Imagine the following situation: You are sitting at your computer terminal late on a Thursday afternoon trying to get enough work finished to make Friday an easy day and then disaster strikes. A message appears on-screen that the computer systems will be unavailable during the weekend because the latest version of the network operating system will be installed.

Did you know about this upgrade? No, of course not. The information technology department never tells you about things like this, but it doesn’t make any difference to you or your validated chromatography data system, does it? Of course not, you think, but unfortunately it does.

When you return on Monday and try to log on — assuming that the upgrade went without any problems — your previously validated chromatography data system is no longer validated. A change has taken place that was unplanned, uncontrolled, untested (except for when you log on and try to use it), and undocumented. Oh dear, what can you do?

As I wrote in the last article in this series (1), the initial validation effort for a chromatography data system from concept to operation is the easy part of the project. This process may take 4–12 months, depending on the size of the project. However, this period is just the start of the validation voyage. You will make a large investment in time and effort in validating the system. The lifetime of a data system can be as long as 10 years, and you’ll need to maintain the validation status of the system throughout that lifetime if you want to maintain the quality of your data. The question is will you sink or swim during the validation voyage?

Consider the challenges that you face with continuing validation of a chromatography data system or any other system. The main theme of this article is managing change in a changing world. The following types of changes can affect an operational chromatography data system:

• finding software bugs and installing associated fixes
• upgrading application software, operating systems, plus any software tools or middleware used by the chromatography data system
• making network improvements, such as changes in hardware, cabling, routers and switches to cope with increased traffic and volume
• making hardware changes, such as PC and server upgrades or increases in memory or disk storage
• interfacing new applications (for example, spreadsheets or laboratory information management systems [LIMS])
• expanding or contracting the system because of work or organizational needs
• adjusting to environmental changes, such as moving or renovating laboratories

All of these changes must be controlled to maintain the validation status of your chromatography data system.

In addition, other factors can affect the system from a validation perspective. These factors include problem reporting and resolution, software errors and maintenance, back-up and recovery of data, archiving and restoring data, maintenance of hardware, disaster recovery (business continuity planning), and written procedures for all of these.
11.2 The extent of validation necessary will depend on a number of factors, including the use to which the system is to be put, whether the validation is to be prospective or retrospective and whether novel elements are incorporated. Validation should be considered as part of the complete life cycle of a computer system. This cycle includes the stages of planning, specification, programming, testing, commissioning, documentation, operation, monitoring, and modification.

11.3 Attention should be paid to the siting of equipment in suitable conditions where extraneous factors cannot interfere with the system.

11.4 A written detailed description of the system should be produced (including diagrams as appropriate) and kept up to date. It should describe the principles, objectives, security measures, and scope of the system and the main features of the way in which the computer is used and how it interacts with other systems and procedures.

11.8 Data should only be entered or amended by persons authorized to do so. Suitable methods of deterring unauthorized entry of data include the use of keys, pass cards, personal codes, and restricted access to computer terminals. There should be a defined procedure for the issue, cancellation, and alteration of authorization to enter and amend data, including the changing of personal passwords. Consideration should be given to systems allowing for recording of attempts to access by unauthorized persons.

11.10 The system should record the identity of operators entering or confirming critical data. Authority to amend entered data should be restricted to nominated persons. Any alteration to an entry of critical data should be authorized and recorded with the reason for the change. Consideration should be given to building into the system the creation of a complete record of all entries and amendments (audit trail).

11.11 Alterations to a system or to a computer program should only be made in accordance with a defined procedure which should include provision for validating, checking, approving and implementing the change. This type of alteration should be implemented only with the agreement of the person responsible for the part of the system concerned and the alteration should be recorded. Every significant modification should be validated.

11.13 Data should be secured by physical or electronic means against willful or accidental damage, in accordance with item 4.9 of the guide. Stored data should be checked for accessibility, durability and accuracy. If changes are proposed to the computer equipment or its programs, the above mentioned checks should be performed at a frequency appropriate for the storage medium being used.

11.14 Data should be protected by backing up at regular intervals. Back-up data should be stored as long as necessary at a separate and secure location.

