Analyst® LC/MS Software and 21 CFR Part 11 Regulations

PURPOSE

The purpose of this paper is to present an approach to assist the user in meeting 21 CFR Part 11 compliance with Analyst® LC/MS Software version 1.2 and above, including Analyst Software 1.4.1, when used in quantitative studies supporting Good Laboratory Practice (GLP) bioanalytical studies. In this paper, we outline the joint responsibilities between a supplier and its customers to support users' 21 CFR Part 11 compliance. We hope you find the information both helpful and educational.

INTRODUCTION

21 CFR Part 11 is a US Food and Drug Administration (FDA) regulation that covers the trustworthiness and reliability of electronic records and electronic signatures.[1] Although the regulation has been effective since August 20, 1997, it is currently undergoing review in light of the FDA's risk-based approach to current Good Manufacturing Practice (cGMP). On February 20, 2003, the Agency issued a draft Guidance for Industry on Part 11 Scope and Applicability and, after a 60-day industry comment period, issued the final version on September 3, 2003.[2] This paper incorporates content from both the initial regulation and the final version of the Guidance for Industry. This paper is not intended to provide legal advice or interpret the law. For a complete statement of terms, reference should be made to the regulation and the complete Guidance for Industry.

CONTENTS

We will discuss the following issues of 21 CFR Part 11 and how Analyst Software can be configured to help meet the regulatory requirements associated with the underlying GLP predicate rule (21 CFR Part 58).

- What is 21 CFR Part 11? A brief history and current status of the regulation
- Discussion of open and closed systems in the context of Analyst Software
- Definition of electronic records and how this is interpreted for Analyst Software
- Controls required for 21 CFR Part 11: technical, administrative and procedural
- Impact of predicate rules for the interpretation of Part 11
- Roles and responsibilities for 21 CFR Part 11 compliance: the importance of partnership between the customer and the supplier
- Detailed discussion of 21 CFR Part 11 and certain of the responsibilities for each section in the regulation
- Examples of how Analyst Software users have implemented and validated its system for Part 11 compliance
- Future developments of Analyst Software

WHAT IS 21 CFR PART 11?

An important driver for the "Electronic Records; Electronic Signatures" Final Rule[1] was the pharmaceutical industry, who approached the FDA with a request to use electronic records so that the industry could take advantage of modern technology and reduce the use of paper. Following the publication of a draft of the regulation in 1994, the final rule was published on March 20, 1997 and became effective on August 20, 1997.

In essence, the regulation provides the basis for the use of electronic records in place of paper records as well as the use of electronic signatures, rather than handwritten ones. Under 21 CFR Part 11, electronic records can be equivalent to the paper records required by predicate regulations (e.g. 21 CFR Part 58, the Good Laboratory Regulations[3]). Electronic signatures can be considered as legal equivalents to handwritten signatures. The regulation further stipulates that both electronic signatures and electronic records must be trustworthy and reliable.

The regulation impacts almost all FDA-regulated work (e.g. pharmaceuticals, medical devices, blood banks, food). It impacts bioanalysis directly when studies are used to support new drug applications or new formulations of existing drugs. Any organization that wishes to register products for sale in the USA, regardless of where the organization is based, must comply with the requirements of this regulation.

KEY REQUIREMENTS OF 21 CFR PART 11

A summary of significant requirements of the regulation is outlined below. For more detailed explanations, including roles and responsibilities, please see the later sections of this paper. Please refer to the regulations themselves for a complete statement of these requirements.

ELECTRONIC RECORDS

Electronic records (covered by Part B of the regulation) generated by any computerized system must be trustworthy and reliable. A number of controls exist in the regulation to support this requirement.

- Systems must be validated
- Systems must be able to detect altered and invalid records
- Only authorized individuals must have access to a system and their access levels must reflect their job
- Audit trails are required to monitor creation of and changes to records, including archive or deletion of data
- People using a system must be trained; this includes all levels of support from system administration to front line users and IT support staff
- Records must be protected for the duration of the records retention period; this may be up to 15-20 years depending on the predicate rule
- Systems must provide the data and associated meta data to an inspector if required
- Signing of records requires the name of the individual, reason for signing, and the date and time displayed at the time of signing
- Signatures must be linked to respective records so that the signatures cannot be removed or copied
- Policies must be established holding individuals accountable for actions taken under their electronic signatures
- Where data confidentiality is required, the addition of security such as file encryption or digital signatures is required to ensure confidentiality

The system, including training and resultant records, must be sufficient to prevent repudiation of electronic signatures as not genuine.

ELECTRONIC SIGNATURES

Part C of the regulation has many requirements for procedural and administrative controls, with relatively few technical requirements. While Part C of the rule is voluntary, and each company can choose to implement electronic signatures or not, there are also pertinent security requirements for the trustworthiness and reliability of electronic records; for example, the ability to detect unauthorized access to a system in §11.300(d).

The main requirements are:

- Individuals using electronic signatures must have their identities verified
- Companies must send a letter to the FDA certifying that when electronic signatures are used, they are the legal equivalent of traditional handwritten signatures
- Electronic signatures must be unique to an individual and never reused by a company
- Controls must be in place to prevent fraud (Fraud would require the collaboration of two or more individuals)
- The system must be able to detect attempts of unauthorized access and notify the appropriate security/management staff

Part 11 Requirements Still Enforced	Part 11 Requirements with Enforcement Discretion
11.10(d) Limiting system access to authorized individuals	11.10(a) Validation
11.10(f) Use of operational system checks	11.10(b) Copies of records
11.10(g) Use of authority checks	11.10(c) Record Retention
11.10(h) Use of device checks	11.10(e) Audit trail
11.10(i) Persons… have the education, training, and experience to perform their assigned tasks	Legacy Systems operating before August 20, 1997
11.10(j) Written policies that hold individuals accountable for actions	
11.10(k) Appropriate controls over systems documentation	
11.30 Controls for open systems	
11.50 Signature manifestations	
11.70 Signature / record linking	
11.100 General requirements	
11.200 Electronic signature components and controls	
11.300 Controls for identification codes/passwords	

Table 1. Enforcement discretion. Note that the remainder of 21 CFR Part 11 is still in operation and will be enforced by the FDA as shown in this table.

IMPACT OF THE PART 11 SCOPE AND APPLICABILITY GUIDANCE

Since 2002, the FDA has been re-evaluating the Good Manufacturing Practice (GMP) regulations and as part of this program,[2] five key sections of the Part 11 regulation include enforcement discretion (Table 1).

