Chapter 2
GALP Implementation Assistance

The GALP Implementation is based on established data management principles.

1. PRINCIPLES

Control is the essential objective behind most data management principles. Effective management and operation of an automated laboratory cannot be assured unless use and design of the LIMS is consistent with principles intended to assure LIMS control. Although accuracy and reliability of data must be ensured by a control based system of management, the most effective management systems invoke the participation of those employees affected by the control process. Most importantly, the GALPs assume laboratory professionals are personally motivated to follow the principles of their professions, and that they will take every practical step to ensure the accuracy and the reliability of the data and analyses produced by their laboratory.

The GALP guidance is built on six principles.

a. *Laboratory management must provide a method of assuring the integrity of all LIMS data.*

Communication, transfer, manipulation, and the storage/recall process all offer potential for data corruption. The demonstration of control necessitates the collection of evidence to prove that the system provides reasonable protection against data corruption.

b. ***The formulas and decision algorithms employed by the LIMS must be accurate and appropriate.***

Users cannot assume that the test or decision criteria are correct; those formulas must be inspected and verified.

c. ***A critical control element is the capability to track LIMS Raw Data entry, modification, and recording to the responsible person.***

This capability utilizes a password system or equivalent to identify the time, date, and person or persons entering, modifying, or recording data.

d. ***Consistent and appropriate change controls, capable of tracking the LIMS operations and software, are a vital element in the control process.***

All changes must follow carefully planned procedures, be properly documented, and when appropriate include acceptance testing.

e. ***Procedures must be established and documented for all users to follow. Control of even the most carefully designed and implemented LIMS will be thwarted if the user does not follow these procedures.***

This principle implies the development of clear directions and SOPs, the training of all users, and the availability of appropriate user support documentation.

f. ***The risk of LIMS failure requires that procedures be established and documented to minimize and manage their occurrence.***

Where appropriate, redundant systems must be installed and periodic system backups must be performed at a frequency consistent with the consequences of the loss of information resulting from a failure. The principle of control must extend to planning for reasonable unusual events and system stresses.

2. IMPLEMENTATION KEY

This page is a key for using the GALP IMPLEMENTATION ASSISTANCE. The model below, with commentary notes, illustrates the format and information that follows.

GALP functional area

GALP subfunctional area

Icon depicting the
GALP functional area

The wording of the particular GALP provision (from Chapter 1).

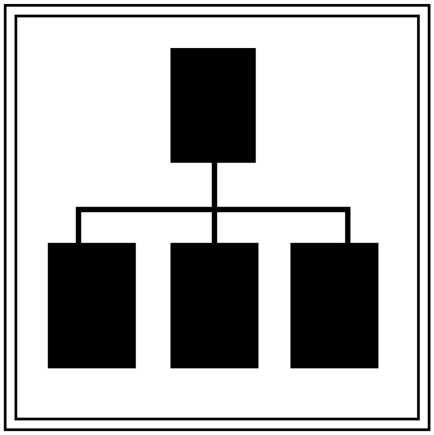
In cases where there are general specifications with distinct subsections or subspecifications, the general specification will always appear with each subspecification with two or three pages of discussion of that subspecification; the next subspecification will repeat the general specification, and follow with its discussion.

EXPLANATION A paragraph that defines the key terms of the provision and explains the intent of the provision.

DISCUSSION A discussion of the kind of compliance evidence that might be gathered, or acceptable ways in which the provision has been or may be met.

SPECIAL CONSIDERATIONS A discussion of potentially relevant facts or noteworthy factors that may be relevant for certain laboratory settings, computer equipment, EPA statutes, or litigation.

NOTES: The GALP Implementation Guidance is a working document. An area on the right-hand page is provided to allow annotation as needed. The size of this area is determined by the space available to complete a page. This variation is not meant to imply any difference in the extent of comment anticipated. Sources for additional guidance are also listed here.



8.1 LABORATORY MANAGEMENT

8.1 Laboratory Management

1) Personnel

When LIMS Raw Data (see 8.4.1) are collected, analyzed, processed, or maintained, laboratory management shall:

1) ensure that personnel clearly understand the function(s) they are to perform on the LIMS.

EXPLANATION

Laboratory management shall be responsible for the use and management of the LIMS. This necessitates that all LIMS support personnel and users are completely familiar with their responsibilities and assigned duties. Written job descriptions are necessary. Laboratory management shall be responsible for ensuring that appropriate professional hiring and assignment criteria are used, coupled with appropriate training, to ensure that all users are able to use the LIMS effectively.

DISCUSSION

Written position descriptions signed by LIMS support personnel and users, with accompanying laboratory management signatures, are a useful vehicle for documenting that personnel clearly understand the functions they are to perform. Because there are not widespread academic certifications or criteria that ensure system user competence, most laboratories rely on a three-part strategy for compliance: 1) Users are provided with clear operating instructions, manuals, and SOPs to enable them to perform assigned system functions; 2) Sufficient training to clarify these instructions is provided to users; 3) Users able to meet operation requirements are eligible to perform these LIMS functions.

SPECIAL CONSIDERATIONS

Because of its significance in evaluating the applicability of the GALPs, the identification and documentation of LIMS Raw Data (LRD) should be provided to all employees involved in the operation of the LIMS. It should be sufficiently specific and unambiguous to enable employees to readily identify LRD (see 8.4.1) so that each employee knows when the GALPs must be followed.

Notes…

8.1 Laboratory Management

2) Quality Assurance Unit

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall:

2) ensure that a Quality Assurance Unit (QAU) monitors LIMS activities as described in 8.3.

EXPLANATION

Laboratory management shall designate a group or individual as the QAU**.** This designation shall be consistent with the provisions set forth in 8.3. The QAU responsibilities are primarily inspection, audit, and review of the LIMS and its data.

DISCUSSION

An organizational plan should be developed to define lines of communication, reporting, inspection, and review of the LIMS and its data. The QAU must be entirely separate from and independent of the personnel engaged in the direction and conduct of a study, and should report to laboratory management. In smaller laboratories, a single individual may have many LIMS managerial responsibilities, but may not be the designated QAU.

Notes…

8.1 Laboratory Management

3) Personnel, Resources, and Facilities

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall:

3) ensure that personnel, resources, and facilities are adequate and available as scheduled.

EXPLANATION

Laboratory management shall ensure that personnel, resources, and facilities are adequate to handle LIMS functions and operation *in a timely fashion.* Resources include the LIMS equipment, materials, software, and training.

DISCUSSION

Laboratory management should ensure that backup staff for critical functions are available. In laboratories where time-critical functions are frequently encountered, laboratory management should be particularly sensitive to the need for adequate staff, backup, and other necessary resources.

Laboratory management should periodically assess the staffing levels for LIMS supervision, support, and operation, in order to determine if resources are adequate. Laboratory management may review training records to maintain awareness of the current status of training received and needed, observe job performance to determine the performance levels of current staff and possible needs for additional training, and examine project schedules and work backlogs to determine the adequacy of current staff and whether the LIMS is receiving proper staffing support.

SPECIAL CONSIDERATIONS

Laboratory management is responsible for *ensuring* all resources are adequate to support LIMS functions, but may find it necessary, particularly in larger operations, to delegate responsibility for *assessing* the adequacy of personnel, resources, and facilities to another individual.

When laboratory management delegates LIMS resource assessment, he/she shall ensure that the designated person has the experience, skills, and education to fulfill the responsibilities. Laboratory management is also responsible for ensuring that the designated person is available and has sufficient time and resources to fulfill the specific responsibilities. These responsibilities must be fully documented and consistent with 8.1.6.

Notes…

8.1 Laboratory Management

4) Quality Assurance Report

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall:

4) receive reports of QAU inspections of the LIMS (see 8.3.3) and audits of LIMS Raw Data (see 8.3.5) and ensure that corrective actions are promptly taken in response to any deficiencies.

EXPLANATION

The flow of information concerning all laboratory operations, including LIMS inspections and LRD audits, should expeditiously move to laboratory management. Laboratory management should review QAU inspection reports and audits, and may recommend remedial actions. It is ultimately the responsibility of laboratory management to ensure that any errors or deficiencies, discovered through QAU activities, are acted upon and rectified.

DISCUSSION

Laboratory policy or SOP should clearly state that all QAU inspection and audit reports are presented in a timely manner to laboratory management for review. These reports should have a provision for laboratory management's signature and date. Likewise, an SOP or policy should define the responsibility of management to follow up on all deficiencies found in the QAU report.

SPECIAL CONSIDERATIONS

A relevant legal concept is that the laboratory should be able to demonstrate due diligence in *carrying out* its own rules, not just have them.

Notes…

8.1 Laboratory Management

5) Approving SOPs and Documenting Deviations

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall:

5) **approve the standard operating procedures (SOPs) setting forth the methods that assure LIMS Raw Data integrity, ensure that any deviations from SOPs and applicable GALP provisions are appropriately documented and that corrective actions are taken and documented, and approve subsequent changes to SOPs (see 8.11).**

EXPLANATION

Laboratory management is ultimately responsible for all activity within the laboratory, including approval of SOPs and any subsequent changes, and implementation of required GALP provisions. An SOP or laboratory policy should state that any departure from laboratory SOPs and applicable GALP provisions will be reported to laboratory management. Laboratory management should then ensure that the deviation is properly documented and that appropriate corrective actions are taken and similarly documented.

DISCUSSION

As part of a comprehensive LIMS policy, there should be documented assurance that laboratory management is made aware of deficiencies or departures from the laboratory SOPs and required GALP provisions. The SOP or policy should state that laboratory management is responsible for ensuring that all deviations are noted and corrective actions taken and documented.

Notes…

8.1 Laboratory Management

6) Compliance With GALP Provisions

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall:

6) assure that each applicable GALP provision is followed. With the exception of 8.1, 8.2, and 8.3, laboratory management may delegate GALP implementation and compliance to one or more responsible persons.

EXPLANATION

Laboratory management is responsible for complying with each GALP provision that is required by the EPA program for which data are submitted. Laboratory management, particularly in large laboratories, may find it necessary to delegate GALP compliance responsibilities to one or more responsible persons. The GALP provisions in **8.1**, **8.2**, and **8.3** may not be delegated.

When GALP compliance responsibilities are delegated, laboratory management shall ensure that the designated responsible persons have the experience, skills, and education necessary to fulfill their responsibilities. Laboratory management is also responsible for ensuring that designated responsible persons are available and provided sufficient time and resources to fulfill their responsibilities.

Laboratory management shall ensure that delegation of GALP compliance responsibilities are fully documented and current. This documentation shall identify the individual who is assigned responsibility for compliance with each GALP provision and shall clearly specify each individual's job responsibilities and duties. The documentation shall be signed by each responsible person to demonstrate that each person is aware of his/her responsibilities.

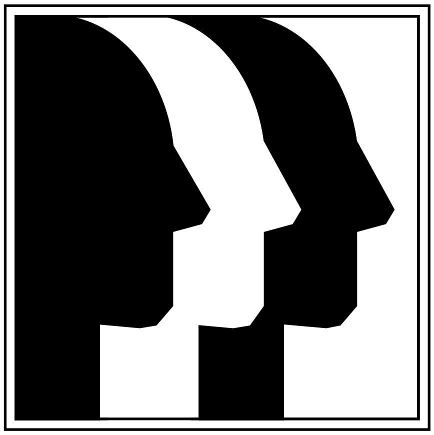
DISCUSSION

The manner by which GALP compliance responsibilities are distributed is at the discretion of laboratory management. At small laboratories, one person may be responsible for compliance with all GALP provisions. At larger laboratories, responsibilities may be distributed among a number of people. Larger laboratories might distribute responsibilities organizationally, functionally, by area of scientific study, or other methods that meet the laboratory's needs.

SPECIAL CONSIDERATIONS

It is strongly recommended that secondary responsible persons be designated. The designation of secondary responsible persons minimizes disruptions in the event of the prolonged absence of the primary responsible person.

Notes…



8.2
PERSONNEL

8.2 Personnel

1) Education

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall ensure that all LIMS support staff and users:

1) have adequate education, training, and experience to perform assigned LIMS functions.

EXPLANATION

All LIMS support staff and users shall have adequate education, training, and experience to perform assigned LIMS functions. This provision encompasses all LIMS functions used to collect, transmit, report, analyze, summarize, store, or otherwise manipulate data. Laboratory management is expected to use appropriate professional hiring and assignment criteria, coupled with appropriate training, to ensure that all users are able to use the LIMS effectively.