11.15 There should be available adequate alternative arrangements for systems that need to be operated in the event of a breakdown. The time required to bring the alternative arrangements into use should be related to the possible urgency of the need to use them. For example, information required to effect a recall must be available at short notice.

11.16 The procedures to be followed if the system fails or breaks down should be defined and validated. Any failures and remedial action taken should be recorded.

11.17 A procedure should be established to record and analyze errors and to enable corrective action to be taken.

11.18 Data should only be entered or authorized for recording of attempts to access by unauthorized persons.
systems; however, they included only the minimum requirements for written procedures (3). These should cover, but not be limited to, the following:

- procedures for the operation and use of computerized systems (hardware and software) and the responsibilities of personnel involved
- procedures for security measures used to detect and prevent unauthorized access and program changes
- procedures and authorization for program changes and the recording of changes
- procedures and authorization for changing equipment (hardware and software), including testing before use if appropriate
- procedures for the periodic testing of the complete system or its component parts and recording the results of these tests
- procedures for maintaining computerized systems and any associated equipment
- procedures for software development and acceptance testing and recording all acceptance testing
- back-up procedures for all stored data and contingency plans in the event of a breakdown
- procedures for archiving and retrieving all documents, software, and computer data
- procedures for monitoring and auditing computerized systems

It is important to realize that if you are working according to GMP regulations, complementary information from good laboratory practice (GLP) regulations is available, and vice versa.

### Change Control and Configuration Management

When I audit any operational computer system, I start my investigation by looking at the changes to the system during any period of time throughout its operation. The explanation is that most computer systems change over time for a variety of reasons, as I described at the beginning of this article. Changes always occur, even to an integrator that uses firmware. Because few systems remain in their initial configuration for long, it is essential to track all modifications to a system over time. Again this reiterates the original purpose of many quality guidelines: being able to repeat conditions under which the work was done originally.

The key question from an inspector’s perspective that must be answered is whether there is demonstrable control of these changes. In many instances there is no control of the changes, and, therefore, the system is out of control.

### Definition of terms: A number of terms must be considered. The first two are change control and configuration management.

#### Change control: Change control is the systematic process by which any change to a computerized system is proposed, coordinated, evaluated, rejected or approved, and implemented (including testing and revalidation as necessary).

#### Configuration management: Configuration management is a system for identifying the configuration of hardware, software, and firmware at discrete points in time with the purpose of systematically controlling changes to the configuration and maintaining the integrity and traceability of the configuration throughout the system’s life cycle.

These two terms are very closely linked and some organizations have condensed them to change management to cover all aspects of the control of a chromatography data system or any other computerized system. Configuration management also can be applied to software development and refers to the control of the versions of the software modules produced. However, for the purposes of this article, I will use it only in the wider context of the configuration of the chromatography data system as I’ll describe below.

Other terms for defining configuration management include configuration item and baseline.

#### Configuration item: Configuration items are the individual components in a configuration management system. Items can include hardware (server or PC), software (application, software utilities, and operating system) and peripherals (analog-to-digital converter [A/D] units, and printers). It is very important that each configuration item is defined carefully; if the definition is too detailed, the process will be too resource-intensive to operate, but if it is too general, the information generated will be useless.

#### Configuration baseline: The configuration baseline is the establishment of the initial configuration of the computerized system from the configuration items. If a system undergoes rapid expansion, it may be necessary to redefine the baseline.

#### Change control process: According to Nakagawa (4), an established change-control process is important. Although this book is about LIMS, the principles for change control are the same for a chromatography data system. The change-control process should aim to establish an environment conducive to open discussions
and exchange of views. The stakeholders in the system should be polled for their views, ideas, and possible solutions; in short, they should be asked to provide any input to improve the quality and performance of the system. This approach avoids the situation outlined at the start of this article in which unannounced changes can destroy the validation status of all systems running on a network, hence the importance of a coordinated approach to managing change.

A typical change-control system is characterized by the following criteria; namely, the responsibilities of all parties are defined, the process is managed, and the process is documented. The process is outlined in Figure 1 and is based in part on the work of Nakagawa (4), Chapman (5), and my experience.