For example:

- Validation of Part 11 requirements
- Copies of records
- Records retention
- Audit trail
- Legacy systems (i.e., systems already in operation before August 20, 1997) do not need to comply with 21 CFR Part 11 regulations, provided they were validated to meet the applicable predicate rule requirements before Part 11 was in effect and any changes do not invalidate their ability to meet predicate rule requirements.

IMPACT OF 21 CFR PART 11 ON BIOANALYTICAL LABORATORIES

When the regulation became effective, no LC/MS systems operating in bioanalytical laboratories were fully compliant with the requirements. Typical problems included:

- No audit trail—only a history log in the data file
- Little or no security (security features if available were difficult to use efficiently and effectively)
- File overwriting, with or without warning
- Changes of data could be made with no record of the original value
- No electronic signatures

LC/MS instruments were used as hybrid systems; meaning that although they generated electronic records, handwritten signatures were applied to paper copies of the records.

KEY PART 11 DEFINITIONS EXPLAINED

Open and closed systems

21 CFR Part 11 classifies computerized systems as either "open" or "closed" in Part A (Scope section); there are only two words of difference between the two definitions (in parentheses below):

Closed (Open) system means an environment in which system access is (not) controlled by persons who are responsible for the content of electronic records that are on the system.

The key points of this definition are:

- The regulation refers to a "System," an application is not mentioned; in fact, there is no place in the regulation that mentions application. System can contain hardware, software, people, training policies, etc.
- "System" is given a wide definition, and includes the information technology (IT) network that traditionally was not included in regulatory inspections prior to the issuance of 21 CFR Part 11

Analyst® Software is Designed for Closed Systems

Current Analyst Software can be used in either a closed or open system. However, it can be configured to support compliance only in a closed system. It can be used within an organization either as a standalone or single system (Figure 1) or in a networked configuration (Figure 2) where multiple acquisition workstations and data processing stations may be connected to a closed network. For the rest of this paper, we will only consider closed systems.

Standalone or single systems?

One or several standalone Analyst Software systems in a bioanalytical laboratory are closed systems. The facility will have physical security and there will be logical security to prevent unauthorized persons from gaining access to the application. However, laboratory personnel should back up each instance of Analyst Software.

Standalone workstations that hold electronic records present an increased risk of disk failure or corruption of records, and require regular backups to support preservation of the electronic records. However, the overhead to back up these records on a workstation-by-workstation basis is considerable. More importantly, the physical access to the data storage location allows more potential avenues to compromise data security. Instead, it is advisable that bioanalytical data be stored on a network drive with appropriate physical and logical access controls in place. The information technology (IT) department often handles the tasks associated with limiting user access, maintaining long-term and mid-term physical data integrity through a sound data backup strategy, and data archival in these network environments.

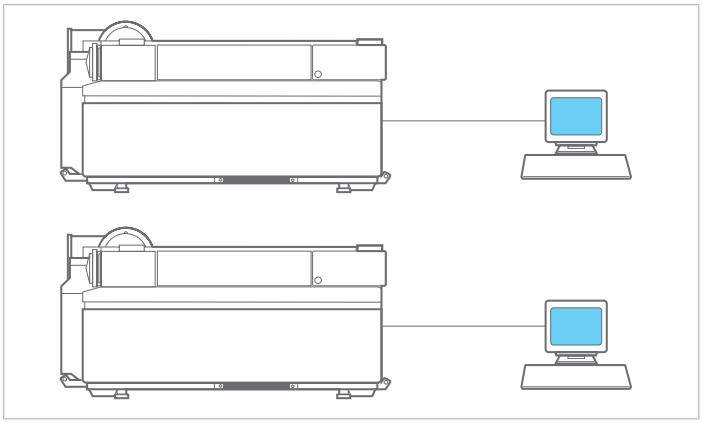

Figure 1. Standalone Analyst® Software systems in a laboratory.

Networked systems

To assist in data storage and backup, Analyst Software has added network data acquisition capability, where data may be acquired to a network server, not the acquisition workstation controlling the MS instrument. It is important to note that the networking of several Analyst Software systems supported by an IT department does not mean that the system is now open. Interpretation of "environment" needs to be wider that just the laboratory, and encompasses the wider organization, including controlled network objects such as network data storage locations and data transmission lines. Networked Analyst Software systems must also have written procedures and documented evidence that protection of records (backup) is undertaken regularly and reliably, in the same manner as standalone systems.

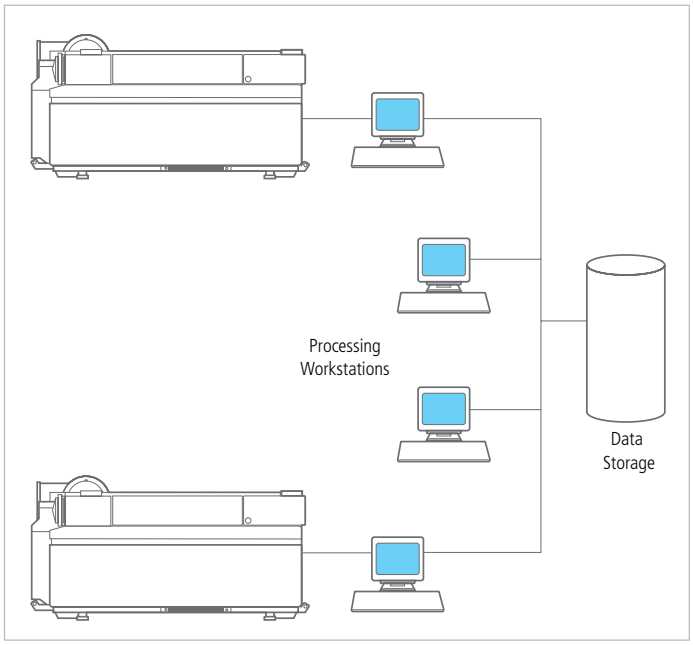

Figure 2. Networked Analyst® software LC/MS systems with data storage by the IT Department.

Electronic records

"Electronic record" is defined in the regulation:

Electronic Record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.[1]

This is a very broad definition. The phrase "other information representation" covers any electronic record in any format.

