Installation Qualification of IBM Systems and Storage for FDA Regulated Companies

Demonstrates how the infrastructure of IBM TotalStorage, eServer pSeries, LTO, and SAN can facilitate regulatory compliance

Uses a sample method to help meet the qualification requirements of FDA 21 CFR Part 11

Shows sample documentation to help meet compliance standards

James R. Bradburn
William F. Drury
Mark Steele

Redbooks

ibm.com/redbooks

International Technical Support Organization

Installation Qualification of IBM Systems and Storage for FDA Regulated Companies

September 2003

SG24-6630-00

Note: Before using this information and the product it supports, read the information in “Notices” on page xi.

First Edition (September 2003)

Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®
BladeCenter™
ChipKill™
Enterprise Storage Server®
eserver™
eserver™
eServer™
FlashCopy®
IBM®
ibm.com®
OS/390®
pSeries™
Redbooks™
Redbooks (logo) ™
RS/6000®
S/390®
Tivoli®
TotalStorage™
xSeries®
z/OS®
zSeries®

The following terms are trademarks of other companies:

Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Preface

This IBM® Redbook contains an Installation Qualification (IQ) executed at a pharmaceutical manufacturer with the help of IBM. The customer purchased IBM equipment to support a major new computerized system that came within the regulatory scope of US 21CFR11. This IQ was performed as one part of an overall systems validation, and a separate system requirements document contained the technical infrastructure requirements, including equipment. The system requirements document is not included in this publication, although it is referenced in this IQ.

The following IBM equipment was installed and qualified by the customer for this project:

- IBM @server™ pSeries™ 670 Server running AIX®, HACMP, and LPARs
- IBM TotalStorage™ Enterprise Storage Server®
- IBM LTO Tape Library
- IBM McData SAN Switches

The IQ was created from drafts of templates and procedures created by an IBM Business Consulting Services Consultant. Adjustments were made to help fit the company's 1) local validation policy, 2) overall system validation plan, and 3) qualification procedures that existed. The test scripts were written by an IBM Business Partner under contract from IBM Life Sciences. In creating this IBM Redbook, the company name and proprietary materials have been removed from the IQ.

US 21CFR11 requires that computerized systems that are within the scope of the regulation be validated. Validation of a computerized system requires that the technical infrastructure be qualified as meeting the system requirements. Specifically, Installation Qualification of the technical infrastructure covers the hardware and related equipment supporting the computer application (such as servers, data storage, backup devices, and network communications devices). Depending on the nature of the system, workstations, including their peripherals and printers, may also be within the scope of the equipment qualification.

Installation Qualification of the equipment verifies:

- The equipment meets the specifications set for it in approved technical design documents.
- The equipment has been properly installed in the required environment.
- The equipment is connected, communicating, and functioning normally.
- The required support procedures are in place to manage the equipment to assure continued operation.

In summary, to accomplish the Installation Qualification, this company created a "Qualification Plan" for its "Installation Qualification" or IQ. This plan is part of an overall computerized system validation plan or protocol for equipment acquired to support a new application, but this sort of plan could also be used as a stand-alone qualification for shared infrastructure. The structure and details of the IQ can vary by company, but robust qualifications will always provide documented evidence that the defined equipment infrastructure meets its specifications and can operate in an acceptably controlled state.

Assumptions and other key points to consider

As already discussed, this IBM Redbook provides an example of one company’s qualification of IBM equipment, performed in early 2003. In reading this IQ, please consider:

- This company is “U.S. based,” and only Title 21 regulations apply. Other firms may have a different or wider scope of regulatory concerns.
- All format, content, and order of the information presented in the IBM Redbook is based on 1) the company’s interpretation of applicable regulations, 2) technical definitions, 3) IT operating procedures or guidelines, 4) strategy or methodology for Installation Qualification activities.
- Installation Qualification of IBM systems and storage components used as examples in this IBM Redbook includes only the IQ activities plus the test scripts for the Operational Qualification (OQ) for an initial, single-site installation at the company’s data center. The qualification activities identified in this IBM Redbook were a component of the company’s requirements for a new computer system validation project.
- Definition of terms and their use in this book are defined by the company to be:
  - Infrastructure: Technology components of a computerized system that support the end-user application, including hardware (servers, storage, backup devices, workstations), operating systems, network, databases, and system utilities.
  - Validation: Documented evidence that provides a high degree of assurance that a computerized system will consistently meet its predetermined specifications and quality attributes. It is an overall process for system-wide compliance with US 21CFR11, including multiple qualification phases.
  - Qualification: Individual validation phase to verify components of total system.
  - Verification: A procedure of review, analysis, and testing to discover errors, determine functionality, and ensure a quality system.
  - Installation Qualification (IQ): Individual validation phase establishing confidence that system infrastructure is compliant with appropriate codes and approved design intentions, and that manufacturer's recommendations are suitably considered.
  - Operational Qualification (OQ): Individual validation phase establishing confidence that the computerized system is capable of consistently operating within established limits and tolerances.
  - Performance Qualification (PQ): Individual validation phase establishing confidence through appropriate testing that the computerized system operating in a production environment meets all release requirements for functionality.
  - Qualification Plan: Description of the activities anticipated to complete a qualification process (any one of the three qualification phases, IQ, OQ, or PQ).
  - Verification or Verification Process: Qualification, meaning one of IQ, OQ, or PQ.
  - User Acceptance: Customer final approval of documentation package for individual validation phase (see the detailed acceptance criteria in 1.3, “Acceptance criteria” on page 7).
- Because this installation was hosted in a company-site data center with multiple regulated systems, standard operating procedures were already in effect for:
  - Configuration and change control
  - Retesting and regression testing
  - Staff training (on procedures)
  - Physical security

  - Facilities management including utility support
  - Quality management, internal audits
  - External (regulator) inspections
  - Problem reporting, corrective action
  - Data Center procedure management, records retention
- This publication includes, for reference purposes, copies of documents published by the U.S. Food and Drug Administration (FDA) in separate appendixes. These were not part of the actual Qualification package, but are included for the reader's information. Because FDA publications do change over time, readers should access the FDA Web site for the latest materials and guidance documents (http://www.fda.gov).

The team that wrote this redbook

This redbook was produced by a team of IBM consultants and an IBM Business Partner.

James R. Bradburn is a Principal Consultant in IBM Business Consulting Services (BCS). He has over 28 years of involvement in pharmaceutical and medical device manufacturing, including plant operations and production management. He has focused for the past 15 years on information technology supporting quality functions and regulatory compliance. He is a member of the Life Sciences Regulatory Compliance team, which is focused on FDA and EU regulations affecting pharmaceutical and medical device manufacturers. He specializes in Title 21 regulations that impact production and quality systems, including those that relate to computer systems. He has also designed, developed, and implemented numerous system applications for drug/device manufacturing operations, including Electronic Document Management, Manufacturing Execution/Electronic Batch Records, Training Management, Corrective Action, Inventory Management, and Cost Accounting systems. He has been a frequent speaker on manufacturing systems, 21CFR11 compliance, and computer validation at industry conferences and seminars for the past 10 years.

William F. Drury, IBM Life Science Services, Clinical and Regulatory Practices. Mr. Drury occupies a broad position at IBM, involved in both clinical and regulatory practices in a strategy, sales, and delivery capacity for internal and external clients. Mr. Drury has developed, streamlined, and taught the operating procedures for a broad range of research-oriented businesses, and has been a key resource involved in the evaluation and re-engineering of research practices at a wide variety of clients, including a major agricultural chemicals firm, a leading teaching hospital, and at some of the world's largest pharmaceutical and biotech companies. Mr. Drury has been an active participant in the regulatory community, from leading the compliance practice at a major consulting firm to presenting frequently and providing expert opinion to various publications. Mr. Drury has also worked as a specialist in branding and marketing for a variety of companies, provided independent consulting for the National Federation of Parents in their peer-education program, created and directed a successful illicit drug and social education program for underprivileged elementary school students, and has entrepreneurial experience running his own business. Mr. Drury was appointed by the President of the United States to the Selective Services Board, and serves on the Advisory Board of Clarix, LLC. Mr. Drury graduated from The University of Texas in Austin, Texas, with a BA in Psychology and Sociology.

Mark Steele is a Senior System Architect at Direct Systems Support (http://www.directsys.com), a California-based IBM Premier Business Partner. He has 13 years of UNIX experience, of which 10 years are specific to AIX. He has specialized in AIX, TSM, HACMP, and networking. He is Cisco certified and holds numerous IBM product Certifications, including the Certified Advanced Technical Expert certification in AIX.

Thanks to the following people for their contributions to this project:

Jason Chu
IBM Business Consulting Services, San Francisco

James R. Darrah
IBM Life Sciences Storage Systems Technical Support

F. Brent Kranendonk
IBM Life Sciences Storage Systems

Robert F. Jacobs
IBM Life Sciences Clinical and Regulatory Support

Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you'll develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our Redbooks™ to be as helpful as possible. Send us your comments about this or other Redbooks in one of the following ways:

- Use the online **Contact us** review redbook form found at:

  ibm.com/redbooks

- Send your comments in an Internet note to:

  redbook@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. JN9B Building 003 Internal Zip 2834
  11400 Burnet Road
  Austin, Texas 78758-3493

Qualification Plan

Document	Qualification Plan
System ID number	[System ID]
Protocol number	[Protocol #]
Version number	1.0 DRAFT
Date of issue	[Date]

Customer address

Document approval

Prepared by: ____ ______________

[Name] Date
[Title]

Reviewed by: ____ _______________

[Name] Date
[Title]

Approved by:____ _______________

[Name] Date
[Title]

Change history

Version	Effective date	Reason for change or changes
1.0		Original document

Part 1

Qualification Plan information

The Qualification Plan contains the following chapters:

- Chapter 1, “Introduction”
- Chapter 2, “Infrastructure description”
- Chapter 3, “Installation qualification preparation”
- Chapter 4, “Risk assessment”
- Chapter 5, “Testing protocol”
- Chapter 6, “Equipment operations and support procedures”
- Chapter 7, “Operations team training”
- Chapter 8, “Regulatory inspection preparation”
- Chapter 9, “Qualification Report and infrastructure acceptance”

1

Introduction

The Technical Infrastructure has several major categories of components:

Hardware Computer equipment, including workstations with input devices and CRTs, servers, data storage devices, output devices, such as printers and data backup, communications equipment, and related connection materials (cables, routers, and hubs).

Operating Systems Software that instructs workstations and servers on basic, “infrastructure level” operations.

Database Software that manages data used to support an application or applications.

General Utility Software that is used to monitor and manage the workstation, servers, output, and storage devices.

In order for system applications to operate as described in their applicable specifications, the components that make up the technical infrastructure must meet the system design requirements, and must be completely and properly installed in the required environment.

The Installation Qualification (IQ) is a portion of the overall system validation process, and its function is to verify that the infrastructure meets its acceptance criteria, and that it is ready for the installation and/or testing of the system application. This package contains a supporting set of quality materials supporting an infrastructure Installation Qualification, including:

- Protocol
- Procedures
- Training materials
- Test scripts

The purpose of this Qualification Plan is to determine all of the steps required to conduct an IQ, and to provide the necessary procedures and materials to execute the IQ protocol.

1.1 Scope

This IQ Plan applies to the installation and configuration of the technical infrastructure only. The tasks required for qualification of the application software itself, including certain normal or challenge tests that relate to the application's interaction with the technical infrastructure (such as volume or stress testing, or performance testing) are part of the Operational Qualification (OQ) or Performance Qualification (PQ) testing, and, as such, are out-of-scope for the installation activities herein described.

Certain utilities that support the administration, security, or monitoring of the infrastructure are included in the IQ since they are related to infrastructure management. Utilities that support the management of any of the applications that use the infrastructure are out-of-scope of the installation qualification.

Figure 1-1 shows the major portions of the system and its supporting infrastructure. It illustrates the boundary between the Installation Qualification and Operational Qualification.

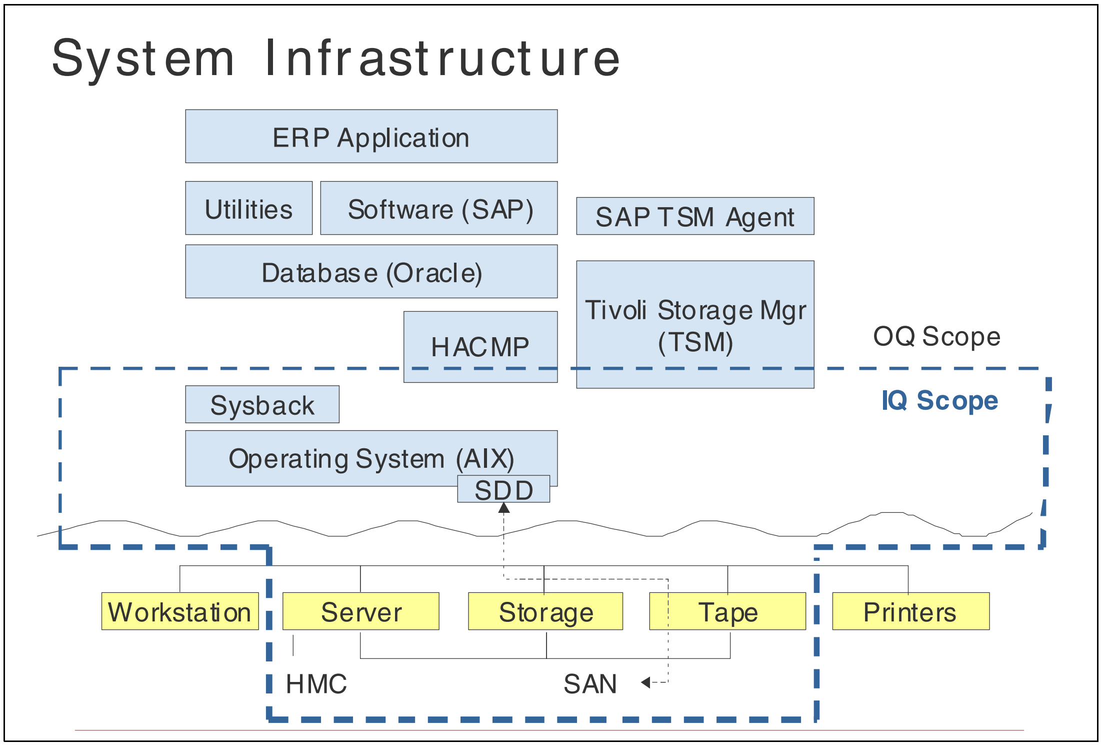

Figure 1-1 System infrastructure

1.2 Structure of the Qualification Package

This package is based upon general practices and standards to satisfy FDA regulations. Appendix S, “Regulation, guidance, and standards cross references” on page 259 provides a mapping of the IQ package to common validation guidance and standards.

This infrastructure installation is based upon the policies, procedures, and practices of the site where the infrastructure is located. This structure of the entire IQ package is:

- **Qualification Plan** (this document)
  This document describes the overall IQ process, and provides basic information that makes up a qualification plan.

- **Procedure Appendixes O, P, Q**
Performance of the tasks described in this plan can be accomplished through the use of individual procedures and templates provided in the Plan appendixes.
- **Protocol Appendix M**
The testing protocol is contained in Appendix M, “Testing protocol” on page 225 of this Plan.
- **Attachments** (as named in the appendixes)

The major sections of the Qualification Plan, and their primary relationships, are found in Figure 1-2.

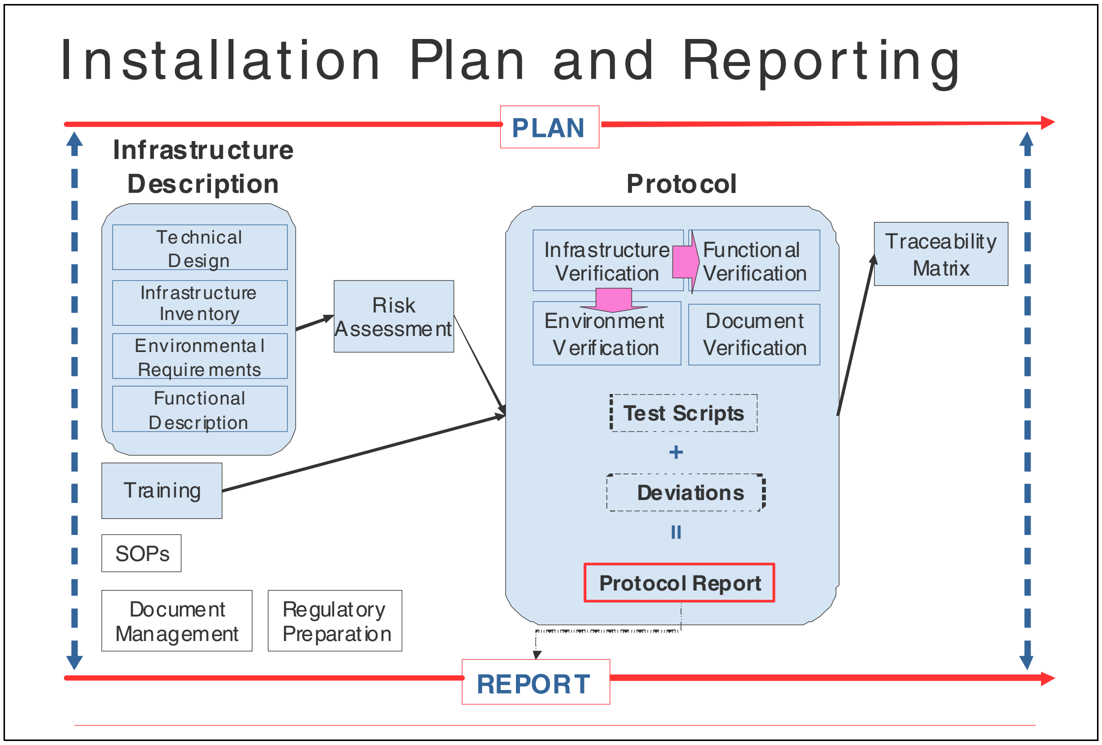

Figure 1-2 Installation Plan and Reporting

1.3 Acceptance criteria

To complete the Infrastructure Qualification, the following tasks must be performed:

1. The Attachments named in the documents will be collected and listed in the Attachments lists.
2. The Qualification Plan (including the remaining Appendixes) will be approved by local management.
3. The tasks described in this plan will be performed and data collected per the Appendixes and/or referenced procedures.
4. Any open issues or deviations resulting from task performance will be identified, managed, and resolved, with appropriate documentation and local management review and approval.

After completion of all the above tasks, a Qualification Report will summarize the results of all activities in this plan. The report will address any open issues from the testing protocol, and any open items or deviations from this plan, with the resolution of such items, and the follow-up actions to be taken, if necessary. The report will provide the conclusion that the Infrastructure meets the criteria of the technical design documents, and will adequately discuss the rationale for allowable deviations to that specification.

When local management approves the Qualification Report, based upon its contents and discussion of the issues, the Infrastructure will have met its acceptance criteria, and is ready for the remaining system validation processes.

1.4 Roles and responsibilities

The roles and responsibilities for executing the tasks defined in this Plan, and its supporting Appendixes or referenced local procedures, are based upon the following structure.

1.4.1 Management roles

Overall management responsibility for the system is based upon three functions, with a representative designated by respective function executives:

- **System Owner**
  The organization that has primary responsibility for the business functions that the system supports, consists of, or represents the system users. The System Owner provides User Requirements and determines the acceptability of the system design and functions. After consulting with Technical Support and Quality functional groups, they are the decision maker on all system issues.
- **Technical Support**
  The organization that is responsible for building and/or installing the system, including both Infrastructure (hardware, O/S, and other “baseline” software) and application software. After implementation, Technical Support maintains the system, and provides support for both Infrastructure and system application functions (Help Desk and Problem Resolution).
- **Quality**
  The organization that is responsible for quality assurance in system design and operation, and for the system compliance to applicable regulations.

Assignment of individuals to represent these functions is based on commitments made by signatories of this plan, particularly Appendix A, “Document master list: Roles and Responsibilities Matrix” on page 35 (for example, Changes in assignments require an update to Appendix A, “Document master list: Roles and Responsibilities Matrix” on page 35).

1.4.2 Qualification and project team roles

The responsibility of executing this plan, including execution of processes detailed in the Appendixes, or referenced local procedures, is assigned to the Validation Leader, and recorded in Appendix A, “Document master list: Roles and Responsibilities Matrix” on page 35. If there is a separate leader for the Installation Qualification rather than the overall Validation Leader, both should be listed in Appendix A, “Document master list: Roles and Responsibilities Matrix” on page 35.

The Validation Leader will make individual assignments for each task described in this Plan, including each document to be created, and those assignments will be recorded in Appendix A, “Document master list: Roles and Responsibilities Matrix” on page 35. Any changes in assignments are also recorded by revision to Appendix A, “Document master list: Roles and Responsibilities Matrix” on page 35, which is reviewed and re-approved by authorized management representatives.

2

Infrastructure description

A primary function of Installation Qualification (IQ) is to verify that the Infrastructure meets the requirements of the system specifications, in that the installed components meet or exceed the Technical Design descriptions of the equipment.

A secondary function of the IQ is to create, after verification testing, an accurate and complete inventory of components that make up the approved Infrastructure. Any additions or replacements can be correctly identified and qualified upon their inclusion so that the complete qualified infrastructure is always on record.

This chapter contains the following topics:

- Technical design documents
- Infrastructure identification/Inventory list
- Equipment Environmental requirements
- Infrastructure (equipment) functional description

2.1 Technical design documents

An attachment to testing protocol will be the approved Technical Design for the Infrastructure components that will be verified during the protocol execution.

2.2 Infrastructure identification/Inventory list

The Technical Design requirements will be expanded into a complete list of the Infrastructure components, which will be individually verified using the protocol. The component list will become the Infrastructure Inventory, and will include the following information:

- Model, Description, and Unique identifier, where possible (may be serial number, asset number, or license number)
- Technical Design Requirements (section or item ID) that is applicable to the component
- Number of items (if there are multiple instances of equipment (groups))

When the Infrastructure Identification verification occurs, the verifier will add the following to the Infrastructure Inventory list:

- Equipment serial number, if any
- Software License number/ID, if applicable
- Location of the equipment, as applicable

The Infrastructure Inventory list will be included within and verified in the testing protocol. The format of the Infrastructure Inventory list is provided in Appendix B, “Infrastructure identification” on page 39.

2.3 Equipment Environmental requirements

Certain equipment may require installation or operation within specific environmental conditions, with power conditioning, safety, or access provisions. Confirmation of the correct equipment for IQ purposes includes verification that the equipment environment meets or exceeds vendor specifications for the proper, reliable operation of the equipment. Appendix C, “Infrastructure environmental requirements” on page 53 is a listing of required vendor environmental specifications.

2.4 Infrastructure (equipment) functional description

For those equipment components that contain automated processes reliant on software or firmware, a description of functions for each component will be provided in an infrastructure (equipment) functions list. The Infrastructure Functional Description List, shown in Appendix D, “Infrastructure functional description” on page 65, is a supplement to the Infrastructure Identification List in Appendix B, “Infrastructure identification” on page 39, and the Functions will be identified based upon items listed in the Infrastructure Identification Lists.

The Function listed for each item will be tested during the IQ testing protocol testing, and the relationship of each Component/Function ID number to the test script will be included in the Trace Matrix.

3

Installation qualification preparation

This Installation Qualification presumes a situation where the System Infrastructure has been installed prior to the Validation process. As a result, the physical installation process is outside the scope of IQ activities beyond verification that the equipment is installed and operational in an acceptable manner. The Installation Qualification herein consists of the Infrastructure verification and testing activities, but not the prior installation tasks.

This chapter contains the following topics:

- Validation team training
- Validation Team training/Qualifications Records
- Signature Log
- Installation manuals and procedures

3.1 Validation team training

The person, or persons, who will complete, approve, and execute the testing protocol must have the training and qualifications that demonstrate their capability to perform their required functions. The Installation Team Training/Qualifications Matrix (Appendix E, “Installation Team Training/Qualifications Matrix” on page 189) identifies assignments for personnel, and states training or qualification requirements for that assignment. The requirements will be based upon anticipated tasks of each assignment, and must include the Appendixes or local procedures that will be used during the assigned tasks.

General training requirements apply to most assignments, and include the following categories.

3.1.1 General Regulatory Training/21CFR11 basics

This training provides general requirements background for FDA-regulated environments, including the following topics:

- The need for/value of a quality system
- The purpose of the quality function
- Defined/approved procedures for tasks
- Procedure compliance and verification
- Qualification of equipment prior to use
- Importance of evidential records of performance
- Inspections and their implications to the business

This training also provides a basic introduction to the requirements of Title 21 Code of Federal Regulations, Part 11 (21CFR11), with emphasis on those areas that affect IT infrastructure. This includes:

- Applicability of the regulation
- Acceptance of electronic records (e-records) based upon rule compliance
- Basic controls requirements (section 11.10 of CFR21 Part11), including:
  - System validation
  - Data protection
  - System access controls/security
  - Education/training requirements (including training evidence documentation)
  - System documentation controls
  - Administrative procedures

The Part 11 specific materials to be used for the training, and the instructor’s guide, are found in Appendix F, “General regulatory and 21CFR11 training” on page 193.

Note: This training course is not meant to be exhaustive. Legal counsel should be consulted in order to help determine compliance.

3.1.2 Good Documentation Practices training

This training covers the rules for recording data and signatures, including controls and methods for entry corrections, making attachments, and page labeling. The materials to be used for this training and an instructor's guide are found in Appendix G, "Good Documentation Practices" on page 201.

3.1.3 Qualification Plan/Protocol training

Persons who perform functions named in the Qualification Plan or the testing protocol must be trained on that document's content prior to performing their assigned tasks. Training may be provided by one of the document approvers. The validation plan, Qualification Plan, or testing protocol documents respectively shall be used as training materials.

3.1.4 Testing Procedures training

Persons who execute the testing scripts must be trained on the Appendixes herein, and any referenced local procedures, that apply to the testing activities. Training can be provided by one of the document approvers or qualified trainers per local policy for local procedures.

3.2 Validation Team training/Qualifications Records

The completion of training requires an associated training record using the format found in Appendix H, "Training/qualifications record" on page 207. For those training requirements met by qualification records, the training form is so noted and the curriculum vita or résumé is attached to the training record. The Trainer will confirm that documented qualifications are adequate background to meet requirements, and will attest to this fact by signing the Training Record with references to attached qualification documentation. Where training records exist at local sites, a copy of the records may be attached to the validation records in lieu of completing a new training record.

3.3 Signature Log

Each person who signs documents as part of this validation plan will make an entry in the Signature log (Appendix J, "Signature log" on page 213), which includes their full legal name, their signature, and initials.

3.4 Installation manuals and procedures

Infrastructure installation manuals (both IBM and third party) will be identified by:

- Document Title
- Document Identification Code/Number, if any
- Publisher name and publish date
- Serial or copy ID, if any

These manuals will be verified in the testing protocol, and their physical locations, or verified Internet locations, including any masters and copies, will be recorded. Location and documentation controls for these manuals will be verified in the testing protocol.

4

Risk assessment

System risk is defined as the potential for failure of the system to operate according to its specifications at some point due to predicted or unforeseen circumstances. Risk may be introduced as a result of the design, implementation, or routine operation of the system, including human interactions or processes.

No system is without risk, as it is impossible to predict every event that will or may occur in the future use of a system. However, an evaluation of the sources of risk, and consideration of features or operational controls that mitigate risks, is an essential part of system design, implementation, and operations.

An assessment of the system risk is based upon the system infrastructure. These risks are matched to the system features and/or procedural controls that mitigate those risks, and then tested. The risk mitigations then can be verified during system testing to assure their effectiveness.

The purpose of the IQ Risk Assessment is to provide a verifiable assurance that system risks are known and mitigated to the most reasonable level that balances cost, efficiency, and compliance. The major tasks of the Risk Assessment process are:

- Describe system risks originating within the Infrastructure.
- Identify actions that mitigate or control those risks.
- Determine and classify the net unmitigated risks.

4.1 Risk identification

The Risk Assessment will be conducted by reviewing the functions of the Infrastructure, and then considering the types of events that might occur in both normal and unusual situations. This may be done by challenging the normal presumptions, and considering the possibilities of unanticipated situations. For each risk event, the underlying (root) cause should be determined that will create the potential risk occurrence.

Risks are ranked by scoring various criteria with appropriate numerical ratings, adding the scores to determine the overall score of each risk, and sorting the risks into descending order based on each score. A risk scoring threshold is established, over which risks must be mitigated using adequate design and/or process controls that will protect the system. Those risks that fall below the threshold are either unmitigated or scheduled for later mitigation. An additional threshold or characteristic of risk can be used to determine the differentiation of non-mitigation versus postponed mitigation. A more complicated risk format is sometimes appropriate, with algorithms developed based on system function, patient safety, and financial liability, but we will not explore this sometimes complicated format in this document.

4.2 Risk mitigation

For each identified risk event, the mitigation for the risk (system design or control features) including manual tasks defined in the system operating procedures, are described in the risk assessment documentation. Risks with rating scores that meet or exceed the Risk Threshold will require mitigation by adding additional system enhancements or procedural controls to the system. The Risk Assessment template and instructions are in Appendix L, “Risk assessment and mitigation plan” on page 221 of this redbook.

4.3 Applying risk to the testing protocol

The Identified Risks in the Risk Assessment are a factor in determining the type of tests required in the testing protocol. A test script should contain verification of each of the design features or controls that are identified to mitigate identified risks. For those controls that are based upon a manual process, the procedures test scripts will contain a verification step to confirm that the procedure has the required instructions to effect mitigation.

The total Risk Score will also be used to determine the level (extent) of testing required for the design features or controls. Higher total Risk Scores will require a greater number of test alternatives, such as additional challenge tests. Test script reviewers will consider the total Risk Scores as part of their review and must consider and accept test script adequacy.

The Trace Matrix will contain links that identify Risk Events (line items) that are verified by test scripts (test step ID numbers).

5

Testing protocol

This chapter describes the testing protocol and contains the following topics:

- Protocol contents
- Roles and responsibilities
- Infrastructure installation/Configuration verification
- Environmental conditions verification
- Documentation verification
- Infrastructure functions verification
- Trace Matrix
- Test script preparation, approval, and changes
- Test execution
- Test testing protocol and Qualification Plan deviations
- Test Report

5.1 Protocol contents

Infrastructure testing and infrastructure test planning will be conducted according to a testing protocol. This testing protocol outlines activities and tasks for infrastructure planning. Appendix M, “Testing protocol” on page 225 illustrates the template and procedures for preparation and approval of the testing protocol.

5.2 Roles and responsibilities

The protocol will contain a responsibility assignment matrix, which will be used to record the names of persons assigned to execute protocol tasks, and to confirm required training for said persons.

5.3 Infrastructure installation/Configuration verification

Test scripts will be created that describe the process for reviewing and conducting inventory of the installed Infrastructure against the technical design document (TDD), including applicable configuration settings. This testing will confirm that the installed Infrastructure meets the TDD specifications.

5.4 Environmental conditions verification

Test scripts will be created to evaluate the environment into which the Infrastructure has been installed. Additional scripts will confirm that the Infrastructure meets the hardware vendor or vendor requirements, and has the necessary support and security procedures in place.

5.5 Documentation verification

The testing protocol will include verifying the presence and identifying the location of all Infrastructure supporting documentation, including, but not limited to, that supplied by the Infrastructure vendors as well as specified in local procedures for equipment operation.

5.6 Infrastructure functions verification

There are many automated functions that are part of the core infrastructure but independent of business applications software programs. These functions may be part of utility packages that are installed with the hardware, or they may result from features of the operating system that are used for hardware management. The functions may also be embedded into firmware that is part of the equipment. Utilities that support business applications functionality and that are installed subsequent to infrastructure installation are likely outside the scope of infrastructure functions verification. Test scripts shall confirm the basic performance of Infrastructure-based automated functions.

5.7 Trace Matrix

Testing must include verification of all Technical Design requirements, as well as design features and controls identified in the Risk Assessment. To provide such assurance, a Trace

Matrix is created that matches requirements to the test script steps. The Trace Matrix template and completion instructions are in Appendix N, “Trace Matrix” on page 231.

Any changes, additions, or adjustments to the technical design document, or Risk Assessment Report, that are made during the IQ preparation or execution will require a review to determine if the testing must be changed as well. The Trace Matrix is used to identify the appropriate tests, and is itself updated if any changes are required.

5.8 Test script preparation, approval, and changes

Test scripts are attached to the testing protocol, and are approved concurrently with testing protocol approval. Any changes in test scripts after testing protocol approval require re-approval by the same persons who originally approved the testing protocol.

5.9 Test execution

The execution of the test scripts by the IQ tester or testers will be performed in accordance with Test Execution Procedures found in Appendix O, “Test execution procedure” on page 233.

5.10 Test testing protocol and Qualification Plan deviations

A deviation is created anytime a process is not executed in accordance with previously approved procedures, or observed results do not match expected results. In each situation, a Deviation Report is created, and the event is investigated, resolved, and the resolution approved. The Template and procedure for deviation creation, review, resolution, approval, and documentation is in Appendix P, “Deviations procedure” on page 239.

5.11 Test Report

At the completion of testing, a Test Protocol Report will close the testing process, and explain the results of testing. All deviations that occurred during testing will be discussed with remedies and re-testing results included in the Test Protocol Report. Additionally, the rationale for concluding that testing is complete, and a summary of all test results will be included. The template and instructions for preparing and approving a Report (for both protocol and Qualification Plan) is presented as Appendix Q, “Validation reports procedure” on page 247.

6

Equipment operations and support procedures

Providing assurance that a system will continue to meet its specified requirements after installation and qualification requires system maintenance and management, and user support. These activities must be performed in accordance with procedures that maintain the system's state of validation.

Part of the Installation Qualification process involves verification that the required system management procedures have been created and approved, and that appropriate support staff training has been completed. This verification will assure that the system can be maintained in a quality environment on an ongoing basis.

The IQ process will include an independent review of the system management procedures to verify that the Infrastructure procedures are ready for use in managing and supporting the system. The procedure verification process will check for inclusion of the following in each procedure:

- The procedure contains subject matter covering the minimum requirements noted in the procedure review checklist.
- The subject matter clearly states the requirements, and contains work instructions that specify how the requirements are to be achieved.
- The level of detail is adequate such that a trained person will consistently meet the requirements by following the procedure content.
- The procedure has been approved and is part of a controlled document system used by the location.
- The staff who will be performing the procedure have been trained on the procedure, and a training record has been created, approved, and is stored in the training records system in use by the location.

Appendix R, "Infrastructure procedures verification checklist" on page 251 is a checklist that identifies areas of system management with the corresponding procedural requirements. The checklist is based upon a general list originally supplied by IBM, and can be modified to meet the specific situation or situations at the individual site. This appendix will be used as a verification record for review of the system procedures. The reviewer will match the requirements to the applicable procedure, and then record the procedure and section, if applicable, that meets the checklist criteria. The reviewer will verify that the procedure meets the above criteria, and then will sign and date the checklist requirement section.

A copy of the reviewed procedure will be attached to the checklist, and the documents will be added to the IQ records. The Quality representative will review the checklist for completion, approve procedure attachments, and randomly audit checklist verifications for consistency with the procedure contents.

This chapter contains the following topics:

- Physical security
- Change control/Configuration management
- Backup and restore
- Infrastructure monitoring
- Periodic/Preventative maintenance
- Resolution
- Disaster Recovery Plan/Continuity Plan
- Training management/records
- Document management
- Periodic review/internal audit

6.1 Physical security

Physical Security procedures provide rules and physical safeguards for managing access to the Infrastructure by persons internal (IT and Non-IT staff) and external (for example, vendors or contractors) to the company. This includes both server/storage data centers as well as remote and external areas such as wiring closets.

6.2 Change control/Configuration management

Once the IQ is complete, the entire Infrastructure inventory must be under configuration control. This means that changes made to any infrastructure components (hardware or software) must occur according to a process that adequately describes the changes, analyzes impact on the system and its functions, provides for appropriate re-testing, and fully documents (with approvals) the changes in the system. The change request/control process manages each request through complete and controlled stages that assure the Infrastructure remains in a qualified state, which requires congruency with current documentation. Note that change control includes service and version updates to the system.

6.3 Backup and restore

Infrastructure procedures will ensure backups are made in accordance with approved schedules that define backup scope, timing, and a retention period prior to media recycling.

Infrastructure procedures will also define methods for media labeling, backup record keeping, protection, and storage of media for the duration of backup periods.

Procedures and testing must also define how the backups will be used in the event of a failure to restore the system, and periodic testing of this procedure must occur and be documented.

6.4 Infrastructure monitoring

Routine monitoring and housekeeping of Infrastructure components by data center or IT support staff must be described in the operating procedures.

6.5 Periodic/Preventative maintenance

Periodic and preventative activities that support the Infrastructure, such as random or periodic checks, cleaning, parts replacement, and so on, must be described in operating procedures. This includes the schedule or methods for determining the frequency of periodic and preventative tasks, and/or methods for coordinating downtime periods for activities that must be done while the system is off-line.

6.6 Resolution

When a system outage occurs due to the failure of a component in the Infrastructure, or when unexpected results or observations occur during the performance of system procedures or other unforeseen reason, the company is required to complete an investigation of the failure. The investigation results and conclusion or conclusions reached should be fully documented, and appropriate corrective action for the failure determined and logged. Additionally, preventative actions to avoid future problems should be defined if applicable.

6.7 Disaster Recovery Plan/Continuity Plan

The data center operations must have a complete testing plan for the continuation of critical systems in the event of partial or complete loss of use of the Infrastructure. The plan will include transfer of the system to an alternative Infrastructure and the controlled return of the system to the primary Infrastructure for the recovery.

The Disaster Plan will contain or link to a user-community business continuity plan for manual, limited, or deferred processing during the period of limited or unavailable system access. This plan will also contain methods of system re-evaluation/revalidation after recovery to assure system integrity has not been compromised by the failure events.

Generally, the difference between backup and restore, and disaster and recovery, is the hardware environment. Backup and restore can happen on the previously qualified infrastructure, while disaster recovery generally requires transfer of operations to a new or temporary infrastructure, then subsequent return of the system to a new environment with the specifications of the originally qualified environment. It is in this instance that a detailed installation qualification is very useful to ensure equivalence of the new infrastructure.

6.8 Training management/records

Data center and/or IT support staff that executes the system management procedures must be trained prior to performing their assigned duties. Training procedures describe the methods used to match training needs to staff duties. These procedures also describe how to organize, schedule, and deliver training programs. Training record keeping should be maintained in an approved system, with record approval and record retention procedures outlined and available should verification by either task assignors or inspectors be required.

6.9 Document management

All documents that support validated systems must be stored and managed with a controlled document process using a manual, computerized, or hybrid (computer and manual) system. The process is described in procedures that cover all aspects of document authorship, review, approval, issues or deviations reporting and resolution, and version (or change) control, with retention of prior versions for later reference or audit support. These procedures must apply not only to site procedures, but also to system documents, such as manuals and any validation records.

6.10 Periodic review/internal audit

After completion of the Installation Qualification, the Infrastructure may be part of a validated system, under the control of the operating procedures. In order to assure that the Infrastructure remains in a qualified state, periodic reviews or internal audits of the Infrastructure and associated procedures are required, particularly since issues or control weaknesses may evolve over time. Periodic, internal, but independent, auditing will also facilitate preservation of the Infrastructure’s qualified state.

7

Operations team training

Initial training of Data Center personnel on the installed infrastructure is within scope of the validation plan, and as records of such training are created, they should be added to or referenced in the validation package. Subsequent changes in staffing, procedures, and resulting re-training will be part of routine Data Center operations procedures and records.

This chapter contains the following topics:

- Training requirements and initial operator training
- Training records

7.1 Training requirements and initial operator training

Upon completion of the testing protocol, the initial Data Center operators who will perform system management tasks must be trained using operating manuals and/or Data Center operating procedures identified in Appendix K, “Infrastructure installation and operating manuals” on page 215.

7.2 Training records

Training records for initial data center operators will be created, using either the form in Appendix H, “Training/qualifications record” on page 207, or forms dictated by site procedures. The forms will be stored in accordance with local training documentation procedures, with a copy attached to or referenced in the validation records.

8

Regulatory inspection preparation

This chapter describes regulatory inspection preparation and contains the following topics:

- Regulatory inspection procedures
- Regulation, guidance, and standards cross-references

8.1 Regulatory inspection procedures

The Infrastructure supporting computer systems under the scope of 21 CFR 11 is subject to audits by FDA field inspectors. These inspections may cover any aspect of the system design, operations and management, and validation documentation. This may include questions regarding Infrastructure management procedures, including Data Center operations and IT support staff tasks in support of the system.

To be adequately prepared for the inspection, the site should have procedures and/or training programs that Data Center/IT support, management, and staff may reference and understand so that they readily address the requirements and demands of an inspection. The content for these programs should minimally include the following:

- Inspection notification of and by management, and creation of an inspection response team
- Inspection tours and escorting rules
- Allowable range of inspection and inspector conduct
- Inspector question response rules (guidance to answers)
  - Determination/clarification of the question content
  - Identification of responder
  - Accuracy, interpretation, and scope of answer
  - Evidence to support answers
  - Documentation of questions and answers
- Documentation (copy) requests
- Inspection conclusion (observations) and company response

8.2 Regulation, guidance, and standards cross-references

The contents and structure of this Qualification Plan, and its accompanying forms and procedures in the Appendixes, were based upon Life Sciences' industry standard practices for Computer System Validation, and specifically Infrastructure Installation Qualification.

As a result, this document's content is compatible with the common documents recognized by the industry, industry consortium/association publications, and other standards regarding computer system validation.

Appendix S, "Regulation, guidance, and standards cross references" on page 259 is a cross reference of the sections of commonly used validation standards that cover the Installation Qualification, related protocols, and validation topics. The validation standards are referenced to the contents of this Qualification Plan.

9

Qualification Report and infrastructure acceptance

Upon completion of all of the tasks defined in this Plan, the Installation Qualification process will be completed, and a final Qualification Report will close-out the Infrastructure Qualification process.

This chapter contains the following topics:

- Infrastructure Final Report and approvals
- Follow-up item tracking
- System and documentation turnover

9.1 Infrastructure Final Report and approvals

A Qualification Report will be prepared that will summarize the activities completed in accordance with this Plan, and list and explain any deviations encountered other than testing deviations that were covered in the Testing Protocol Report. The Qualification Report will provide the rationale to support the conclusion that each element of the acceptance criteria (as described in Section 1.4 of this Plan) has been met. The Report will be supported by and will list accompanying documents and records as evidentiary support of the Report conclusion.

The Template and procedure for preparing Qualification Reports (both Testing Protocol and Final Report) are found in Appendix Q, “Validation reports procedure” on page 247.

9.2 Follow-up item tracking

Any open items or tasks that require follow-up activities after the Qualification Report is completed must be fully explained within the Qualification Report. This includes outlining staff responsibilities for completing the follow-up tasks and the method or methods that will be used to verify completion of the follow-up activities. The methods must also assign persons who will approve the satisfactory completion of tasks, and include a description of the documents and their content that will require approval.

9.3 System and documentation turnover

All of the Qualification documents named in this Plan, and all supporting records referenced by the Plan, Testing Protocol Report, or Final Report will constitute the IQ records. These documents will be placed into binders and labeled by sections that correspond either to the structure stated in the testing protocol for testing records, or to the structure of this Plan for all other records. A Table of Contents will be created, and will link the various binders as components of the total package.

Copies of all electronic files will be included in the package, and a list of the files with file name, size, and time/date stamp will be added to the Table of Contents. The entire package will be stored and maintained in the controlled document repository of the local site, in accordance with local controlled document management procedures in effect for validation packages.

Part 2

Procedure and protocol appendixes

This part contains the following appendixes:

- Appendix A, “Document master list: Roles and Responsibilities Matrix”
- Appendix B, “Infrastructure identification”
- Appendix C, “Infrastructure environmental requirements”
- Appendix D, “Infrastructure functional description”
- Appendix E, “Installation Team Training/Qualifications Matrix”
- Appendix F, “General regulatory and 21CFR11 training”
- Appendix G, “Good Documentation Practices”
- Appendix H, “Training/qualifications record”
- Appendix I, “Resume equivalent for training and qualifications record”
- Appendix J, “Signature log”
- Appendix K, “Infrastructure installation and operating manuals”
- Appendix L, “Risk assessment and mitigation plan”
- Appendix M, “Testing protocol”
- Appendix N, “Trace Matrix”

- Appendix O, “Test execution procedure”
- Appendix P, “Deviations procedure”
- Appendix Q, “Validation reports procedure”
- Appendix R, “Infrastructure procedures verification checklist”
- Appendix S, “Regulation, guidance, and standards cross references”

A

Document master list: Roles and Responsibilities Matrix

The following Roles and Responsibilities Matrix (R&RM) lists the Major Tasks and Qualification documents that will be created and approved for inclusion into the Infrastructure Qualification Binder, with assignments of the persons who will either execute the task or prepare the document. Designated approvers for each document are listed, with tasks or documents. In so much as approvers are not needed, the Approval field shall be marked N/A for “not applicable”.

Changes in Tasks Assignments, Document Preparers, or Approvers will require re-approval of this matrix. If the completed Roles and Responsibilities Matrix Appendix is more than one page, the header must be copied to subsequent pages with the appropriate page number and total number of pages recorded.

Version Date: _______________ Replaces Date: ____________

Page __ of ___

				Approvals by		
Plan Sec number	Doc number	Activity or Document Name	Performed or Prepared by	System Owner	Technical Support	Quality Representative

Roles and Responsibilities Matrix approvals

Document Preparer ____ Date _____________

System Owner: ____ Date _____________

Tech Support: ____ Date _____________

Quality Representative: ____ Date _____________

B

Infrastructure identification

The following is a complete listing of the components of the system infrastructure that is being qualified by this plan. The indicated columns are provided by the person performing the IQ verification.   The completed document will be reviewed to verify that each line number has been verified, and that (if applicable) a location and specific identification number (license number or unit serial number) has been supplied.

Infrastructure Identification Test Script

Hardware Inventory and Installation

Objective: The objective of this test is to verify that the installed hardware is as specified in the System Design Specification.

Set Up: None.

Procedure:

Server One Specifications (IBM Serial #_________________)

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
1	Complete the items in the following table or tables.	All items completed. Expectations satisfied.			

Item ID	Item	Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Make	IBM			
2	Model	P Series 670 (7040-671)			
3	Serial Number	##-####			
4	CPUs	Minimum 8 CPUs			
5	RAM	Minimum 16 GB			
6	Disk space internal	Minimum One 18 GB Hard Disk and One 36 GB Hard Disk			
7	Number of network ports	Minimum 1 Network Port			
8	CPU Speed	Minimum 1.0 GHz			
9	Logical Partition	Yes			

Hardware Inventory and Installation Verification (continued)

Server Two Specifications (IBM serial #________________________)

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
2	Complete the items in the following table or tables.	All items completed. Expectations satisfied.			

Item ID	Item	Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Make	IBM			
2	Model	P Series 670 (7040-671)			
3	Serial Number	##-####			
4	CPUs	Minimum 8 CPUs			
5	RAM	Minimum 16 GB			
6	Disk space internal	Minimum One 18 GB Hard Disk and One 36 GB Hard Disk			
7	Number of network ports	Minimum 1 Network Port			
8	CPU Speed	Minimum 1.0 GHz			
9	Logical Partition	Yes			

Hardware Inventory and Installation Verification (continued)

P670s Console (HMC) Administration Console

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
3	Complete the items in the following table or tables.	All items completed. Expectations satisfied.			

Item ID	Item	Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Host Name	ServerHostName			
2	Operating System	LINUX			
3	Serial Number	##-####			
4	Model Number	HMC 6792-LPU			

IBM TotalStorage ESS 2105-800 Disk Array

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
4	Complete the items in the following table or tables.	All items completed. Expectations satisfied.			

Item ID	Item	Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Host Names	ServerHostName1 and ServerHostName2 (secondary)			
2	Operating System	Minimum AIX 4.3			
3	Serial Number	##-####			
4	Model Number	ESS 2105-800			
5	CPU Type and QTY	Minimum 1 RSA III 64, minimum 600 Mhz			
6	Harddrives	Minimum 16 drives @ 36 GB with 10K RPM			
7	CACHE	Minimum 8 GB			
8	Fiber Channel	Minimum 2			

ESS 2105- 800 Disk Array Console

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
5	Complete the items in the following table or tables.	All items completed. Expectations satisfied.			

Item ID	Item	Minimum Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Host Name	ConsoleName			
2	Operating System	Linux			
3	Serial Number	##-####			
4	Model Number	6792-EDG			
5	CPU Type and QTY	Intel P 3			
6	Harddrive Internal	Minimum 10 GB			

SAN Switches

SAN Switch 1 Serial Number ##-####

Procedure:

Step ID	**Step**	**Expected Results**	**Actual Results**	**Expectations Satisfied (Yes/No)**	**Initial/Date**
6	Complete the items in the following table or tables.	All items completed. Expectations satisfied.			

Item ID	**Item**	**Expected Finding**	**Actual**	**Expectation Satisfied (Yes/No)**	**Initial/Date**
1	Hostname	SwitchName			
2	Model	McData ES-4500, IBM 2031-225			
3	Serial Number	##-####			
4	Number of ports	Minimum 16			

SAN Switch 2 Serial Number ___________________

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
7	Complete the items in the following table or tables.	All items completed. Expectations satisfied.			

Item ID	Item	Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Hostname	SwitchName			
2	Model	McData ES-4500, IBM 2031-224			
3	Serial Number	##-####			
4	Number of ports	Minimum 16			

Tape Backup Libraries

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
8	Complete the items in the following table or tables.	All items completed. Expectations satisfied.			

Backup Library 1

Item ID	Item	Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Hostname	LibraryName			
2	Model	IBM 3584-L32			
3	Number of slots	Minimum 48			
4	Tape type	LTO @ minimum 200 GB capacity			
5	Tape Drives	Minimum 4			

Tape Backup Library 2

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
9	Complete the Items in the following table or tables.	All items completed. Expectations satisfied.			

Item ID	Item	Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Hostname	Library Name			
2	Model	IBM 3583-L36			
3	Number of slots	Minimum 24			
4	Tape type	LTO @ Minimum 200 GB Capacity			
5	Tape Drives	Minimum 2			

Backup Server

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
10	Complete the items in the following table or tables.	All items completed. Expectations satisfied.			

Item ID	Item	Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Server Name	<<ServerName>>			
2	Operating System	Minimum AIX 4.3			
3	Serial Number	##-####			
4	Model Number	7026-6H1			
5	CPU Type and QTY	RS 64 III, Minimum 1 CPU @ Minimum 400 Mhz			
6	Harddrive Internal	Minimum 18 GB, Ultra 3 10K			
7	Network Adapter	Minimum One 2 GB Ethernet SX			
8	RAM	Minimum 2 GB			
9	Back Up	Tivoli® Minimum Release 4.2			
10	Back Up	Sysback Minimum Release 5.0			

Comments:

Summary of Test Script Results		Test Outcome		Deviation Number (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Cabling Test Script

Objective: The objective of this test shall be to verify that the cabling for the hardware, electrical and network, is set up.

Set Up: None

Procedure:

Step ID	Step	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Verify that the server cabling is physically connected to an electrical source or sources	Electrical cabling for P760 Server and back up server to power supplies in place			
2	Verify that the servers are physically connected to network	P760 Server and back up server network connections in place			

Comments:

Summary of Test Script Results		Test Outcome		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

C

Infrastructure environmental requirements

The following are the vendor specifications for the environmental conditions that apply to the Infrastructure components. These conditions will be verified by measurement or independent evaluation during the Installation Qualification.

Equipment/Requirement Type	**Required Conditions**
pSeries 670 Server	
Room Temperature	16 °C to 32 °C (61 °F to 90 °F).
Room Relative Humidity	8% to 80%.
Source Power	▸ Operating voltage @ 50/60 Hz: (3-phase), 60 Amp Circuit. – 200 to 240 V AC. – 380 to 415 V AC. – 480 V AC. ▸ Operating voltage @ 50/60Hz (Single-phase): 200 to 415V AC, 40 Amp Circuit.
Rack Mounting	Systems should be mounted so that alternate rows of racks face each other. Front to front, then back to back, due to air flow requirements.

Equipment/Requirement Type	Required Conditions
Service Clearance	Sufficient clearance around the box to allow doors to be fully opened for servicing.
pSeries 660 Server	
Room Temperature	10 °C to 40 °C (50 °F to 104 °F).
Room Relative Humidity	8% to 80%.
Source Power-CEC	Operating voltage: 200 to 240 V AC 50/60 Hz.
Source Power - I/O Drawer	Operating voltage: 200 to 240 V AC 50/60 Hz.
Service Clearance	Sufficient clearance around the box to allow doors to be fully opened for servicing.
3584 Tape Library	
Room Temperature	16 °C to 32 °C (61 °F to 90 °F).
Room Relative Humidity	20% to 80%.
Source Power	Operating voltage @ 50/60 Hz: (1-phase), 30 Amp Circuit 200 to 240 V AC.
Service Clearance	Sufficient clearance around the box to allow doors to be fully opened for servicing.
4500 McData Switches (IBM 2031-224)	
Room Temperature	4.4 °C to 40 °C (40 °F to 104 °F).
Room Relative Humidity	8% to 80%.
Power Supply	Operating voltage @ 47-63 Hz: (1-phase), 15 Amp Circuit, 100-240VAC.
Rack mount	1U high slot in a 19-in rack.
2105-800 ESS Disk Array	
Room Temperature	16 °C to 32 °C (60 °F to 90 °F).
Room Relative Humidity	20 to 80%.
Power Supply	Operating voltage @ 50-60 Hz: (3-phase), 60 Amp Circuit, 200-240VAC.
Service Clearance	Sufficient clearance around the box to allow doors to be fully opened for servicing.

Environmental Conditions Test Script

Objective: The objective of this test is to verify that the environmental conditions of the room housing the hardware shall be maintained according to the system vendor recommendations.

Set Up: None

Procedure:

Step ID	Step	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Attach IBM specification or specifications for room temperature and humidity.	IBM specification attached.			
2	Record IBM room temperature specification.	Temperature specification recorded: ______________________			
3	Record procedure used to record the room temperature used and equipment details.	Temperature Indicator Manufacturer and Unique Identifier Recorded. Calibration dates recorded. Procedure used to record temperature recorded.	________________________ ________________________ ________________________ ___________________		
4	Record IBM room humidity specification.	Humidity specification recorded: ______________________			
5	Record procedure used to record room humidity, and equipment details.	Humidity Indicator Manufacturer and Unique Identifier recorded. Calibration dates recorded. Procedure used to record humidity recorded.	________________________ ________________________ ________________________ ___________________		

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Power Supply UPS Test Script

Objective: This test will verify that the system has an uninterruptible power source via dual power.