DISCUSSION

In certain cases, specialized training or attendance at special courses and certification programs may substitute for formal education requirements. Demonstrated experience may also substitute for formal education requirements. Either basis for substitution should be thoroughly and accurately documented. In certain cases, especially for personnel with advanced education and training, self-certification may be possible. Laboratory management should use professional judgment as to the appropriateness of self-certification.

Notes…

8.2 Personnel

2) Training

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall ensure that all LIMS support staff and users:

2) have a current summary of their training, experience, and job description, including their knowledge relevant to LIMS design and operation, maintained at the facility.

EXPLANATION

This provision states that documentation of personnel backgrounds, including education, training, and experience, is current and available. Pertinent LIMS design, support, and operations knowledge for each person with access to and responsibility for the LIMS should be included in the documentation. Evidence of training and experience that indicates knowledge sufficient for job requirements is essential.

DISCUSSION

Résumés (including references to education and degrees obtained, professional certificates, previous job titles, and responsibilities), reports of completed training, and current job descriptions may be centrally filed at the facility. Job performance evaluations may be used to demonstrate proper levels of LIMS knowledge and experience. Documentation of prior success in similar responsibilities may be sufficient.

SPECIAL CONSIDERATIONS

When outside vendors are involved, the required education, training, knowledge, and experience may be so indicated on their résumés.

Notes…

8.2 Personnel

3) Number of Persons

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall ensure that all LIMS support staff and users:

3) are of sufficient number for timely and proper operation of the LIMS.

EXPLANATION

Laboratory management is expected to maintain a staff that is adequate in size to ensure that functions for the LIMS will be performed in an accurate and timely manner, including all system-related tasks, and particularly time-critical functions.

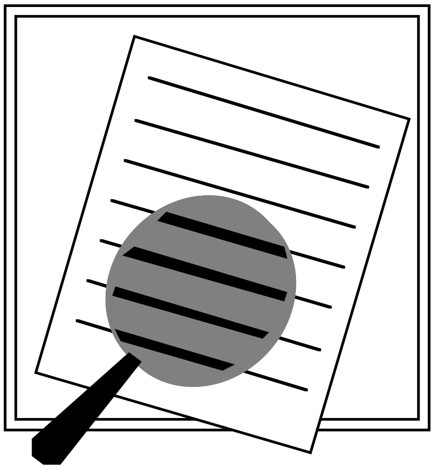
DISCUSSION

By designing and following a work plan for any particular study, laboratory management can anticipate staffing requirements necessary for a particular need. Laboratory management must be aware of any delays in operations due to inadequate staffing and take proper action.

Persistent and excessive overtime, excessive LIMS downtime, or delayed responses to hardware and software changes may indicate insufficient staffing.

Information regarding the adequate competence of personnel is discussed in **8.2.1**.

Notes…



8.3 QUALITY ASSURANCE UNIT

8.3 Quality Assurance Unit

1) Independent QAU

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall designate a Quality Assurance Unit (QAU) to monitor LIMS functions and procedures. The QAU shall:

1) be entirely separate from and independent of LIMS personnel, and shall report directly to laboratory management.

EXPLANATION

The QAU is responsible for assuring laboratory management of the integrity of the LRD; therefore, any real or apparent conflict of interest with LIMS personnel, including LIMS management, shall be avoided. Because laboratory management is ultimately responsible for compliance with all of the GALPs, the QAU shall necessarily report directly to laboratory management.

DISCUSSION

Documentation of the organization should be available providing clear evidence that the QAU reports directly to laboratory management. Similarly, descriptions of the positions and responsibilities of each QAU staff member should be available for review and provide evidence of their independence from LIMS personnel and management. These descriptions should also provide evidence of the role of QAU staff members in monitoring LIMS activities to assure LRD integrity. Organizational charts and job descriptions may be useful in providing this documentation.

SPECIAL CONSIDERATIONS

In LIMS operations where the number of personnel is small, there could be a real or apparent conflict of interest between the QAU and LIMS personnel and managers. In these situations, an extramural QAU may be required in the absence of alternative solutions to resolving the real or apparent conflict of interest.

Notes…

8.3 Quality Assurance Unit

2) Documentation Availability

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall designate a Quality Assurance Unit (QAU) to monitor LIMS functions and procedures. The QAU shall:

2) have immediate access to the LIMS data, SOPs, and other records pertaining to the operation and maintenance of the LIMS.

EXPLANATION

A complete and current set of SOPs shall be available and accessible at all times to the QAU. The QAU should also have access to the most current and version-specific set of LIMS operations and maintenance manuals, data, and other operations and maintenance documentation.

DISCUSSION

A complete and current copy of LIMS SOPs and technical documentation should exist as part of standard documentation and be accessible to the QAU. Documentation of the procedures described above may be set forth in SOPs and/or LIMS management policy. The documentation may be in writing or electronically maintained.

SPECIAL CONSIDERATIONS

If SOPs are stored electronically, the QAU shall be responsible for verifying that they are secure, retrievable, and readable; maintaining a hard copy of the electronic versions; and ensuring that the hard copy versions are identical to the electronic versions.

Notes…

8.3 Quality Assurance Unit

3) Inspections

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall designate a Quality Assurance Unit (QAU) to monitor LIMS functions and procedures. The QAU shall:

3) inspect the LIMS at intervals adequate to ensure the integrity of the LIMS Raw Data (see 8.3.5); prepare inspection reports that include a description of the LIMS operation inspected, the dates of the inspection, the person performing the inspection, findings and problems observed, action recommended and taken to resolve existing problems, and any scheduled dates for reinspection; and report to laboratory management any problems that may affect data integrity.

EXPLANATION

A LIMS that is consistently reliable and accurate is a major goal of QAU activity. To assure reliability and accuracy, the LIMS must be inspected on a regular basis. Inspection shall be performed at a frequency adequate to ensure the integrity of the LRD. The LIMS shall also be inspected immediately after any change to LIMS software or hardware.

Records of each inspection shall be prepared and maintained and shall include the following: the specific LIMS operation inspected, the name of the inspector, and the date of the inspection. Findings from the inspection and any problems observed shall be recorded. Actions recommended and those taken to resolve any problems that were found and scheduled dates for reinspection shall be documented. In all cases where problems affecting the integrity of LRD were observed during inspection, these problems shall be immediately reported to laboratory management. Documentation of reports to laboratory management should be maintained.

DISCUSSION

Although the QAU is responsible for reporting directly to laboratory management and is required to be independent of LIMS personnel, problems affecting the integrity of LRD may also be communicated directly and immediately to the appropriate LIMS personnel; thus a more rapid resolution of these problems can occur.

Notes…

8.3 Quality Assurance Unit

4) Deviations

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall designate a Quality Assurance Unit (QAU) to monitor LIMS functions and procedures. The QAU shall:

4) determine that no deviations from approved SOPs were made without proper authorization (see 8.1.5) and sufficient documentation.

EXPLANATION

The QAU shall ensure that no deviations from SOPs have been made without prior authorization and complete documentation of the change. Authorization for the planned deviation entails obtaining the approval, signature, and date of laboratory management prior to its occurrence. Documentation of any deviation shall include, but not be limited to: an explanation of the departure from methods established in the SOP, the reason for the departure, and the accompanying date of the departure.

DISCUSSION

In order to maintain complete control over LIMS operations and functions, it is important to ensure that the LIMS is consistently operated in compliance with approved SOPs.

In certain situations, unplanned deviations from the SOPs may occur. These deviations must be documented and include the explanation of the departure from the methods established in the SOPs, the reason for the departure, the signature and date of laboratory management, and its affect on the LIMS data.

Notes…

8.3 Quality Assurance Unit

5) LIMS Raw Data Audit

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall designate a Quality Assurance Unit (QAU) to monitor LIMS functions and procedures. The QAU shall:

5) periodically audit the LIMS Raw Data to ensure their integrity.

EXPLANATION

Periodic review of LRD that are being reported or will be reported are conducted to ensure the integrity and reliability of the LRD. By examining reported data and correlating it with the LRD for a specific LIMS reporting activity, the QAU will ensure the integrity of LRD.

DISCUSSION

An audit should be undertaken if QAU inspection problems are found that jeopardize LRD integrity. It is recommended that an SOP be established that requires periodic review of final reports and their corresponding LRD. Integrity problems or deviations arising from these audits should be reported to laboratory management as discussed in **8.3.3**.

If LIMS hardware or software are changed or relocated consistent with **8.7.2** and **8.5.2**, a review of reportable data against LRD is recommended.

SPECIAL CONSIDERATIONS

Movement of non-LIMS equipment, particularly those emitting magnetic radiation in close proximity to LIMS equipment, may affect LRD integrity. In these situations, it is strongly recommended to also review reported data against the LRD.

Notes…

8.3 Quality Assurance Unit

6) Records

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall designate a Quality Assurance Unit (QAU) to monitor LIMS functions and procedures. The QAU shall:

6) ensure that the responsibilities and procedures applicable to the QAU, the records maintained by the QAU, and the method of indexing such records are documented and are maintained.

EXPLANATION

The methods and procedures of the QAU shall be fully documented, consistently followed, and maintained by the QAU. The method of indexing such records shall also be documented and maintained.

DISCUSSION

It is important that the QAU inspection and audit reports discussed in **8.3.3** and **8.3.5** are identified and maintained to include date, time, and investigator(s). The complete set of documentation, including QAU responsibilities and procedures and their inspection reports should be indexed so as to be readily accessible.

Because the QAU must maintain all records and documentation pertaining to their activities, a policy or SOP may be developed to establish specific procedures for this.

Notes…

8.4
LIMS RAW DATA
(LRD)

8.4 LIMS Raw Data

1) Identification and Documentation

Laboratory management shall ensure that:

1) LIMS Raw Data (LRD) and LRD storage media on which they reside (see 9. Definitions LIMS Raw Data and LIMS Raw Data storage media) are identified and documented. This documentation shall be included in the laboratory's SOPs.

EXPLANATION

The objective of the GALPs is to provide EPA with assurance of the integrity of LIMS Raw Data (LRD). Thus the GALPs prescribe how LRD are to be entered, changed, stored, and secured. Laboratory management or designee (see **8.1.6**) shall assess data that are entered in, processed, maintained, or reported by the LIMS to identify and document those data that are LRD. The documentation shall also include a description of the LRD storage medium. LRD and their respective storage media shall be identified in the laboratory's SOPs. Copies of the SOPs shall be made available to all personnel with access to LRD, and laboratory management should assure that these personnel clearly understand the importance of LRD.

DISCUSSION

LRD are original observations recorded by the LIMS that are needed to verify, calculate, or derive data that are or may be reported. Original observations mean the first occurrence of human-readable information. The media to which the LRD are first recorded is the LRD storage media. The media may be paper, microfiche, microfilm, magnetic or optical storage media.

As an example: *Person A* places an environmental sample into a laboratory instrument that analyzes the sample and transmits signals to a personal computer (PC). The PC software captures the signals, analyzes them, and displays a graphical representation of the analyzed signals on a monitor. *Person B* examines the graphic, concludes it is realistic, and then issues a command to the PC software to record the analyzed data on a disk. The data stored on the disk are the LRD, and the disk is the LRD storage medium. The instrument, communications components, PC, PC software, monitor, recording device, and disk are a LIMS (see Figure 1.3).

Alternatively, *Person B* could issue a command to first record the analyzed signal to paper before it is recorded to disk. In this case, the paper is the LRD storage medium.

The documentation for the above example may be an SOP or SOPs that describe data entry, analysis, and recording. For example, a single SOP could be developed and maintained that documents data entry, analysis, and recording. It would specify recording of the instrument, *Person A*, time and date, and *Person B*, time and date, on the disk, and that the LRD and LRD storage medium are those recorded by *Person B* on the disk (or paper, depending on which the LRD are first recorded).

SPECIAL CONSIDERATIONS

1. Some EPA programs may require additional data beyond those discussed in the example above. To demonstrate the reliability of instrumentation, an EPA program may also require that the initial high and low values sent from the instrument to the LIMS be included with the LRD discussed in the example.

2. Original observations that have been recorded prior to entry to the LIMS (see Figure 1.2) are not LRD (see 3. below). However, laboratory management may want to extend the definition of LRD to include these observations, thus ensuring that they are GALP-compliant.