The Guidance on Part 11 Scope and Application[2] narrows the scope of the regulation in certain circumstances. It still allows the use of paper records, if the paper output meets the requirements of the applicable predicate rules. It is often not practical to define the paper records for the raw data output of Analyst® Software due to the number and volume of records that Analyst Software generates with each run. In the context of Analyst Software, the electronic records produced during a bioanalytical run are as follows:

- Data Acquisition Method (DAM) file with any modifications for the run
- Batch methods
- LC/MS data files – single sample in a single WIFF file, multiple samples within a single WIFF, combinations of multiple samples, and multiple WIFF files
- Processing method

Records possibly within or outside of the bioanalytical run are as follows:

- Hardware configuration profile (Equivalent information is stored within the file information of each sample)
- Tuning and instrument parameter settings (The tuning information is copied to the file information of each sample)
- Quantitation results tables including the audit trail incorporated with each results table
- Report templates and display configuration settings
- Processed data file(s)
- Audit trails and history logs
- Applicable Analyst Software application, error and security logs held within the Windows® system logs

Pending the customers SOPs and processing/display practices for the data, some of the above records may not be required.

To help ensure the trustworthiness and reliability of electronic records, each file produced by the system must have the means to be uniquely identified. Therefore, a file naming convention and SOP is strongly

advised to prevent file overwrites by administrators or inadvertent appending of samples into the wrong data file. Analyst 1.2 Software and later versions provide automatic increment of batch and method names for all regular users (administrators may overwrite methods but the default configuration requires a signature for the overwriting of the method/batch). Note that sample data within a WIFF file pair collected under a specific method retains the original method information with the sample data. Analyst Software automatically appends data files with new samples; original data is not overwritten.

Electronic Signature

"Electronic signature" means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.[1]

Electronic signatures that can be used under Part 11 are one of the following three types:

- Electronic signature (password and user ID (identification code which may or may not have elements of the users actual name)). This is the easiest method to implement in many applications used in bioanalysis, but its effectiveness is highly dependent upon the quality of the password chosen by the user. Passwords that are easily remembered can often be easily guessed; this is the so-called password paradox
  - There has been debate on the effectiveness of various password policies. Long complex passwords and frequent changes to password results in people writing passwords down or cycling through passwords. Three fairly common requirements with respect to password length and composition are: 1) 8 characters with 2) alphanumeric combinations and 3) no dictionary words. The National Security Agency (NSA) lists 14 characters as minimum; Microsoft recommends 6 characters as the minimum
  - Password change frequency and reuse frequency: Maximum age 90 days, minimum age 1 day (user must wait one day after setting a password to set a new password). User cannot reuse same password for one year from NSA guides
    - NSA has several documents dealing with computer security, including password policy. **www.nsa.gov/snac**
    - The Microsoft website has several security guides which are usually not as specific as the NSA material **www.microsoft.com/technet/security/topics**
- Biometric signature (based on a measurable human trait such as fingerprint or iris recognition). The prices of fingerprint devices are dropping to reasonable levels and multi-mode verification devices (verifies print + temperature + pulse etc.) are more difficult to fool and are becoming readily available. However, the use of fingerprint technology in a bioanalytical laboratory may be hampered by the need to use gloves for many bioanalytical activities.
- Digital signature (public/private key infrastructure plus a personal pass-phrase or password). Implementing digital signatures usually requires a token or equivalent that generates a random number that is synchronized with the same algorithm running with the application.

Analyst® software relies on the implementation of electronic signatures comprised of user identity and password. Analyst Software security works in conjunction with Microsoft Windows® security, authenticating against network User IDs and passwords or local User IDs and passwords.

The customer must administer passwords through the use of SOPs training and tools to ensure that:

a) The user IDs and user names are unique and never reused

b) Passwords are suitably secure, strong passwords, known only to their user

c) The user ID/password combination is used only by its respective owner

THE ROLE OF THE PREDICATE RULE IN PART 11 INTERPRETATION

Part 11 has always been interpreted using the existing predicate rules. The predicate rule interpretation has been emphasized in the 2003 Guidance for Industry[2] to ensure that a practical scope of Part 11 is made during the review period.

For bioanalysis, the main predicate rule regulation is 21 CFR Part 58[3] (Good Laboratory Practice), although 21 CFR Part 320 (the bioavailability regulations) may also be involved. 21 CFR Part 11 makes no mention of which records must be generated, signed and maintained; this is determined by the applicable predicate rule.

The predicate rule will state those records that are required, and those records requiring signature. Where the predicate rule requires a record, Part 11 says you can have an electronic record. Where the predicate rule requires a signature, Part 11 says you can have an electronic signature. Where the predicate rule does not identify a record or a signature as required, Part 11 requirements do not apply (note that there are records identified specifically in 21 CFR Part 11, such as audit trails, that may not have a direct paper equivalent).

However, bioanalysts working in the pharmaceutical industry or contract research organizations tend to generate paper and sign records regardless of what is actually required by the predicate rules. When implementing ER/ES systems, it is important to understand exactly what signing actions are required and where it is important to identify an individual's actions. For example, when you make a handwritten change to a worksheet, is a full signature required or just initials? This is an important distinction to make and understand. What is the role of the signature or initials? Is it the identification of an individual that denotes who performed an action, or is it the approval or authorization of results or a report?

This is a critical issue, as the implementation of many data systems and LIMS used in bioanalysis can have an "electronic signature" associated with writing to the database. In fact, per the applicable predicate rule, the signing requirements are very limited. However, in many labs it is still the practice to sign and date virtually every scrap of paper.

INTERPRETATION OF PART 11 BY THE GLP PREDICATE RULE

To illustrate the need to understand and correctly interpret the predicate rule, we will first present the predicate rule for equipment design, and then highlight key issues.

21 CFR Part 58.61: Equipment Design[3]

The requirement for equipment design under the GLP predicate rule states:

Equipment used in the generation, measurement, or assessment of data and equipment used for facility environmental control shall be of appropriate design and adequate capacity to function according to the protocol and shall be suitably located for operation, inspection, cleaning and maintenance.

Some of the key elements of this predicate rule requirement for Analyst Software and the API mass spectrometers that they control are as follows:

- Appropriate design – Validation of the system; specify the intended use of the instrument and software and test against the requirements
- Adequate capacity – Part of the specification and testing during the validation must cover the expected uses of the system such as the ability to control the applicable instrumentation hardware, to collect the necessary data for a given sample, to run up to the protocols' maximum number of analytical samples and injections, to report the data, and to store the data collected. The storage capacity of the LC/MS data storage location must be evaluated for suitability
- Suitably located – Location must meet the manufacturer's specifications for physical location/ambient conditions, and provide the services required for effective operation such as electricity and gas supplies
- Maintained – Service and maintenance history for the instrument and software must be provided

Risk Analysis to Determine the Extent of Validation

As the FDA Guidance on Part 11 Scope and Application[2] states:

We recommend that you base your approach on a justified and documented risk assessment and a determination of the potential of the system to affect product quality and safety, and record integrity.