Set Up: None

Procedure:

IBM 2105-800 ESS Disk Array

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Physical verification of power source on primary rack.	Physically verify the primary ESS Rack has a dual power source.	Both Line Cord lights are illuminated.			
2	Physical verification of power source on expansion rack.	Physically verify the expansion ESS Rack has a dual power source.	Both Line Cord lights are illuminated.			
3	Simulate disconnecting power source.	Identify the circuit breaker to one of the power sources for the primary ESS and disable.	One Line Cord light is blinking.			
4	Verify access to storage is not interrupted.	From <ServerName>, run: `lsvg -l vgname`	Command executes normally.			
5	Reconnect power.	Reset the circuit breaker to the on position.	Both Line Cord lights are illuminated.			

P670 Server #1

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Physical identification of the server.	Locate the p670 server with LPAR <ServerName6> and document the serial number of the physical server: Serial Number: ____________________	The serial number for the server has been identified.			
2	Physical verification of the power source.	Physically verify the p670 server has a dual power source.	Two cords are connected to the server.			
3	Simulate disconnecting the power source.	Identify the circuit breaker to one of the power sources for the p670 and disable.	Circuit breaker is off.			
4	Verify system is accessible and view log.	Login to <ServerName6> and run: `errpt –a | head -30` Attach screen print.	Error Log indicates the loss of partial power (environment problem).			
5	Reconnect the power.	Reset the circuit breaker to the on position.	Power is reconnected.			
6	Verify that the system recovered.	Run: `errpt –a | head -30` Attach screen print	Error Log indicates the return of power (Electrical Power Resumed).			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
7	Clear the crontab entry on each LPAR on p670.	For each LPAR, <ServerName3>, <ServerName4>, <ServerName5>, and <ServerName6>, clear the rc.powerfail crontab entry.	Crontab entries are cleared.			
8	Clear the system fault indicator.	Clear the p670's fault indicator, setting the System Attention Indicator to the Normal setting under the Identify and Attention Indicators in system diag.	Fault indicator on p670 is off.			

P670 Server #2

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Physical identification of the server.	Locate the p670 server with LPAR <ServerName> and document the serial number of the physical server: Serial Number: ____________________	The serial number for the server has been identified.			
2	Physical verification of the power source.	Physically verify the p670 server has a dual power source.	Two cords are connected to the server.			
3	Simulate disconnecting the power source.	Identify the circuit breaker to one of the power sources for the p670 and disable.	Circuit breaker is off.			
4	Verify that the system is accessible and view log.	Login to <ServerName> and run: `errpt –a | head -30` Attach screen print.	Error Log indicates the loss of partial power (environment problem).			
5	Reconnect power	Reset the circuit breaker to the on position.	Power reconnected.			
6	Verify that the system recovered.	Run: `errpt –a | head -30` Attach screen print.	Error Log indicates the return of power (Electrical Power Resumed).			
7	Clear the crontab entry on each LPAR on p670.	For each LPAR, <ServerName1>, <ServerName2>, and <ServerName3>, clear the rc.powerfail crontab entry.	Crontab entries are cleared.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
8	Clear the system fault indicator.	Clear the p670’s fault indicator setting the System Attention Indicator to the Normal setting under the Identify and Attention Indicators in system diag.	Fault indicator on p670 is off.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Physical Security Test Script

Objective: The objective of this test is to verify that the system’s physical security exists.

Set Up: None

Procedure:

Step ID	Step	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Attempt to enter the server room without a security authorization access card.	No access to server room.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

D

Infrastructure functional description

The following is the listing of the major automated features that are provided by the Infrastructure, which function independently of the applications that will be supported by the Infrastructure. For each feature, the method of testing is indicated, or the reasons for waiving testing are provided.

Item#	Infrastructure Component	Feature Description	1. Testing Strategy or 2. Rationale for waiving on-site tests
p670 pSeries Server			
1	DASD Predictive Failure	Predictive Failure analysis provides the ability to detect an imminent disk failure and report the finding through an AIX log.	1. Test will simulate message from predictor being processed into AIX log. 2. Test of prediction accuracy would require deliberate progressive damage to disk.
2	Auto-Restart	Auto-restart automatically restarts the system following an unrecoverable software error, software hang, hardware failure, or environmentally produced (AC power) failure.	2. Not an installed option at <Company>.

Item#	Infrastructure Component	Feature Description	1. Testing Strategy or 2. Rationale for waiving on-site tests
3	ChipKill	ChipKill™ Memory protects the server from any single memory chip failure and multi-bit errors from any portion of a single memory chip by detecting, then removing any defective chips from service.	2. Test of feature would require deliberate damage to the selected chips.
45	MicroCode Discovery Service	Using a secure Internet connection and a Web browser, Microcode Discovery Service can capture the machine data and generate a real-time comparison report showing subsystems that may need to be updated.	2. Not required in local infrastructure, but functions in IBM environment to aid in analysis.
5	Inventory Scout	The tool will create a file containing the current level of all microcode (adapters, devices, system, and support processor) levels in the system. This file will be used to compare the system level codes against the latest available levels on the IBM Web site, and generates a report of possible updates.	2. Not an installed option at <Company>.
6	CPU De-allocation	System detects and takes a failing process off-line without requiring a shutdown or re-boot. Systems Admin and/or IBM are notified.	1. Can be tested by disabling a processor manually on systems that have the feature enabled.
7a	I/O Link Failure Recovery	Linkage failure can be detected and recovered automatically.	1. Can be verified by running diagnostics to confirm feature is operational. 2. Challenge test would pose risk to system due to deliberate deactivation of primary linkage.
7b	Environmental Sensing	Auto-detection of environmental conditions.	1. Feature can be verified by a command that will show the sensors are active on hardware that supports this test. 2. In case of <Company>'s equipment, this verification is not possible. Challenge test would add risk of damage to infrastructure.
8	LPAR separation	Separate "computer" within the total system, each with its own processor and operating system copy.	1. Shutdown of an LPAR (simulates a crash) will have no effects on another LPAR. 2. Challenge testing by purposely crashing an LPAR would pose a risk to the operating system and application installation.
9	Workload Manager	Monitors and adjusts system resources to optimal level for maximum performance.	2. Not required for system operation, just improves overall performance.

Item#	Infrastructure Component	Feature Description	1. Testing Strategy or 2. Rationale for waiving on-site tests
10	Cryptographic processors	Ability to support additional security package options for cryptography, digital signatures, and Kerberos.	2. Not installed at <Company>.
11	First Failure Data Capture	Method of recording errors detected by other features.	2. Not a separate feature, but a description of the error detection methods
12	Hardware Management Console (HMC)	Series of functions to create, start, manage, stop, and perform other management tasks for an LPAR.	1. Test by viewing LPAR, then changing and re-viewing LPAR.
13	Power Redundancy	Redundant power for bulk or regulated power supplies.	1. Turn off breakers (downstream of UPS). 2. Testing could produce a power fluctuation that could pose the danger of data corruption.
14	Internal Battery Feature	Provides emergency power if no UPS is active.	2. Not installed at <Company>.
15	Constant Power Monitoring	Constant power monitoring assists in detection of early loss of source power, and notifies the operating system to effect an orderly shutdown.	2. Not installed at <Company>.
16	Persistent Processor De-allocation	When a damaged processor exists, the processor remains out of the configuration when the system is re-booted.	2. Challenge test would require damaging a processor to verify non-boot.
17	Memory Scrubbing	Memory scrubbing is the process of reading the contents of memory during idle time and checking and correcting any single-bit errors that have accumulated.	2. Additional memory check verification, but is not required for normal processing.
18	Memory Predictive Failure Analysis	The service processor initiates a deferred maintenance request on memory cards that have used their spare bits and are experiencing additional correctable errors.	2. Challenge test would require damaging a memory card.
19	Uncorrectable Memory Error Handling	Corrupted data is specially marked until used by a processor, at which time a new synchronous machine check interrupt allows AIX to localize the effect to a single LPAR partition or a software process. This provides the capability of localizing a global system resource to affecting only the partition utilizing the resource instead of 'check-stopping' all system partitions.	2. Test not possible without damaging hardware. Basically, this feature says that if memory goes really bad, instead of crashing the whole machine, only the LPAR that has access to the memory will crash.

Item#	Infrastructure Component	Feature Description	1. Testing Strategy or 2. Rationale for waiving on-site tests
20	Service Focal Point	The SFP collects the serviceable events from different building blocks together in a Service Action Event (SAE) log. The log entries are generated by analysis routines that run on an error that has occurred in a building block. The resource manager for the building block forwards information about the event to the service focal point and the information is placed in the SAE log. The SAE log on the SFP also contains pointers to extended information that may have been recorded at the time of a serviceable event by the building block.	1. Testing is done by accessing some of the SFP features, such as hardware identification (also known as Guiding Light).
21	Service Action Event Log	Extended error collection includes not only the collection of first failure data capture, but also vital product data, partition information, operating system error logs, service processor error logs, error register data, and so on.	1. Testing is done by accessing the Service Action Event Log.
22	Service Agent Component	When a service action event is logged in the SFP, the system needs to communicate the failure back to IBM. During this call-home function, particular error data and system configuration information needs to be sent to IBM to drive the service delivery infrastructure. The SFP utilizes the Service Agent focal point application residing on the HMC along with the HMC modem to initiate the call home and transfer the pertinent error information to IBM Service. When a call home is required, Service Agent manages the connection to IBM, which is used to open a problem record.	1. Testing is accomplished by accessing the feature and sending a test PMR report to IBM.
23	Guiding Light	The SFP can enable the capability to flash LEDs on the respective system unit and drawer that contain the fault.	1. Tested by accessing the Service Focal Point to identify a hardware component.
2031 McData Switches			
24	Capacity on Demand	Additional switch capacity can be added upon demand without interruption of service.	2. Not part of normal processing. Will only be used in upgrades covered by change control.
25	Hot Swap Power	The McData Sphereon 4500 Fabric Switch provides hot-swappable, load-sharing dual power supplies that allow the switch to remain online if one supply fails.	2. Could introduce equipment damaging power fluctuations.
26	Concurrent Firmware Upgrade	Firmware upgrades can be downloaded and activated while the fabric switch remains operational.	2. Not part of normal processing. Will only be used in upgrades covered by change control.
27	SAN Management	Provides monitoring and configuration management for small switched fabrics.	1. Test by viewing configuration, making a change, then re-viewing configuration.

Item#	Infrastructure Component	Feature Description	1. Testing Strategy or 2. Rationale for waiving on-site tests
3584 Tape Library			
28	Automatic re-inventory	When the library door is closed, a bar code reader mounted on the auto-changer scans the cartridge labels, enabling a re-inventory of the cartridges in the library frame.	1. Test is executed by manually running a library inventory.
29	TapeAlert	The 3584 LTO Ultrium drives and library robotics are TapeAlert-compatible, providing tape drive and library error and diagnostic reporting.	2. Challenge test would require damaging a tape drive or library.
30	AutoDrive Cleaning	Drive cleaning is an automatic function performed by the library when required by the drive, without requiring operator intervention.	1. Check Drive records for AutoCleaning events within a time period.
31	Multi-Path	The feature of the 3584 UltraScalable Tape Library allows the library to be shared by multiple heterogeneous servers sharing the library.	2. Not installed at <Company>.
IBM 2105-800 ESS			
32	FlashCopy®	FlashCopy is designed to provide a point-in-time copy capability for logical volumes. FlashCopy creates a physical point-in-time copy of the data, with minimal interruption to applications, and makes it possible to access both the source and target copies.	2. Not used in normal operation of validated system. Copy would be for external, out-of-scope use.
33	Peer-to-Peer Remote Copy (PPRC)	Provides real-time mirroring of logical volumes within an ESS or between two ESSs that can be located up to 103 km from each other. PPRC is a synchronous copy solution where write operations are completed on both copies (primary and secondary ESS) before they are considered done.	2. Not licensed by <Company>.
34	PPRC Extended Distance (PPRC-XD)	Provides a non-synchronous long distance copy option whereby write operations to the primary ESS are considered complete before they are transmitted to the secondary ESS.	2. Not licensed by <Company>.
35	Extended Remote Copy (XRC)	Extended Remote Copy (XRC) is a combined hardware and software business continuance solution for the zSeries® and S/390® environments providing asynchronous mirroring between two ESSs at global distances.	2. Not installed at <Company>.
36	PAV	PAV enables a single zSeries or S/390 server to simultaneously process multiple I/O operations to the same logical volume.	2. Not installed at <Company>.
37	Multiple Allegiance	Multiple Allegiance expands the simultaneous logical volume access capability across multiple zSeries or S/390 servers.	2. Not installed at <Company>.

Item#	Infrastructure Component	Feature Description	1. Testing Strategy or 2. Rationale for waiving on-site tests
38	I/O Priority Queuing	Allows the ESS to use I/O priority information provided by the z/OS® or OS/390® Workload Manager to manage the processing sequence of I/O operations.	2. Not installed at <Company>.
39	Enterprise Storage Server Network	Utilizes a dedicated LAN to support configuration, copy services communications between machines, call home, and remote support capabilities.	1. Test verifies connectivity by a ping test.
40	Enterprise Storage Server Specialist	The ESS Specialist is a Web-based tool for performing logical configuration and copy services (PPRC and FlashCopy) management functions.	1. Test views configuration; any changes pose a threat of data corruption.
41	Enterprise Storage Server Specialist	LUN Masking: Expose/unexpose volumes to Fibre Channel-based initiators and obtain volume access information, including a list of volumes not exposed to any initiator.	1. Use ESS Storage Specialist to display systems allowed access to a specific volume.
42	ESS CLI	► Asset Management: Obtain information about ESS volumes, I/O ports, volume spaces, disk groups, and connected hosts. ► LUN Masking: Expose/unexpose volumes to Fibre Channel-based initiators and obtain volume access information, including a list of volumes not exposed to any initiator. ► Space Management: Query available free space and create new volumes. ► Volume Identification: Assign a user-specified label to a volume. ► Volume Identification: Assign a user-specified label to a volume. ► Host Connections: Define, undefine, and modify host connections and obtain host type information, including host port world-wide name. ► Audit Log: Obtain a log of configuration activity by user ID. ► Audit Log: Obtain a log of configuration activity by user ID. ► Parallel Access Volumes (PAV): List and create new PAVs. ► Copy Services: Query functions to view tasks in the copy services task repository, obtain PPRC path status, and determine completion of the FlashCopy background copy.	2. Tools for system setup and configuration; not used for system operations.
43	SDD	Provides load balancing and enhanced data availability capability in configurations with more than one I/O path between the host server and the ESS.	1. Test is to disrupt a connection and verify that the SDD registers the break.

Logical Partition Installation Test Script

Objective: The objective of this test is to verify that the server logical partitions are as specified in the SAP System Design Specification Document.

Set Up: None.

Procedure:

Server 1, Partition 1

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
1	Complete the items in the following table or tables.	All the items completed. Expectations satisfied.			

Item ID	Item	Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Server Name	<<ServerName>>			
2	Operating System	Minimum AIX 5L Version 5.1			
3	CPU Type and QTY	Power 4 Minimum 1.0 GHz, Minimum 2			
4	Harddrive Internal	Minimum 18 GB Ultra 3 10K			
5	Network Adaptor	Minimum one 2 GB Ethernet SX			
6	RAM	2 GB			

Server 1, Partition 2

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
2	Complete the items in the following table or tables.	All the items completed. Expectations satisfied.			

Item ID	Item	Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Server Name	<<ServerName>>			
2	Operating System	Minimum AIX 5L Version 5.1			
3	CPU Type and QTY	Minimum 2 Power 4 and minimum 1.0 GHz			
4	Harddrive Internal	Minimum 18 GB, Ultra 3 10K			
5	Network Adaptor	Minimum one 2 GB Ethernet SX			
6	RAM	Minimum 2 GB			

Server 1, Partition 3

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
3	Complete the items in the following table or tables.	All the items completed. Expectations satisfied.			

Item ID	Item	Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Server Name	<ServerName>			
2	Operating System	Minimum AIX 5l Version 5.1			
3	CPU Type and QTY	Power 4 1.0 GHz, Minimum 2			
4	Harddrive Internal	Minimum 18 GB, Ultra 3 10K			
5	Network Adaptor	Minimum one 2 GB Ethernet SX			
6	RAM	2 GB			

Server 1, Partition 4

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
4	Complete the items in the following table or tables.	All the items completed. Expectations satisfied.			

Item ID	Item	Minimum Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Server Name	<ServerName>			
2	Operating System	Minimum AIX 5L Version 5.1			
3	CPU Type and QTY	Power 4 1.0 GHz, 2			
4	Harddrive Internal	Minimum 18 GB, Ultra 3 10K			
5	Network Adaptor	Minimum one 2 GB Ethernet SX			
6	RAM	Minimum 2 GB			

Server 2, Partition 1

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
5	Complete the items in the following table or tables.	All the items completed. Expectations satisfied.			

Item ID	Item	Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Server Name	<ServerName>			
2	Operating System	Minimum AIX 5.1			
3	CPU Type and QTY	Power 4 1.0 GHZ, 4			
4	Harddrive Internal	Ultra 3 10K Minimum 18GB			
5	Network Adaptor	Minimum 2GB Ethernet SX			
6	RAM	Minimum 2 GB			

Server 2, Partition 2

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
6	Complete the Items in the following table or tables.	All the items completed. Expectations satisfied.			

Item ID	Item	Minimum Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Server Name	<ServerName>			
2	Operating System	Minimum AIX 5.1			
3	CPU Type and QTY	Power 4 1.0 Minimum GHZ, 2			
4	Harddrive Internal	Minimum 18 GB Ultra 3 10K			
5	Network Adaptor	Minimum 1 Minimum 2 GB Ethernet SX			
6	RAM	Minimum 2 GB			

Server 2, Partition 3

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
7	Complete the items in the following table or tables.	All the items completed. Expectations satisfied.			

Item ID	Item	Minimum Expected Finding	Actual	Expectation Satisfied (Yes/No)	Initial/Date
1	Server Name	<ServerName>			
2	Operating System	Minimum AIX 5L Version 5.1			
3	CPU Type and QTY	Power 4 1.0 Minimum GHz, 2			
4	Harddrive Internal	18 GB Ultra 3 10K			
5	Network Adaptor	Minimum 1 Minimum 2 GB Ethernet SX			
6	RAM	Minimum 2 GB			

Comments:

Summary of Test Script Results		Test Outcome		Deviation Number (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Logical Partition Diagnostic Function Test Script

Objective: The objective of this test is to verify LPAR diagnostic functions.

Set Up: None.

Procedure:

<ServerName>

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
1	Clear the error log.	As root, run: `errclear 0`	Normal command execution.			
2	Enter the diagnostics routines Attach screen print.	As root, run: `diag` Press Enter to continue. Select **Advanced Diagnostics Routines**. Select **System Verification**. Press Enter to select **All Resources**. Press F7 to start the test.	The diagnostics shall complete with a `No trouble was found` message. Screen print attached.			
3	Exit the diagnostics screen.	Press F10.	Will exit the diagnostics screen.			

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
4	Clear the error log.	As root, run: `errclear 0`	Normal command execution.			
5	Enter the diagnostics routines. Attach screen print.	As root, run: `diag` Press Enter to continue. Select **Advanced Diagnostics Routines**. Select **System Verification**. Press Enter to select **All Resources**. Press F7 to start the test.	The diagnostics shall complete with a `No trouble was found` message. Screen print attached.			
6	Exit the diagnostics screen.	Press F10.	Will exit the diagnostics screen.			

<ServerName>

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
7	Clear the error log.	As root, run: `errclear 0`	Normal command execution.			
8	Enter the diagnostics routines. Attach screen print.	As root, run: `diag` Press Enter to continue. Select **Advanced Diagnostics Routines**. Select **System Verification.** Press Enter to select **All Resources**. Press F7 to start the test.	The diagnostics shall complete with a `No trouble was found` message. Screen print attached.			
9	Exit the diagnostics screen.	Press F10.	Will exit the diagnostics screen.			

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
10	Clear the error log.	As root, run: `errclear 0`	Normal command execution.			
11	Enter the diagnostics routines. Attach screen print.	As root, run: `diag` Press Enter to continue. Select **Advanced Diagnostics Routines**. Select **System Verification**. Press Enter to select **All Resources**. Press F7 to start the test.	The diagnostics shall complete with a `No trouble was found` message. Screen print attached.			
12	Exit the diagnostics screen.	Press F10.	Will exit the diagnostics screen.			

<ServerName>

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
13	Clear the error log.	As root, run: `errclear 0`	Normal command execution.			
14	Enter the diagnostics routines. Attach screen print.	As root, run: `diag` Press Enter to continue. Select **Advanced Diagnostics Routines**. Select **System Verification**. Press Enter to select **All Resources**. Press F7 to start the test.	The diagnostics shall complete with a `No trouble was found` message. Screen print attached.			
15	Exit the diagnostics screen.	Press F10.	Will exit the diagnostics screen.			

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
16	Clear the error log.	As root, run: `errclear 0`	Normal command execution.			
17	Enter the diagnostics routines. Attach screen print.	As root, run: `diag` Press Enter to continue. Select **Advanced Diagnostics Routines**. Select **System Verification**. Press Enter to select **All Resources.** Press F7 to start the test.	The diagnostics shall complete with a `No trouble was found` message. Screen print attached.			
18	Exit the diagnostics screen.	Press F10.	Will exit the diagnostics screen.			

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
19	Clear the error log.	As root, run: `errclear 0`	Normal command execution.			
20	Enter the diagnostics routines. Attach screen print.	As root, run: `diag` Press Enter to continue. Select **Advanced Diagnostics Routines**. Select **System Verification**. Press Enter to select **All Resources**. Press F7 to start the test.	The diagnostics shall complete with a `No trouble was found` message. Screen print attached.			
21	Exit the diagnostics screen.	Press F10.	Will exit the diagnostics screen.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Error Reporting Function Test Script

Objective: The objective of this test is to verify the error reporting function.

Set Up: N/A.

Procedure:

<ServerName>

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
1	Place an entry into the AIX Error Log.	As root, run: `errlogger “Test error message”`	Normal command execution.			

2	Verify that the error was placed into the AIX Error Log.
	Attach screen print.
		Run:
		`errpt –a | head -24`
			A normal AIX error log entry shall exist that includes the following properties:
			`LABEL: OPMSG`
			`Date/Time: [shall reflect current system time]`
			`Node Id: [shall reflect server name]`
			`Detailed Data: MESSAGE FROM ERRORLOGGER COMMAND`
			`Test error message`
			Screen print attached.			

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
3	Place an entry into the AIX Error Log.	As root, run: `errlogger “Test error message”`	Normal command execution.			

4	Verify that the error was placed into the AIX Error Log.
	Attach screen print.
		Run:
		`errpt –a | head -24`
			A normal AIX error log entry shall exist that includes the following properties:
			`LABEL:   OPMSG`
			`Date/Time: [shall reflect current system time]`
			`Node Id:   [shall reflect server name]`
			`Detailed Data: MESSAGE FROM ERRORLOGGER COMMAND`
			`Test error message`
			Screen print attached.			

<ServerName>

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
5	Place an entry into the AIX Error Log.	As root, run: `errlogger “Test error message”`	Normal command execution.			

6	Verify that the error was placed into the AIX Error Log.
	Attach screen print.
		Run:
		`errpt –a | head -24`
			A normal AIX error log entry shall exist that includes the following properties:
			`LABEL:   OPMSG`
			`Date/Time: [shall reflect current system time]`
			`Node Id:   [shall reflect server name]`
			`Detailed Data: MESSAGE FROM ERRORLOGGER COMMAND`
			`Test error message`
			Screen print attached.			

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
7	Place an entry into the AIX Error Log.	As root, run: `errlogger “Test error message”`	Normal command execution.			

8	Verify that the error was placed into the AIX Error Log.
	Attach screen print.
		Run:
		`errpt –a | head -24`
			A normal AIX error log entry shall exist that includes the following properties:
			`LABEL:   OPMSG`
			`Date/Time: [shall reflect current system time]`
			`Node Id:   [shall reflect server name]`
			`Detailed Data: MESSAGE FROM ERRORLOGGER COMMAND`
			`Test error message`
			Screen print attached.			

<ServerName>

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
9	Place an entry into the AIX Error Log.	As root, run: `errlogger “Test error message”`	Normal command execution.			

10	Verify that the error was placed into the AIX Error Log.
	Attach screen print.
		Run:
		`errpt –a | head -24`
			A normal AIX error log entry shall exist that includes the following properties:
			`LABEL:   OPMSG`
			`Date/Time: [shall reflect current system time]`
			`Node Id:   [shall reflect server name]`
			`Detailed Data: MESSAGE FROM ERRORLOGGER COMMAND`
			`Test error message`
			Screen print attached.			

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
11	Place an entry into the AIX Error Log.	As root, run: `errlogger “Test error message”`	Normal command execution.			

12	Verify that the error was placed into the AIX Error Log.
	Attach screen print.
		Run:
		`errpt –a │ head -24`
			A normal AIX error log entry shall exist that includes the following properties:
			`LABEL:   OPMSG`
			`Date/Time: [shall reflect current system time]`
			`Node Id:   [shall reflect server name]`
			`Detailed Data: MESSAGE FROM ERRORLOGGER COMMAND`
			`Test error message`
			Screen print attached.			

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
13	Place an entry into the AIX Error Log.	As root, run: `errlogger “Test error message”`	Normal command execution.			

14	Verify that the error was placed into the AIX Error Log.
	Attach screen print.
		Run:
		`errpt –a | head -24`
			A normal AIX error log entry shall exist that includes the following properties:
			`LABEL:   OPMSG`
			`Date/Time: [shall reflect current system time]`
			`Node Id:   [shall reflect server name]`
			`Detailed Data: MESSAGE FROM ERRORLOGGER COMMAND`
			`Test error message`
			Screen print attached.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

LTO Library Connectivity Test Script

Objective: The objective of this test is to verify that the LTO library connectivity is functional.

Set Up: None

Procedure:

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
1	Verify LTO/TSM Server Connectivity.	From the TSM server, run, as root: `lsdev –Cc tape	grep FCP` Attach screen print.	The output shall include: 7 rmt devices and one smc device that show as `Available`. Screen print attached.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

ESS Network Connectivity Test Script

Objective: The objective of this test is to verify the ESS network connectivity function.

Set Up: None

Procedure:

Step ID	**Step**	**Action**	**Expected Results**	**Actual**	**Expectation Satisfied (Yes/No)**	**Initials/Date**
1	Verify the Network Connectivity for ESS.	From a command line on a PC connected to the corporate LAN, verify the network connectivity by running: `ping –n 1 Other<ServerName>` Attach screen print.	All three pings shall be successful. Screen print attached.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

High Availability Cluster Multi-Processing Function Test Script

Objective: The objective of this test is to verify the High Availability Cluster Multi-Processing function.

Set Up: None

Procedure:

<ServerName>

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
1	Verify that the minimum filesets are installed.	On the AIX command line, as root, run:· `lslpp -l cluster` Attach screen print.	Installed fileset returned. Screen print attached.			

<ServerName>

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
2	Verify that the minimum filesets are installed.	On the AIX command line, as root, run: `lslpp -l cluster` Attach screen print.	Installed fileset returned. Screen print attached.			

<ServerName>

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
3	Verify that the minimum filesets are installed.	On the AIX command line, as root, run: `lslpp –l cluster` Attach screen print.	Installed fileset returned. Screen print attached.			

<ServerName>

Step ID	Step	Action	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
4	Verify that the minimum filesets are installed.	On the AIX command line, as root, run: `lslpp –l cluster` Attach screen print.	Installed fileset returned. Screen print attached.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Network Connectivity Test Script

Objective: The objective of this test is to verify network connectivity.

Set Up: None

Procedure:

<ServerName>

Step ID	Step	Expected Results	Actual	Expectation Satisfied (Yes/No)	Initials/Date
1	Determine the PC's IP address by running: `ipconfig`	Record the IP address in the results column.	________________ IP of the machine from which the test is run.		
2	Run a ping test from a PC on the corporate LAN. From a command line, execute: `ping –n Other<ServerName>` Attach screen print of ping result for each.	All pings shall be successful. Screen print attached.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

IBM Service Agent Test Script

Objective: This test will indicate if the IBM Service Agent is installed and functioning properly. The IBM Service Agent is a utility that allows hardware errors to be automatically sent to IBM and local administrators for immediate attention. There are two parts to the Service Agent infrastructure. There are clients and the gateway server. It is the gateway server's responsibility to forward any hardware errors to IBM. This test has to be run from the HMC.

Set Up: None

Procedure:

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Access the Service Agent interface from the Hardware Management Console (HMC).	From the HMC: Login. Expand the HMC hostname folder. Expand the Service Application folder. Select **Service Agent**. Select **Service Agent UI**. Enter password.	The Service Agent Graphical User Interface is launched.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
2	Send a test PMR to IBM.	From the graphical interface: Expand the Test tool folder. In the Test Tools folder, click **TestPMR**. Select any installed machine and click **Generate** to create and send a test PMR to the IBM Service Agent Server. Select **OK** to verify the message. Reply Yes to the prompt of whether to connect to IBM now or later. Click **OK** to clear message.	A call attempt is started.			
3	Monitor the call as it is being executed.	Select the CallLog property to monitor the TestPMR progress for success or failure. Attach screen print.	The description field will indicate a successful call to IBM.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Service Action Event Log Test Script

Objective: The following test scripts access the service action event log.

Set Up: None

Procedure:

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Access the feature from the Hardware Management Console (HMC).	From the HMC: Login. Expand the HMC's hostname folder. Expand **Service Applications**. In the Navigation area, select the **Service Focal Point** icon. In the contents area, click **Select Serviceable Events**.	Access to the Service Action Event Log is granted.			
2	Open the Serviceable Event Log.	Select **OK** to search the log using the default criteria. Attach screen print.	The Serviceable Event Overview window will open.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Processor De-allocation Test Script

Objective: The following script will verify that the processor de-allocation feature is enabled. If the feature is enabled, the script will continue to attempt to de-allocate a processor. In addition, the final step of this procedure is to reboot the server or LPAR to re-enable the CPU.

Set Up: None

Procedure:

<ServerName>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Verify processor de-allocation is enabled on the partition.	Logon to <ServerName>. As root, from the command line, run: `lsattr -E -l sys0 |grep cpuguard` Attach screen print.	The resulting output will indicate that cpuguard is enabled.			
2	List all available processors.	As root, from the command line, run: `lsdev -Cc processor |grep Available` List the processors below (for example, proc3): 1)_____ 2)______ 3)______ 4)______ 5)______ 6)______ 7)______ 8)______	All processors are listed.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
3	Verify the status of all installed processors.	For each processor listed in the previous step, run **`lsattr –E –l <proc name>`** (as listed in step #3) and verify that the state is enabled. Attach screen print.	Each processor will indicate its state as enabled.			
4	Disable a processor.	Only continue if the previous command indicated at least three enabled processors. As root, run **`cpu_deallocate 1`** (This will disable the second CPU).	The command executes normally. (Note: If this process fails, it may be due to a running process being bound to the processor. If a failure of this command occurs, stop ALL running non-operating system processes and retry.)			
5	Verify that the CPU is disabled.	Wait for one minute and run **`lsattr –E –l <proc name>`** (where proc name matches the name recorded in field 2 of step #2). Attach screen print.	Processor state is disabled.			
6	Re-enable the CPU.	Reboot the server: `shutdown –Fr`	Server reboots normally.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
7	List all available processors.	As root, from the command line, run: `lsdev –Cc processor │grep Available` List the processors below (for example, proc3): 1)______ 2)______ 3)______ 4)______ 5)______ 6)______ 7)______ 8)______	All processors are listed.			
8	Verify that the status of all the installed processors is enabled.	For each processor listed in the previous step, run **`lsattr –E –l <proc name>`** (as listed in step #3). Attach screen print.	Each processor will indicate its state as enabled.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
9	Verify processor de-allocation is enabled on the partition.	Logon to <ServerName>. As root, from the command line, run: `lsattr –E –l sys0 |grep cpuguard` Attach screen print.	The resulting output will indicate that cpuguard is enabled.			
10	List all available processors.	As root from the command line run: `lsdev –Cc processor |grep Available` List the processors below (for example, proc3): 1)______ 2)______ 3)______ 4)______	All processors are listed.			
11	Verify the status of all installed processors.	For each processor listed in the previous step, run **`lsattr –E –l <proc name>`** (as listed in step #3) and verify that the state is enabled. Attach screen print.	Each processor will indicate its state as enabled.			
12	Disable a processor.	Only continue if the previous command indicated at least three enabled processors. As root, run **`cpu_deallocate 1`** (This will disable the second CPU).	The command executes normally. (Note: If this process fails, it may be due to a running process being bound to the processor. If a failure of this command occurs, stop ALL running non-operating system processes and retry.)			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
13	Verify that the CPU is disabled.	Wait for one minute and run **`lsattr –E –l <proc name>`** (where proc name matches the name recorded in field 2 of step #2). Attach screen print.	Processor state is disabled.			
14	Re-enable CPU.	Reboot the server: `shutdown –Fr`	Server reboots normally.			
15	List all available processors.	As root, from the command line, run: `lsdev –Cc processor |grep Available` List processors below (for example, proc3): 1)______ 2)______ 3)______ 4)______	All processors are listed.			
16	Verify the status of all installed processors is enabled.	For each processor listed in the previous step, run **`lsattr –E –l <proc name>`** (as listed in step #3). Attach screen print.	Each processor will indicate its state as enabled.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

LPAR Feature Set Test Script

Objective: This test script will prove some of the basic feature set included with an IBM @server pSeries server that has LPAR capabilities. These tests are administered from the Hardware Management Console (HMC). These tests will require halting and restarting a LPAR. It also assumes that the server is completely configured and is *not* running in full system partition mode, but in LPAR mode, with each of its LPARs booted using the normal profile.

Set Up: None

Procedure:

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Identify the partition that will be used for the test.	Identify a partition that can be utilized for this test. This LPAR will be shutdown and restarted twice in this test. Record the hostname and nickname (3 letter short name) in the results column. Partition Name: _______________ Partition Nickname: _______________	The partition name and partition nickname are identified.			
2	Logon to the HMC.	Access the HMC GUI (WebSM) as a valid user. The user will need administrator rights to complete this test script.	The GUI is displayed.			
3	Verify GUI.	In the navigation panel, expand the HMC's hostname section. In the navigation panel, expand the **Server and Partition** folder.	Additional selections are revealed.			
4	Verify connectivity to server.	In the navigation panel, select **Server Management**.	p670 systems are visible.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
5	Verify LPARs	Expand the systems in the contents panel to reveal the p670 frame. Expand the frames. Expand the partitions section to reveal all the partitions currently configured. Attach screen print.	All LPARs except the Full System Partition will show as running.			
6	Verify that the CD-ROM is available to assign to a partition for testing.	► Select the p670 system in the contents panel that includes the partition to which we will assign the CD-ROM. (either ServerName or ServerName). ► Record the system name in the results column. ► In the menu, click **Selected**. ► Select **Properties**. ► Select **I/O**. Attach screen print.	In the I/O properties window, verify that Slot_10/U1.9-P1-I10 is *not* assigned to a partition.			
7	Close the Properties Window.	Select **OK** to close the window.	The window is closed.			
8	Stop the partition to which the CD-ROM will be assigned.	Logon to the LPAR listed in step #1 as root and run: `shutdown -Fh` Attach screen print.	The LPAR will shutdown. The HMC GUI will show the LPAR as ready.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
9	Start the LPAR in SMS mode.	In the HMC GUI: In the contents panel, expand the LPAR selection for the LPAR identified in step #1. Select the SMS profile under the LPAR. From the menu, choose **Selected**. Choose **Activate**. From the Activation screen, verify that the SMS profile is selected, check the **Open Terminal** check box and select OK. Wait for the SMS menu to appear.	SMS menus become visible in the terminal window opened.			
10	Boot the operating system.	In the LPAR Terminal Window: From the initial SMS screen, enter `X`. Press 1 and Enter to exit the SMS menus.	After booting, a login prompt will appear in the terminal window.			
11	Verify the CD-ROM is available.	Log into the LPAR, and run: `lsdev -Cc cdrom` Attach screen print.	The output will show a CD-ROM as `Available`.			
12	Shutdown the LPAR to release the CD-ROM.	Log into the LPAR as root and run: `shutdown -Fh`	LPAR status of `Ready` is displayed in the GUI.			
13	Close the terminal window.	Close the terminal window.	The window is closed.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
14	Start the partition in normal mode.	Select the Normal profile under the LPAR identified in step #1. From the menu, choose **Selected**. Choose **Activate**. From the Activate Menu, verify the normal profile is selected, the open terminal window is *not* selected, and select OK.	The LPAR will boot without any errors.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Service Focal Point Test Script

Objective: Due to the nature of the shared hardware architecture of the p670, a new service called Service Focal Point acts as a filter and gateway for any hardware errors originating from a LPAR. It will avoid a single hardware failure on each LPAR. In addition, it allows for identification of hardware components. By testing this identification facility, it will verify connectivity and functionality.

Set Up: None

Procedure:

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Access the Service Focal Point GUI.	Access the HMC GUI: Logon using an administrative account. Expand the HMC’s hostname selection in the navigation panel. Expand the **Service Applications** folder in the navigations panel. Select **Service Focal Point**. Select the **Hardware Service Function** in the content panel.	The Hardware Service Management Overview window will be opened.			
2	Access the p670 hardware.	Select the managed system which you want to verify and document the system name: p670 Name _______________ Select the List FRUs button.	The FRU LED Management window will be opened.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
3	Test the LED feature.	Select **U1.9**. Select **Activate LED**.	On the p670, the main front indicator lights and indicator lights on the front of the U1.9 I/O drawer will be blinking.			
4	Turn off the LED.	Select **Deactivate LED**. Select **OK** to close the window.	LED will be turned off.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Network Time Protocol Test Script

Objective: For application and system reasons, it is vital to keep the system clocks in synchronization. The facility employed is the Network Time Protocol (NTP). The following will test connectivity to the time server.

Set Up: None

Procedure:

<ServerName1>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

1	Test connectivity to the NTP Server.	Logon as root and run:
		`ntpq –cpeers`
		Attach screen print.
			At least one server will be displayed. At least one server will have a * in the left margin. A sample output is:
			`*209.143.189.32 .GPS.`
			`1 u  202  512  377`
			`4.12   -0.372    0.12`			

<ServerName2>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

2	Test connectivity to the NTP Server.	Logon as root and run:
		`ntpq –cpeers`
		Attach screen print.
			At least one server will be displayed. At least one server will have a * in the left margin. A sample output is:
			`*209.143.189.32 .GPS.`
			`1 u  202  512  377`
			`4.12   -0.372    0.12`			

<ServerName3>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

3	Test connectivity to the NTP Server.	Logon as root and run:
		`ntpq –cpeers`
		Attach screen print.
			At least one server will be displayed. At least one server will have a * in the left margin. Sample output:
			`*209.143.189.32 .GPS.`
			`1 u  202  512  377`
			`4.12   -0.372    0.12`			

<ServerName4>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

4	Test connectivity to the NTP Server.	Logon as root and run:
		`ntpq –cpeers`
		Attach screen print.
			At least one server will be displayed. At least one server will have a * in the left margin. A sample output is:
			`*209.143.189.32 .GPS.`
			`1 u  202  512  377`
			`4.12   -0.372    0.12`			

<ServerName5>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

5	Test connectivity to the NTP Server.	Logon as root and run:
		`ntpq –cpeers`
		Attach screen print.
			At least one server will be displayed. At least one server will have a * in the left margin. A sample output is:
			`*209.143.189.32 .GPS.`
			`1 u  202  512  377`
			`4.12   -0.372    0.12`			

<ServerName6>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

6	Test connectivity to the NTP Server.	Logon as root and run:
		`ntpq –cpeers`
		Attach screen print.
			At least one server will be displayed. At least one server will have a * in the left margin. A sample output is:
			`*209.143.189.32 .GPS.`
			`1 u  202  512  377`
			`4.12   -0.372    0.12`			

<ServerName7>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

7	Test connectivity to the NTP Server.	Logon as root and run:
		`ntpq –cpeers`
		Attach screen print.
			At least one server will be displayed. At least one server will have a * in the left margin. A sample output is:
			`*209.143.189.32 .GPS.`
			`1 u  202  512  377`
			`4.12   -0.372    0.12`			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Fail-over Test Script

Objective: This test will verify that a fail-over process for the system is in place and operational.

Set Up: None

Procedure:

<ServerName> Cluster

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Verify Resource Group Location.	Logon to <ServerName> and run **`/usr/sbin/cluster/utilities/clRGinfo <cluster name>`** (to show that the application is online on <ServerName>). Attach screen print.	Shows resource group online on <ServerName>.			
2	Verify Service Address Location.	Run **`netstat -i`** (to show IP configuration). Attach screen print.	Verify that <ServerName>-svc is assigned to an adapter.			
3	Verify the volume groups are active.	Run **`lsvg -o`** (to show varied on volume groups). Attach screen print.	Verify all volumes groups are listed.			
4	Stop HACMP and force a takeover.	Run: `smit clstop` Verify that the Shutdown Mode is set to `takeover`. Press Enter to run.	The HACMP shutdown procedure starts.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
5	Verify failover.	Logon to the <ServerName> server. Monitor the /tmp/hacmp.out file during the fail-over process on the secondary server. After completion, run: `/usr/sbin/cluster/utilities/clRGinfo <cluster name>` Attach screen print.	The Resource Group will show as being online on the secondary server.			
6	Verify Service Address Location.	Run **`netstat -i`** (to show IP configuration). Attach screen print.	Verify that <ServerName>-svc is assigned to an adapter.			
7	Verify that the volume groups are active.	Run **`lsvg -o`** (to show varied on volume groups). Attach screen print.	Verify all volumes groups are listed.			
8	Fall back to the primary server.	Logon to <ServerName>. Run: `smit clstart` Press Enter to run.	HACMP Startup procedure starts.			
9	Verify fallback.	Logon to the <ServerName> server. Monitor the /tmp/hacmp.out file during the fallback process on the primary server. After completion, run: `/usr/sbin/cluster/utilities/clRGinfo <cluster name>` Attach screen print.	Resource Group will show online on primary server.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
10	Verify Service Address Location.	Run `netstat –i` (to show IP configuration). Attach screen print.	Verify that <ServerName>-svc is assigned to an adapter.			
11	Verify the volume groups are active.	Run `lsvg –o` (to show varied on volume groups). Attach screen print.	Verify that Oracle volumes groups are listed.			

Comments:

Summary of Test Script Results		Test Outcome		Deviation Number (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ______________________________________ Date: ________		
Test Reviewer:		Signature: ______________________________________ Date: ________		

SANPilot Test Script

Objective: SANPilot is the Web-based graphical interface used to administer the McData SAN switch. To test its functionality, we will show connectivity, monitoring capability, and configuration ability.

Set Up: None

Procedure:

<SwitchName>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Connect to SANPilot.	Access the switch via a Web browser: `http://<SwitchName>` Login using the Administrator account.	Access to the graphical interface is granted.			
2	Monitor the ports.	View the ports by: Select **Monitor**. Attach screen print.	The ports and status of the ports on the switch are displayed.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
3	Make a configuration change.	To unblock an inactive port: Select **Configure**. Uncheck the **Block** check box for one of the unused ports. Record the port #: Port # __________ Select **Activate**. Select **Monitor**. Attach screen print.	The port will show as being unblocked.			
4	Set the configuration change back.	To re-block the inactive port: Select **Configure**. Check the **Block** check box for one of the unused ports. Select **Activate**. Select **Monitor**. Attach screen print.	The port will show as being blocked.			

<SwitchName>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
5	Connect to SANPilot.	Access the switch via a Web browser: `http://<SwitchName>` Login using the Administrator account.	Access to the graphical interface is granted.			
6	Monitor the ports.	View the ports by: Select **Monitor**. Attach screen print.	The ports and status of the ports on the switch are displayed.			
7	Make a configuration change.	To unblock an inactive port: Select **Configure**. Uncheck the **Block** check box for one of the unused ports. Record the port #: Port # __________ Select **Activate**. Select **Monitor**. Attach screen print.	The port will show as being unblocked.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
8	Set the configuration change back.	To re-block the inactive port: Select **Configure**. Check the **Block** check box for one of the unused ports. Select **Activate**. Select **Monitor**. Attach screen print.	The port will show as being blocked.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Disk Storage Array Hot-swap Test Script

Objective: This test shall verify that a disk in the storage array can be swapped (hot swapping) when the system is running.

Set Up: None

Procedure:

<ServerName1>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Verify that the operating system is mirrored.	On the LPAR, run **`lspv | grep rootvg`** (should indicated four drives as part of rootvg) and **`lsvg –l rootvg`** (should show twice as many PPs and LPs and indicate syncd for all LVs except any sysdump devices). Attach screen print.	Commands will indicate that the OS mirrored.			
2	Identify the drive location.	Reference appropriate Information Services Technical Diagram (see installation-specific document) and locate drive 5M-08,8 in IBM @server p690 #2.	The drive is identified.			
3	Identify the AIX drive name.	Run **`lsdev -Ccdisk|grep 5M-08-00-8`** and record the drive name (for example, hdisk2): _____________	The command returns the drive name.			
4	Physically remove the drive from the system.	Remove the identified drive from the system.	The drive is removed.			
5	Verify system accessibility.	From the LPAR, run **`df`** to indicate access to the system and storage. Attach screen print.	The command will execute normally.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
6	Show broken mirrors.	From the LPAR, run: `lsvg –l rootvg` Attach screen print.	At a minimum, one LV will now indicate that it is stale.			
7	Reconnect the drive.	Reinsert and seat the removed drive.	The drive is installed.			
8	Reintegrate the drive.	Reconnect the drive and rebuild the mirrors. Run: `chpv –va <drive name recorded in step 3>`	The command will execute normally.			
9	Reboot the system.	Run: `shutdown –Fr`	The system will reboot.			
10	Resync the drives.	Run: `syncvg –v rootvg`	The command will execute normally.			
11	Verify mirrors.	Run **`lsvg –l rootvg`** to verify completion. Attach screen print.	All LVs will indicate syncd.			

<ServerName2>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
12	Verify that the operating system is mirrored.	On the LPAR, run **`lspv | grep rootvg`** (should indicated four drives as part of rootvg) and **`lsvg -l rootvg`** (should show twice as many PPs and LPs and indicate syncd for all LVs except any sysdump devices. Attach screen print.	The commands will indicate that the OS mirrored.			
13	Identify the drive location.	Reference appropriate Information Services Technical Diagram (see installation-specific document) and locate drive 4M-08,8 in IBM @server p690 #1.	The drive is identified.			
14	Identify AIX drive name.	Run **`lsdev -Ccdisk|grep 4M-08-00-8`** and record the drive name (for example, hdisk2): ______________	The command returned the drive name.			
15	Physically remove the drive from the system.	Remove the identified drive from the system.	The drive is removed.			
16	Verify the system accessibility.	From the LPAR, run **`df`** to indicate access to the system and storage. Attach screen print.	The command will execute normally.			
17	Show broken mirrors.	From the LPAR, run: `lsvg -l rootvg` Attach screen print.	At a minimum, one LV will now indicate that it is stale.			
18	Reconnect the drive.	Reinsert and seat the removed drive.	The drive is installed.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
19	Reintegrate the drive.	Reconnect the drive and rebuild the mirrors. Run: `chpv –va <drive name recorded in step 3>`	The command will execute normally.			
20	Reboot the system.	Run: `shutdown –Fr`	The system will reboot.			
21	Resync the drives.	Run: `syncvg –v rootvg`	The command will execute normally.			
22	Verify mirrors.	Run **`lsvg –l rootvg`** to verify completion. Attach screen print.	All LVs will indicate syncd.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Barcode Reader Test Script

Objective: The following test will verify that the barcode reader in the 3584 works correctly. This test will interrupt library operations and needs to be closely scheduled with the TSM administrator.

Set Up: None

Procedure:

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Successfully perform a library inventory.	From the tape library's panel: Press **Menu**. Press Up or Down to highlight **Manual Operations**. Press Enter. Press Up or Down to highlight **Inventory**. Press Enter. Press Up or Down to highlight **Inventory Library**. Press Enter. Press Enter at the warning screen.	After completion, the display will show `Inventory Complete`.			
2	Return the library to its normal state.	On the panel: Press Enter to return to the Manual Operations menu Press Back until you return to the Activity screen.	The Activity screen is displayed.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

LTO Auto-clean Test Script

Objective: The following test will verify that the LTO library is configured and using the Auto-Clean feature.

Set Up: None

Procedure:

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Verify that AutoClean is enabled.	From the LTO's operator panel: Press **Menu**. Press the Up or Down keys to select Settings. Select Enter. Press the Up or Down keys to select **Cleaning Mode**. Select Enter. Verify the feature is **Enabled**.	The feature is enabled. The display will read: `AutoClean is ENABLED`			
2	Return to the main screen.	From the operator panel: Press Back until you return to the Activity screen.	The Activity screen is displayed.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
3	Verify that the cleaning tape has been used.	From the operator panel: Press Menu. Press Up or Down to highlight **Usage Statistics**. Press Enter. Press Up or Down to highlight **Cleaning Cartridge Usage**. Press Enter. Record cleaning cartridge and usage. ______________ ______________ ______________ ______________	At least one tape has a usage count greater than zero.			
4	Return to THE main screen	From the operator panel: Press Back until you return to the Activity screen.	The Activity screen is displayed.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ______________________ Date: ________		
Test Reviewer:		Signature: ______________________ Date: ________		

ESS Web Administration Test Script

Objective: The ESS is configured via a Web-based administrator interface; this test will show that this feature is available and functioning.

Set Up: None

Procedure:

<ESS ServerName>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Verify connectivity.	Access the interface via a browser: `http://<ESS ServerName>` (Accept any security alerts.) Select **ESS Specialist**. (Again, accept any security warnings and grant any authority requests.) Logon. (May be prompted to logon more than once.)	The administration interface is displayed.			
2	Verify the ability to monitor the ESS.	On the ESS Specialist Interface: Select **Storage Allocation**. Select **View All Storage**. Attach screen print.	LUN assignments are shown.			

<ESS ServerName>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
3	Verify connectivity.	Access the interface via a browser: `http://<ESS ServerName>` (Accept any security alerts.) Select **ESS Specialist**. (Again, accept any security warnings and grant any authority requests.) Logon. (May be prompted to logon more than once.)	The administration interface is displayed.			
4	Verify the ability to monitor the ESS.	On the ESS Specialist Interface: Select **Storage Allocation**. Select **View All Storage**. Attach screen print.	LUN assignments are shown.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

SDD Redundancy Test Script

Objective: The SDD handles any failures in the SAN fabric. It maintains multiple links between the server and the storage disks. In the case of a fiber link failure, a SAN switch failure, or a HBA failure, the SDD handles the redundancy.

Set Up: None

Procedure:

<ServerName>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

1	Verify that multiple paths exist and are functioning.	Logon to <ServerName> and run:
		`lspv |grep vpath | tail -1`
		This will select the last available vpath, which we will use for testing. Record the vpath name in the results column.vpath name: _______________
		From the command line, run:
		`datapath query device | grep <vpath name from previous>`
		Record the DEV# as the vpath ID that is associated with the vpath name.
		vpath ID: _______________
			The vpath name (for example, vpath33) and vpath ID (for example, 31) are recorded.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
2	Temporarily start the SDD daemon, if it not running.	Run **`startsrc –s sddsrv`** (may indicate the service is all ready running). Check the SDD by running: `lssrc –l sddsrv` Attach screen print.	The SDD service should show as being active.			
3	Verify that the mode is normal.	From the command line run: `datapath query device <vpath ID listed in results column>` Attach screen print.	The output will show multiple links to the disk space in Open or Close state.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
4	Determine WWN for one of the links.	From the same login session as root, run: `lscfg -v -l fcs#` Where # matches the number following fscsi in the first line under the Adapter/Hard Disk column from the previous step. For example, if the column contains fscsi0/hdisk91, use fcs0. Record the Network Address as WWN #1. WWN #1: ____________________ From the command line, run: `lscfg -v -l fcs#` Where # matches the other number following fscsi under the Adapter/Hard Disk column from the previous step. For example, if the column contains fscsi1/hdisk127, use fcs1. Record the Network Address as WWN #2. WWN #2: ____________________	Will return detailed adapter information. Make a note of both the Network Addresses.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
5	Identify the port.	Access the first switch via the Web-based interface. `http://<ServerName>` Logon as Administrator. Select **Monitor**. Select **Node List**. Find the port number that matches one of the WWN's recorded from step 4. Record the port number. Port Number: ________________	The port that is connected to the server is documented.			

6	Block the port.	From the switch interface:
		Select **Configure**.
		Check the **Block** check box for the port determined in step 5.
		Press **Activate**.
		From the AIX command line, run, as root:
		`cfgmgr –l <vpath name from step 1>`
		Wait two minutes and run:
		`datapath query device <vpath ID # from step 2>`
		Attach screen print.
			The output will show links in the DEAD or CLOSE_DEAD state.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
7	Verify access to storage.	From the AIX command line, run: `df –k` Attach screen print.	The command will execute normally.			
8	Unblock the port	From the switch interface: Select **Configure**. Uncheck the Block check box for the port determined in step 3. Press **Activate**. From the AIX command line as root: Wait for five minutes and run: `datapath query device <device ID # from step 1>` Attach screen print.	The output will show all the links in the OPEN or CLOSE state.			
9	Stop the SDD service.	Run: `stopsrc –s sddsrv`	The command should indicate that the service is stopped.			

<ServerName>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

10	Verify that multiple paths exist and are functioning.	Logon to <ServerName> and run:
		`lspv |grep vpath | tail -1`
		This will select the last available vpath, which we will use for testing. Record the vpath name in the results column:
		vpath name:
		________________
		From the command line, run:
		`datapath query device | grep <vpath name from previous>`
		Record the DEV# as the vpath ID that is associated with the vpath name.
		vpath ID:
		________________
			The vpath name (for example, vpath33) and vpath ID (for example, 31) are recorded.			

11	Temporarily start the SDD daemon if not running.	Run **`startsrc –s sddsrv`** (may indicate the service is all ready running). Check the SDD by running: `lssrc –l sddsrv` Attach screen print.	SDD service should show as active.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
12	Verify that the mode is normal.	From the command line, run: `datapath query device <vpath ID listed in results column>` Attach screen print.	The output will show multiple links to the disk space in OPEN or CLOSE state.			
13	Determine WWN for one of the links.	From the same login session as root, run: `lscfg –v –l fcs#` Where # matches the number following fscsi in the first line under the Adapter/Hard Disk column from the previous step. For example, if the column contains fscsi0/hdisk91, use fcs0. Record the Network Address as WWN #1. WWN #1: ______________________ From the command line, run: `lscfg –v –l fcs#` Where # matches the other number following fscsi under the Adapter/Hard Disk column from the previous step. For example, if the column contains fscsi1/hdisk127, use fcs1. Record the Network Address as WWN #2. WWN #1: ___________________	Will return detailed adapter information. Make a note of both the Network Addresses.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
14	Identify the port.	Access the first switch via the Web-based interface: `http://u<SwitchName>` Logon as Administrator. Select **Monitor**. Select **Node List**. Find the port number that matches one of the WWN’s recorded from step 4. Record the port number. Port Number: ________________	The port that is connected to the server is documented.			