3. For 2. above, some EPA programs require that the original observations be maintained and stored on their original recording medium. For example, the GLPs define raw data as any laboratory worksheets, records, memoranda, notes, or exact copies thereof, that are the result of original observations and activities of a study and are necessary for the reconstruction and evaluation of the report of that study.

Notes…

8.4 LIMS Raw Data

2) Entry and Recording Person

Laboratory management shall ensure that:

2) the individual(s) responsible for entering and recording LIMS Raw Data is (are) uniquely identified when the data are recorded, and the time(s) and date(s) are documented.

EXPLANATION

Laboratory management shall ensure that LRD input is traceable to the person who manually input the LRD or who was responsible for transmission to the LIMS, and, if different, the person who was responsible for the recording of the LRD by the LIMS. The time and date for each of these actions shall also be documented.

DISCUSSION

The usual method for accomplishing this identification is to have the LIMS record a unique user identification code as part of the data being entered or recorded. The user ID code can then be referenced back to the associated data entry or data recording person to allow identification of all entered data.

SPECIAL CONSIDERATIONS

The person who operated the instrument may not be same as the person who transmitted the data. Knowing who operated the instrument, however, may be as important as knowing who entered or recorded the data into the LIMS. Thus, the laboratory should also document the instrument operator with the data entry/recording person(s). Laboratory management should ensure that the time and date for each action above is correct and has not been altered in an unapproved manner.

In the case of manual entry, the original data generally are study raw data (see 8.4.1 Special Considerations) and can be audited; the LRD are derived data.

Notes…

For additional guidance, see: *Automated Laboratory Standards: Evaluation of the Use of Automated Financial System Procedures, EPA/OIRM (June 1990);* and *Automated Laboratory Standards: Evaluation of the Standards and Procedures Used in Automated Clinical Laboratories, EPA/OIRM (May 1990).*

See Chapter 1, **11. SOURCES** for addresses and ordering information.

8.4 LIMS Raw Data

3) Instrument Identification

Laboratory management shall ensure that:

3) the instrument transmitting LIMS Raw Data is uniquely identified when the data are recorded, and the time and date are documented.

EXPLANATION

Laboratory management shall ensure that documentation for instruments that transmit data to the LIMS that are or will become LRD exists, is maintained, and includes the date and time of each transmission. It must be possible to trace to the source instrument the date and time of data transmission to the LIMS.

DISCUSSION

This can be accomplished by including a unique instrument identification code that also documents the date and time during transmission to the LIMS and records this information with the LRD.

Notes…

8.4 LIMS Raw Data

4) Verification

Laboratory management shall ensure that:

4) procedures and practices to verify the accuracy of LIMS Raw Data are documented and included in the laboratory's SOPs, and managed as described in 8.11.

EXPLANATION

The integrity of data can be compromised during data entry, electronic transfer from automated instruments, and particularly during manual entry. Procedures for verifying the accuracy of the LRD entered manually or electronically into the LIMS shall be documented and included in the laboratory's SOPs and managed as described in **8.11**. The implementation of these procedures shall be enforced by laboratory management.

DISCUSSION

Data verification methods, such as double-keying of manually entered data, blind re-keying of data entered automatically, or other proven methods, can be practiced to provide assurance of LRD integrity.

Notes…

For additional guidance, see: *Automated Laboratory Standards: Evaluation of the Use of Automated Financial System Procedures, EPA/OIRM (June 1990).*

See Chapter 1, **11. SOURCES** for addresses and ordering information.

8.4 LIMS Raw Data

5) Changes

Laboratory management shall ensure that:

5) procedures and practices for making changes to LIMS Raw Data are documented and provide evidence of change, preserve the original recorded documentation (see 8.4.2 and 8.4.3), are dated, indicate the reason for the change, identify the person who made the change and, if different, the person who authorized the change. These procedures shall be included in the laboratory's SOPs, and managed as described in 8.11.

EXPLANATION

When LRD are changed after initial recording, documentation shall exist that preserves the original recorded required documentation (see **8.4.2** and **8.4.3**), provides clear evidence that a change was made, explains the reason for the change, records the date of change, the person who made the change and, if different, the person who authorized the change. The laboratory’s SOPs shall include procedures for making changes to LRD in compliance with these recording requirements, and shall specify who has authority to make changes or to authorize changes, if different. These procedures shall be included in the laboratory’s SOPs, and shall be established, approved, and managed as described in **8.11.**

DISCUSSION

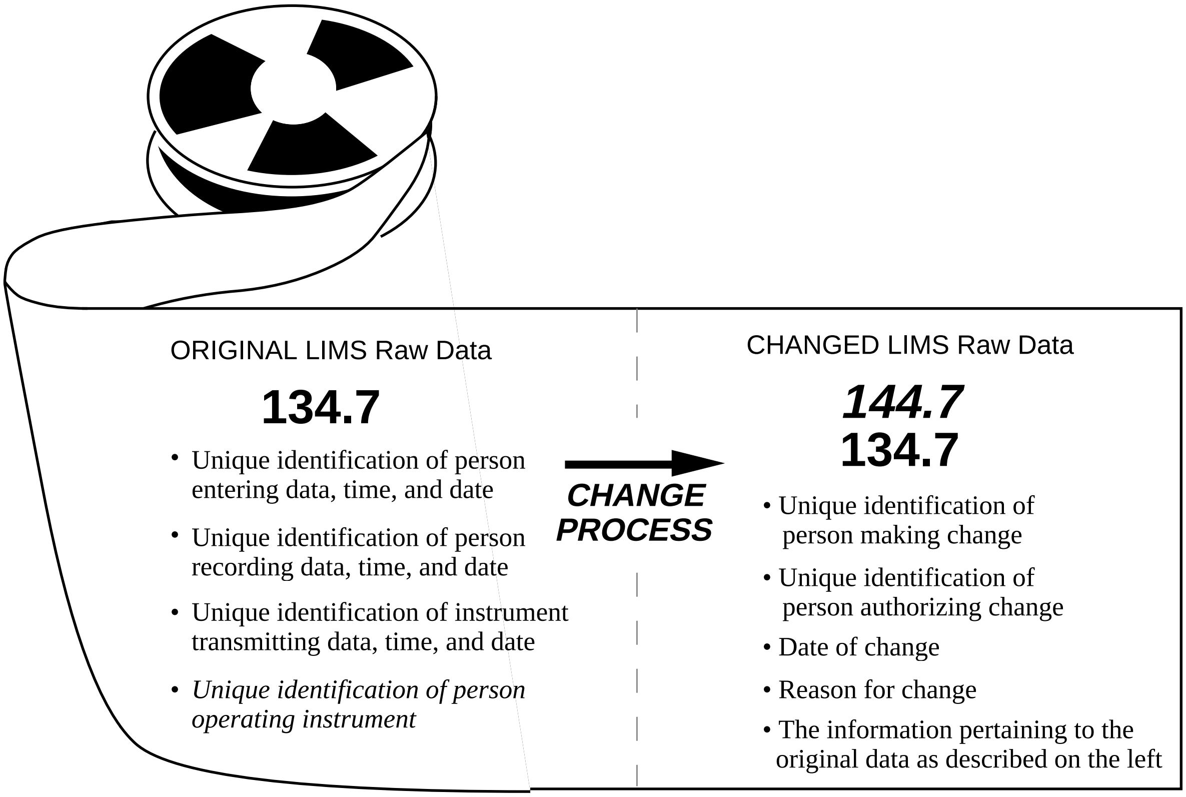
This GALP provision requires maintaining all LRD and changes to LRD so that all modifications are clearly documented. All documented changes shall be stored and retained as specified in **8.9** and **8.10.2**. If LRD are purged from the LIMS, a verified copy of the LRD should be maintained, for at least the required retention period.

SPECIAL CONSIDERATIONS

Recording both a person authorizing a change and a different person entering a change may not be feasible in an existing LIMS. To obviate this problem, laboratories may consider establishing a policy by which only one individual has authority to authorize changes and make changes to data on the LIMS. An alternative may be to retain paper copy authorizations or logs.

8.4 LIMS Raw Data

5) Changes



ORIGINAL LIMS Raw Data

134.7

- Unique identification of person entering data, time, and date
- Unique identification of person recording data, time, and date
- Unique identification of instrument transmitting data, time, and date
- *Unique identification of person operating instrument*

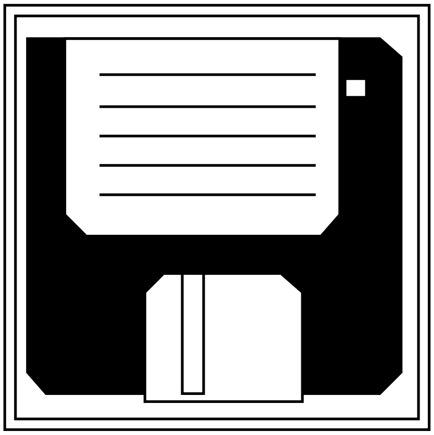
CHANGE PROCESS

CHANGED LIMS Raw Data

144.7
134.7

- Unique identification of person making change
- Unique identification of person authorizing change
- Date of change
- Reason for change
- The information pertaining to the original data as described on the left

Notes…



8.5
SOFTWARE

8.5 Software

1) Standard Operating Procedures

1) Development Methodology

When software is used to collect, analyze, process, or maintain LIMS Raw Data, laboratory management shall ensure that:

1) SOPs are established, approved, and managed as described in 8.11 for:

1) development methodologies that are based on the size and nature of software being developed. EPA and its agents shall comply with *EPA Information Resources Management Policy Manual*, *Chapter 17*.

EXPLANATION

An SOP shall be prepared for LIMS software development methodology. In preparing this SOP, all GALP provisions, especially **8.4** and **8.6**, should be considered. *EPA Information Resources Management Policy Manual*, *Chapter 17*, serves as software development guidance for the Agency. The methodology set forth in this guide shall be used by EPA and its agents (contractors and grantees) when developing software. If an EPA office has supplemented *EPA Information Resources Management Policy Manual* with its own guidance, the laboratory must consider the applicability of this specific guidance to the software to be developed. The SOP documenting the development methodology shall be established, approved, and managed as described in **8.11**.

DISCUSSION

When selecting a LIMS software development methodology, the laboratory's goal is the reliability of LIMS Raw Data. The methodology and techniques selected should contribute to the software's accuracy and reliability in meeting user needs. In most cases, the methodology should include user involvement throughout the development cycle.

Laboratory management should consider several factors in selecting the development methodology. A large system that will be used for several years by many users is a good candidate for the full development methodology documented in *EPA Information Resources Management Policy Manual*. A stand-alone program, a single-user system, or a system that will be used for only a short period of time would more likely be suited to rapid application development techniques and less formally structured development methods.

Notes…

For additional guidance, see: *EPA Information Resources Management Policy Manual*, *Chapter 17 (September 1994).*

See Chapter 1, **11. SOURCES** for addresses and ordering information.

8.5 Software

1) Standard Operating Procedures

2) Testing and Quality Assurance

When software is used to collect, analyze, process, or maintain LIMS Raw Data, laboratory management shall ensure that:

1) SOPs are established, approved, and managed as described in 8.11 for:

2) testing and quality assurance methods to ensure that all LIMS software accurately performs its intended functions, including: acceptance criteria, tests to be used, personnel responsible for conducting the tests, documentation of test results, and test review and approval.

EXPLANATION

SOPs shall be prepared for conducting and documenting testing and quality assurance. Testing and quality assurance involves evaluating new or changed software to determine that it performs correctly and meets user requirements. SOPs shall document when testing and quality assurance are required, as well as how they are to be conducted, the acceptance criteria, personnel responsible for testing, and documentation of test results, test review, and approval. Testing and quality assurance are specified in *EPA Information Resources Management Policy Manual, Chapter 17.* SOPs for testing and quality assurance shall be established, approved, and managed as described in **8.11**.

DISCUSSION

Testing and quality assurance procedures are standard integral parts of the change control process, that also apply to implementation of new software. Users should be involved in testing programs in an environment that will not affect the production system. New software should also be tested in a similar way by potential users. Acceptance criteria should be documented before testing begins to ensure that testing is predicated on meeting those standards, as discussed in **8.5.2.2**. SOPs may include provisions for laboratory management to review the tests and results to ascertain that criteria are appropriate and are met to their satisfaction.