An important issue is to understand how the LC/MS instrument and Analyst® Software subsystems affect the product quality. This can mean quality of the manufactured drug product, and could also be interpreted as the quality of the data generated in bioanalytical reports. Therefore, in the context of Analyst Software, it is the quality of the data generated by the bioanalytical laboratory.

Another issue is: where does the system fit into the development pipeline?

- Late research to identify potential development candidates
- Non-clinical development
- Clinical development

The later in development the system is used, the greater the risk, as the data is used for pharmacokinetic interpretation, bioequivalence studies, etc. There is also a greater possibility that the data will be included in regulatory submissions. If used for two or more development phases, then the extent of validation should be based on the risk in each of the areas of use.

ROLES AND RESPONSIBILITIES INVOLVED IN 21 CFR PART 11

In this section, we will discuss the nature of the Part 11 controls and who is responsible for each (Figure 3).

Three Types of Part 11 Controls

21 CFR Part 11 requirements can be classified into one of three types of control:

- Administrative Controls – These are policies for 21 CFR Part 11 within an organization and can include a company interpretation of the regulation and how the company will verify the identity of individuals, and ensure non-repudiation of electronic signatures
- Procedural Controls – These are essentially standard operating procedures (SOPs) or other written instructions for a system, including how to use the system (this may require two SOPs, one for the system administrator, and one for the users), a list of authorized users against access level (which is reviewed periodically to confirm that it is correct), and backup and recovery procedures
- Technical Controls – Examples of technical controls are the security and access control for the application and the audit trail to monitor changes to the records

Note: you cannot be compliant with Part 11 until all three controls types have been implemented. The number and extent of these controls required for Analyst Software will depend on how the system will be used. For example, when Analyst Software is used as a hybrid system, which appears acceptable to the FDA under the Scope and Applicability guidance, then fewer technical controls are required compared with when it is used with electronic signatures.

Interrelationships Between Technical and Procedural Controls

Some technical controls do not stand on their own. They require a procedure to ensure that they are implemented and are effective. Examples include:

- 11.300(d) The system must have the ability to detect unauthorized use; this is limited to access attempts currently. When unauthorized access is attempted, the software (technical controls portion of the system) notifies administrative/security personnel, who will follow a documented procedure to investigate the issue and report on the outcome
- 11.10(d) limits system access to authorized individuals and 11.10(g) requires authority checks to ensure that people only have access to functions appropriate to their position and training. A SOP must be in place for defining and implementing these two requirements, and also listing the authorized users and their individual access levels

We will look at this in more detail in the pages that follow, as we review the requirements for 21 CFR Part 11.

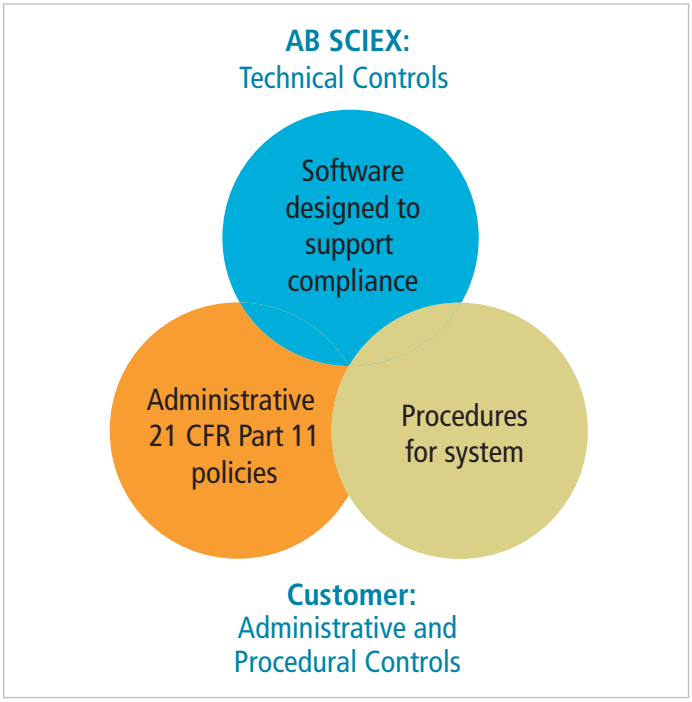

Figure 3. Three types of controls required for 21 CFR Part 11 compliance.

Partnership for Part 11 Compliance

It is important to note that you cannot buy a "21 CFR Part 11-compliant" system. There are applications, such as Analyst® Software, that can be designed as 21 CFR Part 11-ready, but it is the user who is responsible for appropriate configuration of Analyst Software and supporting network/ Windows® system security, as well as providing policies, procedures, and user training to ensure the systems are fully compliant with the applicable regulations.

ANALYST® SOFTWARE FEATURES SUPPORTING 21 CFR PART 11 IMPLEMENTATION AND RESPONSIBILITIES OF CUSTOMER FOR IMPLEMENTATION

§11.10 Controls for Closed Systems

*Note that only versions of Analyst Software version 1.2 and greater have the 21 CFR Part 11 supporting features. New supporting features have been introduced with subsequent versions of Analyst Software. Analyst Software version 1.3 introduced lock out, log off features and version 1.4 introduced network acquisition support; Versions 1.4.1 improved the network acquisition support and introduced centralized administrative features.

