

Focus On Quality

Validation of Spectrometry Software

The author continues his discussion of the principles involved in the backup and recovery of electronic records. This installment looks at the written procedures associated with this process for a spectrometer operating in a regulated laboratory.

R.D. McDowall

Although this column discusses regulatory requirements and issues, it is important not to forget that the main reason for backing up your application and data is a business one. You'll install your software and then configure the system by defining items such as authorised users, user types, access control privileges, user-defined macros, libraries, and so forth. Imagine the problem if your computer hard disk fails and you have no effective backup. What happens next?

You'll have to reinstall the base software from CD and then input all of the configuration data manually — assuming that you remember what each one was. Not a pleasant thought, is it? Furthermore, consider the data and electronic records that you have created since the original installation — how are you going to recreate these? The simple answer is that without backup records you cannot.

Therefore, regardless of the regulations — if you are working in research, development or production — you need an effective backup procedure for business reasons alone. Not convinced yet? Take the example where a spectroscopy laboratory only works with paper. If a regulatory submission is needed and there are spectrometry data to be included you'll have to scan the paper into a format that can be included into the electronic regulatory submission.

Key Sections of the Procedure

Any standard operating procedure usually has the following sections as a minimum:

- Scope and purpose
- Roles and responsibilities
- Details of the procedure
- Generation of documented evidence (to demonstrate that the procedure was followed)



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.

Every company has their own way of writing SOPs and different formats, so we'll focus on the main sections and look at each of these in turn during this column.

Remember that the procedure is a formal document with management and QA approvals required as well as document controls (pagination in the format of page *x* of *y*, document identity, version controls, and so forth), although we will not discuss these aspects here.

Purpose and Scope of the Procedure

The purpose of the procedure should be described in a single sentence or paragraph. Typically, the purpose statement could be written as, "Documenting the procedure for the backup and recovery of the application and electronic records of spectrometer system X," or equivalent. There is no need to go into any more detail if your purpose sentence is simple and explicit.

The scope of the backup and recovery procedure can depend upon whether your spectrometer is a standalone or a networked system. If the system is a standalone one, then you — the lucky user — are responsible for everything. However, if it is a networked system then typically we're dealing with the IT department to back up the system on behalf of the laboratory. In the latter case we're crossing departmental boundaries with all of the communication issues that that entail.

Similar to the purpose statement, there should be a simple scope statement to outline the SOP boundaries and identify what is in the procedure and what is outside of the procedure. Establishing the boundaries of the procedure is important at the beginning of the document to manage the expectations of any reader as to the details of the document.

Roles and Responsibilities

Let's now look at the detail of the procedure by considering who is involved and what they should be doing: the roles and responsibilities of all involved in the process. There are two main roles involved with backup and recovery in a networked environment in most organizations:

- End users
- IT department personnel

I'm assuming that either the spectrometer is networked or the system operates in a standalone mode and the records that

Table I. Combined process flow and task description

Process Flow	Tasks
Schedule backup	<ul style="list-style-type: none"> • Check the backup schedule • Determine if a full or incremental backup is to be performed
Load media into backup device	<ul style="list-style-type: none"> • Select backup media from media storage • Load the media into the backup device
Perform backup	<ul style="list-style-type: none"> • Schedule the backup • Perform the backup
Check backup log	<ul style="list-style-type: none"> • Check the backup file to see if the backup has been performed correctly • Record in the backup log • If any errors are noted, implement procedure for resolution defined in SOP
Return media to storage	<ul style="list-style-type: none"> • Backup media returned to media storage location

are produced are transferred to a network drive for backup and recovery. End-users are responsible for backup and recovery because it is their system and their data. These facts often are overlooked when a backup schedule is developed. Responsibility often can be abrogated and a default schedule given that is not appropriate to the system or the data held on it. Users must be aware that this is their responsibility and that they are accountable, even though the work is carried out by a third party. Some of the user responsibilities:

- Define the data criticality
- Define the type of backup required: full only, full and incremental or full and differential (as outlined in Part IX of this series)
- Define the speed of any data or application recovery in the event of failure

The IT department will carry out the backup and recovery of data on behalf of the end users. The schedule for the backups will be worked out in discussions with the end users and this should be recorded in a service level agreement (SLA) that outlines the roles and responsibilities of

all parties and the schedule. IT will also need to have a procedure that covers:

- What to backup
- How to backup
- How to recover records and the application
- Defining the interface between the laboratory and the IT department

There is a third role that will be involved in the process: quality assurance. QA will be involved in authorizing the SOP as well as checking that any work described in the procedure has been carried out correctly via a periodic audit.