SPECIAL CONSIDERATIONS

Testing and quality assurance procedures should be performed by individuals responsible for installation and operation of the LIMS and not by the QAU (see **8.5.2.2** Special Considerations).

Notes…

For additional guidance, see: *EPA Information Resources Management Policy Manual, Chapter 17 (September 1994).*

See Chapter 1, **11. Sources** for addresses and ordering information.

8.5 Software

1) Standard Operating Procedures

3) Change Control

When software is used to collect, analyze, process, or maintain LIMS Raw Data, laboratory management shall ensure that:

1) SOPs are established, approved, and managed as described in 8.11 for:

3) change control methods that include instructions for requesting, testing, approving, documenting, and implementing changes. When indicated, change control methods shall also include reporting and evaluating problems, as well as implementing corrective actions.

EXPLANATION

SOPs shall be prepared for problem reporting and change control procedures that apply to all layers of software used in the laboratory, including custom-developed and commercially-available software. The procedures should be tailored to each kind of software. SOPs for change control shall be established, approved, and managed as described in **8.11**.

Change control procedures shall specify:

- persons authorized to request software changes
- requirements to be met for approval of change requests
- responsibilities and methods for documenting testing and quality assurance
- approval procedures for changed versions
- procedures for moving changed versions to the production environment.
- forms designed for change request/problem reports
- methods for establishing the priority of change requests
- LIMS archives from which to take copies of programs to be amended (see **8.5.4**)
- procedures for maintaining amended copies that conform with SOPs

8.5 Software

1) Standard Operating Procedures

3) Change Control

DISCUSSION

Change control procedures should also be tailored to handle changes of different priorities. For example, procedures for dealing with emergency problems should expedite corrective action. The laboratory should consider a centralized change control system (manual or automated) that includes all change requests, including emergency problems, corrections to software errors, and enhancement requests. A centralized change control system may allow better tracking and control than separate systems. The change control procedure should designate a person authorized to move changed program versions to the production environment.

Problem report forms with written instructions for completion may be developed, and problem logs may be maintained by a designated person. Analysis and initial reporting may be required within a specific time frame and may be performed by the responsible person until resolution is reached.

Notes…

For additional guidance, see: *EPA Information Resources Management Policy Manual, Chapter 17 (September 1994).*

See Chapter 1, **11. Sources** for addresses and ordering information.

8.5 Software

1) Standard Operating Procedures

4) Version Control

When software is used to collect, analyze, process, or maintain LIMS Raw Data, laboratory management shall ensure that:

1) SOPs are established, approved, and managed as described in 8.11 for:

4) version control methods that document the LIMS software version currently used.

EXPLANATION

SOPs shall be prepared to document the process that establishes and maintains the identification of the LIMS software version in use at the time each data set was created. SOPs for version control shall be established, approved, and managed as described in **8.11**.

DISCUSSION

This process can be met by ensuring that the date and time of generation of all data sets are documented, and that the LIMS software version generating the data set is identified in the data file. The laboratory shall ensure that historical files (see **8.5.4**) are established and maintained to indicate the current version and all previous versions of the software releases and individual programs, including dates and times they were put into and removed from the LIMS production environment.

Notes…

8.5 Software

1) Standard Operating Procedures

5) Historical File

When software is used to collect, analyze, process, or maintain LIMS Raw Data, laboratory management shall ensure that:

1) SOPs are established, approved, and managed as described in 8.11 for:

5) maintaining a historical file of software, software operating procedures (manuals), software changes, and software version numbers.

EXPLANATION

SOPs shall be prepared to document the procedures by which historical files are maintained. These files shall include, but not be limited to, all software versions (see **8.5.1.4**) and software operating procedures for each version. Consistent procedures for management of historical files shall be documented to assure that these files are current, complete, and easily accessible. SOPs for maintaining a historical file of software shall be established, approved, and managed as described in **8.11**.

DISCUSSION

The ability to verify the accuracy of LRD and reportable data necessitates that all software versions, all software changes, and all operating instructions are available, maintained, complete, and current. To assure this, an SOP should specify methods for storage and retention times that comply with **8.9**. The SOP should specify that all historical files be maintained in a designated location that is safe and secure, and that adequately preserves the software for the required retention period.

Notes…

8.5 Software

2) Documentation

1) Existing and Commercially-Available Systems

When software is used to collect, analyze, process, or maintain LIMS Raw Data, laboratory management shall ensure that:

2) documentation is established and maintained to demonstrate the validity of software used in the LIMS:

> **1) for existing and commercially-available LIMS, minimum documentation shall include, but not be limited to: a description of the software and functional requirements; listing of all algorithms and formulas; and, as they occur, testing and quality assurance, installation and operation, maintenance/enhancement, and retirement.**

EXPLANATION

To demonstrate the validity of software used, LIMS software documentation should include, within practical limits, all phases of the software life cycle (see 8.5.2.2). For existing and commercially-available LIMS software, the minimum documentation shall include:

A. LIMS software description and functional requirements

B. algorithms and formulas

C. testing and quality assurance procedures

D. installation and operation, maintenance/enhancement, and retirement procedures

DISCUSSION

For commercially-available software and LIMS software in use prior to publication of the GALPs, the documentation of additional life cycle phases is governed by the magnitude of the programming effort involved in creating the software. Large, complex applications that require lengthy and expensive software development efforts necessitate an equivalent level of effort in the creation of detailed documentation that describes the application throughout each software life cycle phase. A small, less detailed program written by one programmer in a short period of time (such as a week), requires less documentation that may involve only a paragraph describing each phase of the software life cycle.

For existing or commercially-available LIMS software, documentation may be difficult to obtain. However, LIMS software descriptions and functional requirements can be developed. User requirements that lead to the purchase of a commercially-available LIMS can be used to develop the functional requirements documentation.

Software vendors may provide some LIMS software design documentation, but for proprietary reasons, it may not be complete. File layouts, program descriptions, and functional specifications may be provided, but program specifications and source code may be unavailable. If the minimum documentation described above is not provided, an attempt to obtain it from the vendor should be made; however, it may be necessary to reconstruct it in-house.

A. LIMS Software Description and Functional Requirements

A description shall be documented and maintained for the LIMS software that provides detailed information on the functions the software performs. Depending on the nature or internal structure of the software, the documentation for the functional requirements may include: flowcharts or block diagrams that illustrate step-by-step processing of a software module, data flow diagrams that illustrate the movement of data through the LIMS, or entity-relationship diagrams that illustrate the relationship of the data within the database.

B. Algorithms and Formulas

All algorithms and formulas used in the LIMS, and modules that allow user entry of formulas or algorithms, shall be documented and retained. Documentation of the algorithms and formulas should be easily discernible. These listings should identify the locations in which the formulas and algorithms occur in the LIMS software.

Documentation for all such formulas and algorithms can be maintained in a central location. In some cases, formulas and algorithms for purchased software may be obtained from vendor-provided documentation. For software currently in use, it may be possible to extract the formulas and algorithms from source code.

C. Testing and Quality Assurance

Documentation shall be established and maintained to support testing and quality assurance. The documentation should describe procedures that ensure the LIMS works as intended and that it meets organizational standards for performance, reliability, integrity, and availability. Testing documentation should include evidence of integration and validation testing. Test specifications and results (unit tests, system tests, integration tests) should be documented and maintained.

D. Installation and Operation, Maintenance/Enhancement, and Retirement Procedures

Documentation shall be established and maintained to support the initial and continuing operations of the LIMS software. The documentation includes implementation plans and procedures, methods for regulating and controlling software changes (see **8.5.1.3**), routine support requirements, and post-implementation reviews. Retirement plans and procedures identify a means of retrieving LIMS data after the LIMS is replaced or is no longer operational.

Notes…

8.5 Software

2) Documentation

2) New Systems

When software is used to collect, analyze, process, or maintain LIMS Raw Data, laboratory management shall ensure that:

2) documentation is established and maintained to demonstrate the validity of software used in the LIMS:

2) for new LIMS development or modification of existing LIMS, documentation shall cover all phases of the generic software life cycle. EPA laboratories and those of its agents (contractors and grantees) shall comply with the documentation requirements specified in *EPA Information Resources Management Policy Manual, Chapter 17*.

EXPLANATION

The goal of LIMS software documentation efforts shall be to demonstrate the validity of the software used. The documentation shall accurately describe the software's functions and internal structures as they exist, or will exist, during each of the software life cycle phases. The terms used to describe each software life cycle phase have varied over time and have been published using different "standard" terminology However, the general structure and progression of the software life cycle has remained the same for many years.

For new LIMS software (under development, or to be developed) used in EPA-sponsored studies, laboratories shall establish and maintain life cycle documentation that conforms to the specifications of *EPA Information Resources Management Policy Manual*, *Chapter 17*. The extent of the documentation shall be consistent with the software application's size, cost, sensitivity of data, policy implications, and diversity of organizations using the LIMS. New LIMS software documentation should generally include the following, which are intended to cover all phases of the software life cycle:

- initiation
- requirements analysis
- design
- programming
- testing and quality assurance
- installation and operation
- maintenance/enhancement
- retirement

8.5 Software

2) Documentation

2) New Systems

DISCUSSION

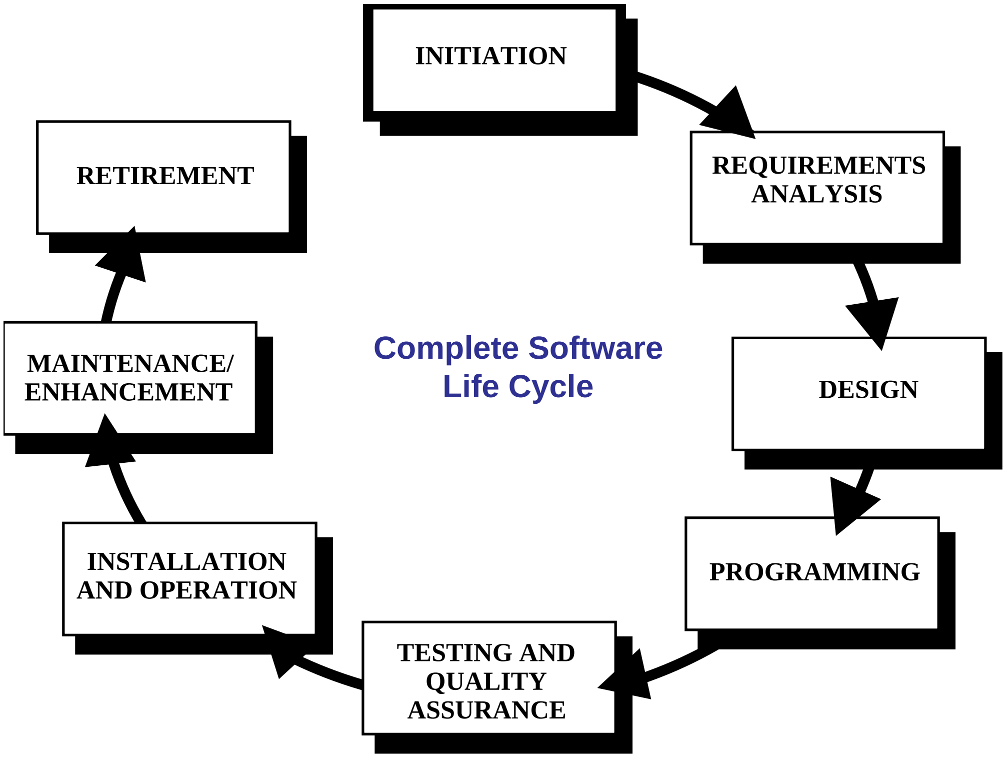
SOPs may be established and maintained to ensure that each phase of the software life cycle is documented. Laboratory management review of milestones ensures that required documentation is available before giving approval for LIMS software development to proceed.

Documentation standards for initiation and requirements analysis can be established. The initiation documentation can include a request for LIMS development or enhancement, and the needs that are resolved. The requirements analysis documentation identifies the functions that the LIMS will perform.

Design and programming standards ensure that minimum requirements are met and foster consistency and uniformity in the software. File layout formats, screen formats, and report formats can be included in the design standards. Explanatory comments, section and function labels, the programming language, identification of the programmer, dates of original writing and all changes, the use of logical variable names, and other programming documentation requirements are established by the programming standards.