21 CFR Part 11 Regulation	AB SCIEX Analyst Software*	Analyst Software Customer
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records	• Provide applicable features to: – prevent change – detect and record changes to electronic records within the system – detect invalid records • All alterations automatically recorded in an audit trail at time of saving • Development of the software under a quality management system	• Responsible for initial validation • Maintain the validation and operate the change control procedure • Write and update the system SOPs
(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency	• Execution of signature, audit trail and all supporting information must be linkable to results • Provision of printing and export to PDF file format features	• Configure the OS and Analyst* Software to prevent deletion or unauthorized copying of files through the operating system • Control the date and time settings on the workstation
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period	• Future software upgrades must be compatible with existing files and data or provide translation to new format • Multiple users must not be allowed concurrent access to the same record • Analyst Software 1.4 allows for collection of data/records to network location for easy IT backup	• Define record retention period • Use network acquisition tools of Analyst Software 1.4 where possible • Write SOPs for backup, recovery, archive and restore • Define any additional software tools necessary for this operation
(d) Limiting system access to authorized individuals	• Software provides means to limit access to application via a unique User ID/password • Software provides means for automatic alert of failed logon attempts (signatures only) • Software prevents the viewing or copying of passwords • Software provides logs of security access and changes to security settings	• SOP on System Security and Access Control must cover the proper configuration and maintenance of Windows® User IDs and passwords • List of current and historical users with access privileges • Enable security features in Analyst Software such as mixed-mode security inactivity lockout and logoff for Analyst Software 1.3 and later. Use Windows screen saver for Analyst Software 1.2
(e) Use of secure, computer-generated, time stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Recorded changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying	• Audit trail for application and system events • Automatic version control to capture content changes • Non-editable audit trail that can only be searched, viewed and printed	• Enable audit trail on installation • SOPs to reflect the retention of records including the corresponding audit trails
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate	• Built into application	• Inactivity lockout must be enabled in the application and/or operating system
(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand	• Software provides ability to define individual user permissions • Software allows updates to access only be allowed through validated secure application screens • Software provides means of authenticating user accessing the application or conducting specific operations within the application	• SOP on System Security and Access Control • Configure Windows® security on computers • Enable mixed mode security in Analyst Software • Configure user access to component features within Analyst Software • Enable electronic signature features
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction	• Built into application • Status polling of devices • Validation of methods against instruments attached	• SOP to cover operation of LC/MS equipment
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks	• Quality system • Documented training records	• Vendor audit or checklist • Signed training records for system users and maintenance staff
(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification	• Not applicable	• Notify FDA of intent to use signatures • SOP on non-repudiation of electronic signatures
(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation	• Link system documentation to a specific release of software • Software provides audit trail for maintenance activities on the instrument	• SOP on Change Control – retention of records dealing with instrument maintenance as part of system maintenance under predicate rules for equipment maintenance • SOP on System Security and Access Control • Version control on all documents

§11.50 Signature Manifestations

21 CFR Part 11 Regulation	AB SCIEX Analyst Software*	Analyst Software Customer
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature	• Software displays the full name of the user on screen at the time of signing • Provision of audit trail linked to the signed records with provisions for items (1), (2) and (3) • Software allows the creation of specific meaning for the signature with the use of the configurable reason options	• SOPs governing user account setup include the input of the person's full name. List of full names to ensure that name is not duplicated (especially in larger companies) • Configure and document the allowable meanings of signatures in the dropdown option
(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout)	• Software provides links through the audit trail that link the records to the signature execution/authentication	• Customer must view and print separately the audit trial manifestation of e-signatures as the record of the e-signature on the applicable electronic records

§11.70 Record and Signature Linking

21 CFR Part 11 Regulation	AB SCIEX Analyst Software*	Analyst Software Customer
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means	• Software records signing event in the audit trail and provides linkage to the applicable record • Software to prevent a reasonable attempt to excise an electronic signature and apply it to another record	• SOP for signing electronic records • Handwritten signatures on electronic records must be cross-referenced to the signed records • Applicable audit trail manifestations of electronic signatures and history of the specific record may need to be printed

§11.100 General Requirements

21 CFR Part 11 Regulation	AB SCIEX Analyst Software*	Analyst Software Customer
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else	• Not applicable	• SOP on System Security and Access Control • Proper configuration of user accounts under Windows® Security (list of User IDs to prevent reissue or reuse of user ID • No group logon permitted • Use mixed mode login and do not configure any group access to Analyst® software
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual	• Not applicable	• SOP for verifying an individual's identity
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857	• Not applicable	• Pharmaceutical company or CRO sends a letter to the FDA
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures	• Not applicable	• SOP on FDA Inspections
(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature	• Not applicable	• SOP on FDA Inspections

§11.200 Electronic Signature Components and Controls

21 CFR Part 11 Regulation	AB SCIEX Analyst Software*	Analyst Software Customer
(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password	• Application uses Windows® Security as source of user identity and password used as electronic signature components	• SOPs identified in previous sections
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual	• Analyst Software provides means to enter user identity and password for initial log into application • Analyst Software allows a user while in a continuous period of controlled access to input their password only for subsequent signings (user ID is provided automatically) • Analyst Software monitors activity and locks out user (ends the session of continuous access) if no user activity is detected	• SOP on System Security and Access Control • Enable mixed mode and automatic inactivity time out • Utilize features in Analyst Software called automatic lock out and log off
(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components	• Analyst Software provides means to enter user identity and password for first signing of each continuous period	• SOP on System Security and Access Control • Enable mixed mode and automatic inactivity time out • Utilize features in Analyst Software called automatic lock out and log off
(1) Be used only by their genuine owners; and	• Analyst Software authenticates user credentials against Windows Security and verifies user identity against list of allowed users in application	• SOPs previously defined • Each user identity is unique and never reused
(2) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals	• Analyst Software does not present passwords on the screen • Analyst Software prevents the excising of passwords by normal means from fields on screen • Analyst Software provides feature to identify when there are unsuccessful attempts to sign into the application	• SOPs around User ID Password Administration issue, locking of accounts, etc. • Configure e-mail notification option in Analyst Software to inform Security or network administration.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners	• Not applicable as biometrics are not used in Analyst Software	• Not applicable

§11.300 Controls for Identification Codes and Passwords

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

21 CFR Part 11 Regulation	AB SCIEX Analyst Software*	Analyst Software Customer
(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password	• Analyst Software provides the ability to show current security configuration with applicable user IDs, and ability to print or show history of security including the addition and deletion of users	• Ensure user identities are never reused • Maintain historical list of User IDs and User Names from Windows® Security • Maintain history of security changes or Windows settings • Maintain list of application security changes (Analyst Software Instrument Audit Trail)
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging)	• Analyst Software retains log of system access events	• Enable automatic password expiry • SOP on System Security and Access Control: check the list of users • SOP for the periodic review of system access logs against list of users
c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls	• Not applicable	• SOP on System Security and Access Control
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management	• Analyst Software generates entry into audit trail • Analyst Software provides lock out, log off feature • Analyst Software provides features for automatic alert sent to Administrator	• Enable inactivity lockout • On the operating system, account policies enable automatic lockout if permitted number of failed attempts is exceeded • Enable automatic alert in Analyst Software for failed password attempts
(e) Initial and periodic testing of devices, such as tokens or cards that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner	• Not applicable to Analyst Software	• Not applicable

ANALYST® SOFTWARE CUSTOMER: VALIDATION AND USE CASE STUDY

The following customer experiences illustrate the validation and use of Analyst LC/MS software and instruments in a regulatory context.