Roles and responsibilities: The three roles outlined in the last article in the series (1) are still important in a regulated or accredited laboratory for change control and configuration management, as well as all other aspects of validation.

- Users hold overall responsibility for the operation of the chromatography data system under the regulations and guidelines, especially in deciding whether to implement changes to the system. They also are responsible for maintaining the configuration records of the system.
- Information technology staff are subcontracted by the users to provide technical expertise to assess the technical feasibility and impact of changes. Information technology managers do not implement changes to operating environments or systems unless authorized. They operate the subcontracted functions of the system in a compliant way.
- The quality assurance personnel provide compliance information and advice and review key documentation to assess compliance with regulations. They also perform periodic reviews of the system to ensure conformance with the regulations and guidelines.

See the Validation Roles and Responsibilities section in the previous article for other responsibilities in validation for these three roles (1).

Procedure: The first part of the process is a request for change; this step requires basic information such as who requested the change, the nature of the change, and justification for the requested change. The request for change may result from a variety of reasons. First, it may be the reporting of a bug or feature of the chromatography data system software that should be resolved, abnormal system performance, or a request for additional resources such as a printer, A/D unit, PC, or extra disk space. Whatever the change, it must be documented. The method for this documentation should be as simple as possible, keep paperwork to a minimum, and encourage everyone using the system to comply with the process. Alternatives for larger organizations include using a central help desk that can document reported requests or an electronic mail system with standard change request forms.

Second, the request should be analyzed for its impact. You must assess a number of facets here; for example, its effect on the laboratory, the organization, and also on the system itself. In examining how the change affects the laboratory, you should consider the time required to implement the change; the cost of the change, including documentation and training; the physical and human resources required to make the change; and the benefits of making the change.

When looking at the effect of the change on the system, consider the following points:

- Does the change provide a major or minor business benefit?
- Is the change only cosmetic?
- Does it affect the system?
• Are the functions already available?
• If the change is implemented, will it cause any problems to procedure requirements such as training or documentation?
• How much retesting and revalidation will be required?
You also should consider the effect of the change on the organization. Evaluate the answers to the following questions:
• How much will the system change? Change has a large continuum — from no impact through to greater effort required to use the system after the change has been made.
• Will the change bring a cost saving to the organization or is it more expensive?
• Will the change allow for time savings?
• What effect will the change have on the documentation of the system?
• What impact will the change have on the system users; will there be any necessity for retraining?
• What is the effect and cost of doing nothing?
After completing the impact analysis, each change can be reviewed. A management group involving the major stakeholders in the system — users, information technology staff, and quality assurance personnel — can undertake this process. Alternatively, this review can be devolved to a small validation or change-control team consisting of a few individuals authorized to consider and recommend changes. The size of the chromatography data system, the business benefit, and the magnitude of the change should decide the approach.
In this analysis, changes can be reviewed and classified into those that bring major or minor benefits. The prioritization of authorized changes probably needs to be balanced with the available budget and resources, because it is unlikely that all authorized changes will proceed. Inevitably some change requests will be rejected for various reasons. Regardless of the decision by the reviewing group, it is of supreme importance that decisions and the rationale for making them are fed back to the requester.
Third, if the change is rejected, the submitter should be informed of the rejection and the reason for it. However, if the request is approved, the resources should be made available to implement the change. The first stage is to formulate a plan to implement the change. This plan should incorporate any relevant aspects of the impact assessment and any technical issues such as the extent of retesting and revalidation of the chromatography data system, update of documentation, and retraining of users.

The change then is made, and the system is released for use. Hold on a minute! Have you forgotten anything? Are you proposing to make changes to a live and operational chromatography data system? Think again. You should consider a test environment that is at least logically — on the same computer system — or ideally a physically separate environment for making and testing the changes and then rolling out the tested changes to the production environment. Remember also that validation must occur, at least in part, on the operational system, so ensure that everything is fully backed up before you start. You had already thought of that, hadn’t you?