Testing and quality assurance standards ensure that the LIMS performs as it was intended. Testing and quality assurance include both unit and integration testing. It assures that the LIMS meets standards for performance, reliability, integrity, and security.

Installation and operation standards assure a smooth transition from existing laboratory operations to the LIMS. Maintenance/enhancement standards improve the continuing operation of the LIMS. The maintenance/enhancement procedures identify change control procedures for resolving problems not discovered during testing, improving LIMS performance, and modifying the LIMS to meet changing needs or new requirements. The retirement standards identify procedures for ending use of the LIMS due to obsolescence or replacement. The retirement procedures identify a means of retrieving historical LIMS data.


INITIATION
REQUIREMENTS ANALYSIS
DESIGN
PROGRAMMING
TESTING AND QUALITY ASSURANCE
INSTALLATION AND OPERATION
MAINTENANCE/ ENHANCEMENT
RETIREMENT
Complete Software Life Cycle

SPECIAL CONSIDERATIONS

Testing and quality assurance must be performed on LIMS software to ensure that it functions as intended and meets applicable standards. Software testing and quality assurance procedures should be performed by individuals responsible for installation and operation of the LIMS and not by the QAU, because the QAU must be entirely separate from and independent of LIMS personnel (see **8.3.1**). However, the QAU may monitor and review quality assurance procedures throughout the software life cycle.

Notes…

For additional guidance, see: *EPA Information Resources Management Policy Manual, Chapter 17 (September 1994).*

See Chapter 1, **11. Sources** for addresses and ordering information.

When software is used to collect, analyze, process, or maintain LIMS Raw Data, laboratory management shall ensure that:

3) all documentation specified in 8.5.2 is readily available in the facility where the software is used, and the SOPs specified in 8.5.1 are readily available in the laboratory areas where procedures are performed.

EXPLANATION

All documentation and SOPs, or copies thereof, shall be available in the work areas of LIMS developers, operators, and/or users, as applicable. SOPs shall be available to each department or work group within a laboratory, and importantly, shall be current.

DISCUSSION

Original SOPs and documents should be maintained centrally to prevent their loss or misplacement. Persons responsible for producing SOPs or documentation manuals may maintain a record of SOPs or documentation issued, their numbers, and identification of persons to whom they were issued, thus facilitating ease in issuing updates. User manuals should be readily available to all users. It is particularly important that SOPs and documentation pertinent to development methodologies, testing and quality assurance, change control, version control, and historical files be immediately available where the work is performed.

Notes…

8.5 Software

4) Historical File

When software is used to collect, analyze, process, or maintain LIMS Raw Data, laboratory management shall ensure that:

4) a historical file of software and the documentation specified in 8.5.2 are retained according to procedures outlined in 8.9.

EXPLANATION

Previously used software, LIMS manuals, user maintenance manuals, and other documents specified in **8.5.2** shall be retained in compliance with **8.9.** If the retention time is not specified, the period should be sufficient to allow the laboratory to support any challenges to the integrity of the LRD.

Files of all versions of software programs shall be created and maintained so that the history of each program is evident. Differences between the versions and the time of their use shall be evident.

DISCUSSION

The laboratory should ensure that historical files indicate all previous versions of software releases and individual programs, including the dates they were placed into and removed from production. Software program listings can include internal references to a project number. For each data set, the historical file should identify the version of software used in creating each set of LRD.

Notes…

For additional guidance, see: *EPA Operations and Maintenance Manual (April 1990).*

See Chapter 1, **11. SOURCES** for addresses and ordering information.

8.6
SECURITY

8.6 Security

Laboratory management shall ensure that security practices to assure the integrity of LIMS data are adequate. EPA laboratories and those of its agents (contractors and grantees) shall comply with EPA's Information Security Policy.

EXPLANATION

Requirements for protecting LIMS data from destruction, disclosure, alteration, delay or undesired manipulation can vary greatly according to laboratory needs and requirements. Laboratory management is responsible for ensuring that threats to the LIMS and its data have been assessed, compensating safeguards implemented, and, where required, other established security requirements implemented.

EPA's Information Security Policy (described in *EPA Information Resource Management Policy Manual*, *Chapter 8*) formally establishes a comprehensive, Agencywide information security program. This policy implements OMB Circular A-130 and describes individual and organizational responsibilities for EPA staff and its agents. A procedural manual, *EPA Information Security Manual*, explains how to comply with this policy and with the congressionally-mandated Computer Security Act of 1987. The following Discussion summarizes the detailed information contained in these documents.

DISCUSSION

Security of LIMS is often an afterthought that LIMS staff and users frequently minimize as an unnecessary imposition, or view as preventing free information exchange, rather than as safeguards for the destructive effects of malicious hackers, LIMS failures or natural disasters. Congress emphasized the importance of security by enacting the Computer Security Act of 1987. Experienced LIMS staff and users are becoming acutely aware of the need for safeguards to protect against undesired and frequently unforeseen events. These events, whether accidental or deliberate, can result in:

- modification or destruction of data,
- unavailability of data or services, or
- the unwanted disclosure of data.

These three general damaging results have shaped the three traditional objectives (see **I. Security Objectives** below) of computer security:

- integrity,
- availability, and
- confidentiality.

They commonly form the basis for all security decisions or initiatives.

Undesired events, commonly referred to as threats (see **III. Threats**), should be identified for all the assets constituting the LIMS. These assets (see **II. Assets**) can include people, hardware, software, physical environment, and others. Reaching a decision about what, if anything, should be done for each identified threat/asset involves two distinct phases:

- risk analysis (see **IV. Risk Analysis**), identifying and estimating the damage of each threat/asset risk; and,
- risk management (see **V. Risk Management**), identifying, selecting, and implementing safeguards to protect against the threat, reduce its impact, or facilitate recovery from its occurrence.

There are some minimum safeguards (see **VI. Minimum Safeguards**) that common sense dictates be implemented to ensure physical protection of LIMS hardware, software, data, and storage media. The cost involved with implementing these safeguards may be very small, if not zero, and thus do not require a formal security risk analysis to justify their implementation.

I. Security Objectives

The **integrity objective** provides owners and users of laboratory data with assurance that their data are reliable and accurate. Achieving this objective necessitates implementation of safeguards for threats to the integrity of data and the applications that process the data. Examples of safeguards for software that provide assurance of integrity include implementing data verification procedures for manual data entry as specified in **8.4.4**, implementing data change requirements described in **8.4.5**, and password-protecting access to LIMS software (see **VI. Minimum Safeguards**).

The **availability objective** provides protection against the loss of information or services. Serious problems can result from loss of LIMS data because they can be costly to replace. Similarly, if the LIMS cannot be used or cannot provide timely services, the production or reporting of LIMS data can be lost or impaired. Examples of safeguards to provide assurance of the availability of LIMS data include implementing a regular schedule for backups, placing storage media in a secured place, and use of an Uninterruptible Power Supply device to provide virtually complete surge protection, a filter for line noise, and backup power in the event of an outage (see **VI. Minimum Safeguards**).

The **confidentiality objective** addresses those situations where disclosure of data would be undesirable or, in some situations unlawful, such as Confidential Business Information (CBI) (see Notes at end of Discussion for references). Confidentiality ensures the protection of private information from being disclosed to anyone who is not authorized to access it. Examples of safeguards to provide assurance of confidentiality include physical access controls, encryption when transmitting data, and disposal practices for reports when they are no longer needed (see **VI. Minimum Safeguards**).

II. Assets

An asset has value and may be tangible or intangible. An organization should identify all assets that must be protected. Some assets have minimal value and do not require protection. A partial list of potential assets includes the following:

Tangibles	Intangibles
Facilities	Personnel
Hardware	Reputation
Software (system and application)	Motivation
Supplies	Morale
Documentation	Goodwill
Data	Opportunity

Traditionally, tangible assets were viewed as only hardware and were the major concern of security. Placing a value on these assets may be relatively easy because in most cases they are purchased items.

However, tangible assets also include software, data, and documentation. It can be difficult to place a value on data and documentation because these assets are usually derived from expenditures of a variety of laboratory resources. LIMS data are obtained from sources such as observations, analytical instruments, and laboratory equipment. If data are the result of an analytical experiment or sample analysis, value can be derived from examining the resources used during the process that produced them.

Another consideration in determining the value of LIMS data is the capability of reproducing the data itself. Data that cannot be reproduced may have a significantly higher value than data that are easily reproduced. In a similar manner, the value of the documentation for the LIMS and its applications must be determined.

The value of intangible assets is somewhat subjective. However, intangible assets must be identified and considered when performing a security risk analysis.

III. Threats

Once LIMS assets are determined, it is necessary to identify **threats**, **potential threats**, and **future threats** to the assets. By identifying these threats, possible vulnerabilities to integrity, confidentiality, and availability can be identified and addressed. Threats may exist in many forms; they can be the result of natural disasters, intentional or accidental action, or malicious or inadvertent destruction.

Natural disasters and environmental hazards are significant threats primarily to LIMS tangible assets. Potential natural disaster can include floods, tornadoes, or hurricanes. Environmental hazards include fires, water damage (from bursting water pipes), and power failures. These disasters can damage or completely destroy the facility, operating environment, documentation, hardware, software, and LIMS data. Disruption can occur to communication, operations, or applications.

Other significant threats can result from unrestricted access to the LIMS assets. Safeguards are most often needed that limit access to the facility, equipment, hardware, software, documentation, and data. Threats must be assessed for every potential avenue of access. LIMS data are especially vulnerable because they are subject to accidental modification or destruction as well as malicious acts of theft or data sabotage. Accidental data corruption can result from faulty procedures or from failures of system software security. Training of personnel and development and compliance with comprehensive SOPs can eliminate much accidental data corruption or loss.

The threat of computer fraud, frequently motivated by greed and malice, should be considered. The greater the LIMS data value the greater the potential for intentional threats. LIMS data should be reviewed to determine if there is value or liability from an intruder in penetrating the LIMS, disclosing its data, or disrupting operations. Similarly, the LIMS data should also be evaluated to determine the impact of decision making and reporting based on incorrect or corrupted data. In addition to physical controls, the development of and compliance with comprehensive SOPs provides safeguards against theft or sabotage.

IV. Risk Analysis

Risk analysis is a process for estimating potential losses that may result from LIMS vulnerabilities and quantifying the damage that may result if adverse events occur. The ultimate goal of risk analysis is to select safeguards that reduce risks to an acceptable level. Risk analysis is a means of determining the resources needed—in budgetary terms of programming, equipment and people— to minimize the loss of LIMS data integrity, availability, or confidentiality. The extent of the risk analysis depends on the complexity of the LIMS system, its uses, the characteristics of its users, and the value of the LIMS data.

EPA Information Security Manual describes methods for performing risk analyses for different types of LIMS assets.

Step 1 Identification of assets and determination of threats;
Step 2 Identification of existing safeguards;
Step 3 Determining the overall risk to the system based on threats identified and effectiveness of existing safeguards;
Step 4 Evaluation and selection of safeguards; and
Step 5 Preparing a summary of findings and recommendations.

This risk analysis can then be used as the basis for establishing a cost-effective risk management program.

V. Risk Management

Risk management ensures that adequate steps are taken to prevent or mediate situations that can interfere with accomplishing the laboratory’s mission. Risk management includes establishing security safeguards and plans for contingencies (disaster recovery plans). A necessary part of risk management is to assure implementation of the safeguards and contingency plans. An important first step is to provide proper training of personnel (security awareness training) to ensure that all employees understand their security roles.

Risk management involves establishing safeguards to improve protection of information and information processing resources and to adequately protect the LIMS data from loss, misuse, unauthorized access or modification, unavailability, or undetected activities. Safeguards may include restricted user interfaces to LIMS system and application software and LIMS data, user verification, isolation of critical LIMS application software, and reviewing and testing the LIMS design. Including safeguards from the start of LIMS development or LIMS procurement effort is the most cost-effective way to optimize integrity, availability, and confidentiality of LIMS data. Risk analysis information, described above, should be used in the design phase of LIMS development to effect the greatest reduction in the annual loss expectancy at the least total cost. This information can also guide laboratory management in developing procedures to meet the LIMS security objectives of integrity, availability, and confidentiality. To maintain LIMS security, audits of security practices assist laboratory management in monitoring security needs and in maintaining reliable compliance with established safeguards.