Pharmacia*

Jeff Duggan at Pharmacia's Department of Drug Metabolism at the Skokie, Illinois facility has been involved with the validation of Analyst Software version 1.2 when used as a hybrid system (electronic records and handwritten signatures on paper records).

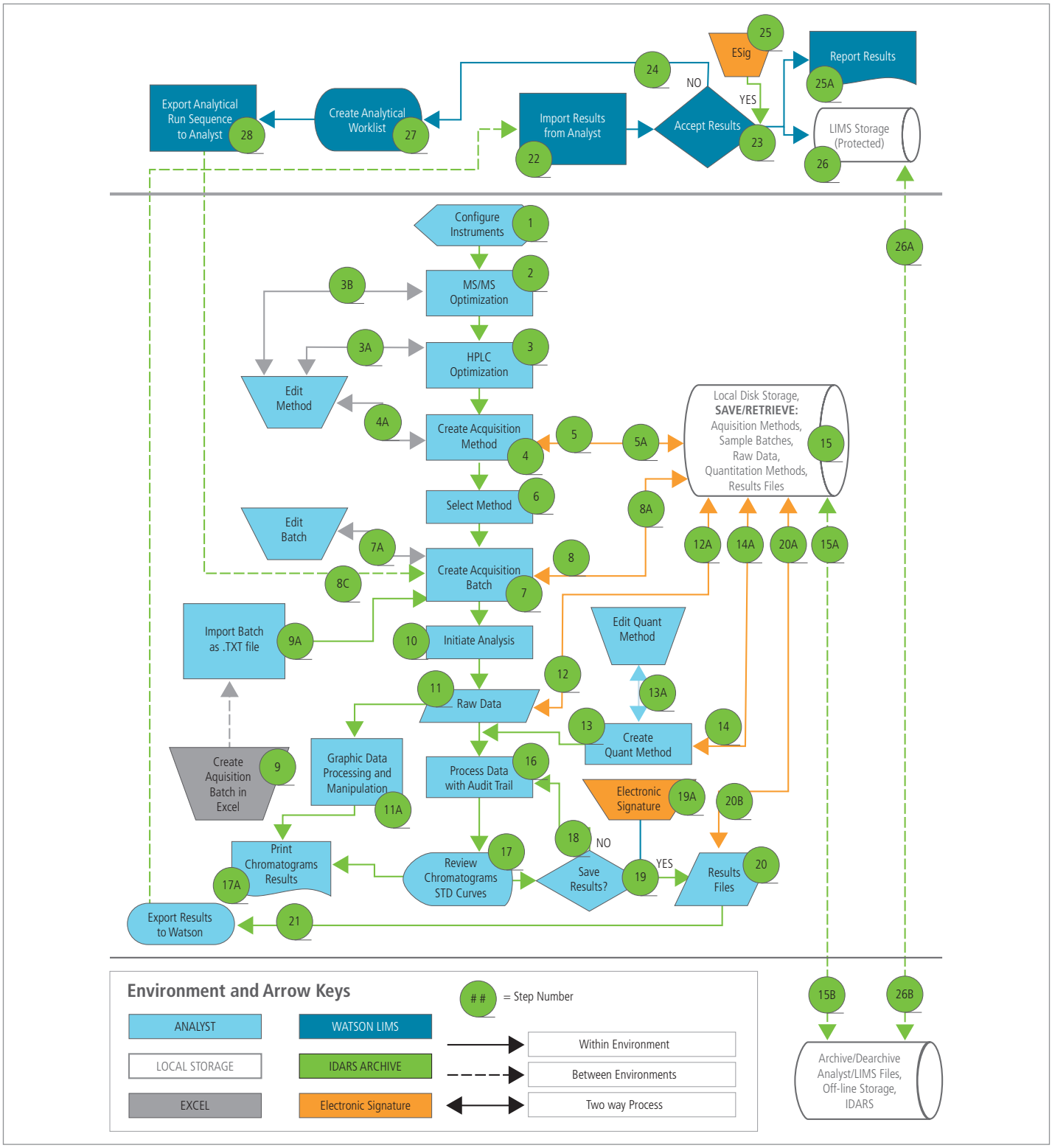

Figure 4. Workflow diagram for the Analyst® Software validation process at Pharmacia*

The validation carried out at Skokie was a global project undertaken by a validation team with participants at two US and one European site, validating 27 networked Analyst® Software workstations. (*Pharmacia was purchased by Pfizer in 2003).

Configuring user security is an important consideration before the validation can start. There are four types of users within the system: administrators, analysts, operators and users. The user types in Analyst Software were linked to network groups rather than individual users, since creating a separate security database on each individual machine would have made such a large system difficult to manage. Two added advantages of the network-resident groups for each user type are: 1) Users are easily added to or removed from the entire system by the network IT administrator simply removing or adding a user name from the appropriate group, and 2) Any user can use Analyst Software in any location provided that they are in the proper network group. The latter feature allowed global company users to use systems at different geographic sites, if necessary.

This version of Analyst Software can only acquire data to the local hard drive. To protect the data generated, there was an automated disk-to-disk copy at 5:00 am every day via a backup to a protected server. Once stored on the server, data are archived weekly via tape backup. The acquisition workstation hard drive remains the storage site for raw data. Therefore, the data area of each acquisition station hard drive is write protected to prevent file overwrites or erasures.

Within the server environment, file security is defined so that only administrators have the right to delete data, but the ability to do so is controlled by local SOP (an example of mixing technical and procedural controls of Part 11). Furthermore, each user has their own file share with restricted access to prevent data overwriting.

Validation involved writing a "user requirements specification" (URS) around the intended use and workflow of the software and LC/MS instrument. The workflow diagram shown in Figure 4 was numbered to indicate each major step to be tested via scripts. Processes integrated to data generation such as the front end and back end connections to the LIMS system and the network-based data backup system were included in the workflow for scripting.