15	Block the port.	From the switch interface:
		Select **Configure**.
		Check the **Block** check box for the port determined in step 5.
		Press **Activate**.
		From the AIX command line, run, as root:
		`cfgmgr –l <vpath name from step 1>`
		Wait two minutes and run:
		`datapath query device <vpath ID # from step 2>`
		Attach screen print.
			The output will show links in the DEAD or CLOSE_DEAD state.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
16	Verify access to storage.	From the AIX command line, run: `df –k` Attach screen print.	The command will execute normally.			
17	Unblock the port	From the switch interface: Select **Configure**. Uncheck the **Block** check box for the port determined in step 3. Press **Activate**. From the AIX command line as root: Wait for five minutes and run: `datapath query device <device ID # from step 1>` Attach screen print.	The output will show all the links in the OPEN or CLOSE state.			
18	Stop SDD service.	Run: `stopsrc –s sddsrv`	The command will indicate that the service is stopped.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

SDD Installation Test Script

Objective: The following script will determine that the SDD is installed and that multiple paths between the server and storage exist and are available.

Set Up: None

Procedure:

<ServerName1>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Validate that the SDD is installed.	From the AIX command line as root, run: `lslpp -l ibmSdd*` Attach screen print.	The output will show which flavor and version of the SDD is installed on the system.			
2	Verify multiple links on systems with SAN drives installed.	From the AIX command line as root, run: `datapath query adapter` Attach screen print.	For each adapter, the number of paths is equal.			

<ServerName2>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
3	Verify that the SDD is installed.	From the AIX command line, as root, run: `lslpp -l ibmSdd*` Attach screen print.	The output will show which flavor and version of the SDD is installed on the system.			
4	Verify multiple links on systems with SAN drives installed.	From the AIX command line, as root, run: `datapath query adapter` Attach screen print	For each adapter, the number of paths is equal.			

<ServerName3>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
5	Verify that the SDD is installed.	From the AIX command line, as root, run: `lslpp -l ibmSdd*` Attach screen print.	The output will show which flavor and version of the SDD is installed on the system.			
6	Verify multiple links on systems with SAN drives installed.	From the AIX command line, as root, run: `datapath query adapter` Attach screen print.	For each adapter, the number of paths is equal.			

<ServerName4>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
7	Verify that the SDD is installed.	From the AIX command line, as root, run: `lslpp -l ibmSdd*` Attach screen print.	The output will show which flavor and version of the SDD is installed on the system.			
8	Verify multiple links on systems with SAN drives installed.	From the AIX command line, as root, run: `datapath query adapter` Attach screen print.	For each adapter, the number of paths is equal.			

<ServerName5>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
9	Verify that the SDD is installed.	From the AIX command line, as root, run: `lslpp -l ibmSdd*` Attach screen print.	The output will show which flavor and version of the SDD is installed on the system.			
10	Verify multiple links on systems with SAN drives installed.	From the AIX command line, as root, run: `datapath query adapter` Attach screen print.	For each adapter, the number of paths is equal.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

Sysback/6000 Test Script

Objective: Sysback/6000 is a backup and restore facility that enhances the standard AIX facilities.

Set Up: None

Procedure:

<ServerName>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied Yes/No)	Initial/Date

1	Verify that the last sysback backup completed successfully.	From an AIX command line, as root, run:
		`/usr/sbin/sbalog –o`
		Attach screen print.
			The output will show the status of the last backup and the backup was completed successfully. For example:
			`Command: /usr/sbin/sysback -h<ServerName> -f/dev/rmt0 -x -T chrp -k mp`
			`Date: Wed Oct 23 12:55:16 PDT 2002`
			`Backup ended Wed Oct 23 13:01:58 PDT 2002`
			`SUCCESS: System backup completed successfully.`			

<ServerName1>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

2	Verify that the last sysback backup completed successfully.	From an AIX command line, as root, run:
		`/usr/sbin/sbalog –o`
		Attach screen print.
			The output will show the status of the last backup and the backup was completed successfully. For example:
			`Command: /usr/sbin/sysback -h<ServerName1> -f/dev/rmt0 -x -T chrp -k mp`
			`Date: Wed Oct 23 12:55:16 PDT 2002`
			`Backup ended Wed Oct 23 13:01:58 PDT 2002`
			`SUCCESS: System backup completed successfully.`			

<ServerName2>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

3	Verify that the last sysback backup completed successfully.	From an AIX command line, as root, run:
		`/usr/sbin/sbalog –o`
		Attach screen print.
			The output will show the status of the last backup and the backup was completed successfully. For example:
			`Command:`
			`/usr/sbin/sysback`
			`–h<ServerName2>`
			`-f/dev/rmt0 -x -T chrp`
			`-k mp`
			`Date: Wed Oct 23`
			`12:55:16 PDT 2002Backup`
			`ended Wed Oct 23`
			`13:01:58 PDT 2002`
			`SUCCESS: System backup`
			`completed successfully.`			

<ServerName3>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

4	Verify that the last sysback backup completed successfully.	From an AIX command line, as root, run:
		`/usr/sbin/sbalog –o`
		Attach screen print.
			The output will show the status of the last backup and the backup was completed successfully. For example:
			`Command: /usr/sbin/sysback -h<ServerName3> -f/dev/rmt0 -x -T chrp -k mp`
			`Date: Wed Oct 23 12:55:16 PDT 2002`
			`Backup ended Wed Oct 23 13:01:58 PDT 2002`
			`SUCCESS: System backup completed successfully.`			

<ServerName4>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

5	Verify that the last sysback backup completed successfully.	From an AIX command line, as root, run:
		`/usr/sbin/sbalog –o`
		Attach screen print.
			The output will show the status of the last backup and the backup was completed successfully. For example:
			`Command: /usr/sbin/sysback –h<ServerName4> -f/dev/rmt0 -x -T chrp -k mp`
			`Date: Wed Oct 23 12:55:16 PDT 2002`
			`Backup ended Wed Oct 23 13:01:58 PDT 2002`
			`SUCCESS: System backup completed successfully.`			

<ServerName5>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

6	Verify that the last sysback backup completed successfully.	From an AIX command line, as root, run:
		`/usr/sbin/sbalog –o`
		Attach screen print.
			The output will show the status of the last backup and the backup was completed successfully. For example:
			`Command: /usr/sbin/sysback -h<ServerName5> -f/dev/rmt0 -x -T chrp -k mp`
			`Date: Wed Oct 23 12:55:16 PDT 2002`
			`Backup ended Wed Oct 23 13:01:58 PDT 2002`
			`SUCCESS: System backup completed successfully.`			

<ServerName6>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

7	Verify that the last sysback backup completed successfully.	From an AIX command line, as root, run:
		`/usr/sbin/sbalog –o`
		Attach screen print.
			The output will show the status of the last backup and the backup was completed successfully. For example:
			`Command: /usr/sbin/sysback -h<ServerName6> -f/dev/rmt0 -x -T chrp -k mp`
			`Date: Wed Oct 23 12:55:16 PDT 2002`
			`Backup ended Wed Oct 23 13:01:58 PDT 2002`
			`SUCCESS: System backup completed successfully.`			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

TSM Service Manager Test Script

Objective: TSM is a centralized backup application. Clients connect via the network and backup files to the server. The server is responsible for placing the data on tape and maintaining versioning data. This test is from a client machine and proves basic backup and restore capability. It assumes the server being tested has been configured properly.

Set Up: None

Procedure:

<ServerName1>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

1	Backup a file to the TSM server.	From an AIX command line, as root, run:
		`cd /tmp`
		`cp /etc/profile testfile`
		`dsmc incr testfile`
			The file is successfully backed up.			

2	Remove the file.	From the command line, run: `rm testfile`	The file is removed successfully.			
3	Restore the file.	From the command line, run: `dsmc restore testfile` Attach screen print.	The file is restored correctly.			
4	Verify the file is the same.	From the command line, run: `diff /etc/profile testfile`	The command will show *no* output, verifying the restored file is the same as the original file.			

<ServerName2>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

5	Backup a file to the TSM server.	From an AIX command line, as root, run:
		`cd /tmp`
		`cp /etc/profile testfile`
		`dsmc incr testfile`
			The file is successfully backed up.			

6	Remove the file.	From the command line, run: `rm testfile`	The file is removed successfully.			
7	Restore the file.	From the command line, run: `dsmc restore testfile` Attach screen print.	The file is restored correctly.			
8	Verify the file is the same.	From the command line, run: `diff /etc/profile testfile`	The command will show *no* output, verifying the restored file is the same as the original file.			

<ServerName3>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

9	Backup a file to the TSM server.	From an AIX command line, as root, run:
		`cd /tmp`
		`cp /etc/profile testfile`
		`dsmc incr testfile`
			The file is successfully backed up.			

10	Remove the file.	From the command line, run: `rm testfile`	The file is removed successfully.			
11	Restore the file.	From the command line, run: `dsmc restore testfile` Attach screen print.	The file is restored correctly.			
12	Verify the file is the same.	From the command line, run: `diff /etc/profile testfile`	The command will show *no* output, verifying the restored file is the same as the original file.			

<ServerName4>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

13	Backup a file to the TSM server.	From an AIX command line, as root, run:
		`cd /tmp`
		`cp /etc/profile testfile`
		`dsmc incr testfile`
			The file is successfully backed up.			

14	Remove the file.	From the command line, run: `rm testfile`	The file is removed successfully.			
15	Restore the file.	From the command line, run: `dsmc restore testfile` Attach screen print.	The file is restored correctly.			
16	Verify the file is the same.	From the command line, run: `diff /etc/profile testfile`	The command will show *no* output, verifying the restored file is the same as the original file.			

<ServerName5>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

17	Backup a file to the TSM server.	From an AIX command line, as root, run:
		`cd /tmp`
		`cp /etc/profile testfile`
		`dsmc incr testfile`
			The file is successfully backed up.			

18	Remove the file.	From the command line, run: `rm testfile`	The file is removed successfully.			
19	Restore the file.	From the command line, run: `dsmc restore testfile` Attach screen print	The file is restored correctly.			
20	Verify the file is the same.	From the command line, run: `diff /etc/profile testfile`	The command will show *no* output, verifying the restored file is the same as the original file.			

<ServerName6>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

21	Backup a file to the TSM server.	From an AIX command line, as root, run:
		`cd /tmp`
		`cp /etc/profile testfile`
		`dsmc incr testfile`
			The file is successfully backed up.			

22	Remove the file.	From the command line, run: `rm testfile`	The file is removed successfully.			
23	Restore the file.	From the command line, run: `dsmc restore testfile` Attach screen print.	The file is restored correctly.			
24	Verify the file is the same.	From the command line, run: `diff /etc/profile testfile`	The command will show *no* output, verifying the restored file is the same as the original file.			

<ServerName7>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date

25	Backup a file to the TSM server.	From an AIX command line, as root, run:
		`cd /tmp`
		`cp /etc/profile testfile`
		`dsmc incr testfile`
			The file is successfully backed up.			

26	Remove the file.	From the command line, run: `rm testfile`	The file is removed successfully.			
27	Restore the file.	From the command line, run: `dsmc restore testfile` Attach screen print.	The file is restored correctly.			
28	Verify the file is the same.	From the command line, run: `diff /etc/profile testfile`	The command will show *no* output, verifying the restored file is the same as the original file.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:	Signature: ____ Date: ________			
Test Reviewer:	Signature: ____ Date: ________			

Logical Security Test Script

Objective: This test shall verify that access to system is restricted to authorized personnel only. This test shall also verify that a log of successful and failed access is captured in the system.

Set Up: None

Procedure:

<ServerName>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
1	Logon attempt as an invalid user.	From a command prompt on a network attached PC, run: `telnet <ServerName>` Login as invalid. Password as `guest`.	Login attempt fails.			
2	Logon with invalid password.	From a command prompt on a network attached PC, run: `telnet <ServerName>` Login as root. Password as `guest`.	Login attempt fails.			
3	Logon granted with valid login and password.	From a command prompt on a network attached PC, run: `telnet <ServerName>` Log onto <ServerName> as a valid user with administrator privileges.	Login attempt is successful.			

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
4	Login attempts are logged.	On <ServerName>, run: `who/etc/security/failedlogin | tail`	The command will show failed login attempts.			

<ServerName1>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
5	Logon attempt as an invalid user.	From a command prompt on a network attached PC, run: `telnet <ServerName1>` Login as invalid. Password as `guest`.	Login attempt fails.			
6	Logon with invalid password.	From a command prompt on a network attached PC, run: `telnet <ServerName1>` Login as root. Password as `guest`.	Login attempt fails.			
7	Logon granted with valid login and password.	From a command prompt on a network attached PC, run: `telnet <ServerName1>` Log onto <ServerName1> as a valid user with administrator privileges.	Login attempt is successful.			
8	Login attempts are logged.	On <ServerName1>, run: `who /etc/security/failedlogin | tail`	The command will show failed login attempts.			

<ServerName2>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
9	Logon attempt as an invalid user.	From a command prompt on a network attached PC, run: `telnet <ServerName2>` Login as invalid. Password as `guest`.	Login attempt fails.			
10	Logon with invalid password.	From a command prompt on a network attached PC, run: `telnet <ServerName2>` Login as root. Password as `guest`.	Login attempt fails.			
11	Logon granted with valid login and password.	From a command prompt on a network attached PC, run: `telnet <ServerName2>` Log onto <ServerName2> as a valid user with administrator privileges.	Login attempt is successful.			
12	Login attempts are logged.	On <ServerName2>, run: `who /etc/security/failedlogin | tail`	The command will show failed login attempts.			

<ServerName3>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
13	Logon attempt as an invalid user.	From a command prompt on a network attached PC, run: `telnet <ServerName3>` Login as invalid. Password as guest.	Login attempt fails.			
14	Logon with invalid password.	From a command prompt on a network attached PC, run: `telnet <ServerName3>` Login as root. Password as `guest`.	Login attempt fails.			
15	Logon granted with valid login and password.	From a command prompt on a network attached PC, run: `telnet <ServerName3>` Log onto <ServerName3> as a valid user with administrator privileges.	Login attempt is successful.			
16	Login attempts are logged.	On <ServerName3>, run: `who /etc/security/failedlogin | tail`	The command will show failed login attempts.			

<ServerName4>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
17	Logon attempt as an invalid user.	From a command prompt on a network attached PC, run: `telnet <ServerName4>` Login as invalid. Password as `guest`.	Login attempt fails.			
18	Logon with invalid password.	From a command prompt on a network attached PC, run: `telnet <ServerName4>` Login as root. Password as `guest`.	Login attempt fails.			
19	Logon granted with valid login and password.	From a command prompt on a network attached PC, run: `telnet <ServerName4>` Log onto <ServerName4> as a valid user with administrator privileges.	Login attempt is successful.			
20	Login attempts are logged.	On <ServerName4>, run: `who /etc/security/failedlogin | tail`	The command will show failed login attempts.			

<ServerName5>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
21	Logon attempt as an invalid user.	From a command prompt on a network attached PC, run: `telnet <ServerName5>` Login as invalid. Password as `guest`.	Login attempt fails.			
22	Logon with invalid password.	From a command prompt on a network attached PC, run: `telnet <ServerName5>` Login as root. Password as guest.	Login attempt fails.			
23	Logon granted with valid login and password.	From a command prompt on a network attached PC, run: `telnet <ServerName5>` Log onto <ServerName5> as a valid user with administrator privileges.	Login attempt is successful.			
24	Login attempts are logged.	On <ServerName5>, run: `who /etc/security/failedlogin | tail`	The command will show failed login attempts.			

<ServerName6>

No.	Description	Steps	Expected Results	Actual Result	Expectations Satisfied (Yes/No)	Initial/Date
25	Logon attempt as an invalid user.	From a command prompt on a network attached PC, run: `telnet <ServerName6>` Login as invalid. Password as `guest`.	Login attempt fails.			
26	Logon with invalid password.	From a command prompt on a network attached PC, run: `telnet <ServerName6>` Login as root. Password as `guest`.	Login attempt fails.			
27	Logon granted with valid login and password.	From a command prompt on a network attached PC, run: `telnet <ServerName6>` Log onto <ServerName6> as a valid user with administrator privileges.	Login attempt is successful.			
28	Login attempts are logged.	On <ServerName6>, run: `who /etc/security/failedlogin | tail`	The command will show failed login attempts.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

E

Installation Team Training/Qualifications Matrix

The individuals who install or verify the system infrastructure must be qualified to perform their assigned responsibilities. Qualification can be established with either previous training and experience, or by training provided in support of the installation project, prior to the execution of assigned tasks.

The purpose of the Training/Qualifications Matrix is to identify the required capabilities for each role in the installation and verification process, as a guide to the required accumulation of training and qualification records that provide evidence of adequate qualifications (or expertise) for each person involved.

The Matrix is organized by major activities in the Installation and Verification activities, and identifies the roles applicable for each task, and the required qualifications. Persons assigned to those tasks are identified. Records that support the Training/Qualifications or the persons assigned are attached to the Matrix, and will consist of either of the following:

- Qualification Certificates

  When a person's qualification consists of a Certificate of Qualification, the supporting documentation must be a copy of the certificate, containing the person's name, certificate title and issuing organization, and issue date.

- Training Record

  When training for the task was supplied either as part of the project, or through other site programs, a copy of the training record will supply qualification evidence. The form of the training record can either follow that presented in Appendix H, “Training/qualifications record” on page 207, or an equivalent local form that identifies at least the following:

  - Person’s Name
  - Name of Document/Task training was completed for
  - Date of training
  - Dated Signature of Qualified Trainer

- Prior Experience

  When a person has adequate prior experience that provides the equivalent capabilities of a Qualification certificate or project/site training classes, a copy of the person's resume may be used as the Qualification Record. The resume will be attached to the Resume Equivalency form presented in Appendix S, “Regulation, guidance, and standards cross references” on page 259, which is noted with the Qualification requirements evidenced by the resume, and must be signed by the either the project manager or other site technical manager, and quality representative.

The names of the persons assigned to each task are added to the matrix. When the Qualifications or training is verified as present or completed for each person, the documents are attached to the matrix (training record form, certificate, or equivalency form with resume). The person who verifies that requirements are met signs and dates the verification documents. The Quality Representative will review the completed matrix, and approve with a dated signature.

Qualifications/Training Matrix

Role	Task	Qualification/Training Requirement	Task Assignment	Verified by/date
Installation/ Verification	Install/Verify IBM @server p690 Server Install/Verify IBM TotalStorage Storage Install/Verify McData Switches Install/Verify Tape Library Install/Verify AIX O/S Install/Verify Tivoli (TSM) Install/Verify HACMP	IBM CE (Customer Engineer), plus written qualification memo from IBM		
IQ Protocol	Infrastructure Verification Infrastructure Functional Verification	Installer's Qualification (per above) General Regulatory Training/21CFR11 Basics Good Documentation Practices Installation Qualification Plan Test Script Execution Procedure Testing Deviation Procedure		
	Environment Verification Documentation Verification	General Regulatory Training/21CFR11 Basics Good Documentation Practices Installation Qualification Plan Test Script Execution Procedure Testing Deviation Procedure		
Plan/Report Completion	Risk Assessment	General Regulatory Training/21CFR11 Basics Good Documentation Practices Validation Plan		
	Trace Matrix	General Regulatory Training/21CFR11 Basics		
	Procedures Verification	General Regulatory Training/21CFR11 Basics Good Documentation Practices Validation Plan		
	Protocol ReportPlan Report	General Regulatory Training/21CFR11 Basics Good Documentation Practices Validation Plan Installation Qualification Plan Test Script Execution Procedure Testing Deviation Procedure		

Approved by: ______________________________________ Date ______________

Instructions

The Training Matrix form is used to document Qualifications/Training requirements and verify that persons assigned have met those requirements for each task.

The form is completed as follows:

Task Assignment — The name of the person or persons who are assigned by the project manager or designee for each task indicated.

Verified by/Date — The signature of the person who verifies and attaches Qualification/Training records that demonstrate the assigned person has met the requirements. The verifier must attached the supporting documents to the Matrix (Certificate, Training Record, or Equivalency form with resume).

The Quality Representative will review the Training Matrix for completeness and accuracy, and will approve the completed Matrix.

F

General regulatory and 21CFR11 training

This appendix describes the general regulatory and 21 CFR11 training.

Training course goals

Persons who perform tasks that are part of the validation process should have, in addition to the specific technical training and/or qualifications that apply to their assigned tasks, an understanding of the Quality/Regulatory environment within which they are operating. This awareness provides an appreciation of the reasons for the controlled processes and the exacting documentation requirements, which in turn, helps enhance their compliance with the detailed procedures and record keeping required in a Life Sciences environment.

Note that this course is not meant to be an exhaustive review or analysis of the regulations or what is needed to comply with them. Legal counsel should be consulted to help answer any questions.

Training course contents and approach

This course has two sections that should be taken in sequence. Each course consists of a set of topics that the Trainer will review with the Trainee, with a short narrative provided for each topic. The Trainer will elaborate on each topic as required, depending on the Trainee's prior background and/or questions.

Topic 1: General quality system and regulatory training

This section provides a general introduction to the Quality/Regulatory environment, which creates the fundamental reasons for controlled processes, documented evidence of compliance, and the implications of inspections by governing bodies.

1. **Purpose and value of a Quality System**

   Products produced by a Life Sciences company are used for the diagnosis, treatment, or prevention of disease or medical conditions. As a result, there is a risk to human health if defects in the product exist due to either product design or errors in the production methods. A Quality System is a methodology used by an organization to assure the highest possible quality in its products by:

   - Designing and proving the methods for its operations
   - Describing those methods in detailed procedures
   - Controlling the processes to assure complete compliance to those procedures
   - Structuring the organization staffing, roles, and responsibilities to manage quality into the processes, so that all specifications and requirements are always met

   Quality systems are described in an organized set of documents, starting from a high level set of quality policies that then link down to the specific procedures and organizational roles and responsibilities for carrying out the described tasks.

2. **Functions of a Quality Organization**

   A key requirement of a Quality System is to have a separate group within each organization that is focused entirely on developing and maintaining quality controls over defined processes, assuring that every cycle of activity or batch of product meets defined specifications and procedural requirements.

   This Quality function is involved in the design of processes and development of procedures, monitors process execution, and evaluates (or tests) outcomes to assure adherence to the specifications.

As a result, the Quality Representative is required to review all procedures, plans, and protocols, for adequacy of controls and verification of requirements. The execution of the processes described must be verified by a Quality Representative, who must also review and approve the collected data records. For this reason, all documents must be approved by the designate Quality Representative or Representatives to the system, and their signature constitutes the finalization of the document.

3. **Procedures to control processes/tasks**

   Every process that has a quality impact upon the products, or relates to any FDA regulation, must be adequately described in a written procedure and approved by a Quality Representative. The organization (structure and format) of the procedures is set by a standardized method for the company that also prescribes the process to be followed for review and approval.

   Procedures must be controlled, meaning changes cannot be made unless a new version is created, and approved by the same level of authority that approved the original version. When fully approved, the new version will override the previous version, on the date that the new version becomes effective.

   Each company has a process, called Controlled Document Management, to assure that suggested revisions to any document/procedure flows through a defined set of reviewers and approvers that include both the technical expertise and Quality Representative. The approved procedures are then distributed as required to various users, and returned and superseded when overridden with a new version. This process is designed to provide the highest possible assurance that the approved and current procedures exist for any quality/regulated process in the company.

4. **Procedure compliance and verification**

   Having detailed procedures that contain quality assuring tasks are of little value if the procedures are not followed every time. Thus, the company must have assurance that all of the required procedures for any process are followed every single time the process is executed. This will require a combination of:

   - Training the persons who perform the process in the procedures
   - Supervising the process execution to assure procedure compliance
   - Promptly identifying and resolving exceptions that may occur

   Training programs must exist for every work area, as the staff must be trained on all procedures that apply to their assigned tasks. Periodic retraining, and training updates when a procedure is revised, are part of the overall training program.

   Adequate supervision means having the availability and attention of managerial and/or technical personnel to support the processes and immediately address any problems that surface during procedure execution. Any exceptions or deviations from procedure require prompt investigation and resolution, with corrective and preventative actions taken that will assure non-reoccurrence of the problem.

5. **Purpose and value of qualification of equipment/systems**

   In addition to using written procedures, the equipment, instruments, and computer systems that are used in any procedure must be assured to function exactly as they were designed, or even the proper actions will not assure a correct outcome. This means that complete testing of the functioning of any tools used in the procedure must have been done prior to use to assure the actual operations (according to the procedures) will always yield the designed results.

This pre-use testing process is called *qualification*. The qualification goal is to define the requirements and structure of the equipment (infrastructure) or system, then conduct a set of carefully controlled tests that will prove the equipment/system will function as expected when used in accordance with the procedures. Qualification requires explicit documentation of the design and expected results, and then testing runs with detailed records that can be compared to the expected results to prove the design.

6. **Records to evidence specification/procedure compliance**

   The steps enumerated above that are part of the company quality system are documented in written form, and will provide the specifications and procedures for the execution of each process. However, each time the described process is executed, records of the process outcomes must also be generated as evidence that the cycle was always under control and yielded the expected results. These records are reviewed by the Quality function, and when approved, the cycle can be considered complete. The reviewed records must be retained for possible review by FDA inspectors evaluating if the records prove the process was acceptable, indicating the operations are compliant to the requirements of the regulations.

7. **21CFR Regulations that apply to Life Sciences**

   The Food, Drug, and Cosmetics laws (FD&C acts) were enacted to protect the public from dangerous, defective, or ineffective drugs and/or medical devices. The FDA has established a series of regulations controlling how medical products are developed, approved, manufactured, marketed, and supported by the Life Sciences industry. These are found in Title 21 of the Code of Federal Regulations (CFR).

   Virtually every aspect of the company operations that relate to its products (other than very early stage research or financial transactions) is covered by FDA regulations. The most common regulations that affect areas where IT systems are used are:

   – **21CFR50**, **21CFR54**, and **21 CFR56**: Good Clinical Practices (GCPs) that cover the conduct of clinical trials of new drugs or medical devices to prove they are safe and effective.

   – **21CFR211** and **21CFR820**: Good Manufacturing Practices (GMPs) that set requirements for the manufacturing and qualify verification activities to produce drug/device products.

   – **21CFR58**: Good Laboratory Practices (GLPs) that set requirements for laboratory testing processes.

   These regulations have specific requirements for each area of operation, and broad general requirements around the principles of Quality systems previously covered. Any violation of these standards becomes a violation of the applicable US statutes the regulation supports. In addition, there are regulations for other areas, such as Blood Products, Tissue Products, Food, and Cosmetics, to name a few.

8. **US FDA enforcement of regulations**

   The Food and Drug Administration (FDA) is the federal law enforcement agency with the responsibility for carrying out Federal Government duties assigned to it by laws (and the supporting regulations) and assuring that companies, including Life Sciences companies, comply with the laws.

   The FDA includes several departments, or bureaus, each with a different role in law enforcement and regulation compliance. Some departments are responsible for reviewing and approving applications by companies for approval to market new drugs and medical devices. Other departments conduct field investigations (inspections or audits) of Life Sciences companies operations, to determine their compliance to 21CFR regulations.

   Legal actions will be initiated against companies that do not comply with the regulations. Penalties may include product seizure, injunctions, or even criminal prosecution.

9. **FDA inspections and their implications to the business**

   FDA auditors may visit each company site where product manufacturing takes place at any time or for special reasons. The inspector may request detailed information on, and can evaluate the processes, equipment, procedures, organization, systems, and data records.

   FDA inspectors focus heavily on the documentation and records kept by the company. Since the inspector only infrequently visits the site, and often attempts to understand the processes that are taking place over considerable periods of time between audits, analyzing the documentation and data collected by the company provides considerable insight not obtainable from just listening to the answers provided to auditor questions. The inspector expects to see evidence of the quality processes in the form of procedures and records, which provide evidence that the procedures are followed.

   Issues that the inspector believes are a concern for the quality of the company products, or its compliance to the 21CFR regulations, are described in a Federal Document form FDA-483, which the inspector provides to the site management at the conclusion of the audit. Site management will often respond to the FDA-483 with either an explanation/rebuttal or commitment to take corrective action. If the FDA district office is unsatisfied with the company response or with completion of the committed actions, they may chose to convert the FDA-483 into a formal warning to the company chief executive, indicating further actions will be taken unless prompt and acceptable company action is taken to resolve the issue or issues documented in the warning.

21 CFR 11 training (electronic records and electronic signatures)

This section provides a general introduction to the specific FDA regulation governing the use of computer systems that contain electronic records and/or signatures. For reference, each Trainee should be provided a copy of 21CFR11, with the explanation that the actual rule contents begin on page 13464, column 3. The comments on the prior pages (13430 to 13464), are explanatory statements by the FDA.

1. **Applicability of the regulation to computer systems**

   The regulation applies to computer systems that create, modify, maintain archive, or transmit records (data or signatures, except faxes) that either:

   a. Must be submitted to the FDA, such as data from clinical trials of a new drug or medical device.

      or

   b. Must be kept to support the company's compliance with any other FDA regulation, including Good Clinical Practices (GCPs), Good Manufacturing Practices (GMPs), and Good Laboratory Practices (GLPs). This may be data collected during production or product testing, field information such as product complaints or distribution records of critical devices, and many other types of internally collected data.

   In general, if the data found within a system pertains to the design, development, production, or quality of a company's products, it is likely that the system is within the scope of 21CFR11.

2. **Acceptance of e-records and e-signatures based upon rule compliance**

   The 21CFR11 regulation provides that the FDA will accept the authenticity of electronic versions of records and signatures only if the computer system that creates and maintains the records meets requirements set forth in the regulation. If the system does not meet the requirements, the records/signatures are not valid for FDA use, which probably means the company cannot prove compliance to whatever regulation the record would normally support. This places the company in jeopardy of FDA action.

3. **Basic controls requirements (section 11.10)**

   The regulation prescribes a series of control requirements that are expected of any in-scope computer system. The major requirements are:

   – System validation (11.10-a)

     The Computer System must be validated. The regulation does not provide any description or details of what validation is. However, there are several FDA guidance documents that describe the validation process.

   – Invalid or altered records detection (11.10-a)

     The system must be able to indicate when a record is changed, or the content of the record is invalid. This is typically part of the software input and/or edits routine, to verify correct user input, or notation of a replacement entry. It may also involve database integrity checking for changes made directly to the storage, outside the normal system processes.

   – Records copies (11.10-b)

     FDA inspectors may ask for copies of any records that are within scope of any FDA regulation during an inspection. 21CFR11 requires that if the records are electronic, that the company will provide both a printed copy and an electronic copy in a format that the FDA can use. If the records are kept in a non-standard format or database, the company is responsible to provide (convert) the records into an FDA-usable format.

   – Record protection (11.10-c)

     Most records that are within the scope of FDA regulations must be kept for a defined period of time (retention period). The company must be able to produce a usable record at any time during the retention period. As a result, the database or databases of records must, at all times, be protected from loss, damage, or inability to read the record at all times

   – System access controls (11.10-d)

     Each system must have adequate security features that protect it from unauthorized persons (internal or external) accessing the system.

   – Audit trails (11.10-e)

     Each completed input that creates a record must have an audit trail created that is part of or linked to that record and show the time and date that the record was created. If a record is to be changed, the change must not erase the original record and its audit trail (but may replace it in processing) so that a complete history of all entries (original and updates) with their respective time/date stamps will always exist.

   – Authority checks (11.10-g)

     Even with authority to access a computer system, users must be restricted to being able only to use those functions of the system, equipment, and the like, that match their authority.

   – Sequence and Device checks (11.10-f and 11.10-h)

     When appropriate, the system must be able to limit user functions to the proper sequence of actions. In addition, if applicable, the system should be able to check the location or device where the data record or signature was entered in order to determine the validity of the source of the input.

- Education/training requirements (11.10-i)

  In addition to user training for a system, the regulation also requires qualifications (education, training, and experience) to be established for those persons who develop and maintain in-scope computer systems. This will apply to software developers, system implementers, and Data Center and IT support staffs.

- System documentation controls (11.10-k)

  The system documentation (technical and user manuals) that supports the use and maintenance of the system must be controlled and managed according to the same principles as company procedures.

4. **Additional controls for "open" systems (section 11.30)**

   The controls in section 11.10 apply to all systems within a company that come within the scope of the regulation. However, some systems that a company may use are outside the control of the company, such as those managed by a third party or supported through the Internet. "Open" systems are ones where control (ability to manage access to the system) is not solely within the company.

   For an "open" system, the regulation requires all of the controls in section 11.10 above be in effect, as well as additional security measures, such as data encryption or the use of digital signature technology (such as PKI), which must be applied to provide additional security.

5. **Electronic signatures (sections 11.50, 11.70, 11.100, 11.200, 11.300)**

   In addition to the controls required for all records (whether for data or signatures), the use of an electronic signature transaction to indicate that a person has "signed" their name is allowed, but only if the following requirements are met by the system:

   - Signature policy (11.10-j)

     In order to deter user misuse of electronic signatures, such as impersonation or signing for another person (with or without their permission) the regulation requires the company to establish written polices that hold persons accountable for the use of their signature. This requires a strong management policy with disciplinary actions for falsification of a person's signature.

   - Signature details

     Whenever a signature is recorded in the database, it must have or be linked to a signature audit trail. This will be the same time/date stamp as for any electronic record, with two additional fields of data included:

     - The signer's actual name (not a user ID or coded value)
     - The meaning of their signature (why they signed)

     These details must be part of any display of the signature or records that were signed for by the signature entry.

   - Signature linking to e-record or e-records

     When a person signs for data records (with an e-signature) those records must be linked to the signature in such a way that it would be difficult to deliberately or unknowingly attribute that signature to any other record. For example, if records are added to a dataset after the person signed their approval for the records, it cannot appear as if the post-signature records were covered under the original signature.

- Signature issue requirements

  The procedures under which electronic signature components are issued to persons must have controls to assure that:

  - Signatures are totally unique to a specific person. Two people cannot ever (in perpetuity) have the same code combination or the same name represented as a signature.
  - When signature codes are issued, the identity of the person must be positively confirmed.

- Signature components, allowance, and requirements

  It is acceptable to use either biometric methods (measuring body characteristics such as a fingerprint or retina scan) to confirm a person's identity when they sign their name or to use the standard keyboard input of a User ID code and a separate password. However, the biometric scan or the dual-key entry must be supplied every single time a person signs a record or screen.

  Under certain situations, such as when the system has some features that can guarantee the user has not left the workstation, a single key-entry can be used for a signature (after the first dual key signature entry).

  When key-entry codes are used, the passwords must be checked and/or changed on a regular basis.

- Signature components controls

  It is acceptable to use badges or tokens to represent one of the two signature components for dual key-entry (such as swiping the employee badge for the user ID). However, procedures must exist to manage the replacement for a lost badge/token, including controls over temporary card use. In addition, periodic checking of the reliability of the badge/tokens must be conducted

- Misuse of safeguards and alarms

  Whatever method the company uses for electronic signatures, there must be controls in place that assure that e-signature components can never be used by anyone other than their rightful owners. If the company uses biometric means for signatures, then the system should be designed to make it impossible to falsify a signature.

  The system must also have detection capability such that if anyone ever attempts to misuse signature identification codes, the system will immediately alert the system security personnel and, if necessary, the company management of the security violation.

G

Good Documentation Practices

This appendix describes Good Documentation Practices.

Detailed explanations of Good Documentation Practices (GDP)

All documents and records that are either submitted to the FDA or must be kept to prove compliance to any FDA regulation must be originated in such a fashion that there is no reasonable doubt of record authenticity. This is critical to all areas of regulatory compliance, because the records (documents, data, and signatures) may someday become involved in court proceedings, where they may be introduced as evidence.

Good Documentation Practices (GDP) are a common set of principles and practices used throughout the FDA-regulated industry for the documentation and the records of data/signatures.

There is no specific guidance or standard published by FDA on the subject, but inferences are found through many different FDA documents. As a result, each company has its own internal standard for GDPs, and minor variations will exist from firm to firm. However, the general principles are widespread and usually consistent.

The following are the common general rules of Good Documentation Practices.

Entries or signatures must always be clear and legible

Each handwritten entry must be clearly legible. Entry-makers must exercise great care to assure that misinterpretation of their recorded data does not occur due to poor penmanship. For signatures, the person must use their unique personal signature, and should include at least the first initial and full last name. Initials may be used only if the document contains a legend that matches those initials to a full signature. If the person’s natural signature is not readily identifiable, the project or local records must have a signature register (matches a printed identification to a signature sample) to positively identify each signer.

Entry-makers must sign their recordings

The persons who record the original data entries, or observations, or who make comments or corrections or addenda to any data entries, must identify themselves with a signature that clearly indicates what input they have provided (what data they are signing for).

Signatures must be authentic

A person signing any document or record may only supply their own identifying signature. It is absolutely prohibited for one person to sign another person's name. When a person is signing for another person, they must sign their own name, but the signature may include the commentary that identifies who they are signing for (example: John Doe signs a document as a designee for Tom Brown. John signs the records as: “John Doe for Tom Brown”. Signature stamps are prohibited.

Entries or signatures must be made in ink

Entries made in pencil could be erased, therefore altering the original information. Ink entries are more difficult to erase, reducing the possibility of undetectable modification of the original information. Blue or black ink is preferred, and with a specific color or colors dependent on the superior of corporate or site policies.

Each original data entry or signature cannot be removed

Any original entry (the first recording of the observation or signature) cannot be removed, deleted, erased, or otherwise taken away. It does not matter if the entry is incorrect, accidental, or voided, the fact that an entry or signature was originally made (and what it was) must be part of the history of the record. Erasures, white-out, correction tape, and so on are prohibited. Post-it notes cannot be used for data collection or signatures, as they can be removed from the attached document. “Write-overs” (going over a value again to change its original entry) are prohibited.

Corrections require a replacement entry that does not obscure the original

If an entry is incorrect, or needs to be replaced or updated, the change must be made by supplying a new value or signature. The new value will be a second, complete entry, which can be determined to supersede the original entry. In a paper system, this is done by drawing a single line through the first entry (but not so as to obscure the original entry or make it unreadable) and then supplying the new replacement entry or signature, next to or above the ‘lined-out” entry.

If another correction needs to be made, the replacement entry is similarly “lined-out” and another (now the 3rd) entry or signature is made.

If space limitations begin to make it difficult to provide legible entries, a footnote or asterisk can be used to link the original entry to space in another part of the same document where the replacement entry will be made. Back or reverse pages should be avoided unless absolutely necessary, and then the footnote must note the back of the page is the location. If multiple such off-location entries are made, the notations should be numbered to clarify which remote corrections tie to which original entries.

For computerized entries, the entry record must show a sequence identifier or other technique that will make it absolutely clear the order that entries were made to a data or signature field.

Correction entries require a signature, date, and reason

When a replacement entry is made, the entry-maker should then sign the second entry, and date that signature. Entries made to Clinical Records will also require a reason for corrections. Local GSP procedures may also require reasons for other or all types of corrections.

Corrections should normally be made by the person making the original entry, but may be made by another person, in which case the reason notation must explain the reason for another person making the correction.

If a correction is made to a document after it has been approved, the document must be re-approved.

Voided entries or documents must be identified and retained

If an entry (data or signature) is made to a field in error, it is voided as a correction with “Void” as the correcting entry, which is made in accordance with the correction rules. If a document is not to be completed, or voided, it is to be marked as “Void” across the face of the document, with the signature, data, and reason of the person voiding the document. The voided document must be retained, and attached to a replacement document, if any.

An entry or a signature must be labeled as to what it represents

The meaning or purpose of a signature must be clear as to what the person is signing for. This may be indicated on the form or document for paper records, or it may be the signature field label for electronic signatures. In either case, the purpose and intent of the person’s signature must be clear, and the signature label must match the signer’s intent.

Signature reasons will be defined by local procedures. Typical reasons for signatures are:

- Performed by: (Means the signer personally did the task or recorded the data.)
- Checked by: (The signer did not perform or record, but verified what someone else did.)
- Verified by: (Same as Checked by:.)
- Supervised by: (Area or functional authority over person performing the task.)
- Approved by: (The signer provided management authority to accept the results.)

Approvers cannot approve their own tasks performed, documents originated, or data recorded.

Recopied data must have its source identified, attached, or both

While data should normally be only recorded once, there could be circumstances where data is recorded by copying from another original entry. In this case, the copied entry is not the original data, but a copy of the data transferred from the first source. In such a situation, the copied entry must be labeled as “Transcripted from [document ID] [version or copy ID]“. This demonstrates from where the data originated.

The originating source of the data must be retained. If it is not another official document, it should be attached to the document that references it (that is, if the original entry was on “scrap paper”, that paper must be attached to the official form).

Rewriting a document or form is strongly discouraged. If necessary, the original document must be attached to the transcript (copy), which must contain the notation that explains the reason for the re-writing, and the entries or section that was transcribed.

Date and times must be unambiguous

There must never be confusion over the actual date and/or time that is in a record. If the time is recorded in the AM/PM mode, the AM/PM indicator must be used. If the time is recorded in military (24-hour) clock mode, no such indicator is required. Local procedures may dictate time standards regarding format, and these must be followed.

Dates must include the full identification of month, day, and year, and must be in a standard format, as defined by local procedures. The local standard will prescribe at least the following:

- The order of the periods (typically, the US standard is mm/dd/yy(yy), and European standard is typically, but not universally, dd/mm/yy(yy).)
- The year length (either 2-digits or 4-digits)

- The month as either a numeral or written month
- Use of military or AM/PM time recording

Blank fields must be "N/A" unless obvious

A blank field on a completed form may either mean the field was not needed, or that it was inadvertently skipped or missed. Blank fields not needed should be marked "N/A" to indicate that they are not applicable. A line can be draw from the "N/A" to the end of the blank fields if necessary. An allowable exception is when a defined set of options is provided, where it is obvious that only one space is to be indicated, and then all other spaces will not be used (For example, when the fields Yes ___ No ___ N/A ___ are set, if one is checked, then the others must be blank, or when an exclusive list of alternate boxes is provided).

When a large number of fields, even multiple pages of a form, are not required for reasons that will be obvious (such as stopping a test cycle and not continuing), individual "N/A"s are not required. Whole pages can be marked with a slanted line across the page and a single "N/A" used to indicate the entire page (or major section) is not required to be filled out.

Ditto Marks for blank fields (intended to mean "same as above") or continuous lines (arrows) that are intended to indicate the same data as the first entry may or may not be permissible, depending on local procedures. Entry makers must verify the acceptability of either approach according to local GDP procedures prior to the use of each.

Entries are made, signed, and dated immediately, not ex post facto

Entries and signatures are to be made to the records contemporaneously, *after* the task is completed, and/or the data observed, and as soon as practically possibly. Recording data or task completion well after the fact (as next day) is not acceptable. If a delay occurs, and the recording takes place later (next or later day), the entry must be identified as such with the notation: "Observed or performed on [actual day] but recorded or signed on [record day]."

If the person who performed the task or observed the data is not the person recording the data, but the information is derived from alternative means (such as phone call), the means by which that information was derived must be a comment with the entry, which will identify the source or person who performed the task and observed the data, along with the signature of the person recording that data.

It is never permissible to record task completion or data observed in advance. Back-dating of a signature (signing with a prior date) is also prohibited.

Document attachments must be positively linked to their point-of-origination

Document attachments may be required when supplemental information (additional data, comments, and explanations) cannot fit in the document space, or additional pages of supplemental or other information (such a screen prints, printout, or referenced documents) are required to completely record the data or support the reason for a signature on a document

When an attachment exists, the referring document must be noted by the field, comment, or additional data entry place for which an attachment exists. The name of the attachment, if applicable, is noted, along with a page count of the attachment, if it contains multiple pages.

Document attachments must be labeled and paginated

Document attachments must have labeling on each page that is sufficient to identify the page as part of the attachment set. This identification must be precise enough so that if a page is removed from the attachment and co-mingled with other attachment, it can positively be located and replaced into the correct attachment.

At least the first page of any attachment must have linkage identification to the referring document, adequate to assure that the attachment can always be positively linked to its referring document

The attachment pages must sequentially numbered, with a total page count indicated, on either the first page, or on each page as "nn of nn pages".

Work organizers and work aids

A work organizer/work aid is a document that consists solely of checklists, "to-do" lists, or other items that are used by work performers to track progress completing a procedure. These are never used to record the actual results, attest to completion, or define the acceptability of the results, and so are not data records. Local procedures will determine whether these must be retained upon completion of the tasks.

Document workflows and records retention

Local procedures will define the routing order and rules (workflows), storage methods, and retention periods for all records. Documentation originators and approvers will follow those procedures. With the exception of totally unused blank forms (unless a serial numbered copy) and work aids (if local procedures allow), all documentation, completed or not, will always be turned over to the repository or documentation custodian by the end of the project.

H

Training/qualifications record

Name: ___________________________ Emp./Serial#: ________

Organization: ______________________

Document /Task ID	Version or Date	Training Method	Training Date	Trainee Signature/Date	Train/Qualification Approver Signature/Date

Approved By: ____________________ Date: __________ Sheet ____ of ____

Instructions

The Training Record form is used to document training provided as part of the validation project that qualifies a person to meet the requirements of the Qualifications/Training Matrix. A separate Training Record will be prepared for each person who performs a task named in the validation plan or protocol, and/or who records data or signs any document that is referenced in the reports that close either the validation plan or testing protocol. The form is completed as follows:

- Document/Task ID
  The name or ID number of the document or the name of the Task as defined in the document (if training is only conducted on a single procedure task).
- Version or Date
  The document version or issue date that defines the version of the document being trained on.
- Training Method
  The method used to conduct the training, such as:
  - Classroom
  - Read and Review (with Trainer)
- Training Date
  The date that the training was completed.
- Trainee Signature/Date
  Dated signature of the Trainee, attesting to training completion.
- Trainer Signature/Date
  Dated signature of the Trainer, attesting to satisfactory completion of training.

The Project Manager or designee will review the Training record for completeness and accuracy, and will approve the completed record.

Multiple sheets may be used for additional training records for a person, and forms will be page numbered accordingly.

I

Resume equivalent for training and qualifications record

The attached Resume (or Curriculum Vita (CV)) has been reviewed and accepted as evidence of equivalent experience that meets the Qualification/Training requirements for the assigned tasks.

Resume Attached for: ____

Equivalent Requirement(s): ____

____

____

____

Approved for Equivalency ____Date ______

Quality Reviewer: ____ Date ______

Training and Qualifications Test Script

Objective: The objective of this verification is to ensure that the person or persons who perform the installation shall have the training and qualifications that demonstrate their capability to perform the required functions.

Set Up: None.

Procedure:

Table I-1

Step #	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
1	The hardware installers have been certified by the manufacturer to have the appropriate qualifications to install their equipment as documented in a certification letter. Attach certificates to the document.	Certification letter is provided by vendor stating that the installers are qualified to install manufacturer's equipment. Certificates attached to the document.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

J

Signature log

The signature log contains a signature and initial specimen for each person who signs or initials any document, next to their printed (full) name. The log then enables any signature/initial set on any document to be identified to the person.

Each person makes a single line entry with their full legal name (per the company personnel records) then signs with their normal signature, and initials, and dates the entry.

Signature identification			
Printed full legal name	**Signature**	**Initials**	**Date**

K

Infrastructure installation and operating manuals

The following is the complete listing of the manuals that are used to install, configure, and support the infrastructure. The indicated columns are provided by the person performing the IQ verification.

The following manuals are published by the IBM Corporation.

			Provided during IQ verification		
Line	**Manual Title**	**IBM Order Number**	**Local ID Serial #**	**Location**	**Verified by/date**
	2105 Enterprise Storage Server				
1	*IBM TotalStorage Enterprise Storage Server Introduction and Planning Guide*	GC26-7444			
2	*IBM TotalStorage Enterprise Storage Server User's Guide*	SC26-7445			
3	*IBM TotalStorage Enterprise Storage Server Host Systems Attachment Guide*	SC26-7446			
4	*IBM TotalStorage Enterprise Storage Server Web Interface User's Guide*	SC26-7448			
5	*IBM TotalStorage Enterprise Storage Server Copy Services Command-Line Interface User's Guide*	SC26-7449			
6	*IBM TotalStorage Enterprise Storage Server Subsystem Device Driver User's Guide*	SC26-7478			

			Provided during IQ verification		
7	*IBM TotalStorage Enterprise Storage Server Configuration Planner for S/390 and IBM @server zSeries Hosts*	SC26-7476	Not Applicable		
8	*IBM TotalStorage Enterprise Storage Server Configuration Planner for Open-Systems Hosts*	SC26-7477			
	3584 Linear Tape Open Library				
9	*IBM 3584 UltraScalable Tape Library Planning and Operator Guide*	GA32-0408			
10	*IBM Ultrium Device Driver Installation and User's Guide* (English)	GA32-0430			
11	*Translated Safety Notices for External Storage Devices*	SA26-7197			
	7014 Rack				
12	*7014 Series Model T00 and T42 Installation and Service Guide*	SA38-0577			
	RS/6000® Enterprise Server				
13	*Enterprise Server Model H80 and pSeries 660 Model 6H1 Installation Guide*	SA38-0575	Not Applicable		
14	*RS/6000 Enterprise Server Model H80 System Unit Safety Information*	SA23-2652	Not Applicable		
	pSeries 670				
15	*IBM @server pSeries 670 Installation Guide*	SA38-0613			
16	*RS/6000 and pSeries PCI Adapter Placement Reference*	SA38-0538			
17	*IBM @server pSeries 670 Installation Guide*	SA38-0613			
	pSeries 690				
18	*IBM @server pSeries 690 Installation Guide*	SA38-0587	Not Applicable		
19	*RS/6000 Enterprise Server Model H80 System Unit Safety Information*	SA23-2652	Not Applicable		
20	*RS/6000 and pSeries PCI Adapter Placement Reference*	SA38-0538	Not Applicable		
	AIX Version 4.3				
21	*AIX Version 4.3 Quick Installation and Startup Guide*	SC23-4111			
22	*AIX Version 4.3 Installation Guide*	SC23-4112			
23	*AIX Version 4.3 Network Installation Management Guide and Reference*	SC23-4113			

			Provided during IQ verification		
24	*AIX Version 4.3 Quick Beginnings*	SC23-4114			
25	*AIX Version 4.3.0 Release Notes*	GI10-0697			

The following manual is published by McData Corporation.

			Provided during IQ verification		
Line#	**Manual Title**	**Part Number**	**Local ID Serial #**	**Location**	**Verified by/date**
	2031 McData Switch				
26	*McData Sphereon™ 4500 Fabric Switch Product Manager User Manual*	P/N 620158000-0000 Rev A			

Document Prepared by: ________________________________ Date _____________

Approved by: ________________________________ Date _____________

Document and Manual Verification Test Script

Objective: The objective of this verification is to provide a record of the Vendor Documentation at the time of installation of the hardware and software.

Set Up: None.

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectations Satisfied (Yes/No)	Initial/Date
1	Verify IBM system document list.	IBM List of system documents.			
2	Attach list to the protocol	List attached to protocol			
3	Verify documents on list can be viewed	Record of viewing of each individual document on list by testerComment and sign off by tester on list indicating that all documents have been viewed by the tester.			
4	Record document location for all documents	IBM intranet or IBM maintained hardcopy. Result recorded for all documents.			

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

L

Risk assessment and mitigation plan

Instructions for preparation of the Risk Assessment:

1. Each potential risk event is described and evaluated on a separate line, identified with a sequential index number (column #1)
2. The risks are organized by major categories, titled in column #2, as:
   - Database Integrity
   - Security
   - Performance/Availability
3. Each risk is described with a title, which relates to the event that will result from the occurrence (realization) of the risk. (column #3)
4. For each risk event, the underlying (root) cause that creates the risk event is described. In cases where the event could be caused by multiple difference causes, each is individually identified. The cause or causes are listed for each risk, in column #4.
5. Each risk event (line item#) must be evaluated and scored with numerical rankings based upon the following criteria:
   - Severity

     This ranking indicates the criticality of the event by its impact on the operation of the system. The highest rating is given to a risk that the system might fail if the event occurs, either through the inability of the system to continue, or corruption of the accumulated data occurring. A lower ranking will be used for impacts that do not stop the system, nor corrupt data, and can be offset via other mechanisms, including manual workarounds.

   - Probability

     This ranking indicates the probability that the event will actually occur sometime during the system's life. The highest ranking goes to the event that can be expected to occur at some point, with lower rankings to those events that only might occur, or are not expected to occur at all.

   - Detection

     If the risk event is detected, via other system or manual activities, prior to the time that the risk event causes an impact, that detection likelihood reduces the risk. The highest ranking goes to events that are not likely to be detected, and lower rankings are used for possible or expected degrees of detection of the event.

   The total Risk Score is the result of multiplying all three risk scores (columns 5 X 6 X 7 = column 8).

6. For each Risk Event that meets or exceeds the Risk Threshold Value, a Risk Mitigation must be determined, based on either a design feature that will prevent the risk event from occurring, or a manual process that is described within an identified system procedure (list SOP# and applicable section ID). Providing a description of Risk Mitigation for events that score below the risk threshold level is optional. The Risk Mitigation will be verified during the IQ Testing, either as present in an SOP (if mitigation is a process control) or as part of a verified feature (if part of a design control).

7. The Risk Assessment document must be approved by the System Owner, Technical Representative, and Quality Representative.

Risk Assessment Document

Risk Threshold Value that requires on-site testing: ___________

				RISK SCORING				
Risk #	**Category**	**PotentialFailure Event**	**PotentialCause**	**Severity Rating**	**Probability Rating**	**Detection Rating**	**Total Score**	**Design and Process Controls**
			.					
			.					
			.					
			.					
			.					
			.					

Prepared by: ______________________________________ Date ____________________

System Owner
Approved by: ______________________________________ Date ____________________

Technical
Representative
Approved by: ______________________________________ Date ____________________

Quality
Representative
Approved by: ______________________________________ Date ____________________

Risk Assessment Document Legend:

Column	Code	Meaning
Severity Rating	1	Low - No risk to system function, little impact on system compliance
	2	Medium - Minor but recoverable effects on system
	3	High - System failure would result
Probability Rating	1	Unlikely - Not expected to occur during system life
	2	Possible - May occur at least once during system life
	3	Probable - Likely to occur, maybe more than once
Detection Rating	1	High - Would be detected before severity levels are reached
	2	Maybe - Might be detected prior, but definitely after severity level is reached
	3	Unlikely - Would not be detected prior, maybe not immediately after it occurs

M

Testing protocol

The following are the protocol contents, which will be inserted into the protocol format of the local procedures.