**Changes to a chromatography data system:** Figure 2 is a stylized view of a client—server chromatography data system with a client and a server linked by a network. The server and client comprise hardware, the operating system, and the chromatography data system application software. Note this figure is a stylized representation and may not represent all data systems. I would like to use this diagram as a means of discussing any changes to the chromatography data system to illustrate their impact. Consider the following possible changes to any chromatography data system and the impact that each would have:
• changing the network such as replacement of the cabling or upgrade of hubs or routers; will these have any impact on the operation of the chromatography data system?
• changing a PC client from a 133-MHz PC to a 500-MHz PC
• updating the operating system from Microsoft Windows NT, version 4, service pack 3 to service pack 5
• fitting a software patch to the chromatography data system software to fix a software error
• installing a new version of chromatography data system software

You must assess the effect that each potential change could have on the validation status. For example, a hardware change from a 133- to a 500-MHz client PC is relatively small compared with the upgrade from Microsoft Windows NT, version 4, service pack 3 to service pack 5 or the new version of the chromatography data system software.

**Configuration management:** Configuration management, as defined above, is a set of procedures to ensure adequate identification, control, visibility, and security of any changes made to hardware; firmware; networks; software, including any patches and macros; specialized equipment associated with the application, such as the A/D units for your chromatography data system; and peripherals, such as printers and plotters. Furthermore, all modifications should be authorized before a change is made, and the personnel making the changes also should
be authorized to do so by management through the change-control process as outlined above. Therefore, configuration management and change control are very closely linked.

The goal of configuration management is to demonstrate that the system is under control and all modifications to it are tested and validated when appropriate. Someone can recreate either the current or any previous versions of the system from the information in the configuration management log. The system can be recreated at any time; this capability safeguards the laboratory and users against loss of data and also enables users to see the effect of a problem found after a change has been implemented.

The process of configuration management is quite simple. First the initial configuration is established and then all changes are tested, authorized, and monitored, as described below.

• Establish the baseline or initial configuration by compiling a list of the system components. This list should include the release numbers and serial numbers, when appropriate, of the application software programs; the software tools such as a database; and the operating system. If communications or network software are used, the components of this software also should be included or excluded if the network responsibility is another functional unit. The components comprising the hardware—disks, memory, type of central processing unit, add-in boards for the application or communications, and any peripherals—also should be listed. Any documentation used with the chromatography data system should be included in the configuration management system and listed in the log.

• The baseline configuration should be established after the installation of a new chromatography data system, even if the system is used as a test environment before becoming operational. This procedure has a number of advantages: First, all testing and training occur in a controlled environment. Second, the procedures and principles of configuration management are known, understood, and modified, if necessary, before the system is rolled out for operational use. The information for the baseline configuration comes from the purchase order and will be checked off following installation.

• Modifications to the system configuration then can be made and the information recorded in the configuration log or
its equivalent. When new versions of the software are available and installed, master copies of the old version and the relevant documentation should be archived, because they should be considered equivalent to raw data.

**Documentation**

Documentation can be divided into several categories, and each will be discussed in this section. Excluded from discussion is the documentation produced during development and initial validation of the system, which was discussed in detail in part III of this series (1).

**System-specific documentation:** In this article, I will not discuss the documentation supplied with the chromatography data system application or system, user notes, and user standard operating procedures because they are too specific and dependent upon the management approach in an individual laboratory. However, the importance of this system-specific documentation for validation should not be underestimated. Keeping this documentation current should be considered a vital part of ensuring the operational validation of any computerized system. Users should know where to find the current copies of documentation to enable them to do their jobs. The old versions of user standard operating procedures and system and user documentation should be archived.

**Standard operating procedures:** Standard operating procedures are required for the operation of both the chromatography data system applications software and the system itself. As explained above, I have not considered user standard operating procedures in detail. Standard operating procedures are the main media for formalizing procedures by describing the exact procedures to achieve a defined outcome. According to Hambloch (6), standard operating procedures have the advantage that the same task is undertaken consistently, that it is done correctly, and that nothing is omitted. In addition, a written procedure means that new employees are trained faster. The goal is to ensure a quality operation. Laboratory staff are accustomed to working with standard operating procedures; however, if a large system is supported by a central computer group, they may not be used to working with standard operating procedures and even less ready to document their work. To provide a service to a regulated laboratory, a computer department must provide a suitably documented procedure. Indeed, EU GMP Annex 11 (2) requires that a third-party supplier should have a documented operation.

