure that the delivered product is fit for purpose. Especially for software, in contrast to normal research and development

activities, both the supplier and the purchaser have responsibilities for the specification, selection, installation, and support of the software product.

The first of the user's responsibilities is the writing of an SRS as outlined in a previous "Focus on Quality" column (1). Of course, if the purchaser ignores its responsibilities, then one of the main principles of ISO 9000-3 simply collapses. This is the quickest way to throw the investment in any software product down the drain.

The uniqueness of software is shown in the fact that the ISO 9000-3 guideline is double the size of the ISO 9001 document; a simple, but empirical, method of demonstrating the complexity of the system development life cycle. Therefore, look closely at the ISO certificate from your vendor.

- Which version of ISO is it?
- What is the scope of certification?

Would a computer application produced by a vendor with ISO 9002 certification be useful for you? Consider the design: it is not covered under this scope of certification. Why? Was the application designed on the backs of used envelopes and cigarette packets? Alternatively, with an increasing number of companies, the software may be written in one country, yet the ISO certification is for marketing in another country. Again, the bottom line is: do not take things at face value.

ISO 9000 and Regulatory Compliance

The *FDA Draft Guidance for Industry* states, "We do not consider commercial marketing alone to be sufficient proof of a program's performance suitability" (3).

Any ISO accreditation scheme is voluntary and not mandatory, unlike GMP. A company can voluntarily enter and leave the scheme. Alternatively, if problems exist, the accreditation body can suspend an organization's certification, or the organization can voluntarily withdraw from the scheme.

With programming costs rising in the developed world, many companies are outsourcing their programming to third-world countries where these costs are lower. Some companies with this practice can be ISO 9000 registered; however, often the scope of accreditation means that only the overall process may be covered. Sometimes the detailed programming and testing was done in another country — usually India, which writes about 50% of the world's software — and the company used may not be ISO 9000 accredited.

Marketing Hype and Contracts

It is interesting to look at the Dr. Jekyll and Mr. Hyde approach of companies when it comes to marketing their products through proposals and protecting themselves through contracts. For large purchases, if you have not already done so, it is very useful to read both the marketing material and the contract. This process can be very instructive, as we can see from the sales response to

questions on compliance with GLP guidelines and their contract terms and conditions.

The actual example in the sidebar (on pg. 72) is from a proposal by a company with ISO 9001 certification. In the top paragraphs, we can see the proposal showing the benefits of the quality approach and the way that regulatory inspection can be facilitated. Compare this with the bottom paragraph, which shows the appropriate section from the contract of the same company; it states that the company is not responsible for errors in their own software.

This contrast is interesting; vendors are carrying out a delicate balancing act between trying to sell the product while maintaining their legal position. The difference between the two is the type of person who is writing the individual document and their goals. Again, the bottom line is to balance the sales message with the realism of the contract.

This situation again emphasizes the fact that you and you alone are responsible for ensuring that the product you purchase is fit for purpose.

Again, nothing in ISO 9000 addresses the fitness for *your* purpose nor the quality of the product. These aspects will always remain the buyer's responsibility — as the regulations, guidelines, and vendor's contracts make absolutely clear. Being informed is better than being unaware, and you can make better decisions. ISO 9000 or not — buyer beware!

The Scope of an Audit

Having arranged the audit with the vendor, what type of audit will you perform? Three main types of audit are possible: company, quality system, and product audits.

Normally a checklist is used as a guide to the audit. Any checklist will have to be customized for each vendor and the associated product as there may be specific areas to audit. The key to determining what you do is to match what the system or product is going to do with the impact that it will have. For a very critical system, all three areas may be audited; for a lower-risk application, only the company should be audited.

The coverage for each area is typically as follows:

• The company — covers general background information such as company history, size, previous experience with the industry you are working in, and written standards and procedures for the life cycle of the product using a defined life-cycle model. This kind of investigation can also include the delivery and installation services, service support after purchase, training of personnel, training services, and escrow services (to ensure you have access to the software if the company goes bankrupt). This type of audit can be used as the basis of a remote audit if some specific product questions are added. This audit can also be a part of the selection process by asking the company to present an overview of itself and its approaches to quality.

• The quality management system (QMS) — the quality system of the vendor is examined through a series of questions about the quality system and how it is reviewed and maintained. If the vendor is certified, the standard and scope of certification should be established with a copy of the certificate. There should be written standards for developing, programming, and testing the application coupled with procedures for change control, configuration management, and document review. Training of staff in the application of the QMS, as well as the roles and responsibilities of individuals, should be clearly stated in each. Evidence of continuous improvement and evolution of the quality system is very important. A rough rule of thumb is that if the quality system is static, it means it is not working and is just being used for marketing purposes.

• The product — a product audit may look at similar topics to the quality system, with the exception that the questions are focused more narrowly on a specific product or service. Some overlap with the quality system questions may arise, but this is part of the customization process. Ask here about the programming and structural testing of the product, where individual units

and modules of code are integrated together and tested until the final product is ready. If different operating systems and hardware platforms are supported, ask how much development and testing your version received compared with other units; you may be surprised to find out how little was — especially if you are the old purchaser of this configuration. Manufacture and dispatch of the software, change control, communication of problems, and software updates are all areas to examine.

The overall aim of these areas is to gain the confidence that the company knows what it is doing and that the quality of the product you are purchasing is adequate for the purpose to which it will be put.

The Role of a Checklist

Audit preparation? Yes, please! Preparation for an on-site vendor audit is essential because your time will usually be limited, and you must concentrate on key areas. In my experience, a checklist is a good way to go, but do not become a slave to the checklist. If concerns appear in critical areas, then pursue them and leave some other parts of the checklist incomplete.