Another aspect of risk management involves the development of contingency plans (or disaster recovery plans) for LIMS operations in the event of a failure or emergency from a number of potential sources such as natural disasters or equipment malfunction. Laboratory management should develop workable procedures that ensure the continuance of essential functions in the event that LIMS functions are interrupted. The primary objective of contingency planning is to protect against unacceptable data loss. It is also important to provide protection for source documents, input and output data, and application software. It may also be necessary to anticipate the need for alternate hardware and equipment. Contingency plans should include procedures for remote storage of backup data and recovery of data from backup data files. Contingency planning should be coordinated with other hardware safeguards, backup procedures, and recovery plans.

Security awareness training is an important first step in implementing any risk management plan. All employees involved in the management, use, design, development, maintenance, or operation of the LIMS should be aware of their security responsibilities. Laboratory management should select and implement appropriate security awareness techniques such as training, lectures and seminars, posters, and orientation booklets. Incentives for adherence by staff to security procedures may include assigning employee responsibility for security, publicity of security breaches, and rewards for employees who prevent breaches.

Specific requirements for security and disaster recovery plans are found in *EPA Information Security Manual* and *EPA Operations and Maintenance Manual*.

VI. Minimum Safeguards by Asset: Stand-alone, Networked, and Data Center Computing

Meeting the objectives of data integrity, availability, and confidentiality necessitates that certain minimum safeguards be implemented for the LIMS. Minimum safeguards are those common sense measures which may be implemented without performing a risk analysis. These safeguards ensure the physical and environmental protection of LIMS equipment and media, and the effective management of the LIMS.

The cost involved in implementing these safeguards should be minimal. If the LIMS contains sensitive information, OMB Bulletin No. 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*, (July 9, 1990) applies. (Data are considered sensitive if they meet the criteria established in Federal statutes (see Notes at end of Discussion) and/or are defined as sensitive through risk analysis. Sensitive data also is defined by legal agreement protecting information such as site location or source information.)

This section describes minimum safeguards by LIMS asset, arranged into three categories:

A. Stand-alone Computing
B. Networked Computing
C. Data Center Computing

"Stand-alone computing" is defined as those LIMS that have no physical or logical connection to any other computer system. A logical connection is an active network connection; it is a connection to another computer. A physical connection is a communication connection (wire or optic cable) to another computer or network. Generally, stand-alone computers are those personal computers or workstations that have no connection whatsoever (physical) to a network or to another computer. However, a computer could be considered a stand-alone system if it is physically connected to a network or another computer, but does not

VI. Minimum Safeguards by Asset: Stand-alone, Networked, and Data Center Computing

have the ability to transmit to or receive data from the network or system. Examples include:

- a computer with no physical connection to another computer
- a computer with a physical connection, but the installed networking software is disabled or is inactive

“Networked computing” is defined as those LIMS that have an active logical connection to a network or to another computer system. In practice, most networked computers are personal computers, workstations, or minicomputers that have active connections to a local area network (LAN) or wide area network (WAN). Many of these systems are increasingly participating in client/server relationships that share the workload over several computers. The majority of these computer systems are usually physically located on or near an employee’s work space.

“Data center computing” is defined as those LIMS that are physically located within the confines of a special facility dedicated to computing. Data center computers are almost always large minicomputers and mainframes with specialized peripherals such as external disk arrays, tape drives, and telecommunications interfaces. Certain security issues, mostly those involving special physical and environmental safeguards, apply to data center computers.

Some LIMS computing environments do not fall neatly into one of these categories. For example, most data center computers have active connections to a network. With the rapidly evolving sophistication of networking software, it is conceivable that a stand-alone computer can have small networking modules activated that permit trivial, but highly secure, networking operations to take place. When the system’s computing configuration or environment appears to overlap a category, the more stringent safeguard should be applied.

VI. Minimum Safeguards by Asset: Stand-alone, Networked, and Data Center Computing

A. Stand-alone Computing

1. Meeting the Objectives of Data Integrity, Availability, and Confidentiality

Stand-alone LIMS are sometimes considered the least susceptible to the viruses and hacking that have become a threat to networked systems. However, the data integrity and availability of stand-alone systems can be easily compromised if the physical and environmental safeguards specified below are not followed. Data integrity and availability are improved by adherence safeguards for the storage and use of magnetic media and backups. Assurance of integrity can also be improved by carefully avoiding situations that may subject the stand-alone system to viruses borne by removable media such as diskettes. Software copyrights and licensing are a factor that may affect data availability. Data confidentiality can be compromised if stand-alone systems are easily accessible to unauthorized personnel. Data confidentiality of stand-alone systems is best improved by defining, training for, and adhering to, individual safeguard responsibilities.

2. Security Responsibility and Training

At least one person, or functional group, should be assigned the overall responsibility for maintaining stand-alone LIMS security. The responsible person or group should have the authority and opportunity to contribute to policy decisions regarding the security topics discussed within this section (physical and environmental, magnetic media safeguards, backups, etc.). All LIMS users should be provided with security awareness training.

3. Physical and Environmental Safeguards

Position stand-alone LIMS equipment in rooms with locking doors whenever possible, and lock the doors when the room is not in use. Otherwise, locate equipment away from easily accessible areas and install a locking device (pad or hardened cables) to the extent possible. Use a standard keyed system cabinet lock. Place equipment and peripherals on stable and secure platforms away from objects that could fall on them.

Store all portable LIMS in a locked cabinet when not in use. Ensure that at least one individual within the organization is responsible for tracking the location of portables on a regular basis, and institute logging procedures that include the release and return dates for authorized users.

Install surge protection devices to protect against electrical power surges. Do not install the electronic equipment, especially personal computers, in direct sunlight or in a location with extremes of hot and cold temperatures (less than 50 degrees Fahrenheit or greater than 100 degrees Fahrenheit). Do not leave a portable in a parked car, which would also subject it to temperature extremes.

Do not eat, drink, or smoke in the immediate vicinity of LIMS equipment and media. Install, as far as practical, away from overhead water pipes or sprinkler heads. Install and use humidifiers when the ambient air is extremely dry.

4. Magnetic Media Safeguards

Keep all magnetic media in a secure area away from electrical devices and, especially, magnets. Magnets can be found in magnetic paper clip holders, building passes and credit cards with magnetized strips, PC hard drive units, speakers, and telephones. Do not flex diskettes, touch their surfaces, or write on them directly with a pencil or hard-tipped pen. Store them in disk file containers as soon as they are removed from equipment. Store cartridge tapes and removable disk cartridges in their original containers. Backup all files on a fixed disk at regular intervals.

VI. Minimum Safeguards by Asset: Stand-alone, Networked, and Data Center Computing

5. Backups

Routine backup procedures should be established to ensure availability of the LIMS data. Stand-alone personal computers are often the least likely to be backed up. While a precise set of criteria for determining how often to make these backups cannot be provided, frequency of modifications to data files, cumulative development time, and the relative importance of the data are key factors to consider. Many organizations perform backups at least once a week.

The appropriate backup media can vary and may include diskettes, cartridge tapes, removable disk cartridges, or remote hosts such as minicomputers.

In all cases, the resultant backup media should be tested at a frequency adequate to ensure that backup procedures are working correctly. More than one person within an organization should have the knowledge required to perform backups to avoid backup schedule interruptions due to personal leave or termination.

6. Software Copyrights and Licenses

Commercial software is frequently subject to copyright laws and accompanied by a licensing agreement that specifies copying regulations. A copyright generally means that any duplicating, selling, or other distribution of the software for other than backup use by the lawful user(s) is unlawful. Many of these copyrighted software packages may affect data availability. Some software applications cease to function upon expiration of the license; previous data access provided by the software may be lost. Licenses are usually available for single systems or for entire sites. LIMS management should be vigilant to eliminate unlicensed software and maintain current licenses for stand-alone personal computers. Supervisory personnel should educate LIMS users on the importance of adhering to copyright law.

VI. Minimum Safeguards by Asset: Stand-alone, Networked, and Data Center Computing

Registering all copies of commercial software with the vendor can result in significant cost savings in free user assistance, reduced price software upgrades, or free replacement if the software is lost, stolen, or damaged.

7. Viruses

A computer virus is an extra program hidden within an apparently normal program or software package. The normal program or software is referred to as the virus "host" or "Trojan Horse." Some viruses are relatively harmless and only flash a message on the monitor before destroying themselves. Others are truly malicious and modify or destroy programs and data. One means to avoid viruses on stand-alone LIMS is to purchase only commercially-produced software (although commercial software is not immune to viruses, either), and to run a virus scanning program on every diskette before reading the diskette or copying files from it. To combat viruses, a number of specialized programs or software "vaccines" have been developed. Some are available at low cost, or through the operating system vendor. New software should also be tested for viruses on stand-alone computers. A relevant publication, NIST Special Publication 500-166, *Computer Viruses and Related Threats: A Management Guide* (August 1989), should be consulted.

B. Networked Computing

1. Meeting the Objectives of Data Integrity, Availability, and Confidentiality

Networked computing is highly vulnerable to security threats, because of its use by large numbers of individuals throughout an organization or, in the case of the Internet, the world. Due to their predominance on WANs such as the Internet, workstations, minicomputers, and even mainframes historically were the prime targets of viruses and hackers. The lack of security and

VI. Minimum Safeguards by Asset: Stand-alone, Networked, and Data Center Computing

auditing software available for personal computer operating systems makes these systems singularly ill-equipped to deal with sophisticated threats that can exist on local or wide-area networks.

Networked LIMS computing is subject to the same physical and environmental threats as stand-alone or data center LIMS computing. Data integrity, availability, and confidentiality of networked systems may be compromised if the physical and environmental safeguards specified below are not followed. Data integrity, availability, and confidentiality can be improved by adherence to safeguards regarding the treatment of magnetic media, backups, and by implementing safeguards to protect against viruses borne by a local or wide-area network.

Networked computing should implement the minimum operating system and application safeguards described below. Networked personal computers, workstations, file servers, print servers, database servers, and minicomputers that operate outside the confines of a data center should adhere to the minimum safeguards described in **A. Stand-alone Computing**. Networked data center computers should adhere to the operating system and application safeguards (below) in addition to the safeguards described in **C. Data Center Computing.**

2. Operating System and Application Security Safeguards

Minimum application security safeguards are implemented largely according to the sensitivity of data stored within a LIMS system. The presence of sensitive data on a LIMS necessitates more stringent measures than those described below. For LIMS that process sensitive data on a multi-user system, laboratory management should research the cited references (see Notes at end of Discussion) for details regarding application security safeguards for sensitive data. Safeguards can be applied to the operating system, commercial and internally developed software programs running on the multi-user system, and data stored on the system.

Minimum operating system safeguards on a networked LIMS include:

- implementation of individual username and password management programs
- file access safeguards maintained by the data or file owner
- assignment of operating system privileges only to systems management personnel
- monitoring of system events such as logon failures or break-in attempts
- emergency, backup, disaster recovery, and contingency plans
- application-specific safeguards

Usernames should be assigned and maintained by the individual or group responsible for maintaining the LIMS. Usernames should be provided only to individuals, whenever possible. If group IDs are necessary, they should be assigned limited privileges and revoked as soon as feasible.

Password maintenance is ultimately the responsibility of the individual LIMS user, but basic syntax rules are necessary, especially where the LIMS is susceptible to password cracking schemes used by hackers through dial-up modems, LANs, or WANs. Passwords should be:

1) a minimum of six characters in length,
2) consist of numerals and alphabetic characters,
3) changed at least once every 90 days, and
4) should avoid common names, words found in a dictionary, or repetitive character sequences.

File access safeguards should be implemented to restrict the use of LIMS data to only users with authorized access. Group or public file access should

VI. Minimum Safeguards by Asset: Stand-alone, Networked, and Data Center Computing

be discouraged. Assigning write or delete privileges to increasing numbers of LIMS users effectively cancels several safeguards because of the increased opportunity to modify the LIMS data.

Operating system privileges should be assigned very sparingly, and only to those individuals working directly with the operating systems. Assigning system privileges to the general user population causes a wide array of security problems.

Whenever possible, a system for monitoring events such as logon failures or break-in attempts should be implemented. After three failed logon attempts, the account should be automatically disabled. Event logs should be reviewed on a frequent, and regular, basis. Most minicomputer and mainframe operating systems provide system event logging at no extra cost.