Purpose

The purpose of this testing protocol is to verify that the Infrastructure that was specified in the applicable sections of the referenced Technical Design has been installed and configured to the Design requirements, is within a controlled environment that meets the equipment vendors' specifications, and is functioning normally.

Scope

The scope of testing is confined to the components that are listed in the referenced technical design documents for the system or systems that the Infrastructure will be supporting. The type of testing of the Infrastructure components is limited to verification of proper installation, and confirmation that the components' major features are operational.

An evaluation of the degree of risk to the functioning of the application or applications that the Infrastructure will be supporting will identify the critical areas that will require additional testing of the functionality of the component. The extent of testing demonstrated in the test cases/scripts has been based upon the approved Risk Assessment document.

Responsibilities

The persons who will execute this protocol are listed below, by their respective roles.

Role	Person or persons assigned
Test Manager	
Perform Infrastructure Verification Tests	
Perform Environment Verification Tests	
Perform Documentation Verification Tests	
Perform Functions Verification Tests	
Review/Approve Test results	
Prepare Testing Protocol Report	
Approve Testing Protocol Report	

Prerequisites

Prior to the issue of the test cases/scripts to the Testers, the Test Manager will verify that the following prerequisites have been met:

Technical design document

The technical design document, containing Infrastructure requirements (including equipment capacity specifications, configuration settings, and other technical Infrastructure requirements) must be approved, and an official copy attached to the Infrastructure Verification test case copy issued under this protocol

Training

The persons assigned functions listed in role and responsibility table must be qualified and/or trained as per the requirements of the training matrix attached to either this protocol, or the validation plan referenced by this protocol. The Test Manager will confirm that the Qualification document, or Training Record, requirement or requirements are met for each person assigned becomes part of the validation records.

Infrastructure preparation

The Infrastructure to be verified and/or tested must be completely installed, set up, and available for the testing process. The Test Manager will contact the Infrastructure manager or managers and technical staff, and verify the entire Infrastructure, as described in the Infrastructure Identification document referenced by this protocol, is ready for testing.

Infrastructure access authority and security

The Tester must obtain, using current approved data center procedures, the following access authorities.

Infrastructure component	Access requirement
Servers	Root password
Storage	User ID/Password
HMC	User ID/Password
McData Switches	Admin Password

The Testers assigned in section 3.0 must be granted physical access to the Infrastructure, in accordance with current approved Data Center security procedures. The applicable procedure is listed in the reference section of this protocol.

Test cases/scripts

The test cases/scripts that will be used for the testing are identified in the following listings.

Testing category	Test case/Script ID #
Infrastructure Verification	
Environmental Conditions Verification	
Documentation Verification	
Infrastructure Functions Verification	

Testing procedures

The procedures to be used by the Test Manager, Testers, and Test reviewers are those listed in the reference section of this protocol.

Infrastructure manuals

The Testing will include verification that the required Infrastructure manuals, as identified by the list named in the Reference section of this protocol, have been located, confirmed by title and IBM manual number, and are stored under controlled documents procedures of the site, as listed in the Reference section.

Acceptance criteria

The Infrastructure that is listed in the Infrastructure Identification named in the Reference section of this protocol has qualified that all the test cases/scripts are completed, reviewed, and either:

1. No deviations are present.
2. Any deviations are resolved, closed, approved, and the Summary report supports the conclusion that the technical design document is adequately met, and is approved.

Test Report

This protocol will be summarized and the testing activities closed by a Protocol Report that will be prepared after all testing tasks are concluded, including the resolution and/or retesting of all deviations that are generated by this protocol. The report will be prepared and approved according to the procedure listed in the reference section of this protocol.

References

The following are the documents that are referenced by this protocol.

Section	Referenced document	Document ID	Version/Issue
1.0, 4.1	Technical Design Document	[Site document]	
2.0	Risk Assessment and Mitigation Plan	[Appendix M, “Testing protocol” on page 225]	
4.3	Infrastructure Identification	[Appendix B, “Infrastructure identification” on page 39]	
4.2	Qualifications/Training Matrix	[Appendix E, “Installation Team Training/Qualifications Matrix” on page 189]	
7.0	Infrastructure Installation/Operating Manuals	[Appendix H, “Training/qualifications record” on page 207]	
6.0	Good Documentation Practices	[Appendix G, “Good Documentation Practices” on page 201]	
4.2	Training/Qualifications Record	[Appendix H, “Training/qualifications record” on page 207]	

Section	Referenced document	Document ID	Version/Issue
4.2	General Regulatory and 21CFR11 Training	[Appendix F, “General regulatory and 21CFR11 training” on page 193]	
6.0	Test Execution Procedure	[Appendix O, “Test execution procedure” on page 233]	
6.0	Deviations Procedure	[Appendix P, “Deviations procedure” on page 239]	
9.0	Validations Reports Procedure	[Appendix Q, “Validation reports procedure” on page 247]	
4.4	Data Center Security Procedure	[Site SOP #]	
7.0	Controlled Documents Procedure	[Site SOP#]	

N

Trace Matrix

The Trace Matrix lists each item (line or ID#) on the documents that provide requirements or identify specifications for the Infrastructure. For each line, the test script name/ID and individual test or test step that verifies the requirement, specification, or risk-mitigating design control is identified and recorded. When multiple test scripts or multiple test steps within a script are required for verification then all should be listed, demonstrating what may be shown as a range of test steps, if applicable, within the same (expanded) cell. When a single test script or test step, or steps, verifies a number of requirements/specs or design mitigations, the latter may be grouped within a cell to make a single match.

#	Document/Requirement	Line/ID #	Test Script	Step/ID #
	Technical Design Document: [Doc ID#]			
	Infrastructure Functional Specification: [Doc ID#]			
	Risk Assessment: [Doc ID #]			

#	Document/Requirement	Line/ID #	Test Script	Step/ID #

Document Prepared by: ______________________________ Date ____________

Approved by: ______________________________ Date ____________

O

Test execution procedure

This appendix describes the test execution procedure.

Purpose

The purpose of this procedure is to completely and properly execute the test cases that are part of all approved testing protocol, identify any deviations that occur, and adequately document the testing results so that a testing report can be approved.

Scope

This procedure applies to performance of the test case that is part of a validation testing protocol, and so identified by a listing within the protocol. It does not apply to informal (bench) testing or trial runs that may be done prior to the formal (per protocol) testing.

Roles and responsibilities

The persons who will use this procedure, by title and activities performed, are shown in the following table.

Role	Responsibility
Test Manager (may also be the Project or Validation Manager)	► Assigns the test cases to the Tester or Testers ► Verifies required training is completed and any required equipment/database/datasets are ready for use ► Provides approved copies of test cases or scripts, and logs issuance ► Reviews all completed test cases for completeness and adequacy of accompanying documentation ► Logs and manages all deviations to completion ► Incorporates all completed, approved, test case results and documentation into validation records
Tester	► Performs the actions indicated in the test case or script, and records the results ► Creates a deviation form if actual results do not match the expected results ► Prints, labels, and attaches any applicable hardcopy to the test case or deviation ► Repeats any tests as specified on a completed deviation, when a retest is indicated

Prerequisites

The following must be completed and documented before the Tester may begin to perform any testing. The Test Manager is responsible for performing or verifying these pre-requisites are met and documented in the validation records, before testing begins:

Protocol and test cases/Scripts approved

The testing protocol and the test cases that it references must be approved.

Testing assignments

The Test Manager will determine, based upon testing resources, schedule, and test case content, which Testers will perform each test. The test cases referenced in the protocol must all be assigned to the Testers, either as indicated in the protocol, or by a separate assignment log, prepared and signed by the Test Manager.

Training

The validation plan or testing protocol, or both, will specify the qualifications and/or training the Test Manager and Tester or Testers will require. The documentation as specified in the validation plan must be completed, approved, and in the validation records.

Equipment, database, and dataset or datasets preparation

Any preparation of the testing environment, according to the testing protocol, or as specified in any of the test cases, must be completed prior to the start of any test cases that require that preparation be complete in advance. If any test cases require a reset of any portion of the test environment (from the conduct of a prior test), then the Test Manager will monitor the testing progress, and assure that such a reset takes place as described in the testing protocol or test case.

Instructions: Test Manager

Here are the instructions for the performance of the Test Manager's duties.

Test assignments and log

The Test Manager will make copies of each test case/script from approved Masters (which are retained with validation records), and will log the issue of the test case/scripts on the Test Assignment Log (Example Attached). This form is used to track the issue and return the status of all assigned Tests. The Test Manager will assure that all issued Tests are returned and logged. The Project Manager or Quality Representative will review the Assignment Log to verify all Tests are accounted for and will approve the Log.

Deviations management

When notified by a Tester that a deviation has occurred during a test, the Test Manager will issue and log a deviation form to the Tester, according to the deviations procedure in effect for the testing. Resolution of the deviation will be managed by that procedure.

If, for any reason, the testing does not follow the testing protocol requirements (such as tests cases not performed), a deviation will be created by the Test Manager.

Test case/Script review

The completed test scripts are returned from the Tester and reviewed by either the Test Manager or the Quality Representative. If any Tests are performed by the Test Manager, the reviewer must be a Quality Representative. The Test reviews should include verification of the following:

- The executed Test cases/scripts (copies) match the Masters retained in the validation files, without any modifications or missing pages
- All Test scripts were completed. If any tests or steps within a test were not completed and recorded, a deviation must be created and logged.
- Actual test results must meet expected test results, or a deviation must have been created. The Deviations Log will be checked to verify any discrepancies.

- All test records follow Good Documentation Practices
- Test results are signed by Tester, as indicated on the test case/script
- Hardcopy pages as identified on a test script are attached to completed tests, and are labeled per the instructions in "Screen prints and reports" on page 236.

Instructions: Tester

Here are the instructions for the performance of the Tester's duties.

Test case/Script execution

The Tester will perform the test script, following the test instructions provided, and will record in the "Actual Result" column the actual system response or displayed value provided by the system, as appropriate. When the system result is an action completely identified in the "Expected Result" column, it is permissible to record results as an answer "yes" or "no" if the expected results are observed. If data values are displayed, the actual value must be written in the column, or must be in a screen printout attached to the test script, even if the values are the same as expected.

Each test case/script step must be initialed by the tester as testimony that the test results are accurate.

Variable input data values

Input data (if applicable) that is used during the conduct of the test is indicated in the "Data" column or section of the test script. In some cases, the data is not predefined on the test script, either because it will become apparent during the conduct of the test (such as when it's the result of a prior output or display), or the data value is determined by tester-specific information (such as user ID/password). In these cases the data column or section will show the input data as an explanation within brackets [nnnnn] and the explanation will indicate how to determine the data value.

In these cases, the actual test results must include the recording of the actual data input value supplied by the tester.

Screen prints and reports

For tests where the test instructions indicate a report or screen print is to be done, a screen print or report must be generated and attached to the test script. The printout should be labeled with the following information, on each page:

1. System identification (name and version, if applicable)
2. Protocol ID
3. Test case/script and step ID
4. Page n of nn

When a report is generated that includes a report title, date/time stamp, and page counts as printed values on each page, then the above information is only required on the first page.

Screen printing instructions will be found in the test script or protocol instructions. A default set of instructions for screen printing from any workstation running Microsoft Windows is as follows:

- Hold down the Alt key and press PrtSc.
- Open MS Word, MS WordPad, or MS Notepad.
- Select **Edit** -> **Paste**.
- Confirm that the screen display is fully pasted into the screen.
- Select **File** -> **Print**, and choose the printer you want to use.

Test discrepancies

If the actual results are not as expected, the actual results will be recorded as observed, and also marked “Fail” (or “No” if the actual results are a Yes/No answer) The Test Manager must be informed, and a Test Deviation form supplied by the Test Manager must be completed. A hardcopy screen printout of the results will be attached to the Deviation form. The test script step where the deviation occurred will be noted with the deviation number. The deviation will be turned over to the Test Manager.

Test review and signature

The Tester must review the test cases/scripts that they have completed, and verify that the required screen prints and reports are attached. They will review and verify the following:

- All test case/script pages are present, and the steps were completed and documented.
- Every test step is initialed by the person performing that step.
- Every test step that has hardcopy requirements (screen print or report) has that document attached to that test page.
- If any test steps have variable input data (values are in brackets), the actual value used is recorded in the actual results column or section.
- Actual results exist for all tests. If any results are not as expected, the test step is marked “Fail” or “No” and a Deviation Form number is indicated.
- All Test records follow Good Documentation Practices.
- Test results are signed by Tester, as indicated on the test case/script
- Hardcopy pages identified on the test script are attached to completed tests, and are labeled per the instructions in “Screen prints and reports” on page 236.

The test case/script (or section done by the Tester) must be signed as testimony that they have completed the tests (or sections) and reviewed the documents per the above checklist. The signed test case/script is turned over to the Test Manager.

Test Assignment Log

System: ______________________

Protocol #: ____________________ Page ___ of ___

Test case/ Script ID	Issued to	Issue date	Return date	Comments

Reviewed by: ________________________________ Date ___________________

Legend

This lists the legend of the Test Assignment Log:

- Test ID is found on upper left corner of each approved script
- Issued To is person assigned to perform testing
- Issue Date is date copy of script given for testing
- Return Date is date test results returned, approved, to Project Manager
- Comments explain any anomalies in script control, dates, or returns

P

Deviations procedure

This appendix describes the deviations procedure.

Purpose

The purpose of this procedure is to ensure that any exceptions to the testing protocol instructions, or variances from expected results that are found during testing, are investigated, fully resolved, and documented to their completion.

Scope

This procedure applies to performance of the test case that is part of a validation testing protocol, and that is identified by a listing within the protocol. It does not apply to informal (bench) testing or trial runs that may be done prior to the formal (per protocol) testing.

Roles and responsibilities

The people who will use this procedure, by role title and activity, are listed in the following table.

Role	Responsibility
Tester	Prepares the Deviation form if actual results do not match the expected results. Prints, labels, and counts/documents pages of any applicable hardcopy evidence to the test case. Repeats tests of any test errors after receipt of resolved Deviation Report when a retest is indicated.
Technical Staff	Investigates and/or corrects the problem identified in the deviation, or develops reasons for no-correction, and identifies re-testing required to verify problem correction.
Test Manager	Confirms that the issue is a deviation and issues a Deviation form for Tester completion. Creates all deviations related to testing protocol conduct (non-testing related). Logs and tracks all deviations to closure. Aids in investigations and corrective action determination. Reassigns retesting. Assures all deviations are closed, and documentation is entered into validation records.

Instructions: Tester

Here are the instructions for the Tester to resolve deviations.

Deviation request

If any test results do not match the preprinted expected results on the test case, the tester will contact the Test Manager. Upon confirmation that the issue does indicate a deviation, the Tester will receive a deviation (see attached), and will complete the “Deviation Identification” section. The Field “Suspected Cause” will only have Tester input if the information is readily evident to the Tester.

Deviation documentation

The Tester will make a copy of the test case/script for the step where the deviation occurred, and attach it to the deviation form. Also attached will be any screen prints and reports that were generated as required by the test instructions. In addition, the Tester will create any screen prints, as applicable, that will aid the investigation.

The deviation will note all attachments that exist. All the attached documents will be labeled per the Testing procedure instructions.

The deviation number (top left of form) that is assigned by the Test Manager will be noted on the test case/script where the deviation occurred. When the Tester cannot readily determine the applicable test step, the deviation number notation will be placed at the point where the deviation became apparent, which may be the end of the test script.

Deviation package delivery

The Tester will provide the deviation, along with its attached supporting documentation, to the Test Manager. The Tester fills out the top portion, explaining what the actual results are, and provides the document, along with a copy of the test case (appropriately marked to show the test that failed), and any hardcopy, such as screen prints, that may aid in analysis of the error, to the Validation Manger.

Retesting

If the resolution of the deviation requires retesting, the Tester repeats the original test on a second copy of the original test case/script that is marked as such, which is provided by the Test Manager to the Tester. The retest results, with the documentation specified in the test case/script and/or the retest instructions on the deviation, will be attached to the deviation. The Tester will return the retested deviation to the Test Manager.

Instructions: Technical Staff

Here are the instructions for the Technical Staff to resolve deviations.

Deviation investigation

Upon being contacted by the Test Manager regarding a deviation, the Technical Staff will evaluate the deviation package and its accompanying documentation. The cause of the discrepancy will be evaluated and the cause will be determined. Based upon that result, one of the following actions will be indicated:

- Incorrect Expected Result: If the error occurred because the test case has an incorrect expected result, the deviation will be so noted and the correct expected result will be described. An explanation for the difference between original and corrected expected results must be provided.
- Change Required: If a change to the infrastructure or program code is required, the deviation will be so noted, and the correction made to the system environment. If the environment or system code is under change control, the applicable procedures for change control will be followed.
- No Corrective Action: If analysis of the circumstances results in a decision not to make any changes, due to technical issues, insufficient risk, or other reasons, that conclusion will be noted and fully explained on the deviation.

Deviation resolution documentation

Any documents that are created as part of the investigation or resolution, including repeats of the original failed tests that were done to evaluate the issue, must be attached to the deviation. The attachments will be labeled per the Testing Instructions, with the additional notation of the deviation number.

Retesting requirements

If the deviation requires a change to the environment or system code, the retesting required to confirm the successful change must be determined. This will normally be a repeat of the original test, but additional testing may be required. The additional tests will either be described on the deviation (along with expected results) or will be added as formatted test scripts as a deviation attachment.

Deviation package

The Technical Staff will turn over the resolved deviation and all attachments to the Test Manager, who will manage retesting and/or deviation closure.

Instructions: Test Manager

Here are the instructions for the Test Manager to resolve deviations.

Deviation identification

When notified by a Tester of an apparent discrepancy in a test case/script, the Test Manager will review the situation, and confirm that a deviation has occurred. If a consultation with the Technical Staff is required, the Test Manager will contact the appropriate person. If a deviation is indicated, the Test Manager will initiate a Deviation form, and provide the Identification information (protocol ID and deviation number). The deviation number will be assigned from the next sequential number in the Deviations Log.

Deviation logging and tracking

The Test Manager will manage the deviations until they are resolved, and will indicate in the log all changes in status. The Test Manager will monitor the log for timely response and return of the deviation from the person in possession of the deviations. When all deviations are closed, the Log will be reviewed by the Quality Representative to verify the deviations are resolved, closed, and part of the Testing Protocol Report and validation records.

Deviation investigation and resolution

The Test Manager will ensure that all deviations are fully and completely investigated, including complete and accurate determination of the root cause of the discrepancy.

Any deviations that are indicated as “Incorrect Expected Results” should be adequately explained, and, if applicable, reviewed and confirmed by the test case/script preparer and approvers.

Any deviations that are indicated as “No Change” must have an accompanying explanation that is obvious and sufficient to withstand challenge. Attachments might be required to provide sufficient space for a full justification.

Deviations with change and retesting

If a change is indicated, either in the system environment or code, the Test Manager will coordinate the update of the system with retesting, as indicated in the deviation. Additional copies of the original test case/script sections applicable to the deviation will be made, logged on the Test Assignment Log, and provided to the Tester.

Deviation review and closure

When the deviation is completed (after resolution or retesting, if applicable), the Test Manager will review the deviation and attached documentation and verify:

- All fields on the deviation are completed, or Not Applicable, and so marked.
- All indicated attachments are present, and labeled as per the testing procedures.
- Rationale for "Incorrect Expected Results" or "No Change" is adequate enough to withstand a reasonable challenge

After confirmation, the Test Manager will sign the deviation to indicate verification and closure of the deviation.

Non-testing deviations

If events occur during the conduct of the protocol, where there are any exceptions to the protocol instructions, or execution of any test cases/scripts (other than results from the tests) the Test Manager will originate the deviation. The deviation will be logged, tracked, and resolved in the same methods as testing deviations, except that Tester and/or Technical Staff involvement may not be required.

Deviation Report

The following tables list the Deviation Report information.

Protocol ID #:	**Deviation #:**

Deviation identification

Test case/Script #: ______________ Applicable Step: __________________
Reported by: _____________________ Date ORIGINATED: ______________
DESCRIPTION:

SUSPECTED CAUSE:

Deviation resolution

Required Action: Change Expected Results □ Change Required □ No Change □
Resolved by: _________________
Details of Code Change or Reason for No Code Change:

Retest results

Retested by: ______________________ Retest Date: ____________
Retest Results:

Retest Approved by: ______________________ Date: _____________

Deviation Reviewed by: ___________________________ Date: _____________

Deviations log

System: ______________________

Protocol #: ____________________ Page ___ of ___

Test case /Script ID	Issued to	Issue Date	Return Date	Resolved by	Resolved date	Closed date

Reviewed by: ________________________________ Date ___________________

Legend

This lists the legend for the deviations log table:

- Test ID is found on the upper left corner of each approved script.
- Issued To is the person preparing the deviation.
- Issue Date is the date the Deviation form was provided to the requestor.
- Return Date is the date that the completed deviation (with documents) is provided to the Test Manager.
- Resolved by is the person assigned to investigate, resolve, and determine corrective action or actions.
- Resolved date is the date the deviation was returned for closure or retesting.
- Closure date is the date the deviation has final approval.

Q

Validation reports procedure

This appendix describes the Validation reports procedure.

Purpose

The purpose of this procedure is to create and approve reports that will summarize and close out major validation activities.

Scope

This procedure applies to protocols that cover computer system testing and validation plans that cover all, or a portion of, a computer system validation.

Roles and responsibilities

The people who will use this procedure, by role title and activity, are listed in the following table.

Role	Responsibility
Report Preparer	Prepares the Report, and verifies all referenced documentation and records is attached.
Quality Representative	Reviews the Report and attached documentation, records, and verifies report conclusions are justified

Instructions: Report Preparer

Here are the instructions for the Report Preparer to prepare the Validation report.

Report preparation

At the completion of the activities described in the protocol or validation plan, the person who has been assigned the report per the protocol/plan will gather the documentation generated by the prescribed activities in the protocol/plan. A report summarizing the results of the completion of those activities will be prepared, with the following sections:

Purpose

This section will explain the reports functions and summarize the activities, list and discuss the deviations or exceptions, and then determine and explain the conclusion for acceptance.

Scope

This section specifies the system, version, applicable protocol and/or plan, and range of activities that the report covers. In cases where an interim report is created to finalize only a portion of the protocol/plan, the scope of the interim report explains the limitations of the report conclusion. The final report will explain the coverage relationship between the interim and final reports.

Results

This section summarizes the results of the tasks covered in the protocol or plan, including either verification that the tasks were all completed, or an explanation of any incomplete tasks.

Deviations

This section lists all deviations, and summarizes the reasons for accepting the deviations that do not preclude accepting the protocol and/or validation. Any open items that require follow-up tasks must be clearly identified, with the tasks assigned to specific persons and a scheduled date for completion.

Exceptions

During the course of the protocol or validation activities, minor variances from the protocol/plan may surface that are not related to the meeting of any acceptance criteria, but only superfluous items, such as documentation formats, terminology, or personnel assignments. These do not require a deviation to be prepared, but the differences in the protocol/plan statements and the actual validation documents and records must be explained and justified as to why the variance does not require a full deviation.

Between the deviations and the listed exceptions, the validation report must be able to conclude that all the exact statements in the protocol or plan have been completely and precisely met.

Discussion

Since the presence of deviations creates the potential for challenge to the conclusion that the protocol/plan have been met, a discussion of the overall impact of the results will explain the rationale for the conclusion that the acceptance criteria have been demonstrated. The discussion section will provide the conclusion commentary.

Conclusion

This section will contain the statement of conclusion that the protocol or plan demonstrates testing and/or system (or portion named) acceptance. If that conclusion carries any conditions (such as limitations on system use), they must be fully explained.

Follow-up actions

A detailed list of any follow-up actions, tied to specific deviations or risk considerations, must be provided. Each follow-up action must be assigned to a specific person, with a defined completion schedule (due date).

Attachments

Any attachments must be listed in the report. Protocol attachments will at least include the completed test cases/scripts, and all deviations. Plan attachments will be on all the validation records, and may be the table of contents of the validation binder or binders.

Documentation

The report will contain a listing of attachments that will be the documentation and records that support all sections covered in the report.

For a test protocol

The attached documentation will include the test cases/scripts and deviations.

For a Validation report

The attached documentation will be all of the validation records that are within the scope of the validation plan (which may be the table of contents to the validation package).

Instructions: Quality Representative

Here are the instructions for the Report Preparer to prepare the validation report.

Report Quality Review

The designated Quality Representative (according to the protocol or validation plan) will review the report and its accompanying documentation and verify the following:

- The validation records listed in the report are complete and individually approved. Attachments listed in a validation record are complete.
- The validation records demonstrate that every requirement statement in the protocol or plan has been accomplished
- All deviations are completed, closed, and approved. If any follow-up tasks are indicated from a deviation, those tasks have been identified and assigned to a specific person, with a defined completion date.
- Any exceptions have reasonable justification that a deviation is not required.
- The conclusion has adequate support for its argument that the protocol or plan has demonstrated the acceptance criteria has been met, in spite of any deviations.
- There are no follow-up tasks that would require completion before the report conclusion can be accepted.
- The Preparer, system owner representative, and technical representative have reviewed and approved the report.

Report approval

The Quality Representative approval closes the report. For a protocol, this authorizes the next actions defined per the validation plan. For a validation plan, this releases the system (or system section depending on scope) for production use.

R

Infrastructure procedures verification checklist

This appendix contains the infrastructure procedures verification checklist.

Category	Requirement	Procedure #/Section #	Verified by/date
Physical Security	Data Center Personnel access rules ▸ Authorized persons limitations ▸ Visitor escorting rules ▸ Contractor registration and controls		
	Equipment room key card issue, use, recovery, voiding, and periodic verification		

Category	Requirement	Procedure #/Section #	Verified by/date
Change Control	Change Request identification, approval, and processing, including: ► Impact Analysis ► Identification of retesting needs (both new functions and regression) ► Workflow and approvals logic ► Service removal planning, user notification, and status identification ► Documentation updates and reviews ► Return to service planning and user notification ► Change Request records and retention		
	Equipment Configuration Controls		
	Infrastructure inventory records updates and periodic verification		
Backup/Restore	Backup schedule/scope maintenance and approval		
	Backup methods (routine and special)		
	Backup media qualification, recycling, and periodic verification		
	Backup labeling standards and logging records		
	Media storage environmental controls and monitoring (including offsite)		
	Restore authorization, methods, and restore re-verification		
Monitoring and Maintenance	Routine and periodic system monitoring ► Message logs ► Housekeeping tasks ► System Clock verification ► Performance and Capacity checking		
	Anti-virus checking/data file updates		
	Periodic System Maintenance/Cleaning		

Category	Requirement	Procedure #/Section #	Verified by/date
	Preventative/Periodic Maintenance (normal wear replacements)		
	Spare Parts inventory		
Incident Reporting	Problem reporting and classification		
	Investigations and root cause determination		
	Corrective Action definition and approval		
	Resolution completion and records		
	Follow-up actions and verification		
Disaster Plan	Alternate Infrastructure Preparation/Qualification		
	Disaster Declaration and Notification		
	Alternate processing conversion and verification		
	Temporary processing and Business Continuity		
	Recovery and post-recovery verification		
	Period DRP Testing		
Training	Training Plan and Schedule		
	Training Records creation, approval, and retention		
	Revision creation, workflow assignments, commenting, and approval rules		
	Version management (activation, replacement, and obsolescence)		
	Version notification (supervisors/operators) and re-training		
	Document retention, storage, and change history		
Internal Audit	Periodic internal reviews ▸ Procedure content verification ▸ Operator performance verification ▸ Training records verification		

Category	Requirement	Procedure #/Section #	Verified by/date
	Infrastructure Inventory accuracy checks		
	Security logs reviews and authority verification checks		
	Backup verification (storage, records, and integrity sampling)		

Infrastructure Procedures Verification Checklist Signatures

Prepared by: _____________________________________ Date _________

Approved by: ______________________________________ Date _________

Procedure Verification Checklist Test Script

Objective: The objective of this test is to verify that approved procedures as required in the Qualification Plan exist and are available.

Set Up: None.

Procedure:

Step ID	Step	Expected Results	Actual Results	Expectation Satisfied (Yes/No)	Initial/Date
1	Complete the items following tables	All the items completed. Expectations satisfied.			

Item ID	Expectation	Effective Date/Revision	Title	ID	Location	Expectation Satisfied (Yes/No)	Initial/Date
1	Change Control SOP						
2	Deviation Management SOP						
3	CTS Procedure						
4	IBM P670 Startup and Shutdown						
5	IBM P670 Installation Procedure						
6	IBM 2105 Enterprise Storage ServerStartup and Shutdown Procedure						
7	IBM 2105 Enterprise Storage ServerInstallation Procedure						
8	3584 Linear Tape Open LibraryInstallation Procedure						
9	3583 Linear Tape Open LibraryStartup and Shutdown Procedure						

Item ID	Expectation	Effective Date/Revision	Title	ID	Location	Expectation Satisfied (Yes/No)	Initial/Date
10	3583 Linear Tape Open LibraryInstallation Procedure						
11	7014 Rack Installation Procedure						
12	Back Up ServerStartup and Shutdown Procedure						
13	Back Up ServerInstallation Procedure						

Comments:

Summary of Test Script Results		**Test Outcome**		**Deviation Number** (if applicable)
Test Execution Completion Initial/Date:		□ Pass	□ Fail	
Tester:		Signature: ____ Date: ________		
Test Reviewer:		Signature: ____ Date: ________		

S

Regulation, guidance, and standards cross references

This appendix contains the regulation, guidance, and standards cross references.

Regulations, guidance, and standards to IBM Installation Qualification requirements

The following table list regulations, guidance, and standards to IBM suggested Installation Qualification requirements.

IQ					
Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
1	Backup Recovery	21 CFR Parts 210 and 211: cGMP in Manufacturing, Processing, Packing, and Holding of Drugs and Finished Pharmaceuticals (21 CFR 211.68(b)) Revised April 1, 2001 **FDA**	A backup file of data entered into the computer or related system shall be maintained except where certain data, such as calculations performed in connection with laboratory analysis, are eliminated by computerization or other automated processes. In such instances, a written record of the program shall be maintained along with appropriate validation data. Hard copy or alternative systems, such as duplicates, tapes, or microfilm, designed to assure that backup data are exact and complete and that it is secure from alteration, inadvertent erasures, or loss shall be maintained.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
2	Backup Recovery	Guidance to Inspection of Computerized Systems in Drug Processing (Section V:G) February 1983 **FDA**	Determine the firm's shutdown recovery procedure and whether or not, in the event of computer failure, the process is brought into a “safe” condition to protect the product. … Look for inappropriate duplication of steps in the resumption of the process. -- Note recovery time for delay-sensitive processes and investigate instances where excessive delays compromise product quality or where established time limits (21 CFR 211.111) are exceeded.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
3	Calibration	Guidance to Inspection of Computerized Systems in Drug Processing (Section VI:A) February 1983 **FDA**	… the hardware of a computer system is considered to be equipment within the meaning of CGMP regulations. Therefore, those sections of the regulations which address equipment apply to hardware. For example, … 3. 21 CFR 211.68(a) -- States that computers may be used and requires a calibration program.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
4	Change Control	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 4.7) January 11, 2002 **FDA**	Whenever software is changed, a validation analysis should be conducted not just for validation of the individual change, but also to determine the extent and impact of that change on the entire software system.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
5	Change Control	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.5) January 11, 2002 **FDA**	Once a software product has been baselined (approved), any change to that product should have its own “mini life cycle” including testing. Testing of a changed software product requires additional effort. Not only should it demonstrate that the change was implemented correctly; testing should also demonstrate that the change did not adversely impact other parts of the software product.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
6	Change Control	Guidance to Inspection of Computerized Systems in Drug Processing (Section III:C:6) February 1983 **FDA**	Are systems in place to initiate revalidation when significant changes are made?	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
7	Change Control	Guidance to Inspection of Computerized Systems in Drug Processing (Section IV:D:5) February 1983 **FDA**	Are systems in place to initiate revalidation when program changes are made?	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
8	Change Control Configuration Control	Electronic Records; Electronic Signatures 21 CFR Part 11.10 (k:2) Revised April 1, 2001 **FDA**	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
9	Contract Manufacturers	21 CFR Parts 210, 211: cGMP in Manufacturing, Processing, Packing, and Holding of Drugs and Finished Pharmaceuticals (21 CFR 211.22) Revised April 1, 2001 **FDA**	The quality control unit shall be responsible for approving or rejecting drug products manufactured, processed, packed or helped under contract by another company.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
10	Definition	Electronic Records; Electronic Signatures 21 CFR Part 11.3 (b:4) Revised April 1, 2001 **FDA**	Closed system means an environment in which system access is controlled by persons who are responsible for the content of the electronic records that are on the system.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
11	Definition	Electronic Records; Electronic Signatures 21 CFR Part 11.3 (b:9) Revised April 1, 2001 **FDA**	Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
12	Definition User Site Testing	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.6) January 11, 2002 **FDA**	Terms such as beta test, site validation, user acceptance test, installation verification, and installation testing have all be used to describe user site testing. For purposes of this guidance, the term “user site testing” encompasses all of these and any other testing that takes place outside of the developer's controlled environment. This testing should take place at a user's site with the actual hardware and software that will be part of the installed system configuration.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
13	Definitions	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 2.5) January 11, 2002 **FDA** **Reference to FDA GGPPV, GCSSDT)**	Definitions of … and additional information regarding IQ/OQ/PQ may be found in FDA's Glossary of Computerized System and Software Development Terminology.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
14	Definitions Software	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 4.10) January 11, 2002 **FDA**	Software components come in many different forms (e.g. application software, operating systems, compilers, debuggers, configuration management tools, and many more.)	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
15	Design Traceability	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.3) January 11, 2002 **FDA**	A traceability analysis should be conducted to verify that the software design implements all of the software requirements. … the traceability analysis should also certify that all aspects of the design are traceable to software requirements.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
16	Deviations	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.1) January 11, 2002 **FDA**	Procedures should be created for reporting and resolving software anomalies found through validation or other activities.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
17	Deviations	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.7) January 11, 2002 **FDA**	All problems discovered during maintenance of the software should be documented. The resolution of each problem should be tracked to ensure it is fixed, for historical reference, and for trending.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
18	Deviations	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.7) January 11, 2002 **FDA**	Software organizations frequently maintain documentation, such as software problem reports that describe software anomalies discovered and the specific corrective action taken to fix each anomaly. Too often … mistakes are repeated because software developers do not take the next step to determine root causes of problems and make the process and procedural changes needed to avoid recurrence...	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
19	Deviations	Guidance to Inspection of Computerized Systems in Drug Processing (Section V:C) February 1983 **FDA**	Input/output error handling has been a problem in computer systems. Determine the firms' errors handling procedures including documentation, error verification, correction verification, and allowed error overrides including documentation of overrides.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
20	Documentation	21 CFR Parts 210, 211: cGMP in Manufacturing, Processing, Packing, and Holding of Drugs and Finished Pharmaceuticals (21 CFR 194 (8b) Revised April 1, 2001 **FDA**	Complete records shall be maintained of the periodic calibration of laboratory instruments, apparatus, gauges, and recording devices required by 211.60(b)(4).	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
21	Documentation	21 CFR Parts 210, 211: cGMP in Manufacturing, Processing, Packing, and Holding of Drugs and Finished Pharmaceuticals (21 CFR 211.68(b)) April 1, 2001 **FDA**	Appropriate controls shall be exercised over computer or related systems to assure that changes in master production and control records or other records are instituted only by authorized personnel. Input to and output from the computer or related system of formulas or other records of data shall be checked for accuracy. The degree and frequency of input/output verification shall be based on the complexity and reliability of the computer or related system.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
22	Documentation	Electronic Records; Electronic Signatures 21 CFR Part 11.10 (k:1) Revised April 1, 2001 **FDA**	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
23	Documentation	Electronic Records; Electronic Signatures 21 CFR Part 11.1e Revised April 1, 2001 **FDA**	Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
24	Documentation	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.5) January 11, 2002 **FDA**	Test procedures, test data, and test results should be documented in a manner permitting objective pass/fail decisions to be reached. They should also be suitable for review and objective decision making subsequent to running the test, and they should be suitable for use in a subsequent regression testing.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
25	Documentation	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.6) January 11, 2002 **FDA**	Documented evidence of all testing procedures, test input data, and test results should be retained.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
26	Documentation	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.7) January 11, 2002 **FDA**	Documentation should be carefully reviewed to determine which documents have been impacted by a change. All approved documents (e.g. specifications, test procedures, user manuals, etc.) that have been affected should be updated in accordance with configuration management procedures. Specification should be updated before any maintenance and software changes are made.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
27	Documentation	Guidance to Inspection of Computerized Systems in Drug Processing (Section III:C:5) February 1983 **FDA**	Documentation should include a validation protocol and test results which are specifics and meaningful in relation to the attribute being tested.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
28	Documentation	Guidance to Inspection of Computerized Systems in Drug Processing (Section VI:B) February 1983 **FDA**	… software is regarded as records or standard operating procedures (instructions) within the meaning of the CGMP regulations and the corresponding sections of the CGMP regulations apply, for example: 2. 21 CFR 211.180(c) states that records required by the regulations shall be available as part of an authorized inspection ... and are subject to reproduction ... 3. 21 CFR 211.180(d) states that retained records may be original or true copies, and when necessary, copying equipment shall be available. This concept applies to magnetic tape and disks. 4. 21 CFR 211.180(a) states record retention requirements. They are the same for electronic media and paper.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
29	Documentation	Guidance to Inspection of Computerized Systems in Drug Processing (Section VI:B:9) February 1983 **FDA**	21 CFR 211.188(b) requires that batch production and control records includes identification of each person who conducts, supervises or checks each significant step in the process. -- It is quite possible that an automated system can achieve the same, or higher, level of assurance in which case it may not be necessary to have persons document the performance of each event in a series of unbranched automated events ... an acceptable means of complying with the regulation would be all of the following: 1. documentation of the program 2. validation that no step can be missed or poorly executed 3. documentation of the initial and final steps.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
30	Documentation approvals and reviews	Guidance to Inspection of Computerized Systems in Drug Processing (Section IV:D:4) February 1983 **FDA**	Has the software validation been thoroughly documented? Documentation should include a testing protocol and test results which are meaningful and specific to that attribute being tested; individuals who reviewed and approved the validation should be identified in the documentation.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
31	Documentation Testing	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 6.2) January 11, 2002 **FDA**	… validation must be conducted in accordance with a documented protocol, and the validation results must also be documented. Test cases should be documented that will exercise the system to challenge its performance against the pre-determined criteria, especially for its most critical parameters. Test cases should address error and alarm conditions, startup, shutdown, all applicable user functions and operator controls, potential operator errors, maximum and minimum ranges of allowed values, and stress conditions applicable to the intended use of the equipment. The test cases should be executed and the results should be recorded and evaluated to determine whether the results support ... that the software is validated for its intended use.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
32	Documentation Vendor Validation	Guidance to Inspection of Computerized Systems in Drug Processing (Section III:C:6) February 1983 **FDA**	Much of the hardware validation may be performed by the computer vendor. -- Hardware validation data and protocols should be kept at the drug manufacturer's facility. -- When validation information is produced by an outside firm, such as the computer vendor, the records maintained by the drug establishment need not be all inclusive of voluminous test data, however, such records should be reasonably complete (including general results and protocols) to allow the drug manufacturer to assess the adequacy of the validation. A mere certification of suitability from the vendor ... is inadequate.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
33	Documentation Vendor Validation	Guidance to Inspection of Computerized Systems in Drug Processing (Section IV:D) February 1983 **FDA**	… much of the software validation may be accomplished by outside firms … the ultimate responsibility for program suitability rests with the pharmaceutical manufacturer. Records of software validation should be maintained by the drug establishment, although when conducted by outside experts such records need not be voluminous but rather complete enough (including protocols and general results) to allow the drug manufacturer to assess the adequacy of the validation. Mere vendor certification of software suitability is inadequate.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
34	Environment	Guidance to Inspection of Computerized Systems in Drug Processing (Section VI:A) February 1983 **FDA**	… the hardware of a computer system is considered to be equipment within the meaning of CGMP regulations. Therefore, those sections of the regulations which address equipment apply to hardware. For example, … 1. 21 CFR 211.63 -- Equipment be suitable located to facilitate operations for the equipment's intended use. 2. 21 CFR 211.67 -- Requires a maintenance program for equipment 3. 21 CFR 211.68(a) -- States that computers may be used and requires a calibration program.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
35	Equipment Inventory	21 CFR Parts 210, 211: cGMP in Manufacturing, Processing, Packing, and Holding of Drugs and Finished Pharmaceuticals (21 CFR 211.105) Revised April 1, 2001 **FDA**	Major equipment shall be identified by a distinctive identification number or code that shall be recorded in the batch production record to show the specific equipment used in the manufacture of each batch of a drug product.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
36	Equipment Maintenance	21 CFR Parts 210, 211: cGMP in Manufacturing, Processing, Packing, and Holding of Drugs and Finished Pharmaceuticals (21 CFR 211.182) Revised April 1, 2001 **FDA**	A written record of major equipment cleaning, maintenance, and used shall be included in individual equipment logs that show the date, time, product, and lot number of each batch processed.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
37	Hardware Validation Software Validation	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 2.4) January 11, 2002 **FDA (References 21 CFR 11.10(a))**	… computer systems used to create, modify, and maintain electronic records and to manage electronic signatures are also subject to the validation requirements (see 21 CFR 11.10(a). All production and/or quality system software, even if purchased off-the-shelf, should have documented requirements that fully define its intended use, and information against which testing results and other evidence can be compared, to show that software is validated for its intended use.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
38	HW qualification	Guidance to Inspection of Computerized Systems in Drug Processing (Section III:C) February 1983 **FDA**	The suitability of computer hardware for the tasks assigned to pharmaceutical production must be demonstrate through appropriate tests and challenges. The depth and scope of hardware validation will depend upon the complexity of the system and its potential affect on drug quality.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
39	HW testing	Guidance to Inspection of Computerized Systems in Drug Processing (Section III:C:3) February 1983 **FDA**	Have test conditions simulated “worst case” production conditions? A computer may function well under minimal production stress … but falter under high stresses of equipment speed, data input, overload or frequent or continuous multi-shift use (and a harsh environment). -- Some firms may test the circuits of a computer by “feeding” it electrical signals ... but these signal simulators may not pose worst case conditions ... and their accuracy in mimicking input ... should be established. In addition, validation runs should be accomplished on line using actual input devices. Signal simulators ... can be used to train employees ... without actually using production equipment.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
40	HW testing	Guidance to Inspection of Computerized Systems in Drug Processing (Section III:C:4) February 1983 **FDA**	Have hardware tests been repeated enough times to assure a reasonable measure of reproducibility and consistency? In general, at least THREE test runs should be made to cover different operating conditions.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
41	Independence of Review	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 4.9) January 11, 2002 **FDA**	Validation activities should be conducted using the basic quality assurance precept of "independence of review." Self-validation is extremely difficult. When possible, an independent evaluation is always better, especially for higher risk applications.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
42	Input/Output Tests Risk Assessment	Guidance to Inspection of Computerized Systems in Drug Processing (Section V:C) February 1983 **FDA**	(21 CFR) 211.68 … requires that input to and output from the computer system be checked for accuracy. While this does not mean that every bit of input and output need be checked, it does man that checking must be sufficient to proceed a high degree of assurance that input and output are ... accurate. ... reasonable judgment as to the extent and frequency of checking are based on a variety of factors such as the complexity of the computer system.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
43	Installation Testing	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.6) January 11, 2002 **FDA**	Some of the evaluations that have been performed earlier by the software developer at the developer's site should be repeated at the site of actual use. These may include tests for a high volume of data, heavy loads or stresses, security, fault testing (avoidance, detection, tolerance, and recovery), error messages, and implementation of safety requirements. The developer may be able to furnish the user wit some of the test data sets to be used for this purpose.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
44	Installation Testing Configuration, Models, and Versions User Site Testing	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.6) January 11, 2002 **FDA**	There should be evidence that hardware and software are installed and configured as specified. Measures should ensure that all system components are exercised during the testing and that the versions of those components are those specified.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
45	Installation Testing User Site Testing	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.6) January 11, 2002 **FDA References 21 CFR Part 820.170**	Testing at the user site is an essential part of software validation. The Quality System regulation requires installation and inspection procedures (including testing where appropriate) as well as documentation of inspection and testing to demonstrate proper installation. (See 21 CFR Part 820.170.)	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
46	Inventory	Electronic Records; Electronic Signatures 21 CFR Part 11.10 (b) Revised April 1, 2001 **FDA**	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
47	Inventory	Electronic Records; Electronic Signatures 21 CFR Part 11.10 (e) Revised April 1, 2001 **FDA**	Use of secure, computer-generated, time-stamped audit trails to independently records the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
48	IQ for Installation of Monitoring Systems	Guidance to Inspection of Computerized Systems in Drug Processing (Section V:E) February 1983 **FDA**	Determine the degree to which … personnel monitor computerized operations. Is such monitoring continuous or periodic? What functions are monitored? During the inspection … spot-check computer operations such as:(1) Calculations(2) Input recording(3) Component quarantine control(4) Timekeeping(5) Automated cleaning in place(6) Tailings accountability(7) Alarms(8) Shutdown Recovery	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
49	Monitoring	Guidance to Inspection of Computerized Systems in Drug Processing (Section VI:A) February 1983 **FDA**	… the hardware of a computer system is considered to be equipment within the meaning of CGMP regulations. Therefore, those sections of the regulations which address equipment apply to hardware. For example, … 2. 21 CFR 211.67 -- Requires a maintenance program for equipment	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
50	Network IQ	Guidance to Inspection of Computerized Systems in Drug Processing (Section V:A) February 1983 **FDA**	If the firm is on a computer network, it is important to know: 1. what output, such as batch production records, is sent to other parts of the network; 2. what kinds of input (instructions, programs) are received; 3. the identity and location of establishments which interact with the firm 4. the extent and nature of monitoring and controlling activities exercised by remote on-net establishments ... 5. what security measures are used to proven unauthorized entry into the network ... It is possible ... manufacturing operations conducted in one part of the country may be documented ... in some other part of the country. Such records must be immediately retrievable from the computer network at the establishment where the activity took place. (21 CFR 211.180)	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
51	Operational System Checks	Electronic Records; Electronic Signatures 21 CFR Part 11.10 (f) Revised April 1, 2001 **FDA**	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
52	Overrides/Deviations	Guidance to Inspection of Computerized Systems in Drug Processing (Section V:B) February 1983 **FDA**	Functions controlled by computer systems can generally also be controlled by parallel manual back-up systems. -- Determine the interaction of manual and computerized intervention can override or defeat the computerized process. The firm's SOP should describe what manual overrides are allowed, who may execute them, how and under what circumstances. The system may be such that it detects, reacts to and automatically records manual interventions and this should be addressed during the inspection.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
53	Part 11 Scope	Electronic Records; Electronic Signatures 21 CFR Part 11.1b Revised April 1, 2001 **FDA**	This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set for in agency regulations. However, this part does not apply to paper records that are, or have been transmitted by electronic means.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
54	Process Documentation	Guidance to Inspection of Computerized Systems in Drug Processing (Section V:D) February 1983 **FDA**	Process documentation. Most computer systems are capable of generating accurate and detailed documentation of the drug process under computer control. … Records within the scope of the CGMP regulations, which happen to be in computerized form, do contain all of the information required.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
55	Process Documentation	Guidance to Inspection of Computerized Systems in Drug Processing (Section V:G) February 1983 **FDA**	It is important that backup manual systems provide adequate process control and documentation. Determine if back-up manual controls are sufficient to operated the process and if employees are familiar with their operation. Records of manual operations may be less detailed, incomplete, and prone to error, compared to computerized documentation, especially when they are seldom exercised.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
56	Qualifications	Electronic Records; Electronic Signatures 21 CFR Part 11.10 (i) Revised April 1, 2001 **FDA**	A determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
57	Qualifications	Guidance for Industry Computerized Systems Used in Clinical Trials (Section X:A:1) April 1999 **FDA**	Each person who enters or processes data should have the education, training, and experience or any combination thereof necessary to perform the assigned functions.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
58	Qualifications	Guidance for Industry Computerized Systems Used in Clinical Trials (Section X:A:2) April 1999 **FDA**	Individuals responsible for monitoring the trial should have education training, and experience in the use of the computerized system necessary to adequately monitor the trial.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
59	Quality Control	Guidance to Inspection of Computerized Systems in Drug Processing (Section VI:B:8) February 1983 **FDA**	Double Check (if process not) on Computer. 21 CFR 211.101(d) requires verification by a second person for components added to a batch. A single check automated system is acceptable if it provides at least the same assurance of freedom from errors as a double check.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
60	Regression Analysis	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.5) January 11, 2002 FDA	Regression analysis and testing are employed to provide assurance that a change has not created problems elsewhere in the software product. Regression analysis is the determination of the impact of a changed based on review of the relevant documentation (e.g., software requirements specification, software design specification, source code, test plans, test cases, test scripts, etc.) in order to identify the necessary regression tests to be run. Regression testing is the rerunning of test cases that a program has previous executed correctly and comparing the current result to the previous result in order to detect unintended effects of a software change.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
61	Regression Analysis Maintenance	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.7) January 11, 2002 **FDA**	When changes are made to a software system, wither during initial development or during post release maintenance, sufficient regression analysis and testing should be conducted to demonstrate that portions of the software not involved in the change were not adversely impacted.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
62	relevant to IQ?	Guidance to Inspection of Computerized Systems in Drug Processing (Section III:B:5) February 1983 **FDA**	Maintenance procedures should be stated in the firm's standard operating procedures. The availability of spare parts and access to qualified personnel are important to the operation of the maintenance program.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
63	Risk Assessment	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.1) January 11, 2002 **FDA**	Typical Tasks - Quality Planning Risk (Hazard) Management PlanConfiguration Management PlanSoftware Quality Assurance PlanProblem Reporting and Resolution Procedures	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
64	Risk assessment	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 6.1) January 11, 2002 **FDA**	The level of validation effort should be commensurate with the risk posed by the automated operation. In addition to risk, other factors, such as the complexity of the process software and the degree to which the device manufacturer is dependent upon the automated process ... determine the nature and extent of testing as needed as part of the validation effort.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
65	Risk Assessment	Guidance to Inspection of Computerized Systems in Drug Processing (Section VI:B:5) February 1983 **FDA**	factors… must be considered on a case by case basis in determining what is reasonable in accessing a firms' computer. For, example, the effect on drug production is a factor, specifically, if the process of running a program disrupts drug production in an adverse manner then that would be unreasonable. Another factor is ... access to unauthorized information ... we are not entitled to review such as financial data. Consider also that some computer programs are protected by copyright ... and we would not be able to copy and use such programs without prior approval of their owners.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
66	Risk Assessment Documentation	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 6.1) January 11, 2002 **FDA**	Documented requirements and risk analysis of the automated process help to define the scope of the evidence needed to show that the software is validated for its intended use.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
67	Risk Assessment Maintenance	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 6.1) January 11, 2002 **FDA**	… High risk application should not be running in the same operating environment with non-validated software functions, even if those software function are not used. Risk mitigation techniques such as memory partitioning or other approaches to resource protection may need to be considered when high risk applications and lower risk application are used in the same operating environment.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
68	Risk Assessment Software	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 3.1.2) January 11, 2002 **FDA (reference to FDA GCPSSCMD, ISO/IEC)**	Additional guidance regarding safety risk management for software may be found in Section 4 of FDA's Guidance for the Content of Pre-market Submissions for Software Contained in Medical Devices, and in the international standards ISO/IEC 14971-1 and IEC 60601-1-4...	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
69	Risk Assessment Software	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 4.8) January 11, 2002 **FDA**	Validation coverage should be based on the software's complexity and safety risk -- not on firm size or resource constraints.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
70	Security	Electronic Records; Electronic Signatures 21 CFR Part 11.10 (g) Revised April 1, 2001 **FDA**	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
71	Software Configuration Management	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5/2.1) January 11, 2002 **FDA**	A configuration management plan should be developed that will guide and control multiple parallel development activities and ensure proper communications and documentation. … Controls should ensure accurate identification of, and access to, the currently approved versions.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
72	Software Design	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.2) January 11, 2002 **FDA**	The Quality System regulation requires a mechanism for addressing incomplete, ambiguous, or conflicting requirements (see 21 CFR 820.3(c).) Each requirement (e.g. hardware, software, user, operator interface, and safety) identified in the software requirements specification should be evaluated for accuracy, completeness, consistency, testability, correctness, and clarity.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
73	Software Design	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.3) January 11, 2002 **FDA**	Software design specifications should include: Software requirements specification…Software risk analysis …System documentation that describes the system's context in which the program is intended to function, including the relationship of hardware, software, and the physical environment ...Hardware to be used ... Parameters to be measured or recorded ...	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
74	Software Requirements	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.2) January 11, 2002 **FDA**	Software safety requirements are derived from a technical risk management process that is closely integrated with the system requirements development process. Software requirement specification should identify clearly the potential hazards that can result from a software failure in the system as well as any safety requirements to be implemented in software.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
75	Software Requirements	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.2) January 11, 2002 **FDA**	Typical software requirements specify the following … ▸ The intended operating environment for the software, if this is a design constraint) e.g. hardware platform, operating system) ▸ All ranges, limits, defaults, and specific values that the software will accept ▸ All safety related requirements, specifications, features, or functions that will be implemented in software.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
76	Software Testing	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.5) January 11, 2002 **FDA (references: NIST Special Publication 500-235, Structured Testing: A Testing Methodology using the Cyclomatic Complexity MetricNUREG/CR-6293, Verification and Validation Guidelines for High Integrity Systems; IEEE Computer Society Press, Handbook of Software Reliability Engineering)**	Software testing entails running software products under known conditions with defined inputs and documented outcomes that can be compared to their predefined expectations. Test plans and test cases should be created as early in the software development process as feasible. They should identify the schedules, environments, resources (personnel, tools, etc.), methodologies, cases (inputs, procedures, outputs, expected results), documentation, and reporting criteria.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
77	Software Testing	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.5) January 11, 2002 **FDA**	Software testing has limitations that must be recognized and considered when planning the testing of a particular software product. Except for the simplest of programs, software cannot be exhaustively tested. Generally it is not feasible to test a software product with all possible inputs, nor is it possible to test all possible data processing paths that can occur during program execution. -- Testing of all program functionality does not mean all of the program has been tested. -- Software testing that finds no errors should not be interpreted to mean that errors do not exist in the software products; it may mean that testing was superficial.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
78	Software Validation	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 2.4) January 11, 2002 **FDA (References 21 CFR 820, 61 FR 52602)**	Software validation is a requirement of the Quality System regulation… (21 CFR Part 820, 61 FR 52602). Validation requirements apply to software used as components in medical devices, to software that is itself a medical device, and to software used in production of the device or in implementation of the device manufacturer's quality system.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
79	Software Validation	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 2.5) January 11, 2002 FDA	The management and control of the software validation process should not be confused with any other validation requirements, such as process validation for an automated manufacturing process.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
80	Software Validation	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 3.1.2) January 11, 2002 **FDA**	… FDA considers software validation to be "confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled.	"THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
81	Software Validation	Guidance to Inspection of Computerized Systems in Drug Processing (Section IV:D:1) February 1983 **FDA**	Does the program match the assigned operational function?	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
82	Software Validation	Guidance to Inspection of Computerized Systems in Drug Processing (Section IV:D:2) February 1983 **FDA**	A program should be tested, for example, under the most challenging conditions of process speed, data volume, and frequency. Date should be considered in this aspect of validation.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
83	Software Validation	Guidance to Inspection of Computerized Systems in Drug Processing (Section IV:D:3) February 1983 **FDA**	Have tests been repeated enough times to assure consistent reliable results? … In general, at least three separate runs should be made.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
84	Software Validation as it related to Hardware	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 3.1.2) January 11, 2002 **FDA**	Since software is usually par of a larger hardware system, the validation of software typically includes evidence that all software requirements have been implemented correctly and completely and are traceable to system requirements.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
85	SOPs Deviations	21 CFR Parts 210, 211: cGMP in Manufacturing, Processing, Packing, and Holding of Drugs and Finished Pharmaceuticals (21 CFR 211.100(b)) **FDA**	Written production and process control procedures shall be followed in the execution of the various production and process control functions and shall be documented at the time of performance. Any deviation from the written procedures shall be recorded and justified.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
86	Test Planning	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.6) January 11, 2002 **FDA**	User site-testing should follow a pre-defined written plan with a formal summary of testing and a record of formal acceptance.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
87	Testing Maintenance	Electronic Records; Electronic Signatures 21 CFR Part 11.300 (e) Revised April 1, 2001 **FDA**	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
88	Training	21 CFR Parts 210, 211: cGMP in Manufacturing, Processing, Packing, and Holding of Drugs and Finished Pharmaceuticals (21 CFR 211.25) Revised April 1, 2001 **FDA**	Each person engaged in the manufacture, processing, packing, or holding of a drug product shall have education training, and experience, or any combination thereof to enable that person to perform the assigned functions. Training shall be in the particular operations that the employee performs .... There shall be an adequate number of qualified personnel to perform and supervise the manufacture, processing, packing, or holding of each drug product.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ					
Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
89	Training Documentation	Guidance for Industry Computerized Systems Used in Clinical Trials (Section X:C) April 1999 **FDA**	Employee education, training, and experience should be documented.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
90	User Requirements Environmental Conditions	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 6.2) January 11, 2002 **FDA**	The device manufacturer (user) needs to define the expected operating environment including any required hardware and software configurations, … The user also needs to: document requirements for system performance, quality, error handling, startup, shutdown, security, etc....	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
91	User Site Testing	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 5.2.6) January 11, 2002 **FDA**	… Manufacturing equipment must meet specified requirements, and automated systems must be validated for their intended use.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
92	Validation	Electronic Records; Electronic Signatures 21 CFR Part 11.10 (a) Revised April 1, 2001 **FDA**	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
93	Validation	Electronic Records; Electronic Signatures 21 CFR Part 11.10 (h) Revised April 1, 2001 **FDA**	Use of device (e.g. terminal) checks to determine as appropriate, the validity of the source of data input or operational instruction.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
94	Validation	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 6) January 11, 2002 **FDA (references 21 CFR Part 820.70(i))**	The Quality System regulation requires that “when computers of automated data processing systems are used as part of production or the quality system, the manufacturer shall validate computer software of its intended use according to an established protocol. (See 21 CFR 820,70(1). This has been a regulatory requirements of ... GMP regulations since 1978.)	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
95	Validation	ICH Harmonized Tripartite Guideline: Guideline for Good Clinical Practice (Step 4 of the ICH process) (Section 5.5.3) May 1996 **ICH Steering Committee**	When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should: (a) ensure and document that the electronic data processing systems conforms to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance (i.e. validation), (b) Maintains SOPs for using these systems, (c) Ensure that the systems are designed to permit data changes in such a way that the data changes are documented and that there is no deletion of entered data (i.e. maintain an audit trail, data train, edit trail), (d) Maintain a security system that prevents unauthorized access to the data.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
96	Validation Evidence	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 6.1) January 11, 2002 **FDA**	The extent of validation evidence needed for (commercial software applications … used as part of the quality system, e.g. a spreadsheet or statistical package …, a graphics package used for trend analysis, or a commercial database…) depends on the device manufacturer's documented intended use of that software.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
97	Validation Documentation	21 CFR Parts 210, 211: cGMP in Manufacturing, Processing, Packing, and Holding of Drugs and Finished Pharmaceuticals (21 CFR 211.68(a)) Revised April 1, 2001 **FDA**	Automated, mechanical, or electronic equipment or other types of equipment, including computers, or related systems that will perform a function satisfactorily … If such equipment is so used, it shall be routinely calibrated, inspected, or checked according to a written program designed to assure proper performance. Written records of those calibration checks and inspections shall be maintained.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
98	Validation Maintenance	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 6.1) January 11, 2002 **FDA**	When software is upgraded or any chances are made to the software, the … manufacturer should consider how those changes may impact “used portions” of the software and must confirm the validation of those portions of software that are used.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
99	Validation Security	Guidance to Inspection of Computerized Systems in Drug Processing (Section VI:B) February 1983 **FDA**	… software is regarded as records or standard operating procedures (instructions) within the meaning of the CGMP regulations and the corresponding sections of the CGMP regulations apply, for example: 1. 21 CFR 211.68(b) -- requires programs to ensure accuracy and security of computer inputs, outputs, and data.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
100	Validation Security	Guidance to Inspection of Computerized Systems in Drug Processing (Section VI:B:) February 1983 **FDA**	… software is regarded as records or standard operating procedures (instructions) within the meaning of the CGMP regulations and the corresponding sections of the CGMP regulations apply, for example: 1. 21 CFR 211.68(b) -- requires programs to ensure accuracy and security of computer inputs, outputs, and data.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
101	Vendor Audit	General Principals of Software Validation; Final Guidance for Industry and FDA Staff (Section 6.3) January 11, 2002 **FDA**	Where possible and depending upon the device risk involved, the device manufacture should consider auditing the vendor's design and development methodologies used in construction of the OTS (off the shelf) software, and should assess the development and validation documentation ... Some vendors who are not accustomed to operating in a regulated environment may not have a documented life cycle process that can support the decide manufacturer's validation requirement. Other vendors may not permit an audit. Where ... validation information is not available from the vendor, the device manufacturer will need to perform sufficient system level “black box” testing to establish that the software meets their “user needs and intended uses”.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
102		Guidance for Industry Computerized Systems Used in Clinical Trials (Section III:B) April 1999 **FDA**	For each study, documentation should identify what software and, if known, what hardware is to be used in computerized systems that create, modify, maintain, archive, retrieve, or transmit data.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
103		Guidance for Industry Computerized Systems Used in Clinical Trials (Section III:L) April 1999 **FDA**	Security measures should be in place to prevent unauthorized access to the data and to the computerized system.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
104		Guidance for Industry Computerized Systems Used in Clinical Trials (Section IV) April 1999 **FDA**	SOP's (standard operating procedures) should be established for, but not limited to: ► System Setup/Installation ► Data Collection and Handling ► System Maintenance ► Data Backup and Recovery, and Contingency Plans ► Security ► Change Control	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
105		Guidance for Industry Computerized Systems Used in Clinical Trials (Section IX:A) April 1999 **FDA**	Measures should be in place to ensure that versions of software used to generate, collect, maintain, and transmit data are the versions that are stated in the systems documentation.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
106		Guidance for Industry Computerized Systems Used in Clinical Trials (Section IX:C) April 1999 **FDA**	Backup and recovery procedures should be clearly outlined in the SOPs and be sufficient to protect against data loss. Records should be backed up regularly in a way that would prevent a catastrophic loss and ensure the quality and integrity of the data.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
107		Guidance for Industry Computerized Systems Used in Clinical Trials (Section IX:D) April 1999 **FDA**	Backup records should be stored at a secure location specified in the SOPs. Storage is typically offsite or in a building separate from the original records.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
108		Guidance for Industry Computerized Systems Used in Clinical Trials (Section V:C:1) April 1999 **FDA**	Controls should be in place to ensure that the system's date and time are correct.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
109		Guidance for Industry Computerized Systems Used in Clinical Trials (Section V:C:3,4) April 1999 **FDA**	Dates and times are to be local to the activity being documented and should include the year, month, day, hour, and minute. … Calculation of the local time stamp may be derived in such cases from a remote server located in a different time zone.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
110		Guidance for Industry Computerized Systems Used in Clinical Trials (Section VI:C:2) April 1999 **FDA**	When migrating to newer systems, it is important to generate accurate and complete copies of study data and collateral information relevant to data integrity. … The transcription process needs to be validated.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ					
Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
111		Guidance for Industry Computerized Systems Used in Clinical Trials (Section VII:A:1) April 1999 **FDA**	In addition to internal safeguards built into the system, external safeguards should be in place to ensure that access to the computerized system and to the data is restricted to authorized personnel.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
112		Guidance for Industry Computerized Systems Used in Clinical Trials (Section VII:A:2) April 1999 **FDA**	Staff should be thoroughly aware of system security measures and the importance of limiting access to authorized personnel.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
113		Guidance for Industry Computerized Systems Used in Clinical Trials (Section VII:B:2) April 1999 **FDA**	There should be a cumulative record that indicated, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
114		Guidance for Industry Computerized Systems Used in Clinical Trials (Section VII:B:4) April 1999 **FDA**	If a computerized system being used for the clinical study is part of a system normally used for other purposes, efforts should be made to ensure that the study software is logically and physically isolated as necessary to precluded unintended interaction with non-study software. If any of the software programs are changed, the system should be evaluated to determine the effect of the changes on logical security.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
115		Guidance for Industry Computerized Systems Used in Clinical Trials (Section VII:B:5) April 1999 **FDA**	Controls should be in place to prevent, detect, and mitigate effects of computer viruses on study data and software.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
116		Guidance for Industry Computerized Systems Used in Clinical Trials (Section VIII:A) April 1999 **FDA**	Systems documentation should be readily available at the site where clinical trials are conducted. Such documentation should provide an overall description of computerized systems and the relationship of hardware, software, and physical environment.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
117		Guidance for Industry Computerized Systems Used in Clinical Trials (Section VIII:B) April 1999 **FDA**	FDA may inspect documentation, possessed by a regulated company, that demonstrates validation of software.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
118		Guidance for Industry Computerized Systems Used in Clinical Trials (Section VIII:B:b) April 1999 **FDA**	A written test plan based on the design specification, including both structural and functional analysis …	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
119		Guidance for Industry Computerized Systems Used in Clinical Trials (Section VIII:B:c) April 1999 **FDA**	Test results and an evaluation of how these results demonstrate that the predetermined design specification has been met.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
120		Guidance for Industry Computerized Systems Used in Clinical Trials (Section VIII:C:2) April 1999 **FDA**	The impact of any change to the system should be evaluated and a decision made regarding the needs to revalidate. Revalidation should be performed for changes that exceed operational limits or design specifications.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
121		Guidance for Industry Computerized Systems Used in Clinical Trials (Section VIII:C:3) **FDA**	All changes to the system should be documented.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
122		Guidance for Industry Computerized Systems Used in Clinical Trials (Section X:B:1) April 1999 **FDA**	Training should be provided to individuals in the specific operations that they are to perform.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
123		Guidance for Industry Computerized Systems Used in Clinical Trials (Section X:B:2) April 1999 **FDA**	Training should be conducted by qualified individuals on a continuing basis, as needed, to ensure familiarity with the computerized system and with any changes to the system during the course of the study.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
124		Guidance for Industry Computerized Systems Used in Clinical Trials (Section XI:B) April 1999 **FDA**	The sponsor should be able to provide hardware and software as necessary for FDA personnel to inspect the electronic documents and audit trail at the site where an FDA inspection is taking place.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
125		Guidance to Inspection of Computerized Systems in Drug Processing (Section III) February 1983 **FDA**	During the inspection identify the manufacturers/suppliers of important computer hardware, include make and model designations where possible. Hardware to identify this way includes CPUs, disk/tape devices, CRT's, printers, and signal converters.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	**Topic**	**Document Reference (Name, Section or Page, and Date) Source**	**Quote from Document Reference**	**Location within Infrastructure Installation Qualification Plan**	**Comments**
126		Guidance to Inspection of Computerized Systems in Drug Processing (Section III) February 1983 **FDA**	For each significant computerized system, it may be helpful to prepare or OED schematic drawing of the attendant hardware. The drawing need only include major input devices, output devices, signal converters, central processing unit, distribution systems, significant peripheral devices and how they are linked.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
127		Guidance to Inspection of Computerized Systems in Drug Processing (Section III:A:5) February 1983 **FDA**	Networks are generally extensions of distributed processing. -- Potentially, pharmaceutical companies could have international networks …	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
128		Guidance to Inspection of Computerized Systems in Drug Processing (Section III:A:5) February 1983 **FDA**	The interconnection of two or more computers … also known as distributed processing. -- A large CPU may also act as a "host" for one or more other CPUs. When such inspections are encountered during an inspection, it is important to know the configuration of the system and exactly what command and information can be relayed amongst the computers.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
129		Guidance to Inspection of Computerized Systems in Drug Processing (Section III:A:6) February 1983 **FDA**	All computer associated devices external to the CPU can be considered peripheral devices. -- Many peripheral devices can be both input and output … these include CRT's, printers, keyboards, disk drives, modems, and tape drives.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
130		Guidance to Inspection of Computerized Systems in Drug Processing (Section III:B:1:a) February 1983 **FDA**	Hostile Environments. Environmental extremes of temperature, humidity, static, dust, electromagnetic interference should be avoided. Such conditions may be common in certain pharmaceutical operations and the investigator should be alert to locating sensitive hardware in such areas. Environmental safeguards may be necessary ...	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
131		Guidance to Inspection of Computerized Systems in Drug Processing (Section III:B:1:a) February 1983 **FDA**	Physical security is also a consideration in protecting computer hardware from damage.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