Should you give the vendor a copy of your checklist before arriving? Two schools of thought exist on this one: yes and no! Personally, I favor being open because nobody can fabricate a quality system and quality system development documentation in the one or two weeks between sending the checklist and auditing the company. Therefore, I would let a vendor have the checklist as it allows them to prepare and have documentation ready and people available.

It is important to remember that the aim of the audit is to gain an impression of the quality procedures of the vendor. Note the use of the word "impression" — you are getting a snapshot of the process, not an in-depth working knowledge of the vendor's system. To help you draw conclusions as you follow the checklist, you will collect evidence (copies of documents and so forth), subject to confidentiality of the vendor, of the tasks involved in development of the software product that you are proposing to purchase as you go through the audit. This evidence will help you in preparing the audit report later. Take notes as you go through the meeting. If more than one person is involved in the audit from the purchasing organization, the option always exists to split tasks and cover ground in parallel. Alternatively, if all are involved in the audit process together, it is possible to devise roles for each before the meeting takes place. For instance, the lead auditor could conduct the questioning, another could read procedures for correctness, and another listen and ask questions as opportunities arise.

However, do not let the vendor run the audit. You are in charge. Some vendors take the opportunity to run the show and can intimidate unwary auditors. Treat such approaches with caution and dig for information and evi-

dence that activities have been carried out. Care must be exercised, as even the largest software companies can have poor-quality products.

Some items for discussion during the audit include:

• Scope of certification. This is available on the certificate held by the vendor (usually framed in a prominent position in their facilities). A copy of the certificate should always be requested. What does the scope of certification cover? All of the activities for the product or service you require? One or two? None?

• Traceability of a requirement from the concept, through design and testing, to documentation in the user guide. This is very important and essential. It is also instructive to see the quality that is built into the product for one item that is selected at random.

• During the vendor audit, care should be taken to see if there is a procedure whereby management can override the quality system. This can totally negate the quality system, but it will be acceptable under ISO 9001 or ISO 9000-3 as it will be a written procedure. This area must be treated with extreme caution.

• Testing to fail. Most tests are designed to pass by vendors. Quality is also determined by testing to fail. If this procedure is not done adequately when you trace a requirement through the life cycle, what is the implication for the whole product?

Once the main part of the audit is over, the team should have time to collect their thoughts, discuss their findings, and draw conclusions. This is a private meeting for the auditing team to discuss their findings together before the closing meeting.

At the closing meeting, the conclusions of the audit team are presented and discussed with the vendor. This is an opportunity to correct any misinterpretations before the report is written and is therefore a two-way process.

A Practical Approach to Audits

Let's be honest; a vendor audit takes time to prepare, execute, and report for both the vendor and the organization. What should be the approach to a vendor audit? What is fair and reasonable and balances both the vendor's time and your time?

On-site or remote audit? The first question is: should we perform an on-site or remote audit, or both? A remote audit is essentially acquiring an overview of the company and the product's quality profile through material supplied by the vendor. This process is achieved either by asking a number of questions or requesting if an information pack on this subject exists. This approach is cost effective for both the vendor and you because it provides a minimum level of cover for the laboratory. Some information you may obtain this way might be:

- Overview of a vendor's quality policy
- A copy of the ISO 9000 accreditation certificate and scope (Does it cover all aspects of your product or service?)

- Brochure covering the product or service you require
- Documentation covering the development and testing of a product
- Specific answers to your questions. A typical one may be concerning the availability of software source code to regulatory agencies should the need arise, or an escrow agreement if the company goes bankrupt.
- Financial history of the company during the past three to five years (annual reports and so forth).

An alternative approach is the use of the Pharmaceutical Drug Association's Audit Repository Center, which uses a standard checklist outlined in Technical Report 32 (8).

Purchase Order: Defining the Initial Configuration

Once the hurdle of the vendor audit is over, you can agree to any contract changes and then order the instrument and software. The purchase order is important because it defines your initial configuration of the system including instrument, software, and documentation, as we'll see in the next two installments of this series.

Preparing for the Installation

When you order, you also can start preparing the space where the instrument and associated data system will be used. Many spectrometers will not require any preparation apart from cleaning the bench space before delivery; however, some instruments may require checks and installation of services, such as floor loading, electricity and water supply, and so forth. These checks need to be documented to ensure that GMP requirements are met for equipment location.

Next time we'll look at the qualification of the instrument and system.

References

1. R.D. McDowall, *Spectroscopy* **16**(2), 32–43 (2001).
2. R.D. McDowall, *Spectroscopy* **16**(7), 30–34 (2001).
3. "FDA Draft Guidance for Industry, *21 CFR 11* Electronic Records and Electronic Signature Validation," Food and Drug Administration, Washington, DC, 2001.
4. "ISO 9001: Quality Management and Quality Assurance in Design/Development, Production, Installation and Servicing," International Standards Organization, Geneva, Switzerland, 2000.
5. "ISO 9002: Quality Systems. Model for Quality Assurance in Production and Installation," International Standards Organization, Geneva, Switzerland, 2000.
6. "ISO 9003: Quality Systems. Model for Quality Assurance in Final Inspection and Test," International Standards Organization, Geneva, Switzerland, 1988.
7. "ISO 9000-3: Quality Management and Quality Assurance Standards. Part 3, Guidelines for the Application of ISO 9001 to the Development, Supply and Maintenance of Software," International Standards Organization, Geneva, Switzerland, 1991.
8. "Auditing of Suppliers Producing Computerized Products and Services for Regulated Pharmaceutical Operations, Technical Report 32," Pharmaceutical Drug Association, Baltimore, MD, 1999. ■