According to Hambloch (6), a minimum of 12 standard operating procedures are required for the operation of a computer system in a regulated or accredited laboratory. These procedures include the following:

**Standard operating procedure on standard operating procedures:** This procedure should describe the approach taken to writing standard operating procedures within the functional group, the sections, who can authorize the procedure, a description of the procedure, and the distribution list.

**Description of responsibilities:** This document defines the roles and responsibilities of staff supporting the computer system.

**System description of hardware and change-control procedures:** This document describes how the hardware components will be maintained (equivalent to the hardware configuration log) and the procedure to be adopted when the system configuration is changed.

**Preventative maintenance:** This portion describes the procedures for preventative maintenance of the hardware components.

**Prevention, detection, and correction of errors:** Included in this document are the measures and procedures for finding, recording, and resolving errors in the system. This standard operating procedure can be complex, can cover many different aspects of the system, and may refer to sections of the technical manuals provided with the system. It includes good housekeeping tasks such as disk defragmentation or monitoring the space available on all disks.

**System booting and shutdown:** This special standard operating procedure should contain all the specific instructions for starting up and shutting down the system. It may be required in an emergency and, therefore, should be well written and easily available for use.

**Control of environmental conditions:** For systems that require a controlled environment, a standard operating procedure should define the acceptable ranges of temperature, humidity, and power supply. Other environmental considerations might include electrostatic discharges, power surges, fire, lightning strikes, or the use and maintenance of an uninterruptable power supply.

**Contingency plans and emergency operation:** This procedure is a disaster-recovery plan, and it uses alternative plans until the computer system has been recovered. It is important that any disaster recovery plan is tested and verified before any disaster occurs.

**Back-up and restoration of data:** This plan describes the procedures for back-up of data and software programs and restoring data to disks.

**Security:** The logical (software) and physical security of the system is covered with the procedures for setting up and maintaining security.

**Installation and updating of software:** These procedures are undertaken before, during, and after installing software. This process should start with the complete back-up of all disks and then installation of the software and any testing and validation that may be required.

**Development and update of system software procedures:** Software can be written to control the system or help execute functions. This standard operating procedure outlines the procedures for the creation, documentation, and modification of these procedures.

I refer readers to the article by Hambloch (6) for more details about these standard operating procedures. However, it is important to realize that the list above refers to a relatively large computer system that is run by a centralized information technology group. For smaller items of laboratory computer equipment, therefore, the list should be reviewed for applicability and suitability. When a system does not have a disk drive or other means to store raw data, no standard operating procedure is required for data back-up and restoration. The same logic should be applied to the whole list. The converse is also true; this list represents generalized standard operating procedures, and a specialized application may need more standard operating procedures than those that appear above.

**Training records:** All people involved with the selection, installation, operation, and use of the chromatography data system should have and maintain training records to demonstrate that they are qualified to perform their functions. It is especially important to have training records and curricula vitae of installers and operators of a system, because this area is particularly weak, and a system can generate an observation for noncompliance. Major suppliers of chromatography data systems usually provide certificates of training for installation of the system and software. However, many information technology departments run chromatography data systems and frequently their personnel lack the relevant training records or curricula vitae.
Training records for users usually are updated at the launch of a system, but they can lapse when a system becomes mature. To demonstrate operational control, training records must be updated regularly and especially after software changes to the system. Error fixes usually require no additional training. However, major enhancements or upgrades should trigger the consideration of additional training. Prudent laboratories document their decisions and the reasons to forego additional training in this event.

To get the best out of your investment in a system, periodic retraining, refresher training, and advanced training courses can be very useful for large or complex systems. This additional training should be documented.