System and data backups (see C.4 **Data Center Backups**) are the keystone of emergency, backup, disaster recovery, and contingency plans. A well thought-out and tested plan is a significant safeguard against unforeseen natural or man-made disasters. The plan includes notification procedures, recovery operations, LIMS interim processing, and restoration planning.

Application-specific safeguards include the use of application-specific usernames and passwords. The commercial database market includes numerous database products that provide additional internal security safeguards, including application-specific usernames and passwords. Most of these also have complex security protection schemes that grant and revoke database privileges, read/write access, and group protections. In many ways, these application protections are as sophisticated as their operating system counterparts, and should be used to augment operating system safeguards.

VI. Minimum Safeguards by Asset: Stand-alone, Networked, and Data Center Computing

C. Data Center Computing

1. Meeting the Objectives of Data Integrity, Availability, and Confidentiality

Because data centers usually involve large, centralized LIMS, such as mainframe computers, that also participate in local and wide area networks, the security measures that apply to networked LIMS should apply to data center computers. Security training of all data center computer users is essential for maintaining data integrity, availability, and confidentiality. Security awareness is important because enormous amounts of potentially sensitive information are concentrated in one area and, frequently, among a small number of large computer systems. Data availability can be compromised by failure to adhere to physical and environmental safeguards. Data integrity and availability are improved by backup and change control practices.

2. Security Responsibility and Training

At least one person, or functional group, should be assigned the overall responsibility for maintaining LIMS security. A responsible person (see **8.1.6**) or group should have the authority and opportunity to contribute to policy decisions regarding the security topics discussed within this section (physical and environmental, safeguards, backups, etc.). All LIMS data center users should be provided with security awareness training. Because most data centers include a complex local area network, and involve interactive logons, users should be provided with training in password maintenance and file protections.

VI. Minimum Safeguards by Asset: Stand-alone, Networked, and Data Center Computing

3. Physical and Environmental Safeguards

LIMS data center management should strive to locate the data center away from the ground floor, frequently traveled or easily accessible areas, and potential sources of explosions (e.g., boiler rooms, hot water heaters). When choosing a site, take advantage of existing physical security. Limit the number of doors and entrances to those needed for safe and efficient operations. Install and use locks on all windows and doors.

When possible, locate master power switches near emergency exits. The switch should cut off all power to the LIMS and, if possible, should also turn off the air conditioning system if it is not designed to filter out smoke.

Use fire extinguishers designed to avoid damage to computer equipment, and mount them in visible, accessible areas. Install smoke and heat detectors. Avoid installing the computer room underneath water pipes or steam pipes. If this is not possible, use water sensors to detect water seepage. If practical, store waterproof plastic in a visible, accessible location so that it can be draped over equipment in an emergency.

Prohibit eating, drinking, and smoking in the computer room. To reduce dust, avoid coat racks, throw rugs, venetian blinds, and other furnishings that collect dust and static electricity. Vacuum carpeted areas frequently. Control static electrical charges by using anti-static carpeting or sprays. To reduce fire hazards, never store flammable materials in the computer room. Keep on-site paper supplies to a minimum.

4. Backups

A precise set of criteria for determining how often to make backups cannot be provided. Frequency of modifications to data files, cumulative development time, and mission criticality of on-line data are key factors to consider.

VI. Minimum Safeguards by Asset: Stand-alone, Networked, and Data Center Computing

Backups are a key element in disaster recovery plans, and should occur on a regular and published schedule. The resultant backup media and recovery procedures should be tested frequently to ensure that backup procedures are working correctly. The appropriate backup media can vary and can include diskettes, cartridge tapes, removable disk cartridges, or remote hosts such as minicomputers. LAN server backups should occur on a regular and published schedule. More than one person within an organization should have the knowledge required to perform backups to avoid backup schedule interruptions due to personal leave or termination.

5. Change Control

Threats to integrity, availability, and confidentiality are introduced through unauthorized change to hardware or software. To help achieve effective change control, laboratory management shall maintain accurate records of hardware and software inventories, configurations, and locations (see **8.5.4** and **8.7.2**); and shall comply with the terms of software licensing agreements. Prescribe a standardized, formalized method of introducing changes to both software and hardware (see **8.5.1.3** and **8.7.2**). To ensure data availability, prepare a contingency plan, or other procedure to revert to a previous version of the software, in the event that the change does not work as intended.

SPECIAL CONSIDERATIONS

EPA Information Security Manual is currently being revised and is in internal review.

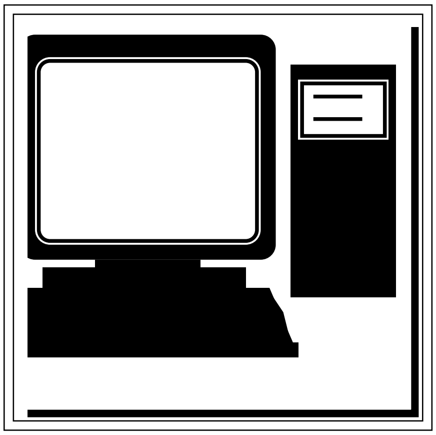
Notes…

Federal statues that set the criteria for sensitive data include *Computer Security Act of 1987, OMB Circular A-130, OMB Bulletin No. 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information" (July 9, 1990), EPA Information Security Manual (December 1989)*, and *EPA Operations and Maintenance Manual (April 1990)*.

For additional information on computer viruses, see: *NIST Special Publication 500-166, Computer Viruses and Related Threats: A Management Guide (August 1989).*

For more information on security, see NIST computer security standards and guidance, "Computer Security Clearinghouse," at this Internet World Wide Web address: http://csrc.ncsl.nist.gov/

See Chapter 1, **11. SOURCES** for addresses and ordering information.



8.7
HARDWARE

8.7 Hardware

1) Design

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall ensure that LIMS hardware and communications components are:

1) of adequate design and capacity, and a description is documented and maintained.

EXPLANATION

LIMS hardware and communications components shall be configured to meet user performance requirements. The LIMS shall be designed to ensure LRD integrity, availability, and confidentiality (see **8.6**). Storage capacity and response times must meet user needs. A system configuration description shall be documented and maintained, and include descriptions of all hardware and communication components. Documentation describing the LIMS hardware, including installation specifications, functions, and usage, should be current and available to laboratory personnel responsible for use and maintenance.

DISCUSSION

Proper performance of the LIMS hardware and communications components is often dependent on the capacity of the system and the appropriate configuration of the components. Periodic review of LIMS design may be valuable in assessing the need for modifications to improve productivity, reduce risk of malfunction, and improve LRD integrity, availability, and confidentiality (see **8.6** Discussion).

Maintaining a current description of the LIMS hardware and communications components assists maintenance personnel in tracking problems with the equipment and in repair and replacement, and assists LIMS personnel in assessing current functionality and future needs.

Notes…

8.7 Hardware

2) Installation and Operation

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall ensure that LIMS hardware and communications components are:

2) installed and operated in accordance with manufacturer's recommendations and, at installation, undergo acceptance testing that conforms to acceptance criteria. SOPs shall be established and maintained to define the acceptance criteria, testing, documentation, and approval required for changes to LIMS hardware and communications components.

EXPLANATION

Installation shall be according to manufacturer's specifications, unless otherwise documented, and shall be tested in conformance with documented acceptance test criteria before the hardware and/ or communications components are determined to be acceptable for use in the LIMS. The installation site should be planned to facilitate use and maintenance of the hardware and communications components.

The laboratory shall develop SOPs for acceptance criteria, testing, documentation, and final approval of LIMS hardware and communications components installation and changes. The SOPs shall be readily available to all personnel with responsibility for modification or changes to LIMS hardware and communications components.

The SOPs shall require that changes are described and documented. The documentation shall include testing and quality assurance criteria and test results, the authorization approval needed prior to implementation of changes or modifications, and dates of each activity.

DISCUSSION

Evaluating user performance requirements is the first step in LIMS hardware modification or enhancement. New user requirements should be periodically reviewed by laboratory management.

Vendor documentation can be obtained for guidance with installation and initial acceptance testing. Diagnostics provided with equipment and normally indicated in the documentation can demonstrate performance in accordance with specifications. However, additional testing beyond vendor components specifications may be necessary to adequately demonstrate proper functioning of changes to LIMS hardware and communications components prior to their actual usage on the LIMS.

Laboratory management should not risk using inadequately tested equipment to receive, store, or manipulate LRD. Laboratory management should review all testing results and documentation before approving hardware and communications components and returning them to production.

Notes…

8.7 Hardware

3) Maintenance

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall ensure that LIMS hardware and communications components are:

3) adequately tested, inspected, and maintained. SOPs for and documentation of these routine operations shall be maintained. Documentation of non-routine maintenance shall also include a description of the problem, the corrective action, acceptance testing criteria, and the acceptance testing performed to ensure that the LIMS hardware and communications components have been adequately repaired.

EXPLANATION

Periodic maintenance of LIMS hardware and communications components shall be performed and include testing and inspecting. The purpose of these routine maintenance operations is to ensure the integrity of LRD. The frequency of these routine maintenance operations shall be described in the SOPs and shall comply with manufacturer's specifications. SOPs shall be developed to describe the operations and the documentation required.

Documentation of the regularly scheduled LIMS hardware and communications components maintenance operations shall be maintained and include: descriptions of operations performed, the names of persons who conducted them, dates operations were performed, and the results.

All repair of malfunctioning or inoperable LIMS hardware and communications components shall be documented and include: a description of the problem, correction action taken, acceptance testing criteria, and the testing performed to ensure proper performance prior to returning the LIMS hardware and communications components to production.

DISCUSSION

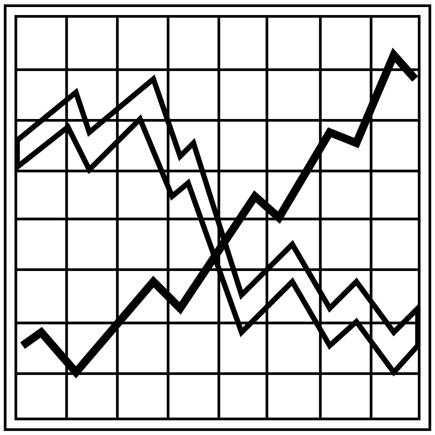
Only personnel with training and experience in testing, inspecting, and maintenance should be authorized to perform these functions. A program of testing, inspecting, and routine maintenance operations should be instituted and designed to assure continued proper operation of the LIMS. The maintenance program and procedures should be determined by the vulnerability of the LIMS.

All maintenance specified in the SOPs, whether performed by in-house personnel or outside contractors, should be included in the documentation. The operations maintenance documentation should be kept with the hardware and communications components for ready access.

SPECIAL CONSIDERATIONS

A “repair log” may be used to document non-routine maintenance performed on the LIMS. It should be easily accessible to the LIMS personnel responsible for updating the log and to the personnel using the LIMS hardware and communications components. This documentation should be retained for as long as needed to support evidence of LRD integrity, or longer if required by other regulations (see 8.9), and should be reviewed on a regular basis by LIMS management. When repairs are performed by the manufacturer’s service representative or other outside personnel, a written report is usually provided. This report can be helpful to document the problem and should be retained. Centralized responsibility for contacting outside service support and maintaining the documentation of service calls may prove beneficial to organization and record keeping. For in-house service, forms may be established to document the required information for the repair log.

Notes…



8.8 COMPREHENSIVE TESTING

8.8 Comprehensive Testing

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall ensure that comprehensive testing of LIMS performance is conducted, at least once every 24 months or more frequently as a result of software (see 8.5.2) or hardware (see 8.7.2) changes or modifications. These tests shall be documented and the documentation shall be retained and available for inspection or audit.

EXPLANATION

In order to ensure ongoing LIMS reliability, performance, and accuracy, comprehensive testing of the LIMS shall be conducted at least once every 24 months.

This testing should also include a complete document review (SOPs; change, security, and training documentation; error logs; problem reports; disaster plans, etc.). Laboratories that change LIMS software or hardware within the 24-month interval shall conduct acceptance testing as required by **8.5.2** and **8.7.2**.

DISCUSSION

A comprehensive testing team can be assembled that may include LIMS users, support personnel, and laboratory management, so that the interests and skills of these individuals can be addressed in the testing process. A test data set can be developed that significantly exercises all important functions of the system. This test data set can then be retained and re-used for future system tests. It may have to be enhanced if new functionality is added to the system. System test protocols and test objectives can be developed and re-used. A checklist can be developed to ensure that all important areas of testing and document review are addressed.