The hardware platform has an installation qualification (IQ) that was followed by the Analyst Software IQ. For multiple installations there was a configuration specification for how to set up the platform, application and user permissions.

Scripts were written to test the workflow on an end-to-end basis (sample preparation to calculation of results). Users were trained, first with an introductory course, and then by a more detailed training for advanced and "power" users. As part of the validation, a vendor audit of AB SCIEX was undertaken in late 2002. There were no major deficiencies, and everyone involved with the audit was willing and cooperative. A summary report was written that covered the validation process: installation, configuration, test script execution, rollout, and user training.

Moving from Paper to Electronic Records

Working electronically requires a change in mindset. The concepts of "raw data" and "derived data" now become simply electronic records—and all must be retained and protected for the records retention period. Electronic records for a chromatography data system or mass spectrometry data system, for example, consist of the actual observed values (for a MS or HPLC run this would be the electronic data file) plus the associated electronic records to interpret the data file such as:

- Method file
- Instrument control file
- Sequence file
- Integration parameters
- Calibration method and results
- Audit trail

The extent of electronic records is much greater than paper. The problem is that paper is a tangible medium, but electronic records are not and can be difficult to visualize.

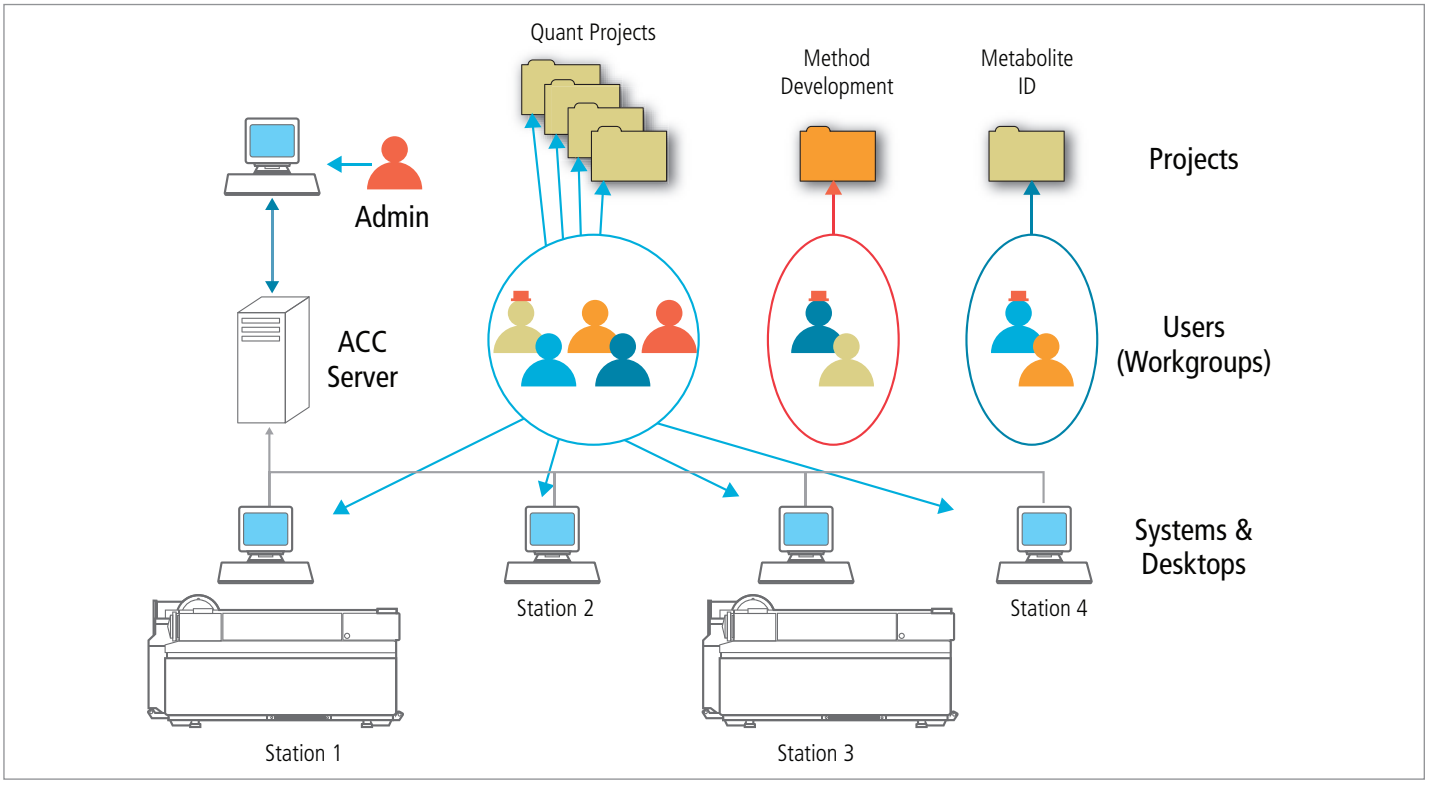

Figure 5. Flexibility of the security setup using the Analyst Administrator Console.

Benefits of 21 CFR Part 11

Process redesign is essential in order for business to fully exploit the benefits of 21 CFR Part 11. And the benefits of working electronically can be considerable, including significant cost and time savings, as well as overall process improvement, and faster, smoother path to regulatory approval. Some of the savings that can be realized are based upon the following activities:

- Eliminating paper
- Reducing number of applications to validate
- Eliminating manual involvement and speeding up the process; e.g., tasks such as typing data into systems, followed by manual transcription errors
- Eliminating redundant tasks from the process to save overall time for process execution

WHERE IS ANALYST® SOFTWARE HEADING?

Continuous improvement of the regulatory compliance of Analyst® software has been a goal since the initial introduction of 21 CFR Part 11 features in Version 1.2. In this section, the new compliance features from Analyst (versions 1.4.1 and above) software are discussed to access how they can help enhance compliance with GLP as well as 21 CFR Part 11.

Analyst Administrator Console (AAC)

Previous versions of Analyst Software required security to be set up and maintained at each workstation on the network. In Analyst (versions 1.4.1 and above) software, the use of the Administrator Console centralizes and simplifies the workstation that impacts the whole Analyst Software network.