**Operational Logbooks**

Several logbooks are required to document the basic operations of the computer system. The term logbook is used flexibly in this context; the actual physical form that the information takes is not the issue, the information required to demonstrate that the procedure actually occurred is more important. The physical form of the log can be a bound notebook, a pro forma sheet, a database, or anything else that records the information needed, as long as security and integrity of the records are maintained.

Typically, operation logs are required for backing up data and program disks on a computer and for recording errors of computer operation and their resolution and maintenance records for the system and its components. I will discuss each log in turn.

**Back-up log**: The goal of a back-up log is to provide a written record of data that have been backed up, the location of duplicate copies of the system (operating system and application software programs), and the data held on the computer. The back-up schedule for the disks can vary. In a larger system, the operating system and applications software will be separated from the data, which are stored on separate disks. The data change on a fast time scale reflects the progress of the samples through a laboratory, and they must be backed up more frequently. In contrast, the operating system and application programs change at a slower pace and therefore are more static; the back-up schedule can reflect this pace.

For smaller systems such as PCs, the data and programs can be located on the same disk and partitioned by the directory structure. If the back-up software is capable of performing selective back-ups, then the comments in the paragraph above apply. However, if the system is unsophisticated, the whole disk may need to be backed up routinely. For PC systems this may be an area to evaluate closely before buying. An alternative is a PC network, in which the programs and data are held on a central server and can be backed up more efficiently and effectively than stand-alone systems.

Some of the key questions to ask when determining the back-up of your chromatography data system are:

- How long should the time between back-ups be? This question can be answered by considering how much data you can afford to lose. If it is as much as a week’s worth, then the back-ups can be weekly. If you cannot afford to lose any data, shadowing or duplicate disks are the start of the answer that may lead you to consider redundant array of inexpensive disks (RAID) technology.
- Who is authorized to perform back-ups, and who signs off on the log? The laboratory manager and the people responsible for the system should decide this answer.
The authorization and any counter signature required should be defined in a standard operating procedure.

- When should duplicate copies be made for the security of the data? This question is related to the security of your data and programs. Duplicate copies should be part of the back-up procedure at predetermined intervals. The duplicate copies should be stored in a separate location, in case of a hazard to the computer, and the original back-ups should be located nearby. Duplicate back-ups also are necessary to overcome problems reading the primary back-up copies.

**Problem recording and recovery:** During the operation of a computer system, boot up, back-up, or other system functions, errors inevitably may occur. It is essential that these errors are recorded and the solutions to resolve them are also written down. Over time, this information can provide a useful historical record about the operation of the computer system and the location of any problem areas in the basic operation.

Areas where these errors can occur include peripherals such as a printer with a stalled print queue. This error is relatively minor; however, the application may fail in other situations because of a previously undetected error. In the latter instance, the error resolution must be linked with the change-control system.

**Software error logging and resolution:** As mentioned previously (1), it is impossible to completely test all of the pathways through chromatography data system software. It is inevitable that errors will occur during the system’s operation. These errors must be recorded and tracked until you find a resolution. Segalstad and Synnevag (7) discussed errors and their resolution, so I will include no detailed discussion in this article. The key elements of this process are to record the error, notify the support group (in-house or vendor), classify the problem, and identify a way to resolve it.

Not all reported problems of a chromatography data system will be resolved. They might be minor and have no fundamental effect on the operation of the system and may not even be fixed. Alternatively, the system may require a work-around solution, which should be documented, and even retraining may be necessary. Other errors can be fatal or major, which means the system cannot be used until fixed. In these situations, the revalidation policy will be triggered and the fix tested and validated before the chromatography data system can be operational again.

**Maintenance records:** All quality systems must demonstrate that the equipment used is properly maintained and, in some instances, calibrated. Computers are no exception to this requirement. Therefore, records of the maintenance of the chromatography data system must be set and updated in line with the work performed on it. The main emphasis of the maintenance records is toward the physical components of a system: hardware, networking, and peripherals. The software maintenance is covered under the error logging system described above.

If the hardware has a preventative maintenance contract, the service records after each call should be placed in a file to create a historical record. Also, the occurrence of any additional problems that require maintenance will be recorded in the system log, so the appropriate records should be cross-referenced there.