IQ

Ref #	Topic	Document Reference (Name, Section or Page, and Date) Source	Quote from Document Reference	Location within Infrastructure Installation Qualification Plan	Comments
132		Guidance to Inspection of Computerized Systems in Drug Processing (Section III:B:1:b) February 1983 **FDA**	Excessive Distances between CPU and Peripheral Devices. Excessively long low voltage electrical lines … are vulnerable to electromagnetic interference. This may result in inaccurate or distorted input data to the computer. In a particularly “noisy” electronic environment, this problem might be solved by the use of fiber optic lines to convey digital signals.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
133		Guidance to Inspection of Computerized Systems in Drug Processing (Section III:B:3) February 1983 **FDA**	Command over-rides. In distributed systems, it is important to know how errors and command over-rides at one computer are related to operations at another computer in the system. The limits on information and command for distributed systems should be clearly established ...	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.
134		Guidance to Inspection of Computerized Systems in Drug Processing (Section III:B:3) February 1983 **FDA**	I/O Device. The accuracy and performance of these devices are vital to the proper operation of the computer system. … Sensors should be systematically calibrated and checked for accurate signal outputs.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.	THIS COLUMN TO BE COMPLETED WHEN APPENDIXES INCLUDING <COMPANY> SITE DOCUMENTS ARE ADDED/ADDENDED TO INFRASTRUCTURE INSTALLATION PLAN.

Part 3

FDA 21 CFR Part 11 and guidance

This section provides regulatory information that is current as of the date of this publication from the FDA Web sites. In this regulatory information, the FDA provides readers other reference sources some of which have been updated since this FDA publication.

This part contains the following appendixes:

- Appendix T, “FDA 21 CFR Part 11 Preamble”
- Appendix U, “FDA 21 CFR Part 11 Final Rule”
- Appendix V, “FDA guidance for industry: Computerized systems in clinical trials”
- Appendix W, “FDA guidance: General principles of software validation”
- Appendix X, “FDA guides to inspections”

T

FDA 21 CFR Part 11 Preamble

WAIS Document Retrieval [Federal Register: March 20, 1997 (Volume 62, Number 54)]
[Rules and Regulations]
[**FDA pages 13429-13466**]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr20mr97-25]
[**FDA page 13429**]

Part II
Department of Health and Human Services

Food and Drug Administration

21 CFR Part 11
Electronic Records; Electronic Signatures; Final Rule
Electronic Submissions; Establishment of Public Docket; Notice
[**FDA page 13430**]
DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

21 CFR Part 11

[Docket No. 92N-0251]
RIN 0910-AA29

Electronic Records; Electronic Signatures

AGENCY: Food and Drug Administration, HHS.

ACTION: Final rule.

SUMMARY: The Food and Drug Administration (FDA) is issuing regulations that provide criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. These regulations, which apply to all FDA program areas, are intended to permit the widest possible use of electronic technology, compatible with FDA's responsibility to promote and protect public health. The use of electronic records as well as their submission to FDA is voluntary. Elsewhere in this issue of the Federal Register, FDA is publishing a document providing information concerning submissions that the agency is prepared to accept electronically.

DATES: Effective August 20, 1997. Submit written comments on the information collection provisions of this final rule by May 19, 1997.

ADDRESSES: Submit written comments on the information collection provisions of this final rule to the Dockets Management Branch (HFA-305), Food and Drug Administration, 12420 Parklawn Dr., rm. 1-23, Rockville, MD 20857.

The final rule is also available electronically via Internet: http://www.fda.gov.

FOR FURTHER INFORMATION CONTACT: Paul J. Motise, Center for Drug Evaluation and Research (HFD-325), Food and Drug Administration, 7520 Standish Pl., Rockville, MD 20855, 301-594-1089. E-mail address via Internet: Motise@CDER.FDA.GOV, [Note 5/21/2001: Current address is mailto:pmotise@ora.fda.gov] or Tom M. Chin, Division of Compliance Policy (HFC-230), Food and Drug Administration, 5600 Fishers Lane, Rockville, MD 20857, 301-827-0410. E-mail address via Internet: TChin@FDAEM.SSW.DHHS.GOV [Note 5/21/2001: Current address is mailto:tchin@ora.fda.gov]

SUPPLEMENTARY INFORMATION:

I. Background

In 1991, members of the pharmaceutical industry met with the agency to determine how they could accommodate paperless record systems under the current good manufacturing practice (CGMP) regulations in parts 210 and 211 (21 CFR parts 210 and 211). FDA created a Task Force on Electronic Identification/Signatures to develop a uniform approach by which the agency could accept electronic signatures and records in all program areas. In a February 24, 1992, report, a task force subgroup, the Electronic Identification/Signature Working Group, recommended publication of an advance notice of proposed rulemaking (ANPRM) to obtain public comment on the issues involved.

In the Federal Register of July 21, 1992 (57 FR 32185), FDA published the ANPRM, which stated that the agency was considering the use of electronic identification/signatures, and requested comments on a number of related topics and concerns. FDA received 53 comments on the ANPRM. In the Federal Register of August 31, 1994 (59 FR 45160), the agency published a proposed rule that incorporated many of the comments to the ANPRM, and requested that comments on the proposed regulation be submitted by November 29, 1994. A complete discussion of the options considered by FDA and other background information on the agency's policy on electronic records and electronic signatures can be found in the ANPRM and the proposed rule.

FDA received 49 comments on the proposed rule. The commenters represented a broad spectrum of interested parties: Human and veterinary pharmaceutical companies as well as biological products, medical device, and food interest groups, including 11 trade associations, 25 manufacturers, and 1 Federal agency.

II. Highlights of the Final Rule

The final rule provides criteria under which FDA will consider electronic records to be equivalent to paper records, and electronic signatures equivalent to traditional handwritten signatures. Part 11 (21 CFR part 11) applies to any paper records required by statute or agency regulations and supersedes any existing paper record requirements by providing that electronic records may be used in lieu of paper records. Electronic signatures which meet the requirements of the rule will be considered to be equivalent to full handwritten signatures, initials, and other general signings required by agency regulations.

Section 11.2 provides that records may be maintained in electronic form and electronic signatures may be used in lieu of traditional signatures. Records and signatures submitted to the agency may be presented in an electronic form provided the requirements of part 11 are met and the records have been identified in a public docket as the type of submission the agency accepts in an electronic form. Unless records are identified in this docket as appropriate for electronic submission, only paper records will be regarded as official submissions.

Section 11.3 defines terms used in part 11, including the terms: Biometrics, closed system, open system, digital signature, electronic record, electronic signature, and handwritten signature.

Section 11.10 describes controls for closed systems, systems to which access is controlled by persons responsible for the content of electronic records on that system. These controls include measures designed to ensure the integrity of system operations and information stored in the system. Such measures include: (1) Validation; (2) the ability to generate accurate and complete copies of records; (3) archival protection of records; (4) use of computer-generated, time-stamped audit trails; (5) use of appropriate controls over systems documentation; and (6) a determination that persons who develop, maintain, or use electronic records and signature systems have the education, training, and experience to perform their assigned tasks.

Section 11.10 also addresses the security of closed systems and requires that: (1) System access be limited to authorized individuals; (2) operational system checks be used to enforce permitted sequencing of steps and events as appropriate; (3) authority checks be used to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform operations; (4) device (e.g., terminal) checks be used to determine the validity of the source of data input or operation instruction; and (5) written policies be established and adhered to holding individuals accountable and responsible for actions initiated under their electronic signatures, so as to deter record and signature falsification.

Section 11.30 sets forth controls for open systems, including the controls required for closed systems in Sec. 11.10 and additional measures such as document encryption and use of appropriate digital signature standards [**FDA page 13431**] to ensure record authenticity, integrity, and confidentiality.

Section 11.50 requires signature manifestations to contain information associated with the signing of electronic records. This information must include the printed name of the signer, the date and time when the signature was executed, and the meaning (such as review, approval, responsibility, and authorship) associated with the signature. In addition, this information is subject to the same controls as for electronic records and must be included in any human readable forms of the electronic record (such as electronic display or printout).

Under Sec. 11.70, electronic signatures and handwritten signatures executed to electronic records must be linked to their respective records so that signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Under the general requirements for electronic signatures, at Sec. 11.100, each electronic signature must be unique to one individual and must not be reused by, or reassigned to, anyone else. Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, the organization shall verify the identity of the individual.

Section 11.200 provides that electronic signatures not based on biometrics must employ at least two distinct identification components such as an identification code and password. In addition, when an individual executes a series of signings during a single period of controlled system access, the first signing must be executed using all electronic signature components and the subsequent signings must be executed using at least one component designed to be used only by that individual. When an individual executes one or more signings not performed during a single period of controlled system access, each signing must be executed using all of the electronic signature components.

Electronic signatures not based on biometrics are also required to be used only by their genuine owners and administered and executed to ensure that attempted use of an individual's electronic signature by anyone else requires the collaboration of two or more individuals. This would make it more difficult for anyone to forge an electronic signature. Electronic signatures based upon biometrics must be designed to ensure that such signatures cannot be used by anyone other than the genuine owners.

Under Sec. 11.300, electronic signatures based upon use of identification codes in combination with passwords must employ controls to ensure security and integrity. The controls must include the following provisions: (1) The uniqueness of each combined identification code and password must be maintained in such a way that no two individuals have the same combination of identification code and password; (2) persons using identification codes and/or passwords must ensure that they are periodically recalled or revised; (3) loss management procedures must be followed to deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification codes or password information; (4) transaction safeguards must be used to prevent unauthorized use of passwords and/or identification codes, and to detect and report any attempt to misuse such codes; (5) devices that bear or generate identification codes or password information, such as tokens or cards, must be tested initially and periodically to ensure that they function properly and have not been altered in an unauthorized manner.

III. Comments on the Proposed Rule

A. General Comments

1. Many comments expressed general support for the proposed rule. Noting that the proposal's regulatory approach incorporated several suggestions submitted by industry in comments on the ANPRM, a number of comments stated that the proposal is a good example of agency and industry cooperation in resolving technical issues.

Several comments also noted that both industry and the agency can realize significant benefits by using electronic records and electronic signatures, such as increasing the speed of information exchange, cost savings from the reduced need for storage space, reduced errors, data integration/trending, product improvement, manufacturing process streamlining, improved process control, reduced vulnerability of electronic signatures to fraud and abuse, and job creation in industries involved in electronic record and electronic signature technologies.

One comment noted that, when part 11 controls are satisfied, electronic signatures and electronic records have advantages over paper systems, advantages that include: (1) Having automated databases that enable more advanced searches of information, thus obviating the need for manual searches of paper records; (2) permitting information to be viewed from multiple perspectives; (3) permitting determination of trends, patterns, and behaviors; and (4) avoiding initial and subsequent document misfiling that may result from human error.

There were several comments on the general scope and effect of proposed part 11. These comments noted that the final regulations will be viewed as a standard by other Government agencies, and may strongly influence the direction of electronic record and electronic signature technologies. One comment said that FDA's position on electronic signatures/electronic records is one of the most pressing issues for the pharmaceutical industry and has a significant impact on the industry's future competitiveness. Another comment said that the rule constitutes an important milestone along the Nation's information superhighway.

FDA believes that the extensive industry input and collaboration that went into formulating the final rule is representative of a productive partnership that will facilitate the use of advanced technologies. The agency acknowledges the potential benefits to be gained by electronic record/electronic signature systems. The agency expects that the magnitude of these benefits should significantly outweigh the costs of making these systems, through compliance with part 11, reliable, trustworthy, and compatible with FDA's responsibility to promote and protect public health. The agency is aware of the potential impact of the rule, especially regarding the need to accommodate and encourage new technologies while maintaining the agency's ability to carry out its mandate to protect public health. The agency is also aware that other Federal agencies share the same concerns and are addressing the same issues as FDA; the agency has held informal discussions with other Federal agencies and participated in several interagency groups on electronic records/electronic signatures and information technology issues. FDA looks forward to exchanging information and experience with other agencies for mutual benefit and to promote a consistent Federal policy on electronic records and signatures. The agency also notes that benefits, such as the ones listed by the comments, will help to offset any system modification costs that persons may incur to achieve compliance with part 11.

B. Regulations Versus Guidelines

2. Several comments addressed whether the agency's policy on electronic signatures and electronic records should be issued as a regulation [**FDA page 13432**] or recommended in a guideline. Most comments supported a regulation, citing the need for a practical and workable approach for criteria to ensure that records can be stored in electronic form and are reliable, trustworthy, secure, accurate, confidential, and authentic. One comment specifically supported a single regulation covering all FDA-regulated products to ensure consistent requirements across all product lines. Two comments asserted that the agency should only issue guidelines or “make the regulations voluntary." One of these comments said that by issuing regulations, the agency is shifting from creating tools to enhance communication (technological quality) to creating tools for enforcement (compliance quality).

The agency remains convinced, as expressed in the preamble to the proposed rule (59 FR 45160 at 45165), that a policy statement, inspection guide, or other guidance would be an inappropriate means for enunciating a comprehensive policy on electronic signatures and records. FDA has concluded that regulations are necessary to establish uniform, enforceable, baseline standards for accepting electronic signatures and records. The agency believes, however, that supplemental guidance documents would be useful to address controls in greater detail than would be appropriate for regulations. Accordingly, the agency anticipates issuing supplemental guidance as needed and will afford all interested parties the opportunity to comment on the guidance documents.

The need for regulations is underscored by several opinions expressed in the comments. For example, one comment asserted that it should be acceptable for supervisors to remove the signatures of their subordinates from signed records and replace them with their own signatures. Although the agency does not object to the use of a supervisor's signature to endorse or confirm a subordinate's actions, removal of an original signature is an action the agency views as falsification. Several comments also argued that an electronic signature should consist of only a password, that passwords need not be unique, that it is acceptable for people to use passwords associated with their personal lives (like the names of their children or their pets), and that passwords need only be changed every 2 years. FDA believes that such procedures would greatly increase the possibility that a password could be compromised and the chance that any resulting impersonation and/or falsification would continue for a long time. Therefore, an enforceable regulation describing the acceptable characteristics of an electronic signature appears necessary.

C. Flexibility and Specificity

3. Several comments addressed the flexibility and specificity of the proposed rule. The comments contended that agency acceptance of electronic records systems should not be based on any particular technology, but rather on the adequacy of the system controls under which they are created and managed. Some comments claimed that the proposed rule was overly prescriptive and that it should not specify the mechanisms to be used, but rather only require owners/users to design appropriate safeguards and validate them to reasonably ensure electronic signature integrity and authenticity. One comment commended the agency for giving industry the freedom to choose from a variety of electronic signature technologies, while another urged that the final rule be more specific in detailing software requirements for electronic records and electronic notebooks in research and testing laboratories.

The agency believes that the provisions of the final rule afford firms considerable flexibility while providing a baseline level of confidence that records maintained in accordance with the rule will be of high integrity. For example, the regulation permits a wide variety of existing and emerging electronic signature technologies, from use of identification codes in conjunction with manually entered passwords to more sophisticated biometric systems that may necessitate additional hardware and software. While requiring electronic signatures to be linked to their respective electronic records, the final rule affords flexibility in achieving that link through use of any appropriate means, including use of digital signatures and secure relational database references. The final rule accepts a wide variety of electronic record technologies, including those based on optical storage devices. In addition, as discussed in comment 40 of this document, the final rule does not establish numerical standards for levels of security or validation, thus offering firms flexibility in determining what levels are appropriate for their situations. Furthermore, while requiring operational checks, authority checks, and periodic testing of identifying devices, persons have the flexibility of conducting those controls by any suitable method. When the final rule calls for a certain control, such as periodic testing of identification tokens, persons have the option of determining the frequency.

D. Controls for Electronic Systems Compared with Paper Systems

4. Two comments stated that any controls that do not apply to paper-based document systems and handwritten signatures should not apply to electronic record and signature systems unless those controls are needed to address an identified unique risk associated with electronic record systems. One comment expressed concern that FDA was establishing a much higher standard for electronic signatures than necessary.

In attempting to establish minimum criteria to make electronic signatures and electronic records trustworthy and reliable and compatible with FDA's responsibility to promote and protect public health (e.g., by hastening the availability of new safe and effective medical products and ensuring the safety of foods), the agency has attempted to draw analogies to handwritten signatures and paper records wherever possible. In doing so, FDA has found that the analogy does not always hold because of the differences between paper and electronic systems. The agency believes some of those differences necessitate controls that will be unique to electronic technology and that must be addressed on their own merits and not evaluated on the basis of their equivalence to controls governing paper documents.

The agency found that some of the comments served to illustrate the differences between paper and electronic record technologies and the need to address controls that may not generally be found in paper record systems. For example, several comments pointed out that electronic records built upon information databases, unlike paper records, are actually transient views or representations of information that is dispersed in various parts of the database. (The agency notes that the databases themselves may be geographically dispersed but linked by networks.) The same software that generates representations of database information on a screen can also misrepresent that information, depending upon how the software is written (e.g., how a query is prepared). In addition, database elements can easily be changed at any time to misrepresent information, without evidence that a change was made, and in a manner that destroys the original information. Finally, more people have potential access to electronic record [**FDA page 13433**] systems than may have access to paper records.

Therefore, controls are needed to ensure that representations of database information have been generated in a manner that does not distort data or hide noncompliant or otherwise bad information, and that database elements themselves have not been altered so as to distort truth or falsify a record. Such controls include: (1) Using time-stamped audit trails of information written to the database, where such audit trails are executed objectively and automatically rather than by the person entering the information, and (2) limiting access to the database search software. Absent effective controls, it is very easy to falsify electronic records to render them indistinguishable from original, true records.

The traditional paper record, in comparison, is generally a durable unitized representation that is fixed in time and space. Information is recorded directly in a manner that does not require an intermediate means of interpretation. When an incorrect entry is made, the customary method of correcting FDA-related records is to cross out the original entry in a manner that does not obscure the prior data. Although paper records may be falsified, it is relatively difficult (in comparison to falsification of electronic records) to do so in a nondetectable manner. In the case of paper records that have been falsified, a body of evidence exists that can help prove that the records had been changed; comparable methods to detect falsification of electronic records have yet to be fully developed.

In addition, there are significant technological differences between traditional handwritten signatures (recorded on paper) and electronic signatures that also require controls unique to electronic technologies. For example, the traditional handwritten signature cannot be readily compromised by being “loaned” or “lost,” whereas an electronic signature based on a password in combination with an identification code can be compromised by being “loaned” or “lost.” By contrast, if one person attempts to write the handwritten signature of another person, the falsification would be difficult to execute and a long-standing body of investigational techniques would be available to detect the falsification. On the other hand, many electronic signatures are relatively easy to falsify and methods of falsification almost impossible to detect.

Accordingly, although the agency has attempted to keep controls for electronic record and electronic signatures analogous to traditional paper systems, it finds it necessary to establish certain controls specifically for electronic systems.

E. FDA Certification of Electronic Signature Systems

5. One comment requested FDA certification of what it described as a low-cost, biometric-based electronic signature system, one which uses dynamic signature verification with a parameter code recorded on magnetic stripe cards.

The agency does not anticipate the need to certify individual electronic signature products. Use of any electronic signature system that complies with the provisions of part 11 would form the basis for agency acceptance of the system regardless of what particular technology or brand is used. This approach is consistent with FDA's policy in a variety of program areas. The agency, for example, does not certify manufacturing equipment used to make drugs, medical devices, or food.

F. Biometric Electronic Signatures

6. One comment addressed the agency's statement in the proposed rule (59 FR 45160 at 45168) that the owner of a biometric/behavioral link could not lose or give it away. The comment stated that it was possible for an owner to “lend” the link for a file to be opened, as a collaborative fraudulent gesture, or to unwittingly assist a fraudulent colleague in an “emergency,” a situation, the comment said, that was not unknown in the computer industry.

The agency acknowledges that such fraudulent activity is possible and that people determined to falsify records may find a means to do so despite whatever technology or preventive measures are in place. The controls in part 11 are intended to deter such actions, make it difficult to execute falsification by mishap or casual misdeed, and to help detect such alterations when they occur (see Sec. 11.10 (introductory paragraph and especially Secs. 11.10(j) and 11.200(b)).

G. Personnel Integrity

7. A few comments addressed the role of individual honesty and trust in ensuring that electronic records are reliable, trustworthy, and authentic. One comment noted that firms must rely in large measure upon the integrity of their employees. Another said that subpart C of part 11, Electronic Signatures, appears to have been written with the belief that pharmaceutical manufacturers have an incentive to falsify electronic signatures. One comment expressed concern about possible signature falsification when an employee leaves a company to work elsewhere and the employee uses the electronic signature illegally.

The agency agrees that the integrity of any electronic signature/electronic record system depends heavily upon the honesty of employees and that most persons are not motivated to falsify records. However, the agency's experience with various types of records and signature falsification demonstrates that some people do falsify information under certain circumstances. Among those circumstances are situations in which falsifications can be executed with ease and have little likelihood of detection. Part 11 is intended to minimize the opportunities for readily executing falsifications and to maximize the chances of detecting falsifications.

Concerning signature falsification by former employees, the agency would expect that upon the departure of an employee, the assigned electronic signature would be “retired” to prevent the former employee from falsely using the signature.

H. Security of Industry Electronic Records Submitted to FDA

8. Several comments expressed concern about the security and confidentiality of electronic records submitted to FDA. One suggested that submissions be limited to such read-only formats as CD-ROM with raw data for statistical manipulation provided separately on floppy diskette. One comment suggested that in light of the proposed rule, the agency should review its own internal security procedures. Another addressed electronic records that may be disclosed under the Freedom of Information Act and expressed concern regarding agency deletion of trade secrets. One comment anticipated FDA's use of open systems to access industry records (such as medical device production and control records) and suggested that such access should be restricted to closed systems.

The agency is well aware of its legal obligation to maintain the confidentiality of trade secret information in its possession, and is committed to meet that obligation regardless of the form (paper or electronic) a record takes. The procedures used to ensure confidentiality are consistent with the provisions of part 11. FDA is also examining other controls, such as use of digital signatures, to ensure submission integrity. To permit legitimate changes to be made, the agency does not believe that it is necessary to restrict submissions to those maintained in [**FDA page 13434**] read-only formats in all cases; each agency receiving unit retains the flexibility to determine whatever format is most suitable. Those intending to submit material are expected to consult with the appropriate agency receiving unit to determine the acceptable formats.

Although FDA access to electronic records on open systems maintained by firms is not anticipated in the near future, the agency believes it would be inappropriate to rule out such a procedure. Such access can be a valuable inspection tool and can enhance efficiencies by reducing the time investigators may need to be on site. The agency believes it is important to develop appropriate procedures and security measures in cooperation with industry to ensure that such access does not jeopardize data confidentiality or integrity.

I. Effective Date/Grandfathering

9. Several comments addressed the proposed effective date of the final rule, 90 days after publication in the Federal Register, and suggested potential exemptions (grandfathering) for systems now in use. Two comments requested an expedited effective date for the final rule. One comment requested an effective date at least 18 months after publication of the final rule to permit firms to modify and validate their systems. One comment expressed concern about how the rule, in general, will affect current systems, and suggested that the agency permit firms to continue to use existing electronic record systems that otherwise conform to good manufacturing or laboratory practices until these firms make major modifications to those systems or until 5 years have elapsed, whichever comes first. Several other comments requested grandfathering for specific sections of the proposed rule.

The agency has carefully considered the comments and suggestions regarding the final rule's effective date and has concluded that the effective date should be 5 months after date of publication in the Federal Register. The agency wishes to accommodate firms that are prepared now to comply with part 11 or will be prepared soon, so as to encourage and foster new technologies in a manner that ensures that electronic record and electronic signature systems are reliable, trustworthy, and compatible with FDA's responsibility to promote and protect public health. The agency believes that firms that have consulted with FDA before adopting new electronic record and electronic signature technologies (especially technologies that may impact on the ability of the agency to conduct its work effectively) will need to make few, if any, changes to systems used to maintain records required by FDA.

The agency believes that the provisions of part 11 represent minimal standards and that a general exemption for existing systems that do not meet these provisions would be inappropriate and not in the public interest because such systems are likely to generate electronic records and electronic signatures that are unreliable, untrustworthy, and not compatible with FDA's responsibility to promote and protect public health. Such an exemption might, for example, mean that a firm could: (1) Deny FDA inspectional access to electronic record systems, (2) permit unauthorized access to those systems, (3) permit individuals to share identification codes and passwords, (4) permit systems to go unvalidated, and (5) permit records to be falsified in many ways and in a manner that goes undetected.

The agency emphasizes that these regulations do not require, but rather permit, the use of electronic records and signatures. Firms not confident that their electronic systems meet the minimal requirements of these regulations are free to continue to use traditional signatures and paper documents to meet recordkeeping requirements.

J. Comments by Electronic Mail and Electronic Distribution of FDA Documents

10. One comment specifically noted that the agency has accepted comments by e-mail and that this provides an additional avenue for public participation in the rulemaking process. Another comment encouraged FDA to expand the use of electronic media to provide information by such open systems as bulletin boards.

The agency intends to explore further the possibility of continuing to accept public comments by e-mail and other electronic means. For this current experiment, the agency received only one comment by e-mail. The comment that addressed this issue was, itself, transmitted in a letter. The agency recognizes the benefits of distributing information electronically, has expanded that activity, and intends to continue that expansion. Although only one e-mail comment was received, the agency does not attribute that low number to a lack of ability to send e-mail because the agency received e-mail from 198 persons who requested the text of the proposed rule, including requests from people outside the United States.

K. Submissions by Facsimile (Fax)

11. One comment said that part 11 should include a provision for FDA acceptance of submissions by fax, such as import form FDA 2877. The comment noted that the U.S. Customs Service accepts fax signatures on its documents, and claimed that FDA's insistence on hard copies of form FDA 2877 is an impediment to imports.

The agency advises that part 11 permits the unit that handles import form FDA 2877 to accept that record in electronic form when it is prepared logistically to do so. As noted in the discussion on Sec. 11.1(b) in comment 21 of this document, the agency recognizes that faxes can be in paper or electronic form, based on the capabilities of the sender and recipient.

L. Blood Bank Issues

12. Two comments addressed blood bank issues in the context of electronic records and electronic signatures and said the agency should clarify that part 11 would permit electronic crossmatching by a central blood center for individual hospitals. One comment stated that remote blood center and transfusion facilities should be permitted to rely on electronically communicated information, such as authorization for labeling/issuing units of blood, and that the electronic signature of the supervisor in the central testing facility releasing the product for labeling and issuance should be sufficient because the proposed rule guards against security and integrity problems.

One comment questioned whether, under part 11, electronic signatures would meet the signature requirements for the release of units of blood, and if there would be instances where a full signature would be required instead of a technician's identification. Another comment asserted that it is important to clarify how the term “batch” will be interpreted under part 11, and suggested that the term used in relation to blood products refers to a series of units of blood having undergone common manufacturing processes and recorded on the same computerized document. The comment contrasted this to FDA's current view that each unit of blood be considered a batch.

The agency advises that part 11 permits release records now in paper form to be in electronic form and traditional handwritten signatures to be electronic signatures. Under part 11, the name of the technician must appear in the record display or printout to clearly identify the technician. The appearance of the technician's identification code [**FDA page 13435**] alone would not be sufficient. The agency also advises that the definition of a “batch” for blood or other products is not affected by part 11, which addresses the trustworthiness and reliability of electronic records and electronic signatures, regardless of how a batch, which is the subject of those records and signatures, is defined.

M. Regulatory Flexibility Analysis

13. One comment said that, because part 11 will significantly impact a substantial number of small businesses, even though the impact would be beneficial, FDA is required to perform a regulatory flexibility analysis and should publish such an analysis in the Federal Register before a final rule is issued.

The comment states that the legislative history of the Regulatory Flexibility Act is clear that, “significant economic impact,” as it appears at 5 U.S.C. 605(b) is neutral with respect to whether such impact is beneficial or adverse.

Contrary to the comment's assertion, the legislative history is not dispositive of this matter. It is well established that the task of statutory construction must begin with the actual language of the statute. (See Bailey v. United States, 116 S. Ct. 595, 597 (1996).) A statutory term must not be construed in isolation; a provision that may seem ambiguous in isolation is often clarified by the remainder of the statute. (See Dept. Of Revenue of Oregon v. ACF Industries, 114 S. Ct. 843, 850 (1994).) Moreover, it is a fundamental canon of statutory construction that identical terms within the same statute must bear the same meaning. (See Reno v. Koray, 115 S. Ct. 2021, 2026 (1995).)In addition to appearing in 5 U.S.C. 605(b), the term “significant economic impact” appears elsewhere in the statute. The legislation is premised upon the congressional finding that alternative regulatory approaches may be available which “minimize the significant economic impact” of rules (5 U.S.C. 601 note). In addition, an initial regulatory flexibility analysis must describe significant regulatory alternatives that “minimize any significant economic impact” (5 U.S.C. 603(c)). Similarly, a final regulatory flexibility analysis must include a description of the steps the agency has taken to “minimize any significant economic impact” (5 U.S.C. 604(a)(5)). The term appeared as one of the elements of a final regulatory flexibility analysis, as originally enacted in 1980. (See Pub. L. No. 96-354, 3(a), 94 Stat. 1164, 1167 (1980) (formerly codified at 5 U.S.C. 604(a)(3)).) In addition, when Congress amended the elements of a final regulatory flexibility analysis in 1996, it re-enacted the term, as set forth above. (See Pub. L. 104-121, 241(b), 110 Stat. 857, 865 (1996) (codified at 5 U.S.C.604(a)(5)).)Unless the purpose of the statute was intended to increase the economic burden of regulations by minimizing positive or beneficial effects, “significant economic impact” cannot include such effects. Because it is beyond dispute that the purpose of the statute is not increasing economic burdens, the plain meaning of “significant economic impact” is clear and necessarily excludes beneficial or positive effects of regulations. Even where there are some limited contrary indications in the statute's legislative history, it is inappropriate to resort to legislative history to cloud a statutory text that is clear on its face. (See Ratzlaff v. United States, 114 S. Ct. 655, 662 (1994).) Therefore, the agency concludes that a final regulatory flexibility analysis is not required for this regulation or any regulation for which there is no significant adverse economic impact on small entities. Notwithstanding these conclusions, FDA has nonetheless considered the impact of the rule on small entities. (See section XVI. of this document.)

N. Terminology

14. One comment addressed the agency's use of the word “ensure” throughout the rule and argued that the agency should use the word “assure”' rather than “ensure” because “ensure” means “to guarantee or make certain” whereas “assure” means “to make confident.” The comment added that “assure” is also more consistent with terminology in other regulations.

The agency wishes to emphasize that it does not intend the word “ensure” to represent a guarantee. The agency prefers to use the word “ensure” because it means to make certain.

O. General Comments Regarding Prescription Drug Marketing Act of 1987 (PDMA)

15. Three comments addressed the use of handwritten signatures that are recorded electronically (SRE's) under part 11 and PDMA. One firm described its delivery information acquisition device and noted its use of time stamps to record when signatures are executed. The comments requested clarification that SRE's would be acceptable under the PDMA regulations. One comment assumed that subpart C of part 11 (Electronic Signatures) would not apply to SRE's, noting that it was not practical under PDMA (given the large number of physicians who may be eligible to receive drug product samples) to use such alternatives as identification codes combined with passwords.

The agency advises that part 11 applies to handwritten signatures recorded electronically and that such signatures and their corresponding electronic records will be acceptable for purposes of meeting PDMA's requirements when the provisions of part 11 are met. Although subpart C of part 11 does not apply to handwritten signatures recorded electronically, the agency advises that controls related to electronic records (subpart B), and the general provisions of subpart A, do apply to electronic records in the context of PDMA. The agency emphasizes, however, that part 11 does not restrict PDMA signings to SRE's, and that organizations retain the option of using electronic signatures in conformance with part 11. Furthermore, the agency believes that the number of people in a given population or organization should not be viewed as an insurmountable obstacle to use of electronic signatures. The agency is aware, for example, of efforts by the American Society of Testing and Materials to develop standards for electronic medical records in which digital signatures could theoretically be used on a large scale.

P. Comments on the Unique Nature of Passwords

16. Several comments noted, both generally and with regard to Secs. 11.100(a), 11.200(a), and 11.300, that the password in an electronic signature that is composed of a combination of password and identification code is not, and need not be, unique. Two comments added that passwords may be known to system security administrators who assist people who forget passwords and requested that the rule acknowledge that passwords need not be unique. One comment said that the rule should describe how uniqueness is to be determined.

The agency acknowledges that when an electronic signature consists of a combined identification code and password, the password need not be unique. It is possible that two persons in the same organization may have the same password. However, the agency believes that where good password practices are implemented, such coincidence would be highly unlikely. As discussed in section XIII. of this document in the context of comments on proposed Sec. 11.300, records are less trustworthy and reliable if it is relatively easy for someone to deduce or execute, by chance, a person's electronic [**FDA page 13436**] signature where the identification code of the signature is not confidential and the password is easily guessed.

The agency does not believe that revising proposed Sec. 11.100(a) is necessary because what must remain unique is the electronic signature, which, in the case addressed by the comments, consists not of the password alone, but rather the password in combination with an identification code. If the combination is unique, then the electronic signature is unique.

The agency does not believe that it is necessary to describe in the regulations the various ways of determining uniqueness or achieving compliance with the requirement. Organizations thereby maintain implementation flexibility.

The agency believes that most system administrators or security managers would not need to know passwords to help people who have forgotten their own. This is because most administrators or managers have global computer account privileges to resolve such problems.

IV. Scope (Sec. 11.1)

17. One comment suggested adding a new paragraph to proposed Sec. 11.1 that would exempt computer record maintenance software installed before the effective date of the final rule, and that would exempt electronic records maintained before that date. The comment argued that such exemptions were needed for economic and constitutional reasons because making changes to existing systems would be costly and because the imposition of additional requirements after the fact could be regarded as an ex post facto rule. The comment said firms have been using electronic systems that have demonstrated reliability and security for many years before the agency's publication of the ANPRM, and that the absence of FDA's objections in inspectional form FDA 483 was evidence of the agency's acceptance of the system.

As discussed in section III.I. of this document, the agency is opposed to “grandfathering” existing systems because such exemptions may perpetuate environments that provide opportunities for record falsification and impair FDA's ability to protect and promote public health. However, the agency wishes to avoid any confusion regarding the application of the provisions of part 11 to systems and electronic records in place before the rule's effective date. Important distinctions need to be made relative to an electronic record's creation, modification, and maintenance because various portions of part 11 address matters relating to these actions. Those provisions apply depending upon when a given electronic record is created, modified, or maintained.

Electronic records created before the effective date of this rule are not covered by part 11 provisions that relate to aspects of the record's creation, such as the signing of the electronic record. Those records would not, therefore, need to be altered retroactively. Regarding records that were first created before the effective date, part 11 provisions relating to modification of records, such as audit trails for record changes and the requirement that original entries not be obscured, would apply only to those modifications made on or after the rule's effective date, not to modifications made earlier. Likewise, maintenance provisions of part 11, such as measures to ensure that electronic records can be retrieved throughout their retention periods, apply to electronic records that are being maintained on or after the rule's effective date. The hardware and software, as well as operational procedures used on or after the rule's effective date, to create, modify, or maintain electronic records must comply with the provisions of part 11.

The agency does not agree with any suggestion that FDA endorsement or acceptance of an electronic record system can be inferred from the absence of objections in an inspection report. Before this rulemaking, FDA did not have established criteria by which it could determine the reliability and trustworthiness of electronic records and electronic signatures and could not sanction electronic alternatives when regulations called for signatures. A primary reason for issuing part 11 is to develop and codify such criteria. FDA will assess the acceptability of electronic records and electronic signatures created prior to the effective date of part 11 on a case-by-case basis.

18. One comment suggested that proposed Sec. 11.1 exempt production of medical devices and in vitro diagnostic products on the grounds that the subject was already adequately addressed in the medical device CGMP regulations currently in effect in Sec. 820.195 (21 CFR 820.195), and that additional regulations would be confusing and would limit compliance.

The agency believes that part 11 complements, and is supportive of, the medical device CGMP regulations and the new medical device quality system regulation, as well as other regulations, and that compliance with one does not confound compliance with others. Before publication of the ANPRM, the agency determined that existing regulations, including the medical device CGMP regulations, did not adequately address electronic records and electronic signatures. That determination was reinforced in the comments to the ANPRM, which focused on the need to identify what makes electronic records reliable, trustworthy, and compatible with FDA's responsibility to promote and protect public health. For example, the provision cited by the comment, Sec. 820.195, states “When automated data processing is used for manufacturing or quality assurance purposes, adequate checks shall be designed and implemented to prevent inaccurate data output, input, and programming errors.” This section does not address the many issues addressed by part 11, such as electronic signatures, record falsification, or FDA access to electronic records. The relationship between the quality system regulation and part 11 is discussed at various points in the preamble to the quality system regulation.

19. One comment asserted that for purposes of PDMA, the scope of proposed part 11 should be limited to require only those controls for assessing signatures in paper-based systems because physicians' handwritten signatures are executed to electronic records. The comment further asserted that, because drug manufacturers' representatives carry computers into physicians' offices (where the physicians then sign sample requests and receipts), only closed system controls should be needed.

The agency believes that, for purposes of PDMA, controls needed for electronic records bearing handwritten signatures are no different from controls needed for the same kinds of records and signatures used elsewhere, and that proposed Sec. 11.1 need not make any such distinction.

In addition, the agency disagrees with the implication that all PDMA electronic records are, in fact, handled within closed systems. The classification of a system as open or closed in a particular situation depends on what is done in that situation. For example, the agency agrees that a closed system exists where a drug producer's representative (the person responsible for the content of the electronic record) has control over access to the electronic record system by virtue of possessing the portable computer and controlling who may use the computer to sign electronic records. However, should the firm's representative transfer copies of those records to a public online service that stores them for the drug firm's [**FDA page 13437**] subsequent retrieval, the agency considers such transfer and storage to be within an open system because access to the system holding the records is controlled by the online service, which is not responsible for the record's content. Activities in the first example would be subject to closed system controls and activities in the second example would be subject to open system controls.

20. One comment urged that proposed Sec. 11.1 contain a clear statement of what precedence certain provisions of part 11 have over other regulations.

The agency believes that such statements are found in Sec. 11.1(c): Where electronic signatures and their associated records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required under agency regulations unless specifically excepted by regulations * * *. and Sec. 11.1(d) ("Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with Sec. 11.2, unless paper records are specifically required."). These provisions clearly address the precedence of part 11 and the equivalence of electronic records and electronic signatures.

To further clarify the scope of the rule, FDA has revised Sec. 11.1 to apply to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act (the act) and the Public Health Service Act (the PHS Act). This clarifies the point that submissions required by these statutes, but not specifically mentioned in the Code of Federal Regulations (CFR), are subject to part 11.

21. Proposed Sec. 11.1(b) stated that the regulations would apply to records in electronic form that are created, modified, maintained, or transmitted, under any records requirements set forth in Chapter I of Title 21. One comment suggested that the word "transmitted" be deleted from proposed Sec. 11.1(b) because the wording would inappropriately apply to paper documents that are transmitted by fax. The comment noted that if the records are in machine readable form before or after transmission, they would still be covered by the revised wording.

The agency does not intend part 11 to apply to paper records even if such records are transmitted or received by fax. The agency notes that the records transmitted by fax may be in electronic form at the sender, the recipient, or both. Part 11 would apply whenever the record is in electronic form. To remedy the problem noted by the comment, the agency has added a sentence to Sec. 11.1(b) stating that part 11 does not apply to paper records that are, or have been, transmitted by electronic means.

22. One comment asked whether paper records created by computer would be subject to proposed part 11. The comment cited, as an example, the situation in which a computer system collects toxicology data that are printed out and maintained as "raw data."

Part 11 is intended to apply to systems that create and maintain electronic records under FDA's requirements in Chapter I of Title 21, even though some of those electronic records may be printed on paper at certain times. The key to determining part 11 applicability, under Sec. 11.1(b), is the nature of the system used to create, modify, and maintain records, as well as the nature of the records themselves.

Part 11 is not intended to apply to computer systems that are merely incidental to the creation of paper records that are subsequently maintained in traditional paper-based systems. In such cases, the computer systems would function essentially like manual typewriters or pens and any signatures would be traditional handwritten signatures. Record storage and retrieval would be of the traditional "file cabinet" variety. More importantly, overall reliability, trustworthiness, and FDA's ability to access the records would derive primarily from well-established and generally accepted procedures and controls for paper records. For example, if a person were to use word processing software to generate a paper submission to FDA, part 11 would not apply to the computer system used to generate the submission, even though, technically speaking, an electronic record was initially created and then printed on paper.