SPECIAL CONSIDERATIONS

Consultation with QAU personnel during comprehensive testing may be advantageous. However, QAU's independence from LIMS staff must be maintained (see **8.3.1**).

Notes…

8.9
RECORDS RETENTION

8.9 Records Retention

Laboratory management shall ensure that retention of LIMS Raw Data, documentation, and records pertaining to the LIMS comply with EPA contract, statute, or regulation; and SOPs for retention are documented, maintained, and managed as described in 8.11.

EXPLANATION

Laboratory management shall ensure that LRD and all LIMS-related data or documentation are retained by the laboratory for the period specified in the EPA contract, regulation, or statute, and that SOPs for retention are documented, maintained, and managed as described in **8.11**.

DISCUSSION

Contract clauses or EPA statutes pertinent to record retention periods can be copied and forwarded to a person designated to manage records retention, who can monitor compliance and disposal or destruction, as appropriate, when retention periods have expired. This individual can be responsible for determining retention periods for any records lacking such information, can ensure that the storage media used is adequate to meet retention requirements, and can institute procedures to copy data stored on magnetic media whose retention capabilities do not meet requirements (see also **8.10.2**).

Notes…

8.10
FACILITIES

8.10 Facilities

1) Environment

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall ensure that:

1) the environmental conditions of the facility housing the LIMS are regulated to protect against LIMS Raw Data loss.

EXPLANATION

The LIMS shall be housed in an environment that allows it to operate correctly. Control systems should be applied to all environmental factors that might affect LRD loss or integrity. At a minimum, LIMS hardware should be installed in accordance with the environmental standards specified by the manufacturer. Control systems (see **8.6 Minimum Safeguards** Discussion) should ensure:

- proper temperature and humidity
- freedom from dust and debris
- adequate power supply and grounding
- protection from power surges and spikes
- fire detection and suppression
- water detection and suppression
- protection from natural disasters

DISCUSSION

The provisions to regulate environmental conditions are discussed in greater detail in **8.6 Minimum Safeguards by Asset**. The provisions are summarized here to emphasize their importance.

Climate control systems

LIMS hardware should be installed according to manufacturer's climate specifications. Heating, ventilation, and air conditioning dedicated to the computer room or other location where hardware is installed should be considered. Monitoring or control devices for temperature and humidity are usually installed. Backup climate control systems may be worthwhile if time is critical.

Power provision

Power supplies should comply with the computer hardware manufacturer specifications. It may be appropriate to install backup power supply systems where electrical outage would cause critical loss or where electrical outage frequently occurs.

Fire and water control systems

Detection and suppression devices for fire and water should be considered. A sprinkler system may be suitable for some facilities, but a CO_2 system may be suitable for others.

Protection against natural disasters

The facility should be designed and protected according to geographic conditions. Where earthquakes are likely, housing should be examined for potential destruction of the LIMS and its data. Where tornadoes are likely, consideration should be given to locating computer equipment on lower levels of the facility. Where flooding is likely, consideration should be given to locating computer equipment on upper levels of the facility.

Operating procedures

Routing procedures for checking and maintaining detection and suppression devices will ensure that devices are in working order. Additional procedures may be established that describe how to operate the LIMS during emergency situations (for example, powering down).

Notes…

8.10 Facilities

2) LIMS Raw Data Storage

When LIMS Raw Data are collected, analyzed, processed, or maintained, laboratory management shall ensure that:

2) environmentally adequate storage capability for retention of LIMS Raw Data, LIMS Raw Data storage media, documentation, and records pertaining to the LIMS are provided.

EXPLANATION

Environmentally satisfactory and adequate storage space shall be available for LRD, LRD storage media, and documentation and records (which may be retained in hard copy format or on magnetic or optical media).

DISCUSSION

Operations personnel should maintain an adequate supply of required tapes, magnetic disks, and/or optical disks and ensure that storage space is sufficient to meet current and anticipated needs. Storage facilities for retention of LRD in hard copy or electronic format must be available and environmentally satisfactory for the LRD storage media. At a minimum, the storage facility should have a heating, ventilation, and air conditioning system to control temperature and humidity that will meet the storage condition specifications of the specific media.

Offsite storage is recommended for backups. Backups can be cycled through the offsite location. For example, the most recent backup may be kept on the premises while the previous backup is kept offsite. This procedure retains the most recent version onsite for convenience while securing another version offsite for use in the event of disaster. Offsite storage facilities must have the same environmental control and security systems required of onsite storage facilities. In addition, fire and water control systems and protection against natural disasters should be considered as discussed in **8.10.1**.

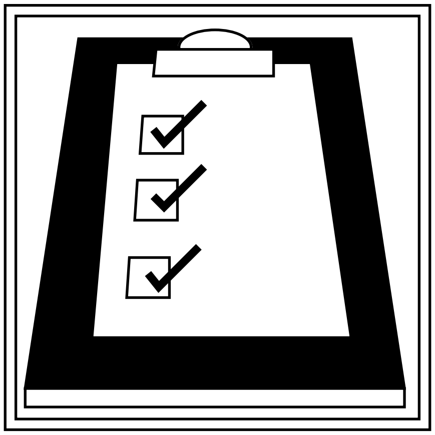
SPECIAL CONSIDERATIONS

National Bureau of Standards Special Publication 500-101, *Care and Handling of Computer Magnetic Storage Media* provides guidelines for appropriate protective measures and factors for evaluating exposure for the storage of electronic information. This publication provides guidelines for performing automated data processing risk analysis, which includes the condition of the storage facility.

Notes…

For additional guidance, see: U.S. Department of Commerce National Bureau of Standards (NBS) Special Publication 500-101, *Care and Handling of Computer Magnetic Storage Media*, June 1983.

See Chapter 1, **11. Sources** for addresses and ordering information.



8.11 STANDARD OPERATING PROCEDURES

8.11 Standard Operating Procedures

1) Availability

Laboratory management shall ensure that:

1) **SOPs include, but are not limited to, those specified in 8.4.1, 8.4.4, 8.4.5, 8.5.1.1** through **8.5.1.5, 8.7.2, 8.7.3, and 8.9. Each current SOP shall be readily available where the procedure is performed.**

EXPLANATION

SOPS shall be established and maintained for, but not limited to:

- LIMS Raw Data and LIMS Raw Data storage media identification and documentation (**8.4.1**)
- LRD verification (**8.4.4**)
- LRD changes (**8.4.5**)
- Software development methodologies (**8.5.1.1**)
- Software testing and quality assurance (**8.5.1.2**)
- Software change control (**8.5.1.3**)
- Software version control (**8.5.1.4**)
- Software historical file (**8.5.1.5**)
- Hardware changes (**8.7.2**)
- Hardware testing, inspection, and maintenance (**8.7.3**)
- Records retention (**8.9**)

Each current SOP or copy shall be placed in a location that allows LIMS staff who are responsible for performing the procedure easy and immediate access to it.

This proximity of the SOP to the LIMS personnel provides assurance that the approved procedures are accessible. When changes to an SOP are approved, the new version of the SOP shall be provided to the LIMS staff responsible for following the procedure. The previous version shall be removed from the work area and retired according to **8.11.4**. If multiple staff perform the same procedure in different locations, copies of SOPs shall be available in each location. When LIMS staff changes occur, the replacement staff shall be provided with the SOPs.

DISCUSSION

If multiple copies of SOPs exist, then maintaining the originals in a secure location is recommended (see also **8.11.4**). Laboratory management should ensure that all copies of SOPs are kept current and that copies of retired versions of SOPs are removed from circulation.

Notes…

8.11 Standard Operating Procedures

2) Periodic Review

Laboratory management shall ensure that:

2) SOPs are periodically reviewed at a frequency adequate to ensure that they accurately describe the current procedures.

EXPLANATION

It is laboratory management's responsibility to establish and ensure that current SOPs accurately document current LIMS activities. Laboratory management shall ensure that SOPs are reviewed at a frequency adequate to assure the integrity of LIMS Raw Data.

DISCUSSION

The adequacy of SOPs is laboratory management's responsibility; therefore, direct and frequent communication with LIMS staff is implied. The QAU can assist laboratory management in assuring that the SOPs are current by reporting any differences between an SOP and the corresponding LIMS activity. Inspections, and SOP review can be used by the QAU for this purpose (see **8.3.3** and **8.3.4**).

SPECIAL CONSIDERATIONS

Changes in critical LIMS support staff or major LIMS hardware and software changes are important milestones for the QAU or laboratory management to review the accuracy of SOPs with respect to LIMS activities.

Notes…

8.11 Standard Operating Procedures

3) Authorization and Change

Laboratory management shall ensure that:

3) SOPs are authorized and changed in accordance with 8.1.5.

EXPLANATION

SOPs set forth and document the methods that assure laboratory management of the integrity of LIMS Raw Data. Thus, laboratory management shall authorize each SOP and any subsequent changes to the SOP. The previous version or copy of the SOP shall be retained according to **8.11.4**.

DISCUSSION

Authorization of SOPs and all changes to SOPs by laboratory management ensures that procedures are consistent with all laboratory policies and requirements. It allows management to exercise control of the activities of the laboratory operations. This also communicates to the LIMS staff the importance of compliance with the approved SOPs. See **8.1.5** for further discussion.

Notes…

8.11 Standard Operating Procedures

4) Historical File

Laboratory management shall ensure that:

4) a historical file of SOPs is maintained.

EXPLANATION

All versions of SOPs, including retired SOPs, shall be maintained in historical files. The effective dates of each SOP shall be indicated. Retired SOPs shall be retained in accordance with **8.9**.

DISCUSSION

A centralized historical file or files of SOPs may be an advantage because of the assurance that the file is properly maintained and effectively managed. However, larger LIMS operations may appropriately maintain separate historical files of SOPs critical to LIMS Raw Data integrity. Depending on the LIMS operations, multiple historical files may be preferable over a single file for all SOPs.

SPECIAL CONSIDERATIONS

Historical files of SOPs may be stored on magnetic media. However, storage conditions must be consistent with **8.10.2** so that the SOPs remain available over time.

Notes…

SOURCES

Page 1 of 2

Copies of the Federal information resources management publications referenced in the GALP can be ordered via mail, telephone, or the Internet.

Computer Security Act of 1987

This is a Federal regulation and should be available in local public libraries.

The Internet World Wide Web address is:

http://www.first.org/secplcy/csa_87.txt

Office of Management and Budget (OMB) publications

Office of Management and Budget
Assistant Director of Administration
OMB Publications
725 17th Street, NW
Washington, D.C. 20503

telephone: (202) 395-7332 (then press 2)

The Internet addresses for OMB publications are:

World Wide Web:	http://www2.infoseek.com/Titles?qt=OMB
Gopher:	gopher://pula.financenet.gov:70/11/docs/central/omb

SOURCES

Page 2 of 2

Copies of the Federal information resources management publications referenced in the GALP can be ordered via mail, telephone, or the Internet.

EPA publications

U.S. Environmental Protection Agency
OARM/FMSD
Publication Distribution Section
Mailcode 3204
401 M St., SW
Washington, D.C. 20460

telephone: (202) 260-5797

For OIRM Automated Laboratory Standards publications, contact:

Rick Johnson	Voice:	(919) 541-1132
EPA (MD-34)	Fax:	(919) 541-1383
RTP, NC 27711	Internet:	johnson.rick@epamail.epa.gov

The Internet addresses for EPA IRM documents are:

World Wide Web:	http://www.epa.gov/docs/IRMPolicy.html
Gopher:	gopher://gopher.epa.gov:70/11/Initiatives/IRM.Policy

National Institute of Standards and Technology (NIST) and National Bureau of Standards (NBS) publications

National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161
(703) 487-4650

The Internet World Wide Web address for NIST is:
http://www.ncsl.nist.gov

The Internet World Wide Web address for FIPS Publications is:
http://www.ncsl.nist.gov/fips/

Contents

Chapter 2 — Implementation Assistance

Implementation Listing

T section is divided into 11 sections which discuss each of the 41 GALP provisions, 8.1 through 8.11 (numbered with reference to Chapter 1). It is intended to provide laboratory management and personnel with additional information to assist in implementing each specific GALP. While atypical situations may require further recommendations and procedures, the explanatory comments, discussion, and special considerations are provided to laboratories to implement the GALP provisions successfully and cost-effectively.

Contents

Contents