Many smaller computer systems have few if any preventative maintenance requirements, which does not absolve laboratories...
from keeping records of system maintenance. If a fault occurs that requires a service visit, then this visit must be recorded as well.

On sites where PC maintenance is performed centrally for reasons of cost or convenience, maintenance records can be held centrally. The central maintenance group may cover all areas of a site or organization, including regulated, accredited, and nonaccredited groups. It is important for the central maintenance group to keep records that are sufficient to demonstrate to inspectors the work they undertake. As defined in EU GMP Annex 11 (2), the third-party undertaking this work should have a service agreement and also have the curricula vitae of its service personnel available and up to date.

**Audit trail:** The integrity of data entered into a chromatography data system must be maintained carefully because the electronic medium holding the data is less robust than the paper-based system it replaces. In practice, this statement means that data, without proper controls and authorization, can be transformed easily or even lost by magnetic media and that data security can be inferior to that achieved with paper. It is incumbent upon system users to ensure that data are not altered without proper authorization. An audit trail is available in some systems, usually those built around databases such as LIMS and the newer chromatography data systems.

In essence, an audit trail is a software utility that monitors changes to selected data sets within the main application. An audit trail is configurable, in that users can decide which data sets are to be monitored. The reason for this configuration is that using an audit trail entails a processor overhead; that is, you need more computing power to operate both the audit trail and the main application than the latter alone. Therefore, the data sets to be monitored should be those that have an impact on the integrity of the data, such as data acquired directly from instruments, results, and supporting data from sample entry and release.

The audit trail must show who made the change, when he or she did it, what the old and the new values (data are not erased) were, and why the data were modified. This information is required for paper systems, and the requirement is stated or indirectly implied for computer systems. Therefore, during the evaluation of a system it is important that the audit trail is evaluated for these features. When preparing the report or archiving the results for a sample, batch, or study, the audit trail should be searched and the audit relating to the specific samples obtained and filed with the raw data and supporting information. This proactive approach can prevent many problems after a system is operational.

### Revalidation Criteria

Any change to a chromatography data system should trigger a consideration of whether revalidation of the system is necessary. Note the use of the word *consideration*. Usually, system administrators have a knee-jerk reaction that any change means that the whole system should be revalidated. You should take a more objective evaluation of the change and its effect before deciding whether full revalidation is necessary.

First, if revalidation is necessary, to what extent is testing required — a software unit, module, or the whole system? Thus, revalidation is defined by Chapman as “repetition of the validation process or a specific portion of it” (5). You may even find instances when no revalidation would be necessary after a change. However, the decision must be documented with the rationale for it.

Therefore, a procedure is required to evaluate the effect of any change to a system and the action taken accordingly. One way to evaluate a change is to review the impact that it would have on data accuracy, security, and integrity, as outlined by Lepore (8). This information will give you an indication of the effect of the change on the system and the affected areas of the application. This evaluation allows you to target a revalidation effort that is appropriate to the change you are going to make.

**Disaster recovery:** Good computing practices require that a documented and tested disaster recovery plan must be available for all major computerized systems. It rarely is. Failure to have a disaster-recovery plan places the data and information stored by major systems at risk, and the ultimate losers are the workers in the laboratory and the organization itself.

Disaster recovery is usually forgotten or not considered because we all say, “it will never happen to me.” The recovery plan should have several shades of disaster documented. For example, the plan should cover how data will be restored from tape or backup storage and updated in the event of a complete loss of the computer room or building caused by fire or natural disaster.

After the plans have been formulated, they should be tested and documented to see if they work. Failure to test the recovery plan will give a false sense of security and compound any disaster.

### Conclusion

To maintain the validation status of a chromatography data system, operational control on a day-to-day basis and effective change control must be established and maintained effectively. Both aspects are interrelated. Errors and features discovered during the operation or initiated change requests require change control. After the change has been initiated, it can have an effect on operational factors such as documentation and operational logs.

### References

(4) A.S. Nakagawa, LIMS: Implementation and Management (Royal Society of Chemistry, Cambridge, United Kingdom, 1994).