When records intended to meet regulatory requirements are in electronic form, part 11 would apply to all the relevant aspects of managing those records (including their creation, signing, modification, storage, access, and retrieval). Thus, the software and hardware used to create records that are retained in electronic form for purposes of meeting the regulations would be subject to part 11.Regarding the comment about “raw data,” the agency notes that specific requirements in existing regulations may affect the particular records at issue, regardless of the form such records take. For example, “raw data,” in the context of the good laboratory practices regulations (21 CFR part 58), include computer printouts from automated instruments as well as the same data recorded on magnetic media. In addition, regulations that cover data acquisition systems generally include requirements intended to ensure the trustworthiness and reliability of the collected data.

23. Several comments on proposed Sec. 11.1(b) suggested that the phrase “or archived and retrieved” be added to paragraph (b) to reflect more accurately a record's lifecycle.

The agency intended that record archiving and retrieval would be part of record maintenance, and therefore already covered by Sec. 11.1(b). However, for added clarity, the agency has revised Sec. 11.1(b) to add “archived and retrieved.”

24. One comment suggested that, in describing what electronic records are within the scope of part 11, proposed Sec. 11.1(b) should be revised by substituting “processed” for “modified” and “communicated” for “transmitted” because “communicated” reflects the fact that the information was dispatched and also received. The comment also suggested substituting “retained” for “maintained,” or adding the word “retained,” because “maintain” does not necessarily convey the retention requirement.

The agency disagrees. The word “modified” better describes the agency's intent regarding changes to a record; the word “processed” does not necessarily infer a change to a record. FDA believes “transmitted” is preferable to “communicated” because “communicated” might infer that controls to ensure integrity and authenticity hinge on whether the intended recipient actually received the record. Also, as discussed in comment 22 of this document, the agency intends for the term “maintain” to include records retention.

25. Two comments suggested that proposed Sec. 11.1(b) explicitly state that part 11 supersedes all references to handwritten signatures in 21 CFR parts 211 through 226 that pertain to a drug, and in 21 CFR parts 600 through 680 that pertain to biological products for human use. The comments stated that the revision should clarify coverage and permit blood centers and transfusion services to take full advantage of electronic systems that provide process controls.

The agency does not agree that the revision is necessary because, under Sec. 11.1(b) and (c), part 11 permits electronic records or submissions under all FDA regulations in Chapter I of Title 21 unless specifically excepted by future regulations.

26. Several comments expressed concern that the proposed rule had inappropriately been expanded in scope [**FDA page 13438**] from the ANPRM to address electronic records as well as electronic signatures. One comment argued that the scope of part 11 should be restricted only to those records that are currently required to be signed, witnessed, or initialed, and that the agency should not require electronic records to contain electronic signatures where the corresponding paper records are not required to be signed.

The agency disagrees with the assertion that part 11 should address only electronic signatures and not electronic records for several reasons. First, based on comments on the ANPRM, the agency is convinced that the reliability and trustworthiness of electronic signatures depend in large measure on the reliability and trustworthiness of the underlying electronic records. Second, the agency has concluded that electronic records, like paper records, need to be trustworthy, reliable, and compatible with FDA's responsibility to promote and protect public health regardless of whether they are signed. In addition, records falsification is an issue with respect to both signed and unsigned records. Therefore, the agency concludes that although the ANPRM focused primarily on electronic signatures, expansion of the subject to electronic records in the proposed rule was fully justified.

The agency stresses that part 11 does not require that any given electronic record be signed at all. The requirement that any record bear a signature is contained in the regulation that mandates the basic record itself. Where records are signed, however, by virtue of meeting a signature requirement or otherwise, part 11 addresses controls and procedures intended to help ensure the reliability and trustworthiness of those signatures.

27. Three comments asked if there were any regulations, including CGMP regulations, that might be excepted from part 11 and requested that the agency identify such regulations.

FDA, at this time, has not identified any current regulations that are specifically excepted from part 11. However, the agency believes it is prudent to provide for such exceptions should they become necessary in the future. It is possible that, as the agency's experience with part 11 increases, certain records may need to be limited to paper if there are problems with the electronic versions of such records.

28. One comment requested clarification of the meaning of the term “general signings” in proposed Sec. 11.1(c), and said that the distinction between “full handwritten” signatures and “initials” is unnecessary because handwritten includes initials in all common definitions of handwritten signature. The comment also suggested changing the term “equivalent” to “at least equivalent” because electronic signatures are not precise equivalents of handwritten signatures and computer-based signatures have the potential of being more secure.

The agency advises that current regulations that require records to be signed express those requirements in different ways depending upon the agency's intent and expectations. Some regulations expressly state that records must be signed using “full handwritten” signatures, whereas other regulations state that records must be “signed or initialed;” still other regulations implicitly call for some kind of signing by virtue of requiring record approvals or endorsements. This last broad category is addressed by the term “general signings” in Sec. 11.1(c).

Where the language is explicit in the regulations, the means of meeting the requirement are correspondingly precise. Therefore, where a regulation states that a signature must be recorded as “full handwritten,” the use of initials is not an acceptable substitute. Furthermore, under part 11, for an electronic signature to be acceptable in place of any of these signings, the agency only needs to consider them as equivalent; electronic signatures need not be superior to those other signings to be acceptable.

29. Several comments requested clarification of which FDA records are required to be in paper form, and urged the agency to allow and promote the use of electronic records in all cases. One comment suggested that proposed Sec. 11.1(d) be revised to read, in part, “* * * unless the use of electronic records is specifically prohibited.”

The agency intends to permit the use of electronic records required to be maintained but not submitted to the agency (as noted in Sec. 11.2(a)) provided that the requirements of part 11 are met and paper records are not specifically required. The agency also wishes to encourage electronic submissions, but is limited by logistic and resource constraints. The agency is unaware of “maintenance records” that are currently explicitly required to be in paper form (explicit mention of paper is generally unnecessary because, at the time most regulations were prepared, only paper-based technologies were in use) but is providing for that possibility in the future. For purposes of part 11, the agency will not consider that a regulation requires “maintenance” records to be in paper form where the regulation is silent on the form the record must take. FDA believes that the comments' suggested wording does not offer sufficient advantages to adopt the change.

However, to enable FDA to accept as many electronic submissions as possible, the agency is amending Sec. 11.1(b) to include those submissions that the act and the PHS Act specifically require, even though such submissions may not be identified in agency regulations. An example of such records is premarket submissions for Class I and Class II medical devices, required by section 510(k) of the act (21 U.S.C. 360(k)).

30. Several comments addressed various aspects of the proposed requirement under Sec. 11.1(e) regarding FDA inspection of electronic record systems. Several comments objected to the proposal as being too broad and going beyond the agency's legal inspectional authority. One comment stated that access inferred by such inspection may include proprietary financial and sales data to which FDA is not entitled. Another comment suggested adding the word “authorized” before “inspection.” Some comments suggested revising proposed Sec. 11.1(e) to limit FDA inspection only to the electronic records and electronic signatures themselves, thus excluding inspection of hardware and software used to manage those records and signatures. Other comments interpreted proposed Sec. 11.1(e) as requiring them to keep supplanted or retired hardware and software to enable FDA inspection of those outdated systems.

The agency advises that FDA inspections under part 11 are subject to the same legal limitations as FDA inspections under other regulations. The agency does not believe it is necessary to restate that limitation by use of the suggested wording. However, within those limitations, it may be necessary to inspect hardware and software used to generate and maintain electronic records to determine if the provisions of part 11 are being met. Inspection of resulting records alone would be insufficient. For example, the agency may need to observe the use and maintenance of tokens or devices that contain or generate identification information. Likewise, to assess the adequacy of systems validation, it is generally necessary to inspect hardware that is being used to determine, among other things, if it matches the system documentation description of such hardware. The agency has concluded that hardware and software used to generate and maintain electronic records and signatures are “pertinent [**FDA page 13439**] equipment” within the meaning of section 704 of the act (21 U.S.C. 374).

The agency does not expect persons to maintain obsolete and supplanted computer systems for the sole purpose of enabling FDA inspection. However, the agency does expect firms to maintain and have available for inspection documentation relevant to those systems, in terms of compliance with part 11, for as long as the electronic records are required by other relevant regulations. Persons should also be mindful of the need to keep appropriate computer systems that are capable of reading electronic records for as long as those records must be retained. In some instances, this may mean retention of otherwise outdated and supplanted systems, especially where the old records cannot be converted to a form readable by the newer systems. In most cases, however, FDA believes that where electronic records are accurately and completely transcribed from one system to another, it would not be necessary to maintain older systems.

31. One comment requested that proposed part 11 be revised to give examples of electronic records subject to FDA inspection, including pharmaceutical and medical device production records, in order to reduce the need for questions.

The agency does not believe that it is necessary to include examples of records it might inspect because the addition of such examples might raise questions about the agency's intent to inspect other records that were not identified.

32. One comment said that the regulation should state that certain security related information, such as private keys attendant to cryptographic implementation, is not intended to be subject to inspection, although procedures related to keeping such keys confidential can be subject to inspection.

The agency would not routinely seek to inspect especially sensitive information, such as passwords or private keys, attendant to security systems. However, the agency reserves the right to conduct such inspections, consistent with statutory limitations, to enforce the provisions of the act and related statutes. It may be necessary, for example, in investigating cases of suspected fraud, to access and determine passwords and private keys, in the same manner as the agency may obtain specimens of handwritten signatures ("exemplars"). Should there be any reservations about such inspections, persons may, of course, change their passwords and private keys after FDA inspection.

33. One comment asked how persons were expected to meet the proposed requirement, under Sec. 11.1(e), that computer systems be readily available for inspection when such systems include geographically dispersed networks. Another comment said FDA investigators should not be permitted to access industry computer systems as part of inspections because investigators would be untrained users.

The agency intends to inspect those parts of electronic record or signature systems that have a bearing on the trustworthiness and reliability of electronic records and electronic signatures under part 11. For geographically dispersed systems, inspection at a given location would extend to operations, procedures, and controls at that location, along with interaction of that local system with the wider network. The agency would inspect other locations of the network in a separate but coordinated manner, much the same way the agency currently conducts inspections of firms that have multiple facilities in different parts of the country and outside of the United States.

FDA does not believe it is reasonable to rule out computer system access as part of an inspection of electronic record or signature systems. Historically, FDA investigators observe the actions of establishment employees, and (with the cooperation of establishment management) sometimes request that those employees perform some of their assigned tasks to determine the degree of compliance with established requirements. However, there may be times when FDA investigators need to access a system directly. The agency is aware that such access will generally require the cooperation of and, to some degree, instruction by the firms being inspected. As new, complex technologies emerge, FDA will need to develop and implement new inspectional methods in the context of those technologies.

V. Implementation (Sec. 11.2)

34. Proposed Sec. 11.2(a) stated that for "records required by chapter I of this title to be maintained, but not submitted to the agency, persons may use electronic records/signatures in lieu of paper records/conventional signatures, in whole or in part, * * *."

Two comments requested clarification of the term "conventional signatures." One comment suggested that the term "traditional signatures" be used instead. Another suggested rewording in order to clarify the slash in the phrase "records/signatures."

The agency advises that the term "conventional signature" means handwritten signature. The agency agrees that the term "traditional signature" is preferable, and has revised Sec. 11.2(a) and (b) accordingly. The agency has also clarified proposed Sec. 11.2(a) by replacing the slash with the word "or."

35. One comment asked if the term "persons" in proposed Sec. 11.2(b) would include devices because computer systems frequently apply digital time stamps on records automatically, without direct human intervention.

The agency advises that the term "persons" excludes devices. The agency does not consider the application of a time stamp to be the application of a signature.

36. Proposed Sec. 11.2(b)(2) provides conditions under which electronic records or signatures could be submitted to the agency in lieu of paper. One condition is that a document, or part of a document, must be identified in a public docket as being the type of submission the agency will accept in electronic form. Two comments addressed the nature of the submissions to the public docket. One comment asked that the agency provide specifics, such as the mechanism for updating the docket and the frequency of such updates. One comment suggested making the docket available to the public by electronic means. Another comment suggested that acceptance procedures be uniform among agency units and that electronic mail be used to hold consultations with the agency. One comment encouraged the agency units receiving the submissions to work closely with regulated industry to ensure that no segment of industry is unduly burdened and that agency guidance is widely accepted.

The agency intends to develop efficient electronic records acceptance procedures that afford receiving units sufficient flexibility to deal with submissions according to their capabilities. Although agencywide uniformity is a laudable objective, to attain such flexibility it may be necessary to accommodate some differences among receiving units. The agency considers of primary importance, however, that all part 11 submissions be trustworthy, reliable, and in keeping with FDA regulatory activity. The agency expects to work closely with industry to help ensure that the mechanics and logistics of accepting electronic submissions do not pose any undue burdens. However, the agency expects persons to consult with the [**FDA page 13440**] intended receiving units on the technical aspects of the submission, such as media, method of transmission, file format, archiving needs, and technical protocols. Such consultations will ensure that submissions are compatible with the receiving units' capabilities. The agency has revised proposed Sec. 11.2(b)(2) to clarify this expectation.

Regarding the public docket, the agency is not at this time establishing a fixed schedule for updating what types of documents are acceptable for submission because the agency expects the docket to change and grow at a rate that cannot be predicted. The agency may, however, establish a schedule for updating the docket in the future. The agency agrees that making the docket available electronically is advisable and will explore this option. Elsewhere in this issue of the Federal Register, FDA is providing further information on this docket.

VI. Definitions (Sec. 11.3)

37. One comment questioned the incorporation in proposed Sec. 11.3(a) of definitions under section 201 of the act (21 U.S.C. 321), noting that other FDA regulations (such as 21 CFR parts 807 and 820) lack such incorporation, and suggested that it be deleted.

The agency has retained the incorporation by reference to definitions under section 201 of the act because those definitions are applicable to part 11.

38. One comment suggested adding the following definition for the term “digital signature:” “data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient.”

The agency agrees that the term digital signature should be defined and has added new Sec. 11.3(b)(5) to provide a definition for digital signature that is consistent with the Federal Information Processing Standard 186, issued May 19, 1995, and effective December 1, 1995, by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST). Generally, a digital signature is “an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.” FDA advises that the set of rules and parameters is established in each digital signature standard.

39. Several comments suggested various modifications of the proposed definition of biometric/behavioral links, and suggested revisions that would exclude typing a password or identification code which, the comments noted, is a repeatable action. The comments suggested that actions be unique and measurable to meet the intent of a biometric method.

The agency agrees that the proposed definition of biometric/behavioral links should be revised to clarify the agency's intent that repetitive actions alone, such as typing an identification code and password, are not considered to be biometric in nature. Because comments also indicated that it would be preferable to simplify the term, the agency is changing the term “biometric/behavioral link” to “biometrics.” Accordingly, Sec. 11.3(b)(3) defines the term “biometrics” to mean “a method of verifying an individual's identity based on measurement of the individual's physical feature, or features, or repeatable action, or actions, where those features and/or actions are both unique to that individual and measurable.”

40. One comment said that the agency should identify what biometric methods are acceptable to verify a person's identity and what validation acceptance criteria the agency has used to determine that biometric technologies are superior to other methods, such as use of identification codes and passwords.

The agency believes that there is a wide variety of acceptable technologies, regardless of whether they are based on biometrics, and regardless of the particular type of biometric mechanism that may be used. Under part 11, electronic signatures that employ at least two distinct identification components such as identification codes and passwords, and electronic signatures based on biometrics are equally acceptable substitutes for traditional handwritten signatures. Furthermore, all electronic record systems are subject to the same requirements of subpart B of part 11 regardless of the electronic signature technology being used. These provisions include requirements for validation.

Regarding the comment's suggestion that FDA apply quantitative acceptance criteria, the agency is not seeking to set specific numerical standards or statistical performance criteria in determining the threshold of acceptability for any type of technology. If such standards were to be set for biometrics-based electronic signatures, similar numerical performance and reliability requirements would have to be applied to other technologies as well. The agency advises, however, that the differences between system controls for biometrics-based electronic signatures and other electronic signatures are a result of the premise that biometrics-based electronic signatures, by their nature, are less prone to be compromised than other methods such as identification codes and passwords. Should it become evident that additional controls are warranted for biometrics-based electronic signatures, the agency will propose to revise part 11 accordingly.

41. Proposed Sec. 11.3(b)(4) defined a closed system as an environment in which there is communication among multiple persons, and where system access is restricted to people who are part of the organization that operates the system.

Many comments requested clarification of the term “organization” and stated that the rule should account for persons who, though not strictly employees of the operating organization, are nonetheless obligated to it in some manner, or who would otherwise be granted system access by the operating organization. As examples of such persons, the comments cited outside contractors, suppliers, temporary employees, and consultants. The comments suggested a variety of alternative wording, including a change of emphasis from organizational membership to organizational control over system access. One comment requested clarification of whether the rule intends to address specific disciplines within a company.

Based on the comments, the agency has revised the proposed definition of closed system to state “an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.” The agency agrees that the most important factor in classifying a system as closed or open is whether the persons responsible for the content of the electronic records control access to the system containing those records. A system is closed if access is controlled by persons responsible for the content of the records. If those persons do not control such access, then the system is open because the records may be read, modified, or compromised by others to the possible detriment of the persons responsible for record content. Hence, those responsible for the records would need to take appropriate additional measures in an open system to protect those records from being read, modified, destroyed, or otherwise compromised by unauthorized and potentially unknown parties. The agency does not believe it is necessary to codify the basis or criteria for authorizing system access, such as existence of a fiduciary [**FDA page 13441**] responsibility or contractual relationship. By being silent on such criteria, the rule affords maximum flexibility to organizations by permitting them to determine those criteria for themselves.

42. Concerning the proposed definition of closed system, one comment suggested adding the words “or devices” after “persons” because communications may involve nonhuman entities.

The agency does not believe it is necessary to adopt the suggested revision because the primary intent of the regulation is to address communication among humans, not devices.

43. One comment suggested defining a closed system in terms of functional characteristics that include physical access control, having professionally written and approved procedures with employees and supervisors trained to follow them, conducting investigations when abnormalities may have occurred, and being under legal obligation to the organization responsible for operating the system.

The agency agrees that the functional characteristics cited by the comment are appropriate for a closed system, but has decided that it is unnecessary to include them in the definition. The functional characteristics themselves, however, such as physical access controls, are expressed as requirements elsewhere in part 11.

44. Two comments said that the agency should regard as closed a system in which dial-in access via public phone lines is permitted, but where access is authorized by, and under the control of, the organization that operates the system.

The agency advises that dial-in access over public phone lines could be considered part of a closed system where access to the system that holds the electronic records is under the control of the persons responsible for the content of those records. The agency cautions, however, that, where an organization's electronic records are stored on systems operated by third parties, such as commercial online services, access would be under control of the third parties and the agency would regard such a system as being open. The agency also cautions that, by permitting access to its systems by public phone lines, organizations lose the added security that results from restricting physical access to computer terminal and other input devices. In such cases, the agency believes firms would be prudent to implement additional security measures above and beyond those controls that the organization would use if the access device was within its facility and commensurate with the potential consequences of such unauthorized access. Such additional controls might include, for example, use of input device checks, caller identification checks (phone caller identification), call backs, and security cards.

45. Proposed Sec. 11.3(b)(5) defined electronic record as a document or writing comprised of any combination of text, graphic representation, data, audio information, or video information, that is created, modified, maintained, or transmitted in digital form by a computer or related system. Many comments suggested revising the proposed definition to reflect more accurately the nature of electronic records and how they differ from paper records. Some comments suggested distinguishing between machine readable records and paper records

created by machine. Some comments noted that the term “document or writing” is inappropriate for electronic records because electronic records could be any combination of pieces of information assembled (sometimes on a transient basis) from many noncontiguous places, and because the term does not accurately describe such electronic information as raw data or voice mail. Two comments suggested that the agency adopt definitions of electronic record that were established, respectively, by the United Nations Commission on International Trade Law (UNCITRAL) Working Group on Electronic Data Interchange, and the American National Standards Institute/Institute of Electrical and Electronic Engineers Software Engineering (ANSI/IEEE) Standard (729-1983).

The agency agrees with the suggested revisions and has revised the definition of “electronic record” to emphasize this unique nature and to clarify that the agency does not regard a paper record to be an electronic record simply because it was created by a computer system. The agency has removed “document or writing” from this definition and elsewhere in part 11 for the sake of clarity, simplicity, and consistency.

However, the agency believes it is preferable to adapt or modify the words “document” and “writing” to electronic technologies rather than discard them entirely from the lexicon of computer technology. The agency is aware that the terms “document” and “electronic document” are used in contexts that clearly do not intend to describe paper. Therefore, the agency considers the terms “electronic record” and “electronic document” to be generally synonymous and may use the terms “writing,” “electronic document,” or “document” in other publications to describe records in electronic form. The agency believes that such usage is a prudent conservation of language and is consistent with the use of other terms and expressions that have roots in older technologies, but have nonetheless been adapted to newer technologies. Such terms include telephone “dialing,” internal combustion engine “horse power,” electric light luminance expressed as “foot candles,” and (more relevant to computer technology) execution of a “carriage return.”

Accordingly, the agency has revised the definition of electronic record to mean “any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.”

46. Proposed Sec. 11.3(b)(6) defined an electronic signature as the entry in the form of a magnetic impulse or other form of computer data compilation of any symbol or series of symbols, executed, adopted or authorized by a person to be the legally binding equivalent of the person's handwritten signature. One comment supported the definition as proposed, noting its consistency with dictionary definitions (Random House Dictionary of the English Language, Unabridged Ed. 1983, and American Heritage Dictionary, 1982). Several other comments, however, suggested revisions. One comment suggested replacing “electronic signature” with ”computer based signature,” “authentication,” or “computer based authentication” because “electronic signature” is imprecise and lacks clear and recognized meaning in the information security and legal professions. The comment suggested a definition closer to the UNCITRAL draft definition:(1) [a] method used to identify the originator of the data message and to indicate the originator's approval of the information contained therein; and (2) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all circumstances, including any agreement between the originator and the addressee of the data message.

One comment suggested replacing “electronic signature” with “electronic identification” or “electronic authorization” because the terms include many types of technologies that are not easily distinguishable and because the preamble to the proposed rule gave a rationale for using “electronic signature” that was too “esoteric for practical consideration.”

[**FDA page 13442**]

The agency disagrees that “electronic signature” as proposed should be replaced with other terms and definitions. As noted in the preamble to the proposed rule, the agency believes that it is vital to retain the word “signature” to maintain the equivalence and significance of various electronic technologies with the traditional handwritten signature. By not using the word “signature,” people may treat the electronic alternatives as less important, less binding, and less in need of controls to prevent falsification. The agency also believes that use of the word signature provides a logical bridge between paper and electronic technologies that facilitates the general transition from paper to electronic environments. The term helps people comply with current FDA regulations that specifically call for signatures. Nor does the agency agree that this reasoning is beyond the reach of practical consideration.

The agency declines to accept the suggested UNCITRAL definition because it is too narrow in context in that there is not always a specified message addressee for electronic records required by FDA regulations (e.g., a batch production record does not have a specific “addressee”).

47. Concerning the proposed definition of “electronic signature,” other comments suggested deletion of the term ``magnetic impulse'' to render the term media neutral and thus allow for such alternatives as an optical disk. Comments also suggested that the term “entry” was unclear and recommended its deletion. Two comments suggested revisions that would classify symbols as an electronic signature only when they are committed to permanent storage because not every computer entry is a signature and processing to permanent storage must occur to indicate completion of processing.

The agency advises that the proposal did not limit electronic signature recordings to “magnetic impulse” because the proposed definition added, “or other form of computer data * * *.” However, in keeping with the agency's intent to accept a broad range of technologies, the terms “magnetic impulse” and “entry” have been removed from the proposed definition. The agency believes that recording of computer data to “permanent” storage is not a necessary or warranted qualifier because it is not relevant to the concept of equivalence to a handwritten signature. In addition, use of the qualifier regarding permanent storage could impede detection of falsified records if, for example, the signed falsified record was deleted after a predetermined period (thus, technically not recorded to “permanent” storage). An individual could disavow a signature because the record had ceased to exist.

For consistency with the proposed definition of handwritten signature, and to clarify that electronic signatures are those of individual human beings, and not those of organizations (as included in the act's definition of “person”), FDA is changing “person” to “individual” in the final rule.

Accordingly, Sec. 11.3(b)(7) defines electronic signature as a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

48. Proposed Sec. 11.3(b)(7) (redesignated Sec. 11.3(b)(8) in the final rule) defined “handwritten signature” as the name of an individual, handwritten in script by that individual, executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The proposed definition also stated that the scripted name, while conventionally applied to paper, may also be applied to other devices which capture the written name.

Many comments addressed this proposed definition. Two comments suggested that it be deleted on the grounds it is redundant and that, when handwritten signatures are recorded electronically, the result fits the definition of electronic signature.

The agency disagrees that the definition of handwritten signature should be deleted. In stating the criteria under which electronic signatures may be used in place of traditional handwritten signatures, the agency believes it is necessary to define handwritten signature. In addition, the agency believes that it is necessary to distinguish handwritten signatures from electronic signatures because, with handwritten signatures, the traditional act of signing one's name is preserved. Although the handwritten signature recorded electronically and electronic signatures, as defined in part 11, may both ultimately result in magnetic impulses or other forms of computerized symbol representations, the means of achieving those recordings and, more importantly, the controls needed to ensure their reliability and trustworthiness are quite different. In addition, the agency believes that a definition for handwritten signature is warranted to accommodate persons who wish to implement record systems that are combinations of paper and electronic technologies.

49. Several comments suggested replacing the reference to “scripted name” in the proposed definition of handwritten signature with “legal mark” so as to accommodate individuals who are physically unable to write their names in script. The comments asserted that the term “legal mark” would bring the definition to closer agreement with generally recognized legal interpretations of signature.

The agency agrees and has added the term “legal mark” to the definition of handwritten signature.

50. One comment recommended that the regulation state that, when the handwritten signature is not the result of the act of signing with a writing or marking instrument, but is applied to another device that captures the written name, a system should verify that the owner of the signature has authorized the use of the handwritten signature.

The agency declines to accept this comment because, if the act of signing or marking is not preserved, the type of signature would not be considered a handwritten signature. The comment appears to be referring to instances in which one person authorizes someone else to use his or her stamp or device. The agency views this as inappropriate when the signed record does not clearly show that the stamp owner did not actually execute the signature. As discussed elsewhere in this preamble, the agency believes that where one person authorizes another to sign a document on his or her behalf, the second person must sign his or her own name (not the name of the first person) along with some notation that, in doing so, he or she is acting in the capacity, or on behalf, of the first person.

51. One comment suggested that where handwritten signatures are captured by devices, there should be a register of manually written signatures to enable comparison for authenticity and the register also include the typed names of individuals.

The agency agrees that the practice of establishing a signature register has merit, but does not believe that it is necessary, in light of other part 11 controls. As noted elsewhere in this preamble (in the discussion of proposed Sec. 11.50), the agency agrees that human readable displays of electronic records must display the name of the signer.

52. Several comments suggested various editorial changes to the proposed definition of handwritten signature including: (1) Changing the word “also” in the last sentence to “alternatively,” (2) clarifying the [**FDA page 13443**] difference between the words “individual” and “person,” (3) deleting the words “in a permanent form,” and (4) changing “preserved” to “permitted.” One comment asserted that the last sentence of the proposed definition was unnecessary.

The agency has revised the definition of handwritten signature to clarify its intent and to keep the regulation as flexible as possible. The agency believes that the last sentence of the proposed definition is needed to address devices that capture handwritten signatures. The agency is not adopting the suggestion that the word “preserved” be changed to “permitted” because “preserved” more accurately states the agency's intent and is a qualifier to help distinguish handwritten signatures from others. The agency advises that the word “individual” is used, rather than “person,” because the act's definition of person extends beyond individual human beings to companies and partnerships. The agency has retained the term “permanent” to discourage the use of pencils, but recognizes that “permanent” does not mean eternal.

53. One comment asked whether a signature that is first handwritten and then captured electronically (e.g., by scanning) is an electronic signature or a handwritten signature, and asked how a handwritten signature captured electronically (e.g., by using a stylus-sensing pad device) that is affixed to a paper copy of an electronic record would be classified.

FDA advises that when the act of signing with a stylus, for example, is preserved, even when applied to an electronic device, the result is a handwritten signature. The subsequent printout of the signature on paper would not change the classification of the original method used to execute the signature.

54. One comment asserted that a handwritten signature recorded electronically should be considered to be an electronic signature, based on the medium used to capture the signature. The comment argued that the word signature should be limited to paper technology.

The agency disagrees and believes it is important to classify a signature as handwritten based upon the preserved action of signing with a stylus or other writing instrument.

55. One comment asked if the definition of handwritten signature encompasses handwritten initials.

The agency advises that, as revised, the definition of handwritten signature includes handwritten initials if the initials constitute the legal mark executed or adopted with the present intention to authenticate a writing in a permanent form, and where the method of recording such initials involves the act of writing with a pen or stylus.

56. Proposed Sec. 11.3(b)(8) (redesignated as Sec. 11.3(b)(9) in the final rule) defined an open system as an environment in which there is electronic communication among multiple persons, where system access extends to people who are not part of the organization that operates the system.

Several comments suggested that, for simplicity, the agency define “open system” as any system that does not meet the definition of a closed system. One comment suggested that the definition be deleted on the grounds it is redundant, and that it is the responsibility of individual firms to take appropriate steps to ensure the validity and security of applications and information, regardless of whether systems are open or closed. Other comments suggested definitions of “open system” that were opposite to what they suggested for a closed system.

The agency has revised the definition of open system to mean “an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.” The agency believes that, for clarity, the definition should stand on its own rather than as any system that is not closed. The agency rejects the suggestion that the term need not be defined at all because FDA believes that controls for open systems merit distinct provisions in part 11 and defining the term is basic to understanding which requirements apply to a given system. The agency agrees that companies have the responsibility to take steps to ensure the validity and security of their applications and information. However, FDA finds it necessary to establish part 11 as minimal requirements to help ensure that those steps are, in fact, acceptable.

VII. Electronic Records--Controls for Closed Systems (Sec. 11.10)

The introductory paragraph of proposed Sec. 11.10 states that: Closed systems used to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. * * *

The rest of the section lists specific procedures and controls.

57. One comment expressed full support for the list of proposed controls, calling them generally appropriate and stated that the agency is correctly accommodating the fluid nature of various electronic record and electronic signature technologies. Another comment, however, suggested that controls should not be implemented at the time electronic records are first created, but rather only after a document is accepted by a company.

The agency disagrees with this suggestion. To ignore such controls at a stage before official acceptance risks compromising the record. For example, if “preacceptance” records are signed by technical personnel, it is vital to ensure the integrity of their electronic signatures to prevent record alteration. The need for such integrity is no less important at preacceptance stages than at later stages when managers officially accept the records. The possibility exists that some might seek to disavow, or avoid FDA examination of, pertinent records by declaring they had not been formally “accepted.” In addition, FDA routinely can and does inspect evolving paper documents (e.g., standard operating procedures and validation protocols) even though they have yet to receive a firm's final acceptance.

58. One comment said proposed Sec. 11.10 contained insufficient requirements for firms to conduct periodic inspection and monitoring of their own systems and procedures to ensure compliance with the regulations. The comment also called for a clear identification of the personnel in a firm who would be responsible for system implementation, operation, change control, and monitoring.

The agency does not believe it is necessary at this time to codify a self-auditing requirement, as suggested by the comment. Rather, the agency intends to afford organizations flexibility in establishing their own internal mechanisms to ensure compliance with part 11. Self-audits, however, may be considered as a general control, within the context of the introductory paragraph of Sec. 11.10. The agency encourages firms to conduct such audits periodically as part of an overall approach to ensure compliance with FDA regulations generally. Likewise, the agency does not believe it is necessary or practical to codify which individuals in an organization should be responsible for compliance with various provisions of part 11. However, ultimate responsibility for part 11 will generally rest with persons responsible for electronic record content, just as responsibility for compliance with paper record requirements generally lies with those responsible for the record's content.

[**FDA page 13444**]

59. Several comments interpreted proposed Sec. 11.10 as applying all procedures and controls to closed systems and suggested revising it to permit firms to apply only those procedures and controls they deem necessary for their own operations, because some requirements are excessive in some cases.

The agency advises that, where a given procedure or control is not intended to apply in all cases, the language of the rule so indicates. Specifically, use of operational checks (Sec. 11.10(f)) and device checks (Sec. 11.10(h)) is not required in all cases. The remaining requirements do apply in all cases and are, in the agency's opinion, the minimum needed to ensure the trustworthiness and reliability of electronic record systems. In addition, certain controls that firms deem adequate for their routine internal operations might nonetheless leave records vulnerable to manipulation and, thus, may be incompatible with FDA's responsibility to protect public health. The suggested revision would effectively permit firms to implement various controls selectively and possibly shield records from FDA, employ unqualified personnel, or permit employees to evade responsibility for fraudulent use of their electronic signatures.

The agency believes that the controls in Sec. 11.10 are vital, and notes that almost all of them were suggested by comments on the ANPRM. The agency believes the wording of the regulation nonetheless permits firms maximum flexibility in how to meet those requirements.

60. Two comments suggested that the word “confidentiality” in the introductory paragraph of proposed Sec. 11.10 be deleted because it is unnecessary and inappropriate. The comments stated that firms should determine if certain records need to be confidential, and that as long as records could not be altered or deleted without appropriate authority, it would not matter whether they could read the records.

The agency agrees that not all records required by FDA need to be kept confidential within a closed system and has revised the reference in the introductory paragraph of Sec. 11.10 to state “* * * and, when appropriate, the confidentiality of electronic records.” The agency believes, however that the need for retaining the confidentiality of certain records is not diminished because viewers cannot change them. It may be prudent for persons to carefully assess the need for record confidentiality. (See, e.g., 21 CFR 1002.42, Confidentiality of records furnished by dealers and distributors, with respect to certain radiological health products.) In addition, FDA's obligation to retain the confidentiality of information it receives in some submissions hinges on the degree to which the submitter maintains confidentiality, even within its own organization. (See, e.g., 21 CFR 720.8(b) with respect to cosmetic ingredient information in voluntary filings of cosmetic product ingredient and cosmetic raw material composition statements.)

61. One comment asked if the procedures and controls required by proposed Sec. 11.10 were to be built into software or if they could exist in written form.

The agency expects that, by their nature, some procedures and controls, such as use of time-stamped audit trails and operational checks, will be built into hardware and software. Others, such as validation and determination of personnel qualifications, may be implemented in any appropriate manner regardless of whether the mechanisms are driven by, or are external to, software or hardware. To clarify this intent, the agency has revised the introductory paragraph of proposed Sec. 11.10 to read, in part, “Persons who use closed systems to create, modify * * *.” Likewise, for clarity and consistency, the agency is introducing the same phrase, “persons who use * * *” in Secs. 11.30 and 11.300.

62. One comment contended that the distinction between open and closed systems should not be predominant because a $100,000 transaction in a closed system should not have fewer controls than a $1 transaction in an open system.

The agency believes that, within part 11, firms have the flexibility they need to adjust the extent and stringency of controls based on any factors they choose, including the economic value of the transaction. The agency does not believe it is necessary to modify part 11 at this time so as to add economic criteria.

63. One comment suggested that the reference to repudiation in the introductory paragraph of Sec. 11.10 should be deleted because repudiation can occur at any time in legal proceedings. Another comment, noting that the proposed rule appeared to address only nonrepudiation of a signer, said the rule should address nonrepudiation of record “genuineness” or extend to nonrepudiation of submission, delivery, and receipt. The comment

stated that some firms provide nonrepudiation services that can prevent someone from successfully claiming that a record has been altered.

In response to the first comment, the agency does not agree that the reference to repudiation should be deleted because reducing the likelihood that someone can readily repudiate an electronic signature as not his or her own, or that the signed record had been altered, is vital to the agency's basic acceptance of electronic signatures. The agency is aware that the need to deter such repudiation has been addressed in many forums and publications that discuss electronic signatures. Absent adequate controls, FDA believes some people would be more likely to repudiate an electronically-signed record because of the relative ease with which electronic records may be altered and the ease with which one individual could impersonate another. The agency notes, however, that the rule does not call for nonrepudiation as an absolute guarantee, but requires that the signer cannot “readily” repudiate the signature.

In response to the second comment, the agency agrees that it is also important to establish nonrepudiation of submission, delivery, and receipt of electronic records, but advises that, for purposes of Sec. 11.10, the agency's intent is to limit nonrepudiation to the genuineness of the signer's record. In other words, an individual should not be able to readily say that: (1) He or she did not, in fact, sign the record; (2) a given electronic record containing the individual's signature was not, in fact, the record that the person signed; or (3) the originally signed electronic record had been altered after having been signed.

64. Proposed Sec. 11.10(a) states that controls for closed systems are to include the validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to conclusively discern invalid or altered records.

Many comments objected to this proposed requirement because the word “conclusively” inferred an unreasonably high and unattainable standard, one which is not applied to paper records.

The agency intends to apply the same validation concepts and standards to electronic record and electronic signature systems as it does to paper systems. As such, FDA does not intend the word “conclusively” to suggest an unattainable absolute and has, therefore, deleted the word from the final rule.

65. One comment suggested qualifying the proposed validation requirement in Sec. 11.10(a) to state that validation be performed “where [**FDA page 13445**] necessary” and argued that validation of commercially available software is not necessary because such software has already been thoroughly validated. The comment acknowledged that validation may be required for application programs written by manufacturers and others for special needs.

The agency disagrees with the comment's claim that all commercial software has been validated. The agency believes that commercial availability is no guarantee that software has undergone “thorough validation” and is unaware of any regulatory entity that has jurisdiction over general purpose software producers. The agency notes that, in general, commercial software packages are accompanied not by statements of suitability or compliance with established standards, but rather by disclaimers as to their fitness for use. The agency is aware of the complex and sometimes controversial issues in validating commercial software. However, the need to validate such software is not diminished by the fact that it was not written by those who will use the software.

In the future, the agency may provide guidance on validation of commercial software used in electronic record systems. FDA has addressed the matter of software validation in general in such documents as the “Draft Guideline for the Validation of Blood Establishment Computer Systems,” which is available from the Manufacturers Assistance and Communications Staff, Center for Biologics Evaluation and Research (HFM-42), Food and Drug Administration, 1401 Rockville Pike, Rockville, MD 20852-1448, 301-594-2000. This guideline is also available by sending e-mail to the following Internet address: CBER__INFO@A1.CBER.FDA.GOV). For the purposes of part 11, however, the agency believes it is vital to retain the validation requirement.

66. One comment requested an explanation of what was meant by the phrase “consistent intended” in proposed Sec. 11.10(a) and why “consistent performance” was not used instead. The comment suggested that the rule should distinguish consistent intended performance from well-recognized service “availability.”

The agency advises that the phrase “consistent intended performance” relates to the general principle of validation that planned and expected performance is based upon predetermined design specifications (hence, “intended”). This concept is in accord with the agency's 1987 “Guideline on General Principles of Process Validation,” which is available from the Division of Manufacturing and Product Quality, Center for Drug Evaluation and Research (HFD-320), Food and Drug Administration, 7520 Standish Pl., Rockville, MD 20855, 301-594-0093). This guideline defines validation as establishing documented evidence that provides a high degree of assurance that a specific process will consistently produce a product meeting its predetermined specifications and quality attributes. The agency believes that the comment's concepts are accommodated by this definition to the extent that system “availability” may be one of the predetermined specifications or quality attributes.

67. One comment said the rule should indicate whether validation of systems does, or should, require any certification or accreditation.

The agency believes that although certification or accreditation may be a part of validation of some systems, such certification or accreditation is not necessary in all cases, outside of the context of any such approvals within an organization itself. Therefore, part 11 is silent on the matter.

68. One comment said the rule should clarify whether system validation should be capable of discerning the absence of electronic records, in light of agency concerns about falsification. The comment added that the agency's concerns regarding invalid or altered records can be mitigated by use of cryptographically enhanced methods, including secure time and date stamping.

The agency does not believe that it is necessary at this time to include an explicit requirement that systems be capable of detecting the absence of records. The agency advises that the requirement in Sec. 11.10(e) for audit trails of operator actions would cover those actions intended to delete records. Thus, the agency would expect firms to document such deletions, and would expect the audit trail mechanisms to be included in the validation of the electronic records system.

69. Proposed Sec. 11.10(b) states that controls for closed systems must include the ability to generate true copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency, and that if there were any questions regarding the ability of the agency to perform such review and copying, persons should contact the agency.

Several comments objected to the requirement for “true” copies of electronic records. The comments asserted that information in an original record (as may be contained in a database) may be presented in a copy in a different format that may be more usable. The comments concluded that, to generate precise “true” copies of electronic records, firms may have to retain the hardware and software that had been used to create those records in the first place (even when such hardware and software had been replaced by newer systems). The comments pointed out that firms may have to provide FDA with the application logic for “true” copies, and that this may violate copyright provisions. One comment illustrated the difference between “true” copies and other equally reliable, but not exact, copies of electronic records by noting that pages from FDA's paper publications (such as the CFR and the Compliance Policy Guidance Manual) look quite different from electronic copies posted to FDA's bulletin board. The comments suggested different wording that would effectively require accurate and complete copies, but not necessarily “true” copies.

The agency agrees that providing exact copies of electronic records in the strictest meaning of the word “true” may not always be feasible. The agency nonetheless believes it is vital that copies of electronic records provided to FDA be accurate and complete. Accordingly, in Sec. 11.10(b), “true” has been replaced with “accurate and complete.” The agency expects that this revision should obviate the potential problems noted in the comments. The revision should also reduce the costs of providing copies by making clear that firms need not maintain obsolete equipment in order to make copies that are “true” with respect to format and computer system.

70. Many comments objected to the proposed requirement that systems be capable of generating electronic copies of electronic records for FDA inspection and copying, although they generally agreed that it was appropriate to provide FDA with readable paper copies. Alternative wording was suggested that would make providing electronic copies optional, such that persons could provide FDA with nothing but paper copies if they so wished. The comments argued that providing FDA with electronic copies was unnecessary, unjustified, not practical considering the different types of computer systems that may be in use, and would unfairly limit firms in their selection of hardware and software if they could only use systems that matched FDA's capabilities (capabilities which, it was argued, would not be uniform throughout the United States). One comment suggested that the rule specify [**FDA page 13446**] a particular format, such as ASCII, for electronic copies to FDA.

The agency disagrees with the assertion that FDA need only be provided with paper copies of electronic records. To operate effectively, the agency must function on the same technological plane as the industries it regulates. Just as firms realize efficiencies and benefits in the use of electronic records, FDA should be able to conduct audits efficiently and thoroughly using the same technology. For example, where firms perform computerized trend analyses of electronic records to improve their processes, FDA should be able to use computerized methods to audit electronic records (on site and off, as necessary) to detect trends, inconsistencies, and potential problem areas. If FDA is restricted to reviewing only paper copies of those records, the results would severely impede its operations. Inspections would take longer to complete, resulting in delays in approvals of new medical products, and expenditure of additional resources both by FDA (in performing the inspections and transcribing paper records to electronic format) and by the inspected firms, which would generate the paper copies and respond to questions during the resulting lengthened inspections.

The agency believes that it also may be necessary to require that persons furnish certain electronic copies of electronic records to FDA because paper copies may not be accurate and complete if they lack certain audit trail (metadata) information. Such information may have a direct bearing on record trustworthiness and reliability. These data could include information, for example, on when certain items of electronic mail were sent and received.

The agency notes that people who use different computer systems routinely provide each other with electronic copies of electronic records, and there are many current and developing tools to enable such sharing. For example, at a basic level, records may be created in, or transferred to, the ASCII format. Many different commercial programs have the capability to import from, and export to, electronic records having different formats. Firms use electronic data interchange (commonly known as EDI) and agreed upon transaction set formats to enable them to exchange copies of electronic records effectively. Third parties are also developing portable document formats to enable conversion among several diverse formats.

Concerning the ability of FDA to handle different formats of electronic records, based upon the emergence of format conversion tools such as those mentioned above, the agency's experience with electronic submissions such as computer assisted new drug applications (commonly known as CANDA's), and the agency's planned Submissions Management and Review Tracking System (commonly known as SMART), FDA is confident that it can work with firms to minimize any formatting difficulties. In addition, substitution of the words “accurate and complete” for “true,” as discussed in comment 69, should make it easier for firms to provide FDA with electronic copies of their electronic records. FDA does not believe it is necessary to specify any particular format in part 11 because it prefers, at this time, to afford industry and the agency more flexibility in deciding which formats meet the capabilities of all parties. Accordingly, the agency has revised proposed Sec. 11.10(b) to read:

The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

71. Proposed Sec. 11.10(c) states that procedures and controls for closed systems must include the protection of records to enable their accurate and ready retrieval throughout the records retention period.

One firm commented that, because it replaces systems often (about every 3 years), it may have to retain supplanted systems to meet these requirements. Another comment suggested that the rule be modified to require records retention only for as long as “legally mandated.”

The agency notes that, as discussed in comment 70 of this document, persons would not necessarily have to retain supplanted hardware and software systems provided they implemented conversion capabilities when switching to replacement technologies. The agency does not believe it is necessary to add the qualifier “legally mandated” because the retention period for a given record will generally be established by the regulation that requires the record. Where the regulations do not specify a given time, the agency would expect firms to establish their own retention periods. Regardless of the basis for the retention period, FDA believes that the requirement that a given electronic record be protected to permit it to be accurately and readily retrieved for as long as it is kept is reasonable and necessary.

72. Proposed Sec. 11.10(e) would require the use of time-stamped audit trails to document record changes, all write-to-file operations, and to independently record the date and time of operator entries and actions. Record changes must not obscure previously recorded information and such audit trail documentation must be retained for a period at least as long as required for the subject electronic documents and must be available for agency review and copying.

Many comments objected to the proposed requirement that all write-to-file operations be documented in the audit trail because it is unnecessary to document all such operations. The comments said that this would require audit trails for such automated recordings as those made to internal buffers, data swap files, or temporary files created by word processing programs. The comments suggested revising Sec. 11.10(e) to require audit trails only for operator entries and actions.

Other comments suggested that audit trails should cover: (1) Operator data inputs but not actions, (2) only operator changes to records, (3) only critical write-to-file information, (4) operator changes as well as all actions, (5) only new entries, (6) only systems where data can be altered, (7) only information recorded by humans, (8) information recorded by both humans and devices, and (9) only entries made upon adoption of the records as official. One comment said audit trails should not be required for data acquisition systems, while another comment said audit trails are critical for data acquisition systems.

It is the agency's intent that the audit trail provide a record of essentially who did what, wrote what, and when. The write-to-file operations referenced in the proposed rule were not intended to cover the kind of “background” nonhuman recordings the comments identified.

The agency considers such operator actions as activating a manufacturing sequence or turning off an alarm to warrant the same audit trail coverage as operator data entries in order to document a thorough history of events and those responsible for such events. Although FDA acknowledges that not every operator “action,” such as switching among screen displays, need be covered by audit trails, the agency is concerned that revising the rule to cover only “critical” operations would result in excluding much information and actions that are necessary to document events thoroughly.

[**FDA page 13447**]

The agency believes that, in general, the kinds of operator actions that need to be covered by an audit trail are those important enough to memorialize in the electronic record itself. These are actions which, for the most part, would be recorded in corresponding paper records according to existing recordkeeping requirements.

The agency intends that the audit trail capture operator actions (e.g., a command to open a valve) at the time they occur, and operator information (e.g., data entry) at the time the information is saved to the recording media (such as disk or tape), in much the same manner as such actions and information are memorialized on paper. The audit trail need not capture every keystroke and mistake that is held in a temporary buffer before those commitments. For example, where an operator records the lot number of an ingredient by typing the lot number, followed by the “return key” (where pressing the return key would cause the information to be saved to a disk file), the audit trail need not record every “backspace delete” key the operator may have previously pressed to correct a typing error. Subsequent “saved” corrections made after such a commitment, however, must be part of the audit trail.

At this time, the agency's primary concern relates to the integrity of human actions. Should the agency's experience with part 11 demonstrate a need to require audit trails of device operations and entries, the agency will propose appropriate revisions to these regulations. Accordingly, the agency has revised proposed Sec. 11.10(e) by removing reference to all write-to-file operations and clarifying that the audit trail is to cover operator entries and actions that create, modify, or delete electronic records.

73. A number of comments questioned whether proposed Sec. 11.10(e) mandated that the audit trail be part of the electronic record itself or be kept as a separate record. Some comments interpreted the word “independently” as requiring a separate record. Several comments focused on the question of whether audit trails should be generated manually under operator control or automatically without operator control. One comment suggested a revision that would require audit trails to be generated by computer, because the system, not the operator, should record the audit trail. Other comments said the rule should facilitate date and time recording by software, not operators, and that the qualifier “securely” be added to the language describing the audit trail. One comment, noting that audit trails require validation and qualification to ensure that time stamps are accurate and independent, suggested that audit trails be required only when operator actions are witnessed.

The agency advises that audit trail information may be contained as part of the electronic record itself or as a separate record. FDA does not intend to require one method over the other. The word “independently” is intended to require that the audit trail not be under the control of the operator and, to prevent ready alteration, that it be created independently of the operator.

To maintain audit trail integrity, the agency believes it is vital that the audit trail be created by the computer system independently of operators. The agency believes it would defeat the purpose of audit trails to permit operators to write or change them. The agency believes that, at this time, the source of such independent audit trails may effectively be within the organization that creates the electronic record. However, the agency is aware of a situation under which time and date stamps are provided by trusted third parties outside of the creating organization. These third parties provide, in effect, a public electronic notary service. FDA will monitor development of such services in light of part 11 to determine if a requirement for such third party services should be included in these regulations. For now, the agency considers the advent of such services as recognition of the need for strict objectivity in recording time and date stamps.

The agency disagrees with the premise that only witnessed operator actions need be covered by audit trails because the opportunities for record falsification are not limited to cases where operator actions are witnessed. Also, the need for validating audit trails does not diminish the need for their implementation.

FDA agrees with the suggestion that the proposed rule be revised to require a secure audit trail--a concept inherent in having such a control at all. Accordingly, proposed Sec. 11.10(e) has been revised to require use of “secure, computer-generated” audit trails.

74. A few comments objected to the requirement that time be recorded, in addition to dates, and suggested that time be recorded only when necessary and feasible. Other comments specifically supported the requirement for recording time, noting that time stamps make electronic signatures less vulnerable to fraud and abuse. The comments noted that, in any setting, there is a need to identify the date, time, and person responsible for adding to or changing a value. One of the comments suggested that the rule require recording the reason for making changes to electronic records. Other comments implicitly supported recording time.

FDA believes that recording time is a critical element in documenting a sequence of events. Within a given day a number of events and operator actions may take place, and without recording time, documentation of those events would be incomplete. For example, without time stamps, it may be nearly impossible to determine such important sequencing as document approvals and revisions and the addition of ingredients in drug production. Thus, the element of time becomes vital to establishing an electronic record's trustworthiness and reliability.

The agency notes that comments on the ANPRM frequently identified use of date/time stamps as an important system control. Time recording, in the agency's view, can also be an effective deterrent to records falsification. For example, event sequence codes alone would not necessarily document true time in a series of events, making falsification of that sequence easier if time stamps are not used. The agency believes it should be very easy for firms to implement time stamps because there is a clock in every computer and document management software, electronic mail systems and other electronic record/electronic applications, such as digital signature programs, commonly apply date and time stamps. The agency does not intend that new technologies, such as cryptographic technologies, will be needed to comply with this requirement. The agency believes that implementation of time stamps should be feasible in virtually all computer systems because effective computer operations depend upon internal clock or timing mechanisms and, in the agency's experience, most computer systems are capable of precisely recording such time entries as when records are saved.

The agency is implementing the time stamp requirement based on the understanding that all current computers, electronic document software, electronic mail, and related electronic record systems include such technologies. The agency also understands that time stamps are applied automatically by these systems, meaning firms would not have to install additional hardware, software, or incur additional burden to implement this control. In recognition of this, the agency wishes to clarify that a primary intent of this provision is to ensure that people take reasonable measures to [**FDA page 13448**] ensure that those built in time stamps are accurate and that people do not alter them casually so as to readily mask unauthorized record changes.

The agency advises that, although part 11 does not specify the time units (e.g., tenth of a second, or even the second) to be used, the agency expects the unit of time to be meaningful in terms of documenting human actions.

The agency does not believe part 11 needs to require recording the reason for record changes because such a requirement, when needed, is already in place in existing regulations that pertain to the records themselves.

75. One comment stated that proposed Sec. 11.10(e) should not require an electronic signature for each write-to-file operation.

The agency advises that Sec. 11.10(e) does not require an electronic signature as the means of authenticating each write-to-file operation. The agency expects the audit trail to document who did what and when, documentation that can be recorded without electronic signatures themselves.

76. Several comments, addressing the proposed requirement that record changes not obscure previously recorded information, suggested revising proposed Sec. 11.10(e) to apply only to those entries intended to update previous information.

The agency disagrees with the suggested revision because the rewording is too narrow. The agency believes that some record changes may not be “updates” but significant modifications or falsifications disguised as updates. All changes to existing records need to be documented, regardless of the reason, to maintain a complete and accurate history, to document individual responsibility, and to enable detection of record falsifications.

77. Several comments suggested replacing the word “document” with “record” in the phrase “Such audit trails shall be retained for a period at least as long as required for the subject electronic documents * * *” because not all electronic documents are electronic records and because the word document connotes paper.

As discussed in section III.D. of this document, the agency equates electronic documents with electronic records, but for consistency, has changed the phrase to read “Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records * * *.”

78. Proposed Sec. 11.10(k)(ii) (Sec. 11.10(k)(2) in this regulation) addresses electronic audit trails as a systems documentation control. One comment noted that this provision appears to be the same as the audit trail provision of proposed Sec. 11.10(e) and requested clarification.

The agency wishes to clarify that the kinds of records subject to audit trails in the two provisions cited by the comment are different. Section 11.10(e) pertains to those records that are required by existing regulations whereas Sec. 11.10(k)(2) covers the system documentation records regarding overall controls (such as access privilege logs, or system operational specification diagrams). Accordingly, the first sentence of Sec. 11.10(e) has been revised to read “Use of secure, computer-generated, time-stamped audit trails to independently record and date the time of operator entries and actions that create, modify, or delete electronic records.”

79. Proposed Sec. 11.10(f) states that procedures and controls for closed systems must include the use of operational checks to enforce permitted sequencing of events, as appropriate.

Two comments requested clarification of the agency's intent regarding operational checks.

The agency advises that the purpose of performing operational checks is to ensure that operations (such as manufacturing production steps and signings to indicate initiation or completion of those steps) are not executed outside of the predefined order established by the operating organization.

80. Several comments suggested that, for clarity, the phrase “operational checks” be modified to “operational system checks.”

The agency agrees that the added modifier “system” more accurately reflects the agency's intent that operational checks be performed by the computer systems and has revised proposed Sec. 11.10(f) accordingly.

81. Several comments suggested revising proposed Sec. 11.10(f) to clarify what is to be checked. The comments suggested that “steps” in addition to “events” be checked, only critical steps be checked, and that “records” also be checked.