The console can be any workstation attached to the Analyst Software server and is used to establish the overall security within the network for Analyst Software by the console administrator. This person is typically a senior user who is responsible for defining the following AAC functions within Analyst Software:

- Projects
- Users
- Roles and the allocation of one to each user
- Workstations
- Workgroups

The supplied default options for audit trail are as follows:

- No audit trail
- Default audit trail
- Full audit trail
- Silent audit trail
- Quantitation only audit

The customer may choose one of these default configurations or may customize their own audit map. The scope of the audit trail covers instruments, projects, quantitation, and administration. This coupled with the history logs within the WIFF data files provides the audit umbrella for Analyst® software.

	Event	Audited	Reason Prompt	Custom Reason	E-Signature
>	**QUANTITATION EVENTS**				
	Quantitation method has been updated	☑	☑	☑	☑
	Quantitation peak has been reverted back to original	☑	☑	☑	☑
	Quantitation peak has been integrated	☑	☑	☑	☑
	Results table has been created	☑	☑	☑	☑
	Quantitation method has been changed	☑	☑	☑	☑

Figure 6. Configuration of the Quantitation Events in the audit trail.

AAC allows the console administrator to establish workgroups that consist of specific users, workstations, projects, and roles. This allows flexible configuration to meet the needs of multiple studies. This arrangement allows the console administrator to set up each study/workgroup so that it is uniquely staffed and resourced and has a common set of defined data storage locations. As shown in Figure 5, a workgroup can have access to all workstations (with instruments or just process instances) for quantitative projects. For other work, access can be restricted to one or two users and even to a single instrument.

Analyst Software security using AC is flexible and can be tailored to a laboratory's specific requirements. In fact, the same user can have different roles in different workgroups or studies.

Configurable Audit Trail and Electronic Signatures

Older versions of Analyst Software had a fixed approach to audit trails and electronic signature. However, with versions 1.4.1 and above, the audit trail and electronic signatures can now be configured to meet a laboratory's needs and an organization's interpretation of 21 CFR Part 11. This accommodates a range of requirements from research to clinical development where Analyst Software can be used.

In addition to the nature of the audit trail, there is further scope for configuration by the users, which should be documented when validating the system. For example, Quantitation Events offers a number of audit events that can be selected by the administrator when the system is being configured after installation, as shown in Figure 6.

For example, for each event:

- Audit
- Prompt reason
- Custom reason (up to 10 user-defined reasons for each auditable event)
- Electronic signature

In addition, there is the possibility to add a free text comment to an audit trail event if required.

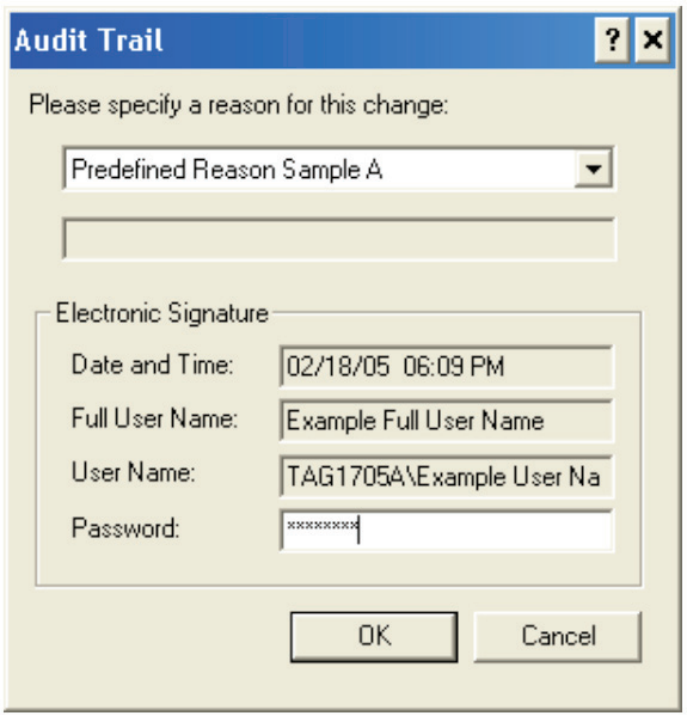

Figure 7. Audit Trail in use—user-defined drop down.

Special Administrator Account

A major issue when using only the workstation's OS for security and Analyst Software single-user mode is that the logging only identifies who logged into the current OS session. Once the system is set up to run by a user and left on, anyone can access the Analyst Software application and all changes could be logged to the original OS user. The use of a special administrator account allows a run, once set up, to proceed. The original user can even log off and the run would continue to the end. This approach allows many different users to submit batches to the server for processing and represents an advance over older versions of Analyst Software. While the project is stored locally on the workstation, the queue resides on the acquisition server.

In addition, while an analysis is in progress, another user can reprocess data from an earlier run. This allows maximum flexibility and use of resources while maintaining compliance by identifying individuals responsible for creating and modifying records.

REFERENCES

1. U.S. Food and Drug Administration
   Federal Register 1997, 62,
   13430-13466

   Regulation Portion:
   Department of Health and Human Services, Food and Drug Administration 21 CFR Part 11, Electronic Records; Electronic Signatures; Final Rule March 20, 1997
   Federal Register/Vol. 62, No. 54/Thursday, March 20, 1997/Rules and Regulations
   13464-13466

2. U.S. Food and Drug Administration Guidance for Industry:
   21 CFR Part 11; Electronic Records; Electronic Signatures Part 11 Scope and Application, 2003

   i) Guidance for Industry Part 11, Electronic Records; Electronic Signatures—Scope and Application (DRAFT GUIDANCE)
   February 20, 2003

   ii) Guidance for Industry Part 11, Electronic Records; Electronic Signatures—Scope and Application
   August 28, 2003

3. U.S. Food and Drug Administration Federal Register 1978, 43, 59986-60020

   Regulation Portion:
   Department of Health, Education and Welfare, Food and Drug Administration 21 CFR Part 58 Good Laboratory Practice for Nonclinical Laboratory Studies December 22, 1978
   60013–60020

   Amendment to 21 CFR Part 58:
   Department of Health and Human Services, Food and Drug Administration 21 CFR Part 58 Good Laboratory Practice Regulations
   Final Rule, September 4, 1987 Federal Register/Vol. 52, No. 172/Friday, September 4, 1987/Rules and Regulations
   33768- 33782

For Research Use Only. Not for use in diagnostic procedures.

1070610-01 08/2010

Headquarters
353 Hatch Drive | Foster City CA 94404 USA
Phone 650-638-5800
www.absciex.com

International Sales
For our office locations please call the division headquarters or refer to our website at
www.absciex.com/offices