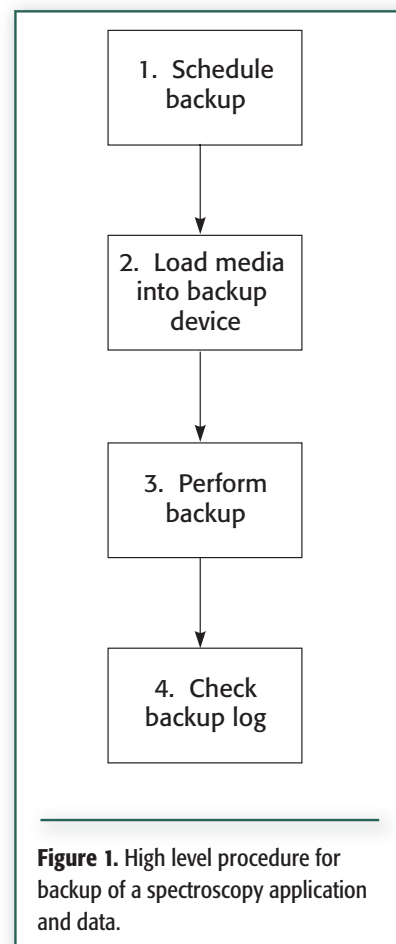
Defining the Backup Procedure

The procedure for performing a backup should be defined in sufficient detail to ensure that any trained person undertaking a backup can repeat the task. How this is to be achieved depends upon your company's approach to writing a procedure. This can be accomplished through one or a combination of the following ways:

- Text
- Number paragraphs
- Flow chart and text

Table II. Example of a basic system backup log

Date	Backup Type	Log	Action	User
June 10	Full	Executed with no errors	N/A	RDM
June 11	Incremental	Executed with no errors	N/A	RDM
June 12	Incremental	Write errors noted on backup log Repeat executed with no errors	Replaced tape and repeated backup	RDM
June 13	Incremental	Executed with no errors	N/A	RDM

**Figure 1. High level procedure for backup of a spectroscopy application and data.**

From a personal viewpoint, I prefer a flow chart and text as this gives a better understanding of the procedure. At the simplest it can be a flow chart that outlines the main points in the procedure plus a textual description of each step. Figure 1 shows a high level procedural flow chart for a backup of a system.

This process flow can be linked to the text by referring to the number in the individual stages of the process. A better approach is to link the two together in a table so that the process flow and work instructions side by side with little room for misinterpretation as shown in Table I. In this approach the process flow and the work instruction are easily and visually linked for easy of interpretation. If further required, any role involved in the process also can be added to the table as a separate column to clearly identify the role with the work instruction.

Defining the Recovery Procedure

The recovery process also needs to be

documented in a similar way to the backup process has been described. Therefore if you use the text or process based approach for the backup this must be mirrored in this section for the recovery process.

Key in this section is to define what events trigger the recovery process? These can vary from the recovery of a single file to the recovery of a whole disk. In any event, the process for obtaining the latest tape or CD from the media store, loading it on the drive and then transferring the files to be recovered to the spectrometer database. There also needs to be a verification step to ensure that the file or files have been correctly copied back to the system.

Documented Evidence

To ensure that there is evidence that the procedure has been followed a backup and recovery logs are required. For practical purposes we'll look at backup only as recovery is simply the mirror image of backup. At its simplest this is a record that each backup has been performed

without error by looking at the log or file produced by the backup software after each backup. The person (user of IT depending if the system is standalone or networked) looks at the log file produced by the backup software to check if there are no problems recorded in it. If there are no issues, then the paper backup log is noted for June 10, 11, and 13. However if there is a problem as seen on June 12 with write errors on the tape; then the tape is replaced and the backup is repeated. This is one way to approach the issue of a failed backup.

Another way, if documented in the procedure, is that the users may take the view that the backup can go for another 24 h before the backup is repeated.

Here, the risks of not backing up immediately following a media failure must be balanced with the time taken out of the working day to ensure that records are preserved. This is your laboratory's judgement call, not mine.

Service Level Agreement

Whatever requirements are needed for

the backup and recovery of a networked spectrometer system, they need to be incorporated in an SLA so that the IT department have a standard to work against. The SLA can also provide a standard or benchmark for QA to audit against, providing that the agreement has specific and measurable performance criteria.

The SLA with the internal or outsourced IT department should cover and document the following parameters as a minimum:

- Backup schedule
- Definition of the software and records to be backed up and the frequency of each
- Recovery procedures

The content of an SLA is outside of the scope of this discussion and the reader is referred to the book by McDowall (1) for further information.

Reference

1. R.D. McDowall, *Validation of Chromatography Data Systems* (Royal Society of Chemistry, Cambridge, UK, 2005). ■