The agency intends the word “event” to include “steps” such as production steps. For clarity, however, the agency has revised proposed Sec. 11.10(f) by adding the word “steps.” The agency does not, however, agree that only critical steps need be subject to operational checks because a given specific step or event may not be critical, yet it may be very important that the step be executed at the proper time relative to other steps or events. The agency does not believe it necessary to add the modifier “records” to proposed Sec. 11.10(f) because creation, deletion, or modification of a record is an event. Should it be necessary to create, delete, or modify records in a particular sequence, operational system checks would ensure that the proper sequence is followed.

82. Proposed Sec. 11.10(g) states that procedures and controls for closed systems must include the use of authority checks to ensure that only authorized individuals use the system, electronically sign a record, access the operation or device, alter a record, or perform the operation at hand.

One comment suggested that the requirement for authority checks be qualified with the phrase “as appropriate,” on the basis that it would not be necessary for certain parts of a system, such as those not affecting an electronic record. The comment cited pushing an emergency stop button as an example of an event that would not require an authority check. Another comment suggested deleting the requirement on the basis that some records can be read by all employees in an organization.

The agency advises that authority checks, and other controls under Sec. 11.10, are intended to ensure the authenticity, integrity, and confidentiality of electronic records, and to ensure that signers cannot readily repudiate a signed record as not genuine. Functions outside of this context, such as pressing an emergency stop button, would not be covered. However, even in this example, the agency finds it doubtful that a firm would permit anyone, such as a stranger from outside the organization, to enter a facility and press the stop button at will regardless of the existence of an emergency. Thus, there would likely be some generalized authority checks built into the firm's operations.

The agency believes that few organizations freely permit anyone from within or without the operation to use their computer system, electronically sign a record, access workstations, alter records, or perform operations. It is likely that authority checks shape the activities of almost every organization. The nature, scope, and mechanism of performing such checks is up to the operating organization. FDA believes, however, that performing such checks is one of the most fundamental measures to ensure the integrity and trustworthiness of electronic records.

Proposed Sec. 11.10(g) does not preclude all employees from being permitted to read certain electronic records. However, the fact that some records may be read by all employees would not [**FDA page 13449**] justify deleting the requirement for authority checks entirely. The agency believes it is highly unlikely that all of a firm's employees would have authority to read, write, and sign all of its electronic records.

83. One comment said authority checks are appropriate for document access but not system access, and suggested that the phrase “access the operation or device” be deleted. The comment added, with respect to authority checks on signing records, that in many organizations, more than one individual has the authority to sign documents required under FDA regulations and that such authority should be vested with the individual as designated by the operating organization. Another comment said proposed Sec. 11.10(g) should explicitly require access authority checks and suggested that the phrase “use the system” be changed to “access and use the system.” The comment also asked for clarification of the term “device.”

The agency disagrees that authority checks should not be required for system access because, as discussed in comment 82 of this document, it is unlikely that a firm would permit any unauthorized individuals to access its computer systems. System access control is a basic security function because system integrity may be impeached even if the electronic records themselves are not directly accessed. For example, someone could access a system and change password requirements or otherwise override important security measures, enabling individuals to alter electronic records or read information that they were not authorized to see. The agency does not believe it necessary to add the qualifier “access and” because Sec. 11.10(d) already requires that system access be limited to authorized individuals. The agency intends the word “device” to mean a computer system input or output device and has revised proposed Sec. 11.10(g) to clarify this point.

Concerning signature authority, FDA advises that the requirement for authority checks in no way limits organizations in authorizing individuals to sign multiple records. Firms may use any appropriate mechanism to implement such checks. Organizations do not have to embed a list of authorized signers in every record to perform authority checks. For example, a record may be linked to an authority code that identifies the title or organizational unit of people who may sign the record. Thus, employees who have that corresponding code, or belong to that unit, would be able to sign the record. Another way to implement controls would be to link a list of authorized records to a given individual, so that the system would permit the individual to sign only records in that list.

84. Two comments addressed authority checks within the context of PDMA and suggested that such checks not be required for drug sample receipt records. The comments said that different individuals may be authorized to accept drug samples at a physician's office, and that the large number of physicians who would potentially qualify to receive samples would be too great to institute authority checks.

The agency advises that authority checks need not be automated and that in the context of PDMA such checks would be as valid for electronic records as they are for paper sample requests because only licensed practitioners or their designees may accept delivery of drug samples. The agency, therefore, acknowledges that many individuals may legally accept samples and, thus, have the authority to sign electronic receipts. However, authority checks for electronic receipts could nonetheless be performed by sample manufacturer representatives by using the same procedures as the representatives use for paper receipts. Accordingly, the agency disagrees with the comment that proposed Sec. 11.10(g) should not apply to PDMA sample receipts.

The agency also advises that under PDMA, authority checks would be particularly important in the case of drug sample request records because only licensed practitioners may request drug samples.

Accordingly, proposed Sec. 11.10(g) has been revised to read: “Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.”

85. Proposed Sec. 11.10(h) states that procedures and controls for closed systems must include the use of device (e.g., terminal) location checks to determine, as appropriate, the validity of the source of data input or operational instruction. Several comments objected to this proposed requirement and suggested its deletion because it is: (1) Unnecessary (because the data source is always known by virtue of system design and validation); (2) problematic with respect to mobile devices, such as those connected by modem; (3) too much of a “how to;” (4) not explicit enough to tell firms what to do; (5) unnecessary in the case of PDMA; and (6) technically challenging. One comment stated that a device's identification, in addition to location, may be important and suggested that the proposed rule be revised to require device identification as well.

FDA advises that, by use of the term “as appropriate,” it does not intend to require device checks in all cases. The agency believes that these checks are warranted where only certain devices have been selected as legitimate sources of data input or commands. In such cases, the device checks would be used to determine if the data or command source was authorized. In a network, for example, it may be necessary for security reasons to limit issuance of critical commands to only one authorized workstation. The device check would typically interrogate the source of the command to ensure that only the authorized workstation, and not some other device, was, in fact, issuing the command.

The same approach applies for remote sources connected by modem, to the extent that device identity interrogations could be made automatically regardless of where the portable devices were located. To clarify this concept, the agency has removed the word “location” from proposed Sec. 11.10(h). Device checks would be necessary under PDMA when the source of commands or data is relevant to establishing authenticity, such as when licensed practitioners order drug samples directly from the manufacturer or authorized distributor without the intermediary of a sales representative. Device checks may also be useful to firms in documenting and identifying which sales representatives are transmitting drug sample requests from licensed practitioners.

FDA believes that, although validation may demonstrate that a given terminal or workstation is technically capable of sending information from one point to another, validation alone would not be expected to address whether or not such device is authorized to do so.

86. Proposed Sec. 11.10(i) states that procedures and controls for closed systems must include confirmation that persons who develop, maintain, or use electronic record or signature systems have the education, training, and experience to perform their assigned tasks.

Several comments objected to the word “confirmation” because it is redundant with, or more restrictive than, existing regulations, and suggested alternate wording, such as “evidence.” Two comments interpreted the proposed wording as requiring that checks of personnel qualifications be performed automatically by computer systems that perform database type [**FDA page 13450**] matches between functions and personnel training records.

The agency advises that, although there may be some overlap in proposed Sec. 11.10(i) and other regulations regarding the need for personnel to be properly qualified for their duties, part 11 is specific to functions regarding electronic records, an issue that other regulations may or may not adequately address. Therefore, the agency is retaining the requirement.

The agency does not intend to require that the check of personnel qualifications be performed automatically by a computer system itself (although such automation is desirable). The agency has revised the introductory paragraph of Sec. 11.10, as discussed in section VII. of this document, to clarify this point. The agency agrees that another word should be used in place of “confirmation,” and for clarity has selected “determination.”

87. One comment suggested that the word “training” be deleted because it has the same meaning as “education” and “experience,” and objected to the implied requirement for records of employee training. Another comment argued that applying this provision to system developers was irrelevant so long as systems perform as required and have been appropriately validated. The comment suggested revising proposed Sec. 11.10(i) to require employees to be trained only “as necessary.” One comment, noting that training and experience are very important, suggested expanding proposed Sec. 11.10(i) to require appropriate examination and certification of persons who perform certain high-risk, high-trust functions and tasks.

The agency regards this requirement as fundamental to the proper operation of a facility. Personnel entrusted with important functions must have sufficient training to do their jobs. In FDA's view, formal education (e.g., academic studies) and general industry experience would not necessarily prepare someone to begin specific, highly technical tasks at a given firm. Some degree of on-the-job training would be customary and expected. The agency believes that documentation of such training is also customary and not unreasonable.

The agency also disagrees with the assertion that personnel qualifications of system developers are irrelevant. The qualifications of personnel who develop systems are relevant to the expected performance of the systems they build and their ability to explain and support these systems. Validation does not lessen the need for personnel to have the education, training, and experience to do their jobs properly. Indeed, it is highly unlikely that poorly qualified developers would be capable of producing a system that could be validated. The agency advises that, although the intent of proposed Sec. 11.10(i) is to address qualifications of those personnel who develop systems within an organization, rather than external “vendors” per se, it is nonetheless vital that vendor personnel are likewise qualified to do their work. The agency agrees that periodic examination or certification of personnel who perform certain critical tasks is desirable. However, the agency does not believe that at this time a specific requirement for such examination and certification is necessary.

88. Proposed Sec. 11.10(j) states that procedures and controls for closed systems must include the establishment of, and adherence to, written policies that hold individuals accountable and liable for actions initiated under their electronic signatures, so as to deter record and signature falsification.

Several comments suggested changing the word “liable” to “responsible” because the word “responsible” is broader, more widely understood by employees, more positive and inclusive of elements of honesty and trust, and more supportive of a broad range of disciplinary measures. One comment argued that the requirement would not deter record or signature falsification because employee honesty and integrity cannot be regulated.

The agency agrees because, although the words “responsible” and “liable” are generally synonymous, “responsible” is preferable because it is more positive and supportive of a broad range of disciplinary measures. There may be a general perception that electronic records and electronic signatures (particularly identification codes and passwords) are less significant and formal than traditional paper records and handwritten signatures. Individuals may therefore not fully equate the seriousness of electronic record falsification with paper record falsification. Employees need to understand the gravity and consequences of signature or record falsification. Although FDA agrees that employee honesty cannot be ensured by requiring it in a regulation, the presence of strong accountability and responsibility policies is necessary to ensure that employees understand the importance of maintaining the integrity of electronic records and signatures.

89. Several comments expressed concern regarding employee liability for actions taken under their electronic signatures in the event that such signatures are compromised, and requested “reasonable exceptions.” The comments suggested revising proposed Sec. 11.10(j) to hold people accountable only where there has been intentional falsification or corruption of electronic data.

The agency considers the compromise of electronic signatures to be a very serious matter, one that should precipitate an appropriate investigation into any causative weaknesses in an organization's security controls. The agency nonetheless recognizes that where such compromises occur through no fault or knowledge of individual employees, there would be reasonable limits on the extent to which disciplinary action would be taken. However, to maintain emphasis on the seriousness of such security breeches and deter the deliberate fabrication of “mistakes,” the agency believes Sec. 11.10 should not provide for exceptions that may lessen the import of such a fabrication.

90. One comment said the agency should consider the need for criminal law reform because current computer crime laws do not address signatures when unauthorized access or computer use is not an issue. Another comment argued that proposed Sec. 11.10(j) should be expanded beyond “individual” accountability to include business entities.

The agency will consider the need for recommending legislative initiatives to address electronic signature falsification in light of the experience it gains with this regulation. The agency does not believe it necessary to address business entity accountability specifically in Sec. 11.10 because the emphasis is on actions and accountability of individuals, and because individuals, rather than business entities, apply signatures.

91. One comment suggested that proposed Sec. 11.10(j) should be deleted because it is unnecessary because individuals are presumably held accountable for actions taken under their authority, and because, in some organizations, individuals frequently delegate authority to sign their names.

As discussed in comments 88 to 90 of this document, the agency has concluded that this section is necessary. Furthermore it does not limit delegation of authority as described in the comment. However, where one individual signs his or her name on behalf of someone else, the signature applied should be that of the delegatee, with some notation of that fact, and not the name of the delegator. This is the [**FDA page 13451**] same procedure commonly used on paper documents, noted as “X for Y.”

92. Proposed Sec. 11.10(k) states that procedures and controls for closed systems must include the use of appropriate systems documentation controls, including: (1) Adequate controls over the distribution, access to, and use of documentation for system operation and maintenance; and (2) records revision and change control procedures to maintain an electronic audit trail that documents time-sequenced development and modification of records. Several comments requested clarification of the type of documents covered by proposed Sec. 11.10(k). One comment noted that this section failed to address controls for record retention. Some comments suggested limiting the scope of systems documentation to application and configurable software, or only to software that could compromise system security or integrity. Other comments suggested that this section should be deleted because some documentation needs wide distribution within an organization, and that it is an onerous burden to control user manuals.

The agency advises that Sec. 11.10(k) is intended to apply to systems documentation, namely, records describing how a system operates and is maintained, including standard operating procedures. The agency believes that adequate controls over such documentation are necessary for various reasons. For example, it is important for employees to have correct and updated versions of standard operating and maintenance procedures. If this documentation is not current, errors in procedures and/or maintenance are more likely to occur. Part 11 does not limit an organization's discretion as to how widely or narrowly any document is to be distributed, and FDA expects that certain documents will, in fact, be widely disseminated. However, some highly sensitive documentation, such as instructions on how to modify system security features, would not routinely be widely distributed. Hence, it is important to control distribution of, access to, and use of such documentation.

Although the agency agrees that the most critical types of system documents would be those directly affecting system security and integrity, FDA does not agree that control over system documentation should only extend to security related software or to application or configurable software. Documentation that relates to operating systems, for example, may also have an impact on security and day-to-day operations. The agency does not agree that it is an onerous burden to control documentation that relates to effective operation and security of electronic records systems. Failure to control such documentation, as discussed above, could permit and foster records falsification by making the enabling instructions for these acts readily available to any individual.

93. Concerning the proposed requirement for adequate controls over documentation for system operation and maintenance, one comment suggested that it be deleted because it is under the control of system vendors, rather than operating organizations. Several comments suggested that the proposed provision be deleted because it duplicates Sec. 11.10(e) with respect to audit trails. Some comments also objected to maintaining the change control procedures in electronic form and suggested deleting the word “electronic” from “electronic audit trails.”

The agency advises that this section is intended to apply to systems documentation that can be changed by individuals within an organization. If systems documentation can only be changed by a vendor, this provision does not apply to the vendor's customers. The agency acknowledges that systems documentation may be in paper or electronic form. Where the documentation is in paper form, an audit trail of revisions need not be in electronic form. Where systems documentation is in electronic form, however, the agency intends to require the audit trail also be in electronic form, in accordance with Sec. 11.10(e). The agency acknowledges that, in light of the comments, the proposed rule may not have been clear enough regarding audit trails addressed in Sec. 11.10(k) compared to audit trails addressed in Sec. 11.10(e) and has revised the final rule to clarify this matter.

The agency does not agree, however, that the audit trail provisions of Sec. 11.10(e) and (k), as revised, are entirely duplicative. Section 11.10(e) applies to electronic records in general (including systems documentation); Sec. 11.10(k) applies exclusively to systems documentation, regardless of whether such documentation is in paper or electronic form.

As revised, Sec. 11.10(k) now reads as follows:

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

VIII. Electronic Records--Controls for Open Systems (Sec. 11.30)

Proposed Sec. 11.30 states that: “Open systems used to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity and confidentiality of electronic records from the point of their creation to the point of their receipt.” In addition, Sec. 11.30 states:

* * * Such procedures and controls shall include those identified in Sec. 11.10, as appropriate, and such additional measures as document encryption and use of established digital signature standards acceptable to the agency, to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

94. One comment suggested that the reference to digital signature standards be deleted because the agency should not be setting standards and should not dictate how to ensure record authenticity, integrity, and confidentiality. Other comments requested clarification of the agency's expectations with regard to digital signatures: (1) The kinds that would be acceptable, (2) the mechanism for announcing which standards were acceptable (and whether that meant FDA would be certifying particular software), and (3) a definition of digital signature. One comment asserted that FDA should accept international standards for digital signatures. Some comments also requested a definition of encryption. One comment encouraged the agency to further define open systems.

The agency advises that Sec. 11.30 requires additional controls, beyond those identified in Sec. 11.10, as needed under the circumstances, to ensure record authenticity, integrity, and confidentiality for open systems. Use of digital signatures is one measure that may be used, but is not specifically required. The agency wants to ensure that the digital signature standard used is, in fact, appropriate. Development of digital signature standards is a complex undertaking, one FDA does not expect to be performed by individual firms on an ad hoc basis, and one FDA does not now seek to perform.

The agency is nonetheless concerned that such standards be robust and secure. Currently, the agency is aware of two such standards, the RSA (Rivest-Shamir-Adleman), and NIST's Digital Signature Standard (DSS). The DSS became Federal Information Processing Standard (FIPS) 186 on December 1, 1994. These standards are incorporated in different software programs. The agency does not seek to certify or otherwise approve of such programs, [**FDA page 13452**] but expects people who use such programs to ensure that they are suitable for their intended use. FDA is aware that NIST provides certifications regarding mathematical conformance to the DSS core algorithms, but does not formally evaluate the broader programs that contain those algorithms. The agency has revised the final rule to clarify its intent that firms retain the flexibility to use any appropriate digital signature as an additional system control for open

systems. FDA is also including a definition of digital signature under Sec. 11.3(b)(5).

The agency does not believe it necessary to codify the term “encryption” because, unlike the term digital signature, it has been in general use for many years and is generally understood to mean the transforming of a writing into a secret code or cipher. The agency is aware that there are several commercially available software programs that implement both digital signatures and encryption.

95. Two comments noted that use of digital signatures and encryption is not necessary in the context of PDMA, where access to an electronic record is limited once it is signed and stored. One of the comments suggested that proposed Sec. 11.30 be revised to clarify this point.

As discussed in comment 94 of this document, use of digital signatures and encryption would be an option when extra measures are necessary under the circumstances. In the case of PDMA records, such measures may be warranted in certain circumstances, and unnecessary in others. For example, if electronic records were to be transmitted by a firm's representative by way of a public online service to a central location, additional measures would be necessary. On the other hand, where the representative's records are hand delivered to that location, or transferred by direct connection between the representative and the central location, such additional measures to ensure record authenticity, confidentiality, and integrity may not be necessary. The agency does not believe that it is practical to revise Sec. 11.30 to elaborate on every possible situation in which additional measures would or would not be needed.

96. One comment addressed encryption of submissions to FDA and asked if people making those submissions would have to give the agency the appropriate “keys” and, if so, how the agency would protect the security of such information.

The agency intends to develop appropriate procedures regarding the exchange of “keys” attendant to use of encryption and digital signatures, and will protect those keys that must remain confidential, in the same manner as the agency currently protects trade secrets. Where the agency and a submitter agree to use a system that calls for the exchange of secret keys, FDA will work with submitters to achieve mutually agreeable procedures. The agency notes, however, that not all encryption and digital signature systems require that enabling keys be secret.

97. One comment noted that proposed Sec. 11.30 does not mention availability and nonrepudiation and requested clarification of the term “point of receipt.” The comment noted that, where an electronic record is received at a person's electronic mailbox (which resides on an open system), additional measures may be needed when the record is transferred to the person's own local computer because such additional transfer entails additional security risks. The comment suggested wording that would extend open system controls to the point where records are ultimately retained.

The agency agrees that, in the situation described by the comment, movement of the electronic record from an electronic mailbox to a person's local computer may necessitate open system controls. However, situations may vary considerably as to the ultimate point of receipt, and FDA believes proposed Sec. 11.30 offers greater flexibility in determining open system controls than revisions suggested by the comment. The agency advises that the concept of nonrepudiation is part of record authenticity and integrity, as already covered by Sec. 11.10(c). Therefore, FDA is not revising Sec. 11.30 as suggested.

IX. Electronic Records--Signature Manifestations (Sec. 11.50)

Proposed Sec. 11.50 requires that electronic records that are electronically signed must display in clear text the printed name of the signer, and the date and time when the electronic signature was executed. This section also requires that electronic records clearly indicate the meaning (such as review, approval, responsibility, and authorship) associated with their attendant signatures.

98. Several comments suggested that the information required under proposed Sec. 11.50 need not be contained in the electronic records themselves, but only in the human readable format (screen displays and printouts) of such records. The comments explained that the records themselves need only contain links, such as signature attribute codes, to such information to produce the displays of information required.

The comments noted, for example, that, where electronic signatures consist of an identification code in combination with a password, the combined code and password itself would not be part of the display.

Some comments suggested that proposed Sec. 11.50 be revised to clarify what items are to be displayed.

The agency agrees and has revised proposed Sec. 11.50 accordingly. The intent of this section is to require that human readable forms of signed electronic records, such as computer screen displays and printouts bear: (1) The printed name of the signer (at the time the record is signed as well as whenever the record is read by humans); (2) the date and time of signing; and (3) the meaning of the signature. The agency believes that revised Sec. 11.50 will afford persons the flexibility they need to implement the display of information appropriate for their own electronic records systems, consistent with other system controls in part 11, to ensure record integrity and prevent falsification.

99. One comment stated that the controls in proposed Sec. 11.50 would not protect against inaccurate entries.

FDA advises that the purpose of this section is not to protect against inaccurate entries, but to provide unambiguous documentation of the signer, when the signature was executed, and the signature's meaning. The agency believes that such a record is necessary to document individual responsibility and actions.

In a paper environment, the printed name of the individual is generally present in the signed record, frequently part of a traditional “signature block.” In an electronic environment, the person's name may not be apparent, especially where the signature is based on identification codes combined with passwords. In addition, the meaning of a signature is generally apparent in a paper record by virtue of the context of the record or, more often, explicit phrases such as “approved by,” “reviewed by,” and “performed by.” Thus, the agency believes that for clear documentation purposes it is necessary to carry such meanings into the electronic record environment.

100. One comment suggested that proposed Sec. 11.50 should apply only to those records that are required to be signed, and that the display of the date and time should be performed in a secure manner.

The agency intends that this section apply to all signed electronic records regardless of whether other regulations require them to be signed. The agency believes that if it is important enough that a record be signed, human readable [**FDA page 13453**] displays of such records must include the printed name of the signer, the date and time of signing, and the meaning of the signature. Such information is crucial to the agency's ability to protect public health. For example, a message from a firm's management to employees instructing them on a particular course of action may be critical in litigation. This requirement will help ensure clear documentation and deter falsification regardless of whether the signature is electronic or handwritten.

The agency agrees that the display of information should be carried out in a secure manner that preserves the integrity of that information. The agency, however, does not believe it is necessary at this time to revise Sec. 11.50 to add specific security measures because other requirements of part 11 have the effect of ensuring appropriate security.

Because signing information is important regardless of the type of signature used, the agency has revised Sec. 11.50 to cover all types of signings.

101. Several comments objected to the requirement in proposed Sec. 11.50(a) that the time of signing be displayed in addition to the date on the grounds that such information is: (1)

Unnecessary, (2) costly to implement, (3) needed in the electronic record for auditing purposes, but not needed in the display of the record, and (4) only needed in critical applications. Some comments asserted that recording time should be optional. One comment asked whether the time should be local to the signer or to a central network when electronic record systems cross different time zones.

The agency believes that it is vital to record the time when a signature is applied. Documenting the time when a signature was applied can be critical to demonstrating that a given record was, or was not, falsified. Regarding systems that may span different time zones, the agency advises that the signer's local time is the one to be recorded.

102. One comment assumed that a person's user identification code could be displayed instead of the user's printed name, along with the date and time of signing.

This assumption is incorrect. The agency intends that the printed name of the signer be displayed for purposes of unambiguous documentation and to emphasize the importance of the act of signing to the signer. The agency believes that because an identification code is not an actual name, it would not be a satisfactory substitute.

103. One comment suggested that the word “printed” in the phrase “printed name” be deleted because the word was superfluous. The comment also stated that the rule should state when the clear text must be created or displayed because some computer systems, in the context of electronic data interchange transactions, append digital signatures to records before, or in connection with, communication of the record.

The agency disagrees that the word “printed” is superfluous because the intent of this section is to show the name of the person in an unambiguous manner that can be read by anyone. The agency believes that requiring the printed name of the signer instead of codes or other manifestations, more effectively provides clarity.

The agency has revised this section to clarify the point at which the signer's information must be displayed, namely, as part of any human readable form of the electronic record. The revision, in the agency's view, addresses the comment's concern regarding the application of digital signatures. The agency advises that under Sec. 11.50, any time after an electronic record has been signed, individuals who see the human readable form of the record will be able to immediately tell who signed the record, when it was signed, and what the signature meant. This includes the signer who, as with a traditional signature to paper, will be able to review the signature instantly.

104. One comment asked if the operator would have to see the meaning of the signature, or if the information had to be stored on the physical electronic record.

As discussed in comment 100 of this document, the information required by Sec. 11.50(b) must be displayed in the human readable format of the electronic record. Persons may elect to store that information directly within the electronic record itself, or in logically associated records, as long as such information is displayed any time a person reads the record.

105. One comment noted that proposed Sec. 11.50(b) could be interpreted to require lengthy explanations of the signatures and the credentials of the signers. The comment also stated that this information would more naturally be contained in standard operating procedures, manuals, or accompanying literature than in the electronic records themselves.

The agency believes that the comment misinterprets the intent of this provision. Recording the meaning of the signature does not infer that the signer's credentials or other lengthy explanations be part of that meaning. The statement must merely show what is meant by the act of signing (e.g., review, approval, responsibility, authorship).

106. One comment noted that the meaning of a signature may be included in a (digital signature) public key certificate and asked if this would be acceptable. The comment also noted that the certificate might be easily accessible by a record recipient from either a recognized database or one that might be part of, or associated with, the electronic record itself. The comment further suggested that FDA would benefit from participating in developing rules of practice regarding certificate-based public key cryptography and infrastructure with the Information Security Committee, Section of Science and Technology, of the American Bar Association (ABA).

The intent of this provision is to clearly discern the meaning of the signature when the electronic record is displayed in human readable form. The agency does not expect such meaning to be contained in or displayed by a public key certificate because the public key is generally a fixed value associated with an individual. The certificate is used by the recipient to authenticate a digital signature that may have different meanings, depending upon the record being signed. FDA acknowledges that it is possible for someone to establish different public keys, each of which may indicate a different signature meaning.

Part 11 would not prohibit multiple “meaning” keys provided the meaning of the signature itself was still clear in the display of the record, a feature that could conceivably be implemented by software.

Regarding work of the ABA and other standard-setting organizations, the agency welcomes an open dialog with such organizations, for the mutual benefit of all parties, to establish and facilitate the use of electronic record/electronic signature technologies. FDA's participation in any such activities would be in accordance with the agency's policy on standards stated in the Federal Register of October 11, 1995 (60 FR 53078).

Revised Sec. 11.50, signature manifestations, reads as follows:

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) The items identified in paragraphs (a)(1), (a)(2), and

(a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

[**FDA page 13454**]

X. Electronic Records--Signature/Record Linking (Sec. 11.70)

107. Proposed Sec. 11.70 states that electronic signatures and handwritten signatures executed to electronic records must be verifiably bound to their respective records to ensure that signatures could not be excised, copied, or otherwise transferred to falsify another electronic record.

Many comments objected to this provision as too prescriptive, unnecessary, unattainable, and excessive in comparison to paper-based records. Some comments asserted that the objectives of the section could be attained through appropriate procedural and administrative controls. The comments also suggested that objectives of the provision could be met by appropriate software (i.e., logical) links between the electronic signatures and electronic records, and that such links are common in systems that use identification codes in combination with passwords. One firm expressed full support for the provision, and noted that its system implements such a feature and that signature-to-record binding is similar to the record-locking provision of the proposed PDMA regulations.

The agency did not intend to mandate use of any particular technology by use of the word “binding.” FDA recognizes that, because it is relatively easy to copy an electronic signature to another electronic record and thus compromise or falsify that record, a technology based link is necessary. The agency does not believe that procedural or administrative controls alone are sufficient to ensure that objective because such controls could be more easily circumvented than a straightforward technology based approach. In addition, when electronic records are transferred from one party to another, the procedural controls used by the sender and recipient may be different.

This could result in record falsification by signature transfer.

The agency agrees that the word “link” would offer persons greater flexibility in implementing the intent of this provision and in associating the names of individuals with their identification codes/passwords without actually recording the passwords themselves in electronic records. The agency has revised proposed Sec. 11.70 to state that signatures shall be linked to their electronic records.

108. Several comments argued that proposed Sec. 11.70 requires absolute protection of electronic records from falsification, an objective that is unrealistic to the extent that determined individuals could falsify records.

The agency acknowledges that, despite elaborate system controls, certain determined individuals may find a way to defeat antifalsification measures. FDA will pursue such illegal activities as vigorously as it does falsification of paper records. For purposes of part 11, the agency's intent is to require measures that prevent electronic records falsification by ordinary means. Therefore, FDA has revised Sec. 11.70 by adding the phrase “by ordinary means” at the end of this section.

109. Several comments suggested changing the phrase “another electronic record” to “an electronic record” to clarify that the antifalsification provision applies to the current record as well as any other record.

The agency agrees and has revised Sec. 11.70 accordingly.

110. Two comments argued that signature-to-record binding is unnecessary, in the context of PDMA, beyond the point of record creation (i.e., when records are transmitted to a point of receipt).

The comments asserted that persons who might be in a position to separate a signature from a record (for purposes of falsification) are individuals responsible for record integrity and thus unlikely to falsify records. The comments also stated that signature-to-record binding is produced by software coding at the time the record is signed, and suggested that proposed Sec. 11.70 clarify that binding would be necessary only up to the point of actual transmission of the electronic record to a central point of receipt.

The agency disagrees with the comment's premise that the need for binding to prevent falsification depends on the disposition of people to falsify records. The agency believes that reliance on individual tendencies is insufficient insurance against falsification. The agency also notes that in the traditional paper record, the signature remains bound to its corresponding record regardless of where the record may go.

111. One comment suggested that proposed Sec. 11.70 be deleted because it appears to require that all records be kept on inalterable media. The comment also suggested that the phrase “otherwise transferred” be deleted on the basis that it should be permissible for copies of handwritten signatures (recorded electronically) to be made when used, in addition to another unique individual identification mechanism.

The agency advises that neither Sec. 11.70, nor other sections in part 11, requires that records be kept on inalterable media. What is required is that whenever revisions to a record are made, the original entries must not be obscured. In addition, this section does not prohibit copies of handwritten signatures recorded electronically from being made for legitimate reasons that do not relate to record falsification. Section 11.70 merely states that such copies must not be made that falsify electronic records.

112. One comment suggested that proposed Sec. 11.70 be revised to require application of response cryptographic methods because only those methods could be used to comply with the regulation. The comment noted that, for certificate based public key cryptographic methods, the agency should address verifiable binding between the signer's name and public key as well as binding between digital signatures and electronic records. The comment also suggested that the regulation should reference electronic signatures in the context of secure time and date stamping.

The agency intends to permit maximum flexibility in how organizations achieve the linking called for in Sec. 11.70, and, as discussed above, has revised the regulation accordingly. Therefore, FDA does not believe that cryptographic and digital signature methods would be the only ways of linking an electronic signature to an electronic document. In fact, one firm commented that its system binds a person's handwritten signature to an electronic record. The agency agrees that use of digital signatures accomplishes the same objective because, if a digital signature were to be copied from one record to another, the second record would fail the digital signature verification procedure.

Furthermore, FDA notes that concerns regarding binding a person's name with the person's public key would be addressed in the context of Sec. 11.100(b) because an organization must establish an individual's identity before assigning or certifying an electronic signature (or any of the electronic signature components).

113. Two comments requested clarification of the types of technologies that could be used to meet the requirements of proposed Sec. 11.70.

As discussed in comment 107 of this document, the agency is affording persons maximum flexibility in using any appropriate method to link electronic signatures to their respective electronic records to prevent record falsification. Use of digital signatures is one such method, as is use of software locks to prevent sections of codes [**FDA page 13455**] representing signatures from being copied or removed. Because this is an area of developing technology, it is likely that other linking methods will emerge.

XI. Electronic Signatures--General Requirements (Sec. 11.100)

Proposed Sec. 11.100(a) states that each electronic signature must be unique to one individual and not be reused or reassigned to anyone else.

114. One comment asserted that several people should be permitted to share a common identification code and password where access control is limited to inquiry only.

Part 11 does not prohibit the establishment of a common group identification code/password for read only access purposes. However, such commonly shared codes and passwords would not be regarded, and must not be used, as electronic signatures. Shared access to a common database may nonetheless be implemented by granting appropriate common record access privileges to groups of people, each of whom has a unique electronic signature.

115. Several comments said proposed Sec. 11.100(a) should permit identification codes to be reused and reassigned from one employee to another, as long as an audit trail exists to associate an identification code with a given individual at any one time, and different passwords are used. Several comments said the section should indicate if the agency intends to restrict authority delegation by the nonreassignment or nonreuse provision, or by the provision in Sec. 11.200(a)(2) requiring electronic signatures to be used only by their genuine owners. The comments questioned whether reuse means restricting one noncryptographic based signature to only one record and argued that passwords need not be unique if the combined identification code and password are unique to one individual. One comment recommended caution in using the term “ownership” because of possible confusion with intellectual property rights or ownership of the computer systems themselves.

The agency advises that, where an electronic signature consists of the combined identification code and password, Sec. 11.100 would not prohibit the reassignment of the identification code provided the combined identification code and password remain unique to prevent record falsification. The agency believes that such reassignments are inadvisable, however, to the extent that they might be combined with an easily guessed password, thus increasing the chances that an individual might assume a signature belonging to someone else. The agency also advises that where people can read identification codes (e.g., printed numbers and letters that are typed at a keyboard or read from a card), the risks of someone obtaining that information as part of a falsification effort would be greatly increased as compared to an identification code that is not in human readable form (one that is, for example, encoded on a “secure card” or other device).

Regarding the delegation of authority to use electronic signatures, FDA does not intend to restrict the ability of one individual to sign a record or otherwise act on behalf of another individual. However, the applied electronic signature must be the assignee's and the record should clearly indicate the capacity in which the person is acting (e.g., on behalf of, or under the authority of, someone else). This is analogous to traditional paper records and handwritten signatures when person “A” signs his or her own name under the signature block of person “B,” with appropriate explanatory notations such as “for” or “as representative of” person B. In such cases, person A does not simply sign the name of person B. The agency expects the same procedure to be used for electronic records and electronic signatures.

The agency intends the term “reuse” to refer to an electronic signature used by a different person. The agency does not regard as “reuse” the replicate application of a noncryptographic based electronic signature (such as an identification code and password) to different electronic records. For clarity, FDA has revised the phrase “not be reused or reassigned to” to state “not be reused by, or reassigned to,” in Sec. 11.100(a).

The reference in Sec. 11.200(a) to ownership is made in the context of an individual owning or being assigned a particular electronic signature that no other individual may use. FDA believes this is clear and that concerns regarding ownership in the context of intellectual property rights or hardware are misplaced.

116. One comment suggested that proposed Sec. 11.100(a) should accommodate electronic signatures assigned to organizations rather than individuals.

The agency advises that, for purposes of part 11, electronic signatures are those of individual human beings and not organizations. For example, FDA does not regard a corporate seal as an individual's signature. Humans may represent and obligate organizations by signing records, however. For clarification, the agency is substituting the word “individual” for “person” in the definition of electronic signature (Sec. 11.3(b)(7)) because the broader definition of person within the act includes organizations.

117. Proposed Sec. 11.100(b) states that, before an electronic signature is assigned to a person, the identity of the individual must be verified by the assigning authority.

Two comments noted that where people use identification codes in combination with passwords only the identification code portion of the electronic signature is assigned, not the password. Another comment argued that the word “assigned” is inappropriate in the context of electronic signatures based upon public key cryptography because the appropriate authority certifies the bind between the individual's public key and identity, and not the electronic signature itself.

The agency acknowledges that, for certain types of electronic signatures, the authorizing or certifying organization issues or approves only a portion of what eventually becomes an individual's electronic signature. FDA wishes to accommodate a broad variety of electronic signatures and is therefore revising Sec. 11.100(b) to require that an organization verify the identity of an individual before it establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature or any element of such electronic signature.

118. One comment suggested that the word “verified” in proposed Sec. 11.100(b) be changed to “confirmed.” Other comments addressed the method of verifying a person's identity and suggested that the section specify acceptable verification methods, including high level procedures regarding the relative strength of that verification, and the need for personal appearances or supporting documentation such as birth certificates. Two comments said the verification provision should be deleted because normal internal controls are adequate, and that it was impractical for multinational companies whose employees are globally dispersed.

The agency does not believe that there is a sufficient difference between “verified” and “confirmed” to warrant a change in this section. Both words indicate that organizations substantiate a person's identity to prevent impersonations when an electronic signature, or any of its elements, is being established or certified. The agency disagrees with the assertion that this requirement is unnecessary.

Without verifying someone's identity at the outset of establishing or certifying [**FDA page 13456**] an individual's electronic signature, or a portion thereof, an imposter might easily access and compromise many records. Moreover, an imposter could continue this activity for a prolonged period of time despite other system controls, with potentially serious consequences.

The agency does not believe that the size of an organization, or global dispersion of its employees, is reason to abandon this vital control. Such dispersion may, in fact, make it easier for an impostor to pose as someone else in the absence of such verification. Further, the agency does not accept the implication that multinational firms would not verify the identity of their employees as part of other routine procedures, such as when individuals are first hired.

In addition, in cases where an organization is widely dispersed and electronic signatures are established or certified centrally, Sec. 11.100(b) does not prohibit organizations from having their local units perform the verification and relaying this information to the central authority. Similarly, local units may conduct the electronic signature assignment or certification.

FDA does not believe it is necessary at this time to specify methods of identity verification and expects that organizations will consider risks attendant to sanctioning an erroneously assigned electronic signature.

119. Proposed Sec. 11.100(c) states that persons using electronic signatures must certify to the agency that their electronic signature system guarantees the authenticity, validity, and binding nature of any electronic signature. Persons utilizing electronic signatures would, upon agency request, provide additional certification or testimony that a specific electronic signature is authentic, valid, and binding. Such certification would be submitted to the FDA district office in which territory the electronic signature system is in use.

Many comments objected to the proposed requirement that persons provide FDA with certification regarding their electronic signature systems. The comments asserted that the requirement was: (1) Unprecedented, (2) unrealistic, (3) unnecessary, (4) contradictory to the principles and intent of system validation, (5) too burdensome for FDA to manage logistically, (6) apparently intended only to simplify FDA litigation, (7) impossible to meet regarding “guarantees” of authenticity, and (8) an apparent substitute for FDA inspections.

FDA agrees in part with these comments. This final rule reduces the scope and burden of certification to a statement of intent that electronic signatures are the legally binding equivalent of handwritten signatures.

As noted previously, the agency believes it is important, within the context of its health protection activities, to ensure that persons who implement electronic signatures fully equate the legally binding nature of electronic signatures with the traditional handwritten paper-based signatures. The agency is concerned that individuals might disavow an electronic signature as something completely different from a traditional handwritten signature. Such contention could result in confusion and possibly extensive litigation.

Moreover, a limited certification as provided in this final rule is consistent with other legal, regulatory, and commercial practices. For example, electronic data exchange trading partner agreements are often written on paper and signed with traditional handwritten signatures to establish that certain electronic identifiers are recognized as equivalent to traditional handwritten signatures.

FDA does not expect electronic signature systems to be guaranteed foolproof. The agency does not intend, under Sec. 11.100(c), to establish a requirement that is unattainable. Certification of an electronic signature system as the legally binding equivalent of a traditional handwritten signature is separate and distinct from system validation. This provision is not intended as a substitute for FDA inspection and such inspection alone may not be able to determine in a conclusive manner an organization's intent regarding electronic signature equivalency.

The agency has revised proposed Sec. 11.100(c) to clarify its intent. The agency wishes to emphasize that the final rule dramatically curtails what FDA had proposed and is essential for the agency to be able to protect and promote the public health because FDA must be able to hold people to the commitments they make under their electronic signatures. The certification in the final rule is merely a statement of intent that electronic signatures are the legally binding equivalent of traditional handwritten signatures.

120. Several comments questioned the procedures necessary for submitting the certification to FDA, including: (1) The scheduling of the certification; (2) whether to submit certificates for each individual or for each electronic signature; (3) the meaning of “territory” in the context of wide area networks; (4) whether such certificates could be submitted electronically; and (5) whether organizations, after submitting a certificate, had to wait for a response from FDA before implementing their electronic signature systems. Two comments suggested revising proposed Sec. 11.100(c) to require that all certifications be submitted to FDA only upon agency request. One comment suggested changing “should” to “shall” in the last sentence of Sec. 11.100(c) if the agency's intent is to require certificates to be submitted to the respective FDA district office.

The agency intends that certificates be submitted once, in the form of a paper letter, bearing a traditional handwritten signature, at the time an organization first establishes an electronic signature system after the effective date of part 11, or, where such systems have been used before the effective date, upon continued use of the electronic signature system.

A separate certification is not needed for each electronic signature, although certification of a particular electronic signature is to be submitted if the agency requests it. The agency does not intend to establish certification as a review and approval function. In addition, organizations need not await FDA's response before putting electronic signature systems into effect, or before continuing to use an existing system.

A single certification may be stated in broad terms that encompass electronic signatures of all current and future employees, thus obviating the need for subsequent certifications submitted on a preestablished schedule.

To further simplify the process and to minimize the number of certifications that persons would have to provide, the agency has revised Sec. 11.100(c) to permit submission of a single certification that covers all electronic signatures used by an organization. The revised rule also simplifies the process by providing a single agency receiving unit. The final rule instructs persons to send certifications to FDA's Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. Persons outside the United States may send their certifications to the same office.

The agency offers, as guidance, an example of an acceptable Sec. 11.100(c) certification:

> Pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations, this is to certify that [name of organization] intends that all electronic signatures executed by our employees, agents, or representatives, located anywhere in the world, are the legally binding equivalent of traditional handwritten signatures.

[**FDA page 13457**]

The agency has revised Sec. 11.100 to clarify where and when certificates are to be submitted.

The agency does not agree that the initial certification be provided only upon agency request because FDA believes it is vital to have such certificates, as a matter of record, in advance of any possible litigation. This would clearly establish the intent of organizations to equate the legally binding nature of electronic signatures with traditional handwritten signatures. In addition, the agency believes that having the certification on file ahead of time will have the beneficial effect of reinforcing the gravity of electronic signatures by putting an organization's employees on notice that the organization has gone on record with FDA as equating electronic signatures with handwritten signatures.

121. One comment suggested that proposed Sec. 11.100(c) be revised to exclude from certification instances in which the purported signer claims that he or she did not create or authorize the signature.

The agency declines to make this revision because a provision for nonrepudiation is already contained in Sec. 11.10.

As a result of the considerations discussed in comments 119 and 120 of this document, the agency has revised proposed Sec. 11.100(c) to state that:

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

XII. Electronic Signature Components and Controls (Sec. 11.200)

122. Proposed Sec. 11.200 sets forth requirements for electronic signature identification mechanisms and controls. Two comments suggested that the term “`identification code” should be defined. Several comments suggested that the term “identification mechanisms” should be changed to “identification components” because each component of an electronic signature need not be executed by a different mechanism.

The agency believes that the term “identification code” is sufficiently broad and generally understood and does not need to be defined in these regulations. FDA agrees that the word “component” more accurately reflects the agency's intent than the word “mechanism,” and has substituted “component” for “mechanism” in revised Sec. 11.200. The agency has also revised the section heading to read “Electronic signature components and controls” to be consistent with the wording of the section.

123. Proposed Sec. 11.200(a) states that electronic signatures not based upon biometric/behavioral links must: (1) Employ at least two distinct identification mechanisms (such as an identification code and password), each of which is contemporaneously executed at each signing; (2) be used only by their genuine owners; and (3) be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

Two comments said that proposed Sec. 11.200(a) should acknowledge that passwords may be known not only to their genuine owners, but also to system administrators in case people forget their passwords.

The agency does not believe that system administrators would routinely need to know an individual's password because they would have sufficient privileges to assist those individuals who forget passwords.

124. Several comments argued that the agency should accept a single password alone as an electronic signature because: (1) Combining the password with an identification code adds little security, (2) administrative controls and passwords are sufficient, (3) authorized access is more difficult when two components are needed, (4) people would not want to gain unauthorized entry into a manufacturing environment, and (5) changing current systems that use only a password would be costly.

The comments generally addressed the need for two components in electronic signatures within the context of the requirement that all components be used each time an electronic signature is executed. Several comments suggested that, for purposes of system access, individuals should enter both a user identification code and password, but that, for subsequent signings during one period of access, a single element (such as a password) known only to, and usable by, the individual should be sufficient.

The agency believes that it is very important to distinguish between those (nonbiometric) electronic signatures that are executed repetitively during a single, continuous controlled period of time (access session or logged-on period) and those that are not. The agency is concerned, from statements made in comments, that people might use passwords that are not always unique and are frequently words that are easily associated with an individual. Accordingly, where nonbiometric electronic signatures are not executed repetitively during a single, continuous controlled period, it would be extremely bad practice to use a password alone as an electronic signature. The agency believes that using a password alone in such cases would clearly increase the likelihood that one individual, by chance or deduction, could enter a password that belonged to someone else and thereby easily and readily impersonate that individual. This action could falsify electronic records.

The agency acknowledges that there are some situations involving repetitive signings in which it may not be necessary for an individual to execute each component of a nonbiometric electronic signature for every signing. The agency is persuaded by the comments that such situations generally involve certain conditions. For example, an individual performs an initial system access or “log on,” which is effectively the first signing, by executing all components of the electronic signature (typically both an identification code and a password). The individual then performs subsequent signings by executing at least one component of the electronic signature, under controlled conditions that prevent another person from impersonating the legitimate signer. The agency's concern here is the possibility that, if the person leaves the workstation, someone else could access the workstation (or other computer device used to execute the signing) and impersonate the legitimate signer by entering an identification code or password.

The agency believes that, in such situations, it is vital to have stringent controls in place to prevent the impersonation. Such controls include: (1) Requiring an individual to remain in close proximity to the workstation throughout the signing session; (2) use of automatic inactivity disconnect measures that would “de-log” the first individual if no entries or actions were taken within a fixed short timeframe; and (3) requiring that the single component needed for subsequent signings be known to, and usable only by, the authorized individual.

The agency's objective in accepting the execution of fewer than all the components of a nonbiometric [**FDA page 13458**] electronic signature for repetitive signings is to make it impractical to falsify records. The agency believes that this would be attained by complying with all of the following procedures where nonbiometric electronic signatures are executed more than once during a single, continuous controlled session: (1) All electronic signature components are executed for the first signing; (2) at least one electronic signature component is executed at each subsequent signing; (3) the electronic signature component executed after the initial signing is only used by its genuine owner, and is designed to ensure it can only be used by its genuine owner; and (4) the electronic signatures are administered and executed to ensure that their attempted use by anyone other than their genuine owners requires collaboration of two or more individuals. Items 1 and 4 are already incorporated in proposed Sec. 11.200(a). FDA has included items 2 and 3 in final Sec. 11.200(a).

The agency cautions, however, that if its experience with enforcement of part 11 demonstrates that these controls are insufficient to deter falsifications, FDA may propose more stringent controls.

125. One comment asserted that, if the agency intends the term “identification code” to mean the typical user identification, it should not characterize the term as a distinct mechanism because such codes do not necessarily exhibit security attributes. The comment also suggested that proposed Sec. 11.200(a) address the appropriate application of each possible combination of a two-factor authentication method.

The agency acknowledges that the identification code alone does not exhibit security attributes. Security derives from the totality of system controls used to prevent falsification. However, uniqueness of the identification code when combined with another electronic signature component, which may not be unique (such as a password), makes the combination unique and thereby enables a legitimate electronic signature. FDA does not now believe it necessary to address, in Sec. 11.200(a), the application of all possible combinations of multifactored authentication methods.

126. One comment requested clarification of “each signing,” noting that a laboratory employee may enter a group of test results under one signing.

The agency advises that each signing means each time an individual executes a signature. Particular requirements regarding what records need to be signed derive from other regulations, not part 11. For example, in the case of a laboratory employee who performs a number of analytical tests, within the context of drug CGMP regulations, it is permissible for one signature to indicate the performance of a group of tests (21 CFR 211.194(a)(7)). A separate signing is not required in this context for each separate test as long as the record clearly shows that the single signature means the signer performed all the tests.

127. One comment suggested that the proposed requirement, that collaboration of at least two individuals is needed to prevent attempts at electronic signature falsification, be deleted because a responsible person should be allowed to override the electronic signature of a subordinate. Several comments addressed the phrase “attempted use” and suggested that it be deleted or changed to “unauthorized use.”

The comments said that willful breaking or circumvention of any security measure does not require two or more people to execute, and that the central question is whether collaboration is required to use the electronic signature.

The agency advises that the intent of the collaboration provision is to require that the components of a nonbiometric electronic signature cannot be used by one individual without the prior knowledge of a second individual. One type of situation the agency seeks to prevent is the use of a component such as a card or token that a person may leave unattended. If an individual must collaborate with another individual by disclosing a password, the risks of betrayal and disclosure are greatly increased and this helps to deter such actions.

Because the agency is not condoning such actions, Sec. 11.200(a)(2) requires that electronic signatures be used only by the genuine owner.

The agency disagrees with the comments that the term “attempted use” should be changed to “unauthorized uses,” because “unauthorized uses” could infer that use of someone else's electronic signature is acceptable if it is authorized.

Regarding electronic signature “overrides,” the agency would consider as falsification the act of substituting the signature of a supervisor for that of a subordinate. The electronic signature of the subordinate must remain inviolate for purposes of authentication and documentation. Although supervisors may overrule the actions of their staff, the electronic signatures of the subordinates must remain a permanent part of the record, and the supervisor's own electronic signature must appear separately. The agency believes that such an approach is fully consistent with procedures for paper records.

As a result of the revisions noted in comments 123 to 127 of this document, Sec. 11.200(a) now reads as follows:

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

128. Proposed Sec. 11.200(b) states that electronic signatures based upon biometric/behavioral links be designed to ensure that they could not be used by anyone other than their genuine owners.

One comment suggested that the agency make available, by public workshop or other means, any information it has regarding existing biometric systems so that industry can provide proper input. Another comment asserted that proposed Sec. 11.200(b) placed too great an emphasis on biometrics, did not establish particular levels of assurance for biometrics, and did not provide for systems using mixtures of biometric and nonbiometric electronic signatures. The comment recommended revising the phrase “designed to ensure they cannot be used” to read “provide assurances that prevent their execution.”

The agency's experience with biometric electronic signatures is contained in the administrative record for this rulemaking, under docket no. 92N-0251, and includes recommendations from public comments to the ANPRM and the proposed rule. The agency has also gathered, and continues to gather, additional information from literature reviews, general press reports, meetings, and the agency's experience with this technology. Interested persons have had extensive opportunity for input and comment regarding biometrics in part 11. In addition, interested persons may continue to contact the agency at any time regarding biometrics or any other relevant technologies. The agency notes [**FDA page 13459**] that the rule does not require the use of biometric-based electronic signatures.

As the agency's experience with biometric electronic signatures increases, FDA will consider holding or participating in public workshops if that approach would be helpful to those wishing to adopt such technologies to comply with part 11.

The agency does not believe that proposed Sec. 11.200(b) places too much emphasis on biometric electronic signatures. As discussed above, the regulation makes a clear distinction between electronic signatures that are and are not based on biometrics, but treats their acceptance equally.

The agency recognizes the inherent security advantages of biometrics, however, in that record falsification is more difficult to perform. System controls needed to make biometric-based electronic signatures reliable and trustworthy are thus different in certain respects from controls needed to make nonbiometric electronic signatures reliable and trustworthy. The requirements in part 11 reflect those differences.

The agency does not believe that it is necessary at this time to set numerical security assurance standards that any system would have to meet.

The regulation does not prohibit individuals from using combinations of biometric and nonbiometric-based electronic signatures. However, when combinations are used, FDA advises that requirements for each element in the combination would also apply. For example, if passwords are used in combination with biometrics, then the benefits of using passwords would only be realized, in the agency's view, by adhering to controls that ensure password integrity (see Sec. 11.300).

In addition, the agency believes that the phrase “designed to ensure that they cannot be used” more accurately reflects the agency's intent than the suggested alternate wording, and is more consistent with the concept of systems validation. Under such validation, falsification preventive attributes would be designed into the biometric systems.

To be consistent with the revised definition of biometrics in Sec. 11.3(b)(3), the agency has revised Sec. 11.200(b) to read, “Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.”

XIII. Electronic Signatures--Controls for Identification Codes/Passwords (Sec. 11.300)

The introductory paragraph of proposed Sec. 11.300 states that electronic signatures based upon use of identification codes in combination with passwords must employ controls to ensure their security and integrity.

To clarify the intent of this provision, the agency has added the words “[p]ersons who use” to the first sentence of Sec. 11.300. This change is consistent with Secs. 11.10 and 11.30. The introductory paragraph now reads, “Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: * * *.”

129. One comment suggested deletion of the phrase “in combination with passwords” from the first sentence of this section.

The agency disagrees with the suggested revision because the change is inconsistent with FDA's intent to address controls for electronic signatures based on combinations of identification codes and passwords, and would, in effect, permit a single component nonbiometric-based electronic signature.

130. Proposed Sec. 11.300(a) states that controls for identification codes/passwords must include maintaining the uniqueness of each issuance of identification code and password.

One comment alleged that most passwords are commonly used words, such as a child's name, a State, city, street, month, holiday, or date, that are significant to the person who creates the password. Another stated that the rule should explain uniqueness and distinguish between issuance and use because identification code/password combinations generally do not change for each use.

FDA does not intend to require that individuals use a completely different identification code/password combination each time they execute an electronic signature. For reasons explained in the response to comment 16, what is required to be unique is each combined password and identification code and FDA has revised the wording of Sec. 11.300(a) to clarify this provision. The agency is aware, however, of identification devices that generate new passwords on a continuous basis in synchronization with a “host” computer. This results in unique passwords for each system access. Thus, it is possible in theory to generate a unique nonbiometric electronic signature for each signing.

The agency cautions against using passwords that are common words easily associated with their originators because such a practice would make it relatively easy for someone to impersonate someone else by guessing the password and combining it with an unsecured (or even commonly known) identification code.

131. Proposed Sec. 11.300(b) states that controls for identification codes/passwords must ensure that code/password issuances are periodically checked, recalled, or revised.

Several comments objected to this proposed requirement because: (1) It is unnecessary, (2) it excessively prescribes “how to,” (3) it duplicates the requirements in Sec. 11.300(c), and (4) it is administratively impractical for larger organizations. However, the comments said individuals should be encouraged to change their passwords periodically. Several comments suggested that proposed Sec. 11.300(b) include a clarifying example such as “to cover events such as password aging.” One comment said that the section should indicate who is to perform the periodic checking, recalling, or revising.

The agency disagrees with the objections to this provision. FDA does not view the provision as a “how to” because organizations have full flexibility in determining the frequency and methods of checking, recalling, or revising their code/password issuances. The agency does not believe that this paragraph duplicates the regulation in Sec. 11.300(c) because paragraph (c) specifically addresses followup to losses of electronic signature issuances, whereas Sec. 11.300(b) addresses periodic issuance changes to ensure against their having been unknowingly compromised. This provision would be met by ensuring that people change their passwords periodically.

FDA disagrees that this system control is unnecessary or impractical in large organizations because the presence of more people may increase the opportunities for compromising identification codes/passwords. The agency is confident that larger organizations will be fully capable of handling periodic issuance checks, revisions, or recalls.

FDA agrees with the comments that suggested a clarifying example and has revised Sec. 11.300(b) to include password aging as such an example. The agency cautions, however, that the example should not be taken to mean that password expiration would be the only rationale for revising, recalling, and checking issuances. If, for example, identification codes and passwords have been copied or compromised, they should be changed.

FDA does not believe it necessary at this time to specify who in an organization is to carry out this system control, although the agency expects [**FDA page 13460**] that units that issue electronic signatures would likely have this duty.

132. Proposed Sec. 11.300(c) states that controls for identification codes/passwords must include the following of loss management procedures to electronically deauthorize lost tokens, cards, etc., and to issue temporary or permanent replacements using suitable, rigorous controls for substitutes.

One comment suggested that this section be deleted because it excessively prescribes “how to.” Another comment argued that the proposal was not detailed enough and should distinguish among fundamental types of cards (e.g., magstripe, integrated circuit, and optical) and include separate sections that address their respective use. Two comments questioned why the proposal called for “rigorous controls” in this section as opposed to other sections. One of the comments recommended that this section should also apply to cards or devices that are stolen as well as lost.

The agency believes that the requirement that organizations institute loss management procedures is neither too detailed nor too general. Organizations retain full flexibility in establishing the details of such procedures. The agency does not believe it necessary at this time to offer specific provisions relating to different types of cards or tokens. Organizations that use such devices retain full flexibility to establish appropriate controls for their operations. To clarify the agency's broad intent to cover all types of devices that contain or generate identification code or password information, FDA has revised Sec. 11.300(c) to replace “etc.” with “and other devices that bear or generate identification code or password information.”

The agency agrees that Sec. 11.300(c) should cover loss management procedures regardless of how devices become potentially compromised, and has revised this section by adding, after the word “lost,” the phrase “stolen, missing, or otherwise potentially compromised.” FDA uses the term “rigorous” because device disappearance may be the result of inadequate controls over the issuance and management of the original cards or devices, thus necessitating more stringent measures to prevent problem recurrence. For example, personnel training on device safekeeping may need to be strengthened.

133. Proposed Sec. 11.300(d) states that controls for identification codes/passwords must include the use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and, detecting and reporting to the system security unit and organizational management in an emergent manner any attempts at their unauthorized use.

Several comments suggested that the term “emergent” in proposed Sec. 11.300(d) be replaced with “timely” to describe reports regarding attempted unauthorized use of identification codes/passwords because: (1) A timely report would be sufficient, (2) technology to report emergently is not available, and (3) timely is a more recognizable and common term.

FDA agrees in part. The agency considers attempts at unauthorized use of identification codes and passwords to be extremely serious because such attempts signal potential electronic signature and electronic record falsification, data corruption, or worse--consequences that could also ultimately be very costly to organizations. In FDA's view, the significance of such attempts requires the immediate and urgent attention of appropriate security personnel in the same manner that individuals would respond to a fire alarm. To clarify its intent with a more widely recognized term, the agency is replacing “emergent” with “immediate and urgent” in the final rule. The agency believes that the same technology that accepts or rejects an identification code and password can be used to relay to security personnel an appropriate message regarding attempted misuse.

134. One comment suggested that the word “any” be deleted from the phrase “any attempts” in proposed Sec. 11.300(d) because it is excessive. Another comment, noting that the question of attempts to enter a system or access a file by unauthorized personnel is very serious, urged the agency to substitute “all” for “any.” This comment added that there are devices on the market that can be used by unauthorized individuals to locate personal identification codes and passwords.

The agency believes the word “any” is sufficiently broad to cover all attempts at misuse of identification codes and passwords, and rejects the suggestion to delete the word. If the word “any” were deleted, laxity could result from any inference that persons are less likely to be caught in an essentially permissive, nonvigilant system.

FDA is aware of the “sniffing” devices referred to by one comment and cautions persons to establish suitable countermeasures against them.

135. One comment suggested that proposed Sec. 11.300(d) be deleted because it is impractical, especially when simple typing errors are made. Another suggested that this section pertain to access to electronic records, not just the system, on the basis that simple miskeys may be typed when accessing a system.

As discussed in comments 133 and 134 of this document, the agency believes this provision is necessary and reasonable. The agency's security concerns extend to system as well as record access. Once having gained unauthorized system access, an individual could conceivably alter passwords to mask further intrusion and misdeeds. If this section were removed, falsifications would be more probable to the extent that some establishments would not alert security personnel.

However, the agency advises that a simple typing error may not indicate an unauthorized use attempt, although a pattern of such errors, especially in short succession, or such an apparent error executed when the individual who “owns” that identification code or password is deceased, absent, or otherwise known to be unavailable, could signal a security problem that should not be ignored. FDA notes that this section offers organizations maximum latitude in deciding what they perceive to be attempts at unauthorized use.

136. One comment suggested substituting the phrase “electronic signature” for “passwords and/or identification codes.”

The agency disagrees with this comment because the net effect of the revision might be to ignore attempted misuse of important elements of an electronic signature such as a “password” attack on a system.

137. Several comments argued that: (1) It is not necessary to report misuse attempts simultaneously to management when reporting to the appropriate security unit, (2) security units would respond to management in accordance with their established procedures and lines of authority, and (3) management would not always be involved.

The agency agrees that not every misuse attempt would have to be reported simultaneously to an organization's management if the security unit that was alerted responded appropriately. FDA notes, however, that some apparent security breeches could be serious enough to warrant management's immediate and urgent attention. The agency has revised proposed Sec. 11.300(d) to give organizations maximum flexibility in establishing criteria for management notification. Accordingly, Sec. 11.300(d) now states that controls for identification codes/passwords must include:

Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report [**FDA page 13461**] in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

138. Proposed Sec. 11.300(e) states that controls for identification codes/passwords must include initial and periodic testing of devices, such as tokens or cards, bearing identifying information, for proper function.

Many comments objected to this proposed device testing requirement as unnecessary because it is part of system validation and because devices are access fail-safe in that nonworking devices would deny rather than permit system access. The comments suggested revising this section to require that failed devices deny user access. One comment stated that Sec. 11.300(e) is unclear on the meaning of “identifying information” and that the phrase “tokens or cards” is redundant because cards are a form of tokens.

FDA wishes to clarify the reason for this proposed requirement, and to emphasize that proper device functioning includes, in addition to system access, the correctness of the identifying information and security performance attributes. Testing for system access alone could fail to discern significant unauthorized device alterations. If, for example, a device has been modified to change the identifying information, system access may still be allowed, which would enable someone to assume the identity of another person. In addition, devices may have been changed to grant individuals additional system privileges and action authorizations beyond those granted by the organization. Of lesser significance would be simple wear and tear on such devices, which result in reduced performance. For instance, a bar code may not be read with the same consistent accuracy as intended if the code becomes marred, stained, or otherwise disfigured. Access may be granted, but only after many more scannings than desired. The agency expects that device testing would detect such defects.

Because validation of electronic signature systems would not cover unauthorized device modifications, or subsequent wear and tear, validation would not obviate the need for periodic testing.

The agency notes that Sec. 11.300(e) does not limit the types of devices organizations may use. In addition, not all tokens may be cards, and identifying information is intended to include identification codes and passwords. Therefore, FDA has revised proposed Sec. 11.300(e) to clarify the agency's intent and to be consistent with Sec. 11.300(c). Revised Sec. 11.300(e) requires initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

XIV. Paperwork Reduction Act of 1995

This final rule contains information collection provisions that are subject to review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3520). Therefore, in accordance with 5 CFR 1320, the title, description, and description of respondents of the collection of information requirements are shown below with an estimate of the annual reporting and recordkeeping burdens. Included in the estimate is the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.

Most of the burden created by the information collection provision of this final rule will be a one-time burden associated with the creation of standard operating procedures, validation, and certification. The agency anticipates the use of electronic media will substantially reduce the paperwork burden associated with maintaining FDA-required records.

Title: Electronic records; Electronic signatures.

Description: FDA is issuing regulations that provide criteria for acceptance of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records. Rules apply to any FDA records requirements unless specific restrictions are issued in the future. Records required to be submitted to FDA may be submitted electronically, provided the agency has stated its ability to accept the records electronically in an agency established public docket.

Description of Respondents: Businesses and other for-profit organizations, state or local governments, Federal agencies, and nonprofit institutions.

Although the August 31, 1994, proposed rule (59 FR 45160) provided a 90-day comment period under the Paperwork Reduction Act of 1980, FDA is providing an additional opportunity for public comment under the Paperwork Reduction Act of 1995, which was enacted after the expiration of the comment period and applies to this final rule. Therefore, FDA now invites comments on: (1) Whether the proposed collection of information is necessary for the proper performance of FDA's functions, including whether the information will have practical utility; (2) the accuracy of FDA's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques, when appropriate, and other forms of information technology. Individuals and organizations may submit comments on the information collection provisions of this final rule by May 19, 1997. Comments should be directed to the Dockets Management Branch (address above).

At the close of the 60-day comment period, FDA will review the comments received, revise the information collection provisions as necessary, and submit these provisions to OMB for review and approval.

FDA will publish a notice in the Federal Register when the information collection provisions are submitted to OMB, and an opportunity for public comment to OMB will be provided at that time. Prior to the effective date of this final rule, FDA will publish a notice in the Federal Register of OMB's decision to approve, modify, or disapprove the information collection provisions. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

Table T-1 Estimated Annual Recordkeeping Burden

21 CFR Section	Annual No. of Recordkeepers	Hours per Recordkeeper	Total Hours
11.10	50	40	2,000
11.30	50	40	2,000
11.50	50	40	2,000
11.300	50	40	2,000
Total annual burden hours			8,000

[**FDA page 13462**]

Table T-2 Estimated Annual Reporting Burden

21 CFR Section	Annual No. of Respondents	Hours per Response	Total Burden Hours
11.100	1,000	1	1,000
Total annual burden hours			1,000

XV. Environmental Impact

The agency has determined under 21 CFR 25.24(a)(8) that this action is of a type that does not individually or cumulatively have a significant effect on the human environment. Therefore, neither an environmental assessment nor an environmental impact statement is required.

XVI. Analysis of Impacts

FDA has examined the impacts of the final rule under Executive Order 12866, under the Regulatory Flexibility Act (5 U.S.C. 601-612), and under the Unfunded Mandates Reform Act (Pub. L. 104-4). Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; and distributive impacts and equity). Unless an agency certifies that a rule will not have a significant economic impact on a substantial number of small entities, the Regulatory Flexibility Act requires an analysis of regulatory options that would minimize any significant impact of a rule on small entities. The Unfunded

Mandates Reform Act requires that agencies prepare an assessment of anticipated costs and benefits before proposing any rule that may result in an annual expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of $100 million (adjusted annually for inflation).

The agency believes that this final rule is consistent with the regulatory philosophy and principles identified in the Executive Order.

This rule permits persons to maintain any FDA required record or report in electronic format. It also permits FDA to accept electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. The rule applies to any paper records required by statute or agency regulations. The rule was substantially influenced by comments to the ANPRM and the proposed rule. The provisions of this rule permit the use of electronic technology under conditions that the agency believes are necessary to ensure the integrity of electronic systems, records, and signatures, and the ability of the agency to protect and promote the public health.

This rule is a significant regulatory action as defined by the Executive Order and is subject to review under the Executive Order. This rule does not impose any mandates on State, local, or tribal governments, nor is it a significant regulatory action under the Unfunded Mandates Reform Act.

The activities regulated by this rule are voluntary; no entity is required by this rule to maintain or submit records electronically if it does not wish to do so. Presumably, no firm (or other regulated entity) will implement electronic recordkeeping unless the benefits to that firm are expected to exceed any costs (including capital and maintenance costs). Thus, the industry will incur no net costs as a result of this rule.

Based on the fact that the activities regulated by this rule are entirely voluntary and will not have any net adverse effects on small entities, the Commissioner of Food and Drugs certifies that this rule will not have a significant economic impact on a substantial number of small entities. Therefore, under the Regulatory Flexibility Act, no further regulatory flexibility analysis is required.

Although no further analysis is required, in developing this rule, FDA has considered the impact of the rule on small entities. The agency has also considered various regulatory options to maximize the net benefits of the rule to small entities without compromising the integrity of electronic systems, records, and signatures, or the agency's ability to protect and promote the public health. The following analysis briefly examines the potential impact of this rule on small businesses and other small entities, and describes the measures that FDA incorporated in this final rule to reduce the costs of applying electronic record/signature systems consistent with the objectives of the rule. This analysis includes each of the elements required for a final regulatory flexibility analysis under 5 U.S.C. 604(a).

A. Objectives

The purpose of this rule is to permit the use of a technology that was not contemplated when most existing FDA regulations were written, without undermining in any way the integrity of records and reports or the ability of FDA to carry out its statutory health protection mandate. The rule will permit regulated industry and FDA to operate with greater flexibility, in ways that will improve both the efficiency and the speed of industry's operations and the regulatory process. At the same time, it ensures that individuals will assign the same level of importance to affixing an electronic signature, and the records to which that signature attests, as they currently do to a handwritten signature.

B. Small Entities Affected

This rule potentially affects all large and small entities that are required by any statute administered by FDA, or any FDA regulation, to keep records or make reports or other submissions to FDA, including small businesses, nonprofit organizations, and small government entities. Because the rule affects such a broad range of industries, no data currently exist to estimate precisely the total number of small entities that will potentially benefit from the rule, but the number is substantial. For example, within the medial devices industry alone, the Small Business [**FDA page 13463**] Administration (SBA) estimates that over 3,221 firms are small businesses (i.e., have fewer than 500 employees). SBA also estimates that 504 pharmaceutical firms are small businesses with fewer than 500 employees. Of the approximately 2,204 registered blood and plasma establishments that are neither government-owned nor part of the American Red Cross, most are nonprofit establishments that are not nationally dominant and thus may be small entities as defined by the Regulatory Flexibility Act.

Not all submissions will immediately be acceptable electronically, even if the submission and the electronic record conform to the criteria set forth in this rule. A particular required submission will be acceptable in electronic form only after it has been identified to this effect in public docket 92S-0251. (The agency unit that can receive that electronic submission will also be identified in the docket.) Thus, although all small entities subject to FDA regulations are potentially affected by this rule, the rule will actually only benefit those that: (1) Are required to submit records or other documents that have been identified in the public docket as acceptable if submitted electronically, and (2) choose this method of submission, instead of traditional paper record submissions. The potential range of submissions includes such records as new drug applications, medical device premarket notifications, food additive petitions, and medicated feed applications. These, and all other required submissions, will be considered by FDA as candidates for optional electronic format.

Although the benefits of making electronic submissions to FDA will be phased in over time, as the agency accepts more submissions in electronic form, firms can, upon the rule's effective date, immediately benefit from using electronic records/signatures for records they are required to keep, but not submit to FDA. Such records include, but are not limited to: Pharmaceutical and medical device batch production records, complaint records, and food processing records.

Some small entities will be affected by this rule even if they are not among the industries regulated by FDA. Because it will increase the market demand for certain types of software (e.g., document management, signature, and encryption software) and services (e.g., digital notaries and digital signature certification authorities), this rule will benefit some small firms engaged in developing and providing those products and services.

C. Description of the Impact

For any paper record that an entity is required to keep under existing statutes or FDA regulations, FDA will now accept an electronic record instead of a paper one, as long as the electronic record conforms to the requirements of this rule. FDA will also consider an electronic signature to be equivalent to a handwritten signature if it meets the requirements of this rule. Thus, entities regulated by FDA may, if they choose, submit required records and authorizations to the agency electronically once those records have been listed in the docket as acceptable in electronic form. This action is voluntary; paper records and handwritten signatures are still fully acceptable. No entity will be required to change the way it is currently allowed to submit paper records to the agency.

1. Benefits and costs

For any firm choosing to convert to electronic recordkeeping, the direct benefits are expected to include:

(1) Improved ability for the firm to analyze trends, problems, etc., enhancing internal evaluation and quality control;

(2) Reduced data entry errors, due to automated checks;

(3) Reduced costs of storage space;

(4) Reduced shipping costs for data transmission to FDA; and

(5) More efficient FDA reviews and approvals of FDA-regulated products.

No small entity will be required to convert to electronic submissions. Furthermore, it is expected that no individual firm, or other entity, will choose the electronic option unless that firm finds that the benefits to the firm from conversion will exceed any conversion costs.

There may be some small entities that currently submit records on paper, but archive records electronically. These entities will need to ensure that their existing electronic systems conform to the requirements for electronic recordkeeping described in this rule. Once they have done so, however, they may also take advantage of all the other benefits of electronic recordkeeping. Therefore, no individual small entity is expected to experience direct costs that exceed benefits as a result of this rule.

Furthermore, because almost all of the rule's provisions reflect contemporary security measures and controls that respondents to the ANPRM identified, most firms should have to make few, if any, modifications to their systems.

For entities that do choose electronic recordkeeping, the magnitude of the costs associated with doing so will depend on several factors, such as the level of appropriate computer hardware and software already in place in a given firm, the types of conforming technologies selected, and the size and dispersion of the firm. For example, biometric signature technologies may be more expensive than nonbiometric technologies; firms that choose the former technology may encounter relatively higher costs. Large, geographically dispersed firms may need some institutional security procedures that smaller firms, with fewer persons in more geographically concentrated areas, may not need. Firms that require wholesale technology replacements in order to adopt electronic record/signature technology may face much higher costs than those that require only minor modifications (e.g., because they already have similar technology for internal security and quality control purposes). Among the firms that must undertake major changes to implement electronic recordkeeping, costs will be lower for those able to undertake these changes simultaneously with other planned computer and security upgrades. New firms entering the market may have a slight advantage in implementing technologies that conform with this rule, because the technologies and associated procedures can be put in place as part of the general startup.

2. Compliance requirements

If a small entity chooses to keep electronic records and/or make electronic submissions, it must do so in ways that conform to the requirements for electronic records and electronic signatures set forth in this rule. These requirements, described previously in section II. of this document, involve measures designed to ensure the integrity of system operations, of information stored in the system, and of the authorized signatures affixed to electronic records. The requirements apply to all small (and large) entities in all industry sectors regulated by FDA.

The agency believes that because the rule is flexible and reflects contemporary standards, firms should have no difficulty in putting in place the needed systems and controls. However, to assist firms in meeting the provisions of this rule, FDA may hold public meetings and publish more detailed guidance. Firms may contact FDA's Industry and Small Business Liaison Staff, HF-50, at 5600 Fishers Lane, Rockville, MD 20857 (301-827-3430) for more information.

[**FDA page 13464**]

3. Professional skills required

If a firm elects electronic recordkeeping and submissions, it must take steps to ensure that all persons involved in developing, maintaining, and using electronic records and electronic signature systems have the education, training, and experience to perform the tasks involved. The level of training and experience that will be required depends on the tasks that the person performs. For example, an individual whose sole involvement with electronic records is infrequent might only need sufficient training to understand and use the required procedures. On the other hand, an individual involved in developing an electronic record system for a firm wishing to convert from a paper recordkeeping system would probably need more education or training in computer systems and software design and implementation. In addition, FDA expects that such a person would also have specific on-the-job training and experience related to the particular type of records kept by that firm.

The relevant education, training, and experience of each individual involved in developing, maintaining, or using electronic records/submissions must be documented. However, no specific examinations or credentials for these individuals are required by the rule.

D. Minimizing the Burden on Small Entities

This rule includes several conditions that an electronic record or signature must meet in order to be acceptable as an alternative to a paper record or handwritten signature. These conditions are necessary to permit the agency to protect and promote the public health. For example, FDA must retain the ability to audit records to detect unauthorized modifications, simple errors, and to deter falsification.

Whereas there are many scientific techniques to show changes in paper records (e.g., analysis of the paper, signs of erasures, and handwriting analysis), these methods do not apply to electronic records. For electronic records and submissions to have the same integrity as paper records, they must be developed, maintained, and used under circumstances that make it difficult for them to be inappropriately modified. Without these assurances, FDA's objective of enabling electronic records and signatures to have standing equal to paper records and handwritten signatures, and to satisfy the requirements of existing statutes and regulations, cannot be met.

Within these constraints, FDA has attempted to select alternatives that provide as much flexibility as practicable without endangering the integrity of the electronic records. The agency decided not to make the required extent and stringency of controls dependent on the type of record or transactions, so that firms can decide for themselves what level of controls are worthwhile in each case. For example, FDA chose to give firms maximum flexibility in determining: (1) The circumstances under which management would have to be notified of security problems, (2) the means by which firms achieve the required link between an electronic signature and an electronic record, (3) the circumstances under which extra security and authentication measures are warranted in open systems, (4) when to use operational system checks to ensure proper event sequencing, and (5) when to use terminal checks to ensure that data and instructions originate from a valid source.

Numerous other specific considerations were addressed in the public comments to the proposed rule. A summary of the issues raised by those comments, the agency's assessment of these issues, and any changes made in the proposed rule as a result of these comments is presented earlier in this preamble.

FDA rejected alternatives for limiting potentially acceptable electronic submissions to a particular category, and for issuing different electronic submissions standards for small and large entities. The former alternative would unnecessarily limit the potential benefits of this rule; whereas the latter alternative would threaten the integrity of electronic records and submissions from small entities.

As discussed previously in this preamble, FDA rejected comments that suggested a total of 17 additional more stringent controls that might be more expensive to implement. These include: (1) Examination and certification of individuals who perform certain important tasks, (2) exclusive use of cryptographic methods to link electronic signatures to electronic records, (3) controls for each possible combination of a two factored authentication method, (4) controls for each different type of identification card, and (5) recording in audit trails the reason why records were changed.

U

FDA 21 CFR Part 11 Final Rule

List of Subjects in 21 CFR Part 11

Administrative practice and procedure, Electronic records, Electronic signatures, Reporting and recordkeeping requirements.

Therefore, under the Federal Food, Drug, and Cosmetic Act, the Public Health Service Act, and under authority delegated to the Commissioner of Food and Drugs, Title 21, Chapter I of the Code of Federal Regulations is amended by adding part 11 to read as follows:

Part 11--Electronic records; electronic signatures

Subpart A: General Provisions

Sec.
11.1 Scope
11.2 Implementation
11.3 Definitions

Subpart B: Electronic Records

11.10 Controls for closed systems
11.30 Controls for open systems
11.50 Signature manifestations
11.70 Signature/record linking

Subpart C: Electronic Signatures

11.100 General requirements
11.200 Electronic signature components and controls
11.300 Controls for identification codes/passwords

Authority: Secs. 201-903 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321-393); sec. 351 of the Public Health Service Act (42 U.S.C. 262).

Subpart A: General Provisions

Sec. 11.1 Scope

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after [**FDA page 13465**] August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with Sec. 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

Sec. 11.2 Implementation

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

Sec. 11.3 Definitions

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) Agency means the Food and Drug Administration.

(3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

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

(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

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

Subpart B: Electronic Records

Sec. 11.10 Controls for closed systems

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

(d) Limiting system access to authorized individuals.

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Sec. 11.30 Controls for open systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to [**FDA page 13466**] ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in Sec. 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

Sec. 11.50 Signature manifestations

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

Sec. 11.70 Signature/record linking

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Subpart C: Electronic Signatures

Sec. 11.100 General requirements

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

Sec. 11.200 Electronic signature components and controls

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Sec. 11.300 Controls for identification codes/passwords

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

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

Dated: March 11, 1997.
William B. Schultz, Deputy Commissioner for Policy.
[FR Doc. 97-6833 Filed 3-20-97; 8:45 am]
BILLING CODE 4160-01-F

V

FDA guidance for industry: Computerized systems in clinical trials

This guide is available at:

http://www.fda.gov/ora/compliance_ref/bimo/ffinalcct.htm

Guidance for Industry

COMPUTERIZED SYSTEMS USED IN CLINICAL TRIALS

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Biologic Evaluation and Research (CBER)
Center for Drug Evaluation and Research (CDER)
Center for Devices and Radiological Health (CDRH)
Center for Food Safety and Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
Office of Regulatory Affairs (ORA)

April 1999

Table of Contents

I. Introduction

This document addresses issues pertaining to computerized systems used to create, modify, maintain, archive, retrieve, or transmit clinical data intended for submission to the Food and Drug Administration (FDA). These data form the basis for the Agency's decisions regarding the safety and efficacy of new human and animal drugs, biologics, medical devices, and certain food and color additives. As such, these data have broad public health significance and must be of the highest quality and integrity.

FDA established the Bioresearch Monitoring (BIMO) Program of inspections and audits to monitor the conduct and reporting of clinical trials to ensure that data from these trials meet the highest standards of quality and integrity and conform to FDA's regulations. FDA's acceptance of data from clinical trials for decision-making purposes is dependent upon its ability to verify the quality and integrity of such data during its onsite inspections and audits. To be acceptable the data should meet certain fundamental elements of quality whether collected or recorded electronically or on paper. Data should be attributable, original, accurate, contemporaneous, and legible. For example, attributable data can be traced to individuals responsible for observing and recording the data. In an automated system, attributability could be achieved by a computer system designed to identify individuals responsible for any input.

This guidance addresses how these elements of data quality might be satisfied where computerized systems are being used to create, modify, maintain, archive, retrieve, or transmit clinical data. Although the primary focus of this guidance is on computerized systems used at clinical sites to collect data, the principles set forth may also be appropriate for computerized systems at contract research organizations, data management centers, and sponsors. Persons using the data from computerized systems should have confidence that the data are no less reliable than data in paper form.

Computerized medical devices, diagnostic laboratory instruments and instruments in analytical laboratories that are used in clinical trials are not the focus of this guidance. This guidance does not address electronic submissions or methods of their transmission to the Agency.

This guidance document reflects long-standing regulations covering clinical trial records. It also addresses requirements of the Electronic Records/Electronic Signatures rule (21 CFR part 11).

The principles in this guidance may be applied where source documents are created (1) in hardcopy and later entered into a computerized system, (2) by direct entry by a human into a computerized system, and (3) automatically by a computerized system.

II. Definitions

Audit Trail means, for the purposes of this guidance, a secure, computer generated, time-stamped electronic record that allows reconstruction of the course of events relating to the creation, modification, and deletion of an electronic record.

Certified Copy means a copy of original information that has been verified, as indicated by dated signature, as an exact copy having all of the same attributes and information as the original.

Commit means a saving action, which creates or modifies, or an action which deletes, an electronic record or portion of an electronic record. An example is pressing the key of a keyboard that causes information to be saved to durable medium.

Computerized System means, for the purpose of this guidance, computer hardware, software, and associated documents (e.g., user manual) that create, modify, maintain, archive, retrieve, or transmit in digital form information related to the conduct of a clinical trial.

Direct Entry means recording data where an electronic record is the original capture of the data. Examples are the keying by an individual of original observations into the system, or automatic recording by the system of the output of a balance that measures subject's body weight.

Electronic Case Report Form (e-CRF) means an auditable electronic record designed to record information required by the clinical trial protocol to be reported to the sponsor on each trial subject.

Electronic Patient Diary means an electronic record into which a subject participating in a clinical trial directly enters observations or directly responds to an evaluation checklist.

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

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

Software Validation means confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through the software can be consistently fulfilled. For the purposes of this document, design level validation is that portion of the software validation that takes place in parts of the software life cycle before the software is delivered to the end user.

Source Documents means original documents and records including, but not limited to, hospital records, clinical and office charts, laboratory notes, memoranda, subjects' diaries or evaluation checklists, pharmacy dispensing records, recorded data from automated instruments, copies or transcriptions certified after verification as being accurate and complete, microfiches, photographic negatives, microfilm or magnetic media, x-rays, subject files, and records kept at the pharmacy, at the laboratories, and at medico-technical departments involved in the clinical trial.

Transmit means, for the purposes of this guidance, to transfer data within or among clinical study sites, contract research organizations, data management centers, or sponsors. Other Agency guidance covers transmission from sponsors to the Agency.

III. General principles

A. Each study protocol should identify at which steps a computerized system will be used to create, modify, maintain, archive, retrieve, or transmit data.

B. For each study, documentation should identify what software and, if known, what hardware is to be used in computerized systems that create, modify, maintain, archive, retrieve, or transmit data. This documentation should be retained as part of study records.

C. Source documents should be retained to enable a reconstruction and evaluation of the trial.

D. When original observations are entered directly into a computerized system, the electronic record is the source document.

E. The design of a computerized system should ensure that all applicable regulatory requirements for recordkeeping and record retention in clinical trials are met with the same degree of confidence as is provided with paper systems.

F. Clinical investigators should retain either the original or a certified copy of all source documents sent to a sponsor or contract research organization, including query resolution correspondence.

G. Any change to a record required to be maintained should not obscure the original information. The record should clearly indicate that a change was made and clearly provide a means to locate and read the prior information.

H. Changes to data that are stored on electronic media will always require an audit trail, in accordance with 21 CFR 11.10(e). Documentation should include who made the changes, when, and why they were made.

I. The FDA may inspect all records that are intended to support submissions to the Agency, regardless of how they were created or maintained.

J. Data should be retrievable in such a fashion that all information regarding each individual subject in a study is attributable to that subject.

K. Computerized systems should be designed: (1) So that all requirements assigned to these systems in a study protocol are satisfied (e.g., data are recorded in metric units, requirements that the study be blinded); and, (2) to preclude errors in data creation, modification, maintenance, archiving, retrieval, or transmission.

Security measures should be in place to prevent unauthorized access to the data and to the computerized system.

IV. Standard operating procedures

Standard Operating Procedures (SOPs) pertinent to the use of the computerized system should be available on site.

SOPs should be established for, but not limited to:

- System Setup/Installation
- Data Collection and Handling
- System Maintenance
- Data Backup, Recovery, and Contingency Plans
- Security
- Change Control

V. Data entry

A. Electronic Signatures

1. To ensure that individuals have the authority to proceed with data entry, the data entry system should be designed so that individuals need to enter electronic signatures, such as combined identification codes/passwords or biometric-based electronic signatures, at the start of a data entry session.
2. The data entry system should also be designed to ensure attributability. Therefore, each entry to an electronic record, including any change, should be made under the electronic signature of the individual making that entry. However, this does not

necessarily mean a separate electronic signature for each entry or change. For example, a single electronic signature may cover multiple entries or changes.

a. The printed name of the individual who enters data should be displayed by the data entry screen throughout the data entry session. This is intended to preclude the possibility of a different individual inadvertently entering data under someone else's name.

If the name displayed by the screen during a data entry session is not that of the person entering the data, then that individual should log on under his or her own name before continuing.

3. Individuals should only work under their own passwords or other access keys and should not share these with others. Individuals should not log on to the system in order to provide another person access to the system.
4. Passwords or other access keys should be changed at established intervals.
5. When someone leaves a workstation, the person should log off the system. Failing this, an automatic log off may be appropriate for long idle periods. For short periods of inactivity, there should be some kind of automatic protection against unauthorized data entry. An example could be an automatic screen saver that prevents data entry until a password is entered.

B. Audit Trails

1. Section 21 CFR 11.10(e) requires persons who use electronic record systems to maintain an audit trail as one of the procedures to protect the authenticity, integrity, and, when appropriate, the confidentiality of electronic records.

   a. Persons must use secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. A record is created when it is saved to durable media, as described under "commit" in Section II, Definitions.

   b. Audit trails must be retained for a period at least as long as that required for the subject electronic records (e.g., the study data and records to which they pertain) and must be available for agency review and copying.

2. Personnel who create, modify, or delete electronic records should not be able to modify the audit trails.
3. Clinical investigators should retain either the original or a certified copy of audit trails.
4. FDA personnel should be able to read audit trails both at the study site and at any other location where associated electronic study records are maintained.
5. Audit trails should be created incrementally, in chronological order, and in a manner that does not allow new audit trail information to overwrite existing data in violation of §11.10(e).

C. Date/Time Stamps

Controls should be in place to ensure that the system's date and time are correct.

The ability to change the date or time should be limited to authorized personnel and such personnel should be notified if a system date or time discrepancy is detected. Changes to date or time should be documented.

Dates and times are to be local to the activity being documented and should include the year, month, day, hour, and minute. The Agency encourages establishments to synchronize systems to the date and time provided by trusted third parties.

Clinical study computerized systems will likely be used in multi-center trials, perhaps located in different time zones. Calculation of the local time stamp may be derived in such cases from a remote server located in a different time zone.

VI. System features

A. Systems used for direct entry of data should include features that will facilitate the collection of quality data.

Prompts, flags, or other help features within the computerized system should be used to encourage consistent use of clinical terminology and to alert the user to data that are out of acceptable range. Features that automatically enter data into a field when that field is bypassed should not be used.

Electronic patient diaries and e-CRFs should be designed to allow users to make annotations. Annotations add to data quality by allowing ad hoc information to be captured. This information may be valuable in the event of an adverse reaction or unexpected result. The record should clearly indicate who recorded the annotations and when (date and time).

B. Systems used for direct entry of data should be designed to include features that will facilitate the inspection and review of data. Data tags (e.g., different color, different font, flags) should be used to indicate which data have been changed or deleted, as documented in the audit trail.

C. Retrieval of Data

Recognizing that computer products may be discontinued or supplanted by newer (possibly incompatible) systems, it is nonetheless vital that sponsors retain the ability to retrieve and review the data recorded by the older systems. This may be achieved by maintaining support for the older systems or transcribing data to the newer systems.

When migrating to newer systems, it is important to generate accurate and complete copies of study data and collateral information relevant to data integrity. This information would include, for example, audit trails and computational methods used to derive the data. Any data retrieval software, script, or query logic used for the purpose of manipulating, querying, or extracting data for report generating purposes should be documented and maintained for the life of the report. The transcription process needs to be validated.

D. Reconstruction of Study

FDA expects to be able to reconstruct a study. This applies not only to the data, but also how the data were obtained or managed. Therefore, all versions of application software, operating systems, and software development tools involved in processing of data or records should be available as long as data or records associated with these versions are required to be retained. Sponsors may retain these themselves or may contract for the vendors to retain the ability to run (but not necessarily support) the software. Although FDA expects sponsors or vendors to retain the ability to run older versions of software, the agency acknowledges that, in some cases, it will be difficult for sponsors and vendors to run older computerized systems.

VII. Security

A. Physical Security

In addition to internal safeguards built into the system, external safeguards should be in place to ensure that access to the computerized system and to the data is restricted to authorized personnel.

Staff should be thoroughly aware of system security measures and the importance of limiting access to authorized personnel.

SOPs should be in place for handling and storing the system to prevent unauthorized access.

B. Logical Security

Access to the data at the clinical site should be restricted and monitored through the system's software with its required log-on, security procedures, and audit trail. The data should not be altered, browsed, queried, or reported via external software applications that do not enter through the protective system software.

There should be a cumulative record that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. The record should be in the study documentation accessible at the site.

If a sponsor supplies computerized systems exclusively for clinical trials, the systems should remain dedicated to the purpose for which they were intended and validated.

If a computerized system being used for the clinical study is part of a system normally used for other purposes, efforts should be made to ensure that the study software is logically and physically isolated as necessary to preclude unintended interaction with non-study software. If any of the software programs are changed the system should be evaluated to determine the effect of the changes on logical security.

Controls should be in place to prevent, detect, and mitigate effects of computer viruses on study data and software.

VIII. System dependability

The sponsor should ensure and document that computerized systems conform to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance.

A. Systems documentation should be readily available at the site where clinical trials are conducted. Such documentation should provide an overall description of computerized systems and the relationship of hardware, software, and physical environment.

B. FDA may inspect documentation, possessed by a regulated company, that demonstrates validation of software. The study sponsor is responsible, if requested, for making such documentation available at the time of inspection at the site where software is used. Clinical investigators are not generally responsible for validation unless they originated or modified software.

1. For software purchased off-the-shelf, most of the validation should have been done by the company that wrote the software. The sponsor or contract research organization should have documentation (either original validation documents or on-site vendor audit documents) of this design level validation by the vendor, and should have itself performed functional testing (e.g., by use of test data sets) and researched known software limitations, problems, and defect corrections.

   In the special case of database and spreadsheet software that is (1) purchased off-the-shelf, (2) designed for and widely used for general purposes, (3) unmodified, and (4) not being used for direct entry of data, the sponsor or contract research organization may not have documentation of design level validation. However, the sponsor or contract research organization should have itself performed functional testing (e.g., by use of test data sets) and researched known software limitations, problems, and defect corrections.

2. Documentation important to demonstrate software validation includes:

   Written design specification that describes what the software is intended to do and how it is intended to do it;

A written test plan based on the design specification, including both structural and functional analysis; and,

Test results and an evaluation of how these results demonstrate that the predetermined design specification has been met.

C. Change Control

Written procedures should be in place to ensure that changes to the computerized system such as software upgrades, equipment or component replacement, or new instrumentation will maintain the integrity of the data or the integrity of protocols.

The impact of any change to the system should be evaluated and a decision made regarding the need to revalidate. Revalidation should be performed for changes that exceed operational limits or design specifications.

All changes to the system should be documented.

IX. System controls

A. Software Version Control

Measures should be in place to ensure that versions of software used to generate, collect, maintain, and transmit data are the versions that are stated in the systems documentation.

B. Contingency Plans

Written procedures should describe contingency plans for continuing the study by alternate means in the event of failure of the computerized system.

C. Backup and Recovery of Electronic Records

Backup and recovery procedures should be clearly outlined in the SOPs and be sufficient to protect against data loss. Records should be backed up regularly in a way that would prevent a catastrophic loss and ensure the quality and integrity of the data.

Backup records should be stored at a secure location specified in the SOPs. Storage is typically offsite or in a building separate from the original records.

Backup and recovery logs should be maintained to facilitate an assessment of the nature and scope of data loss resulting from a system failure.

X. Training of personnel

A. Qualifications

Each person who enters or processes data should have the education, training, and experience or any combination thereof necessary to perform the assigned functions.

Individuals responsible for monitoring the trial should have education, training, and experience in the use of the computerized system necessary to adequately monitor the trial.

B. Training

Training should be provided to individuals in the specific operations that they are to perform.

Training should be conducted by qualified individuals on a continuing basis, as needed, to ensure familiarity with the computerized system and with any changes to the system during the course of the study.

C. Documentation

Employee education, training, and experience should be documented.

XI. Records inspection

A. FDA may inspect all records that are intended to support submissions to the Agency, regardless of how they were created or maintained. Therefore, systems should be able to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the Agency. Persons should contact the Agency if there is any doubt about what file formats and media the Agency can read and copy.

B. The sponsor should be able to provide hardware and software as necessary for FDA personnel to inspect the electronic documents and audit trail at the site where an FDA inspection is taking place.

XII. Certification of electronic signatures

As required by 21 CFR 11.100(c), persons using electronic signatures to meet an FDA signature requirement shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

As set forth in 21 CFR 11.100(c), the certification shall be submitted in paper form signed with a traditional handwritten signature to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville Maryland 20857. The certification is to be submitted prior to or at the time electronic signatures are used. However, a single certification may cover all electronic signatures used by persons in a given organization. This certification is a legal document created by persons to acknowledge that their electronic signatures have the same legal significance as their traditional handwritten signatures. An acceptable certification may take the following form:

“Pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations, this is to certify that [name of organization] intends that all electronic signatures executed by our employees, agents, or representatives, located anywhere in the world, are the legally binding equivalent of traditional handwritten signatures.”

XIII. References

FDA, *Software Development Activities*, 1987.

FDA, *Guideline for the Monitoring of Clinical Investigations*, 1988.

FDA, *Guidance for Industry: Good Target Animal Practices: Clinical Investigators and Monitor*s, 1997.

FDA, *Compliance Program Guidance Manual*, “Compliance Program 7348.810 - Sponsors, Contract Research Organizations and Monitors,” October 30, 1998.

FDA, *Compliance Program Guidance Manual*, “Compliance Program 7348.811 - Bioresearch Monitoring - Clinical Investigators,” September 2, 1998.

FDA, *Information Sheets for Institutional Review Boards and Clinical Investigators*, 1998.

FDA, *Glossary of Computerized System and Software Development Terminology*, 1995.

FDA, *21 CFR Part 11, Electronic Records; Electronic Signatures; Final Rule*. Federal Register Vol. 62, No. 54, 13429, March 20, 1997.

FDA, [draft] *Guidance for Industry: General Principles of Software Validation*, draft 1997.

International Conference on Harmonisation, *Good Clinical Practice: Consolidated Guideline*, Federal Register Vol 62, No. 90, 25711, May 9, 1997.

W

FDA guidance: General principles of software validation

General Principles of Software Validation; Final Guidance for Industry and FDA Staff

Document issued on: January 11, 2002

This document supersedes the draft document, *General Principles of Software Validation*, Version 1.1, dated June 9, 1997.

U.S. Department Of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

This guide is available at:

`http://www.fda.gov/cdrh/comp/guidance/938.html`

Preface

Public comment

Comments and suggestions may be submitted at any time for Agency consideration to Dockets Management Branch, Division of Management Systems and Policy, Office of Human Resources and Management Services, Food and Drug Administration, 5630 Fishers Lane, Room 1061, (HFA-305), Rockville, MD, 20852. When submitting comments, please refer to the exact title of this guidance document. Comments may not be acted upon by the Agency until the document is next revised or updated.

For questions regarding the use or interpretation of this guidance which involve the Center for Devices and Radiological Health (CDRH), contact John F. Murray at (301) 594-4659 or email mailto:jfm@cdrh.fda.gov.

For questions regarding the use or interpretation of this guidance which involve the Center for Biologics Evaluation and Research (CBER) contact Jerome Davis at (301) 827-6220 or email mailto:davis@cber.fda.gov.

Additional copies

CDRH

Additional copies are available from the Internet at: http://www.fda.gov/cdrh/comp/guidance/938.pdf or via CDRH Facts-On-Demand. In order to receive this document via your fax machine, call the CDRH Facts-On-Demand system at 800-899-0381 or 301-827-0111 from a touch-tone telephone. Press 1 to enter the system. At the second voice prompt, press 1 to order a document. Enter the document number 938 followed by the pound sign (#). Follow the remaining voice prompts to complete your request.

CBER

Additional copies are available from the Internet at: http://www.fda.gov/cber/guidelines.htm, by writing to CBER, Office of Communication, Training, and Manufacturers' Assistance (HFM-40), 1401 Rockville Pike, Rockville, Maryland 20852-1448, or by telephone request at 1-800-835-5709 or 301-827-1800.

Table of Contents

General principles of software validation

This document is intended to provide guidance. It represents the Agency's current thinking on this topic. It does not create or confer any rights for or on any person and does not operate to bind Food and Drug Administration (FDA) or the public. An alternative approach may be used if such approach satisfies the requirements of the applicable statutes and regulations.

Section 1. Purpose

This guidance outlines general validation principles that the Food and Drug Administration (FDA) considers to be applicable to the validation of medical device software or the validation of software used to design, develop, or manufacture medical devices. This final guidance document, Version 2.0, supersedes the draft document, *General Principles of Software Validation* [available at: `http://www.fda.gov/ora/inspect_ref/igs/gloss.html`], Version 1.1, dated June 9, 1997.

Section 2. Scope

This guidance describes how certain provisions of the medical device Quality System regulation apply to software and the agency's current approach to evaluating a software validation system. For example, this document lists elements that are acceptable to the FDA for the validation of software; however, it does not list all of the activities and tasks that must, in all instances, be used to comply with the law.

The scope of this guidance is somewhat broader than the scope of validation in the strictest definition of that term. Planning, verification, testing, traceability, configuration management, and many other aspects of good software engineering discussed in this guidance are important activities that together help to support a final conclusion that software is validated.

This guidance recommends an integration of software life cycle management and risk management activities. Based on the intended use and the safety risk associated with the software to be developed, the software developer should determine the specific approach, the combination of techniques to be used, and the level of effort to be applied. While this guidance does not recommend any specific life cycle model or any specific technique or method, it does recommend that software validation and verification activities be conducted throughout the entire software life cycle.

Where the software is developed by someone other than the device manufacturer (e.g., off-the-shelf software) the software developer may not be directly responsible for compliance with FDA regulations. In that case, the party with regulatory responsibility (i.e., the device manufacturer) needs to assess the adequacy of the off-the-shelf software developer's activities and determine what additional efforts are needed to establish that the software is validated for the device manufacturer's intended use.

2.1. Applicability

This guidance applies to:

- Software used as a component, part, or accessory of a medical device;
- Software that is itself a medical device (e.g., blood establishment software);
- Software used in the production of a device (e.g., programmable logic controllers in manufacturing equipment); and
- Software used in implementation of the device manufacturer's quality system (e.g., software that records and maintains the device history record).

This document is based on generally recognized software validation principles and, therefore, can be applied to any software. For FDA purposes, this guidance applies to any software related to a regulated medical device, as defined by Section 201(h) of the Federal Food, Drug, and Cosmetic Act (the Act) and by current FDA software and regulatory policy. This document does not specifically identify which software is or is not regulated.

2.2. Audience

This guidance provides useful information and recommendations to the following individuals:

- Persons subject to the medical device Quality System regulation
- Persons responsible for the design, development, or production of medical device software
- Persons responsible for the design, development, production, or procurement of automated tools used for the design, development, or manufacture of medical devices or software tools used to implement the quality system itself
- FDA Investigators
- FDA Compliance Officers
- FDA Scientific Reviewers

2.3. The least burdensome approach

We believe we should consider the least burdensome approach in all areas of medical device regulation. This guidance reflects our careful review of the relevant scientific and legal requirements and what we believe is the least burdensome way for you to comply with those requirements. However, if you believe that an alternative approach would be less burdensome, please contact us so we can consider your point of view. You may send your written comments to the contact person listed in the preface to this guidance or to the CDRH Ombudsman. Comprehensive information on CDRH's Ombudsman, including ways to contact him, can be found on the Internet at:

http://www.fda.gov/cdrh/resolvingdisputes/ombudsman.html

2.4. Regulatory requirements for software validation

The FDA's analysis of 3140 medical device recalls conducted between 1992 and 1998 reveals that 242 of them (7.7%) are attributable to software failures. Of those software related recalls, 192 (or 79%) were caused by software defects that were introduced when changes were made to the software after its initial production and distribution. Software validation and other related good software engineering practices discussed in this guidance are a principal means of avoiding such defects and resultant recalls.

Software validation is a requirement of the Quality System regulation, which was published in the Federal Register on October 7, 1996 and took effect on June 1, 1997. (See Title 21 Code of Federal Regulations (CFR) Part 820, and 61 Federal Register (FR) 52602, respectively.) Validation requirements apply to software used as components in medical devices, to software that is itself a medical device, and to software used in production of the device or in implementation of the device manufacturer's quality system.

Unless specifically exempted in a classification regulation, any medical device software product developed after June 1, 1997, regardless of its device class, is subject to applicable design control provisions. (See of 21 CFR §820.30.) This requirement includes the completion of current development projects, all new development projects, and all changes made to existing medical device software. Specific requirements for validation of device software are found in 21 CFR §820.30(g). Other design controls, such as planning, input, verification, and reviews, are required for medical device software. (See 21 CFR §820.30.)

The corresponding documented results from these activities can provide additional support for a conclusion that medical device software is validated.

Any software used to automate any part of the device production process or any part of the quality system must be validated for its intended use, as required by 21 CFR §820.70(i). This requirement applies to any software used to automate device design, testing, component acceptance, manufacturing, labeling, packaging, distribution, complaint handling, or to automate any other aspect of the quality system.

In addition, computer systems used to create, modify, and maintain electronic records and to manage electronic signatures are also subject to the validation requirements. (See 21 CFR §11.10(a).) Such computer systems must be validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Software for the above applications may be developed in-house or under contract. However, software is frequently purchased off-the-shelf for a particular intended use. All production and/or quality system software, even if purchased off-the-shelf, should have documented requirements that fully define its intended use, and information against which testing results and other evidence can be compared, to show that the software is validated for its intended use.

The use of off-the-shelf software in automated medical devices and in automated manufacturing and quality system operations is increasing. Off-the-shelf software may have many capabilities, only a few of which are needed by the device manufacturer. Device manufacturers are responsible for the adequacy of the software used in their devices, and used to produce devices. When device manufacturers purchase “off-the-shelf" software, they must ensure that it will perform as intended in their chosen application. For off-the-shelf software used in manufacturing or in the quality system, additional guidance is included in Section 6.3 of this document. For device software, additional useful information may be found in FDA’s *Guidance for Industry, FDA Reviewers, and Compliance on Off-The-Shelf Software Use in Medical Devices* [available at: `http://www.fda.gov/cdrh/ode/guidance/585.html`].

2.4. Quality system regulation vs pre-market submissions

This document addresses Quality System regulation issues that involve the implementation of software validation. It provides guidance for the management and control of the software validation process. The management and control of the software validation process should not be confused with any other validation requirements, such as process validation for an automated manufacturing process.

Device manufacturers may use the same procedures and records for compliance with quality system and design control requirements, as well as for pre-market submissions to FDA. This document does not cover any specific safety or efficacy issues related to software validation. Design issues and documentation requirements for pre-market submissions of regulated software are not addressed by this document. Specific issues related to safety and efficacy, and the documentation required in pre-market submissions, should be addressed to the Office of Device Evaluation (ODE), Center for Devices and Radiological Health (CDRH) or to the Office of Blood Research and Review, Center for Biologics Evaluation and Research (CBER). See the references in “Appendix A - References” on page 426 for applicable FDA guidance documents for pre-market submissions.

Section 3. Context for software validation

Many people have asked for specific guidance on what FDA expects them to do to ensure compliance with the Quality System regulation with regard to software validation. Information on software validation presented in this document is not new. Validation of software, using the principles and tasks listed in Sections 4 and 5, has been conducted in many segments of the software industry for well over 20 years.

Due to the great variety of medical devices, processes, and manufacturing facilities, it is not possible to state in one document all of the specific validation elements that are applicable. However, a general application of several broad concepts can be used successfully as guidance for software validation. These broad concepts provide an acceptable framework for building a comprehensive approach to software validation. Additional specific information is available from many of the references listed in “Appendix A - References” on page 426.

3.1. Definitions and terminology

Unless defined in the Quality System regulation, or otherwise specified below, all other terms used in this guidance are as defined in the current edition of the FDA *Glossary of Computerized System and Software Development Terminology* [available at `http://www.fda.gov/ora/inspect_ref/igs/gloss.html`].

The medical device Quality System regulation (21 CFR 820.3(k)) defines “*establish*” to mean “define, document, and implement.” Where it appears in this guidance, the words “establish” and “established” should be interpreted to have this same meaning.

Some definitions found in the medical device Quality System regulation can be confusing when compared to commonly used terminology in the software industry. Examples are requirements, specification, verification, and validation.

3.1.1 Requirements and specifications

While the Quality System regulation states that design input requirements must be documented, and that specified requirements must be verified, the regulation does not further clarify the distinction between the terms “requirement” and “specification.” A *requirement* can be any need or expectation for a system or for its software. Requirements reflect the stated or implied needs of the customer, and may be market-based, contractual, or statutory, as well as an organization's internal requirements. There can be many different kinds of requirements (e.g., design, functional, implementation, interface, performance, or physical requirements). Software requirements are typically derived from the system requirements for those aspects of system functionality that have been allocated to software. Software requirements are typically stated in functional terms and are defined, refined, and updated as a development project progresses. Success in accurately and completely documenting software requirements is a crucial factor in successful validation of the resulting software.

A *specification* is defined as “a document that states requirements.” (See 21 CFR §820.3(y).) It may refer to or include drawings, patterns, or other relevant documents and usually indicates the means and the criteria whereby conformity with the requirement can be checked. There are many different kinds of written specifications, e.g., system requirements specification, software requirements specification, software design specification, software test specification, software integration specification, etc. All of these documents establish “specified requirements” and are design outputs for which various forms of verification are necessary.

3.1.2 Verification and validation

The Quality System regulation is harmonized with ISO 8402:1994, which treats “verification” and “validation” as separate and distinct terms. On the other hand, many software engineering journal articles and textbooks use the terms “verification” and “validation” interchangeably, or in some cases refer to software “verification, validation, and testing (VV&T)” as if it is a single concept, with no distinction among the three terms.

Software verification provides objective evidence that the design outputs of a particular phase of the software development life cycle meet all of the specified requirements for that phase. Software verification looks for consistency, completeness, and correctness of the software and its supporting documentation, as it is being developed, and provides support for a subsequent conclusion that software is validated. Software testing is one of many verification activities intended to confirm that software development output meets its input requirements. Other verification activities include various static and dynamic analyses, code and document inspections, walkthroughs, and other techniques.

Software validation is a part of the design validation for a finished device, but is not separately defined in the Quality System regulation. For purposes of this guidance, FDA considers software validation to be "*confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled.*" In practice, software validation activities may occur both during, as well as at the end of the software development life cycle to ensure that all requirements have been fulfilled. Since software is usually part of a larger hardware system, the validation of software typically includes evidence that all software requirements have been implemented correctly and completely and are traceable to system requirements. A conclusion that software is validated is highly dependent upon comprehensive software testing, inspections, analyses, and other verification tasks performed at each stage of the software development life cycle. Testing of device software functionality in a simulated use environment, and user site testing are typically included as components of an overall design validation program for a software automated device.

Software verification and validation are difficult because a developer cannot test forever, and it is hard to know how much evidence is enough. In large measure, software validation is a matter of developing a "level of confidence" that the device meets all requirements and user expectations for the software automated functions and features of the device. Measures such as defects found in specifications documents, estimates of defects remaining, testing coverage, and other techniques are all used to develop an acceptable level of confidence before shipping the product. The level of confidence, and therefore the level of software validation, verification, and testing effort needed, will vary depending upon the safety risk (hazard) posed by the automated functions of the device. Additional guidance regarding safety risk management for software may be found in Section 4 of FDA's *Guidance for the Content of Pre-market Submissions for Software Contained in Medical Devices* [available at: `http://www.fda.gov/cdrh/ode/57.html`], and in the international standards ISO/IEC 14971-1 and IEC 60601-1-4 referenced in "Appendix A - References" on page 426.

3.1.3 IQ/OQ/PQ

For many years, both FDA and regulated industry have attempted to understand and define software validation within the context of process validation terminology. For example, industry documents and other FDA validation guidance sometimes describe user site software validation in terms of installation qualification (IQ), operational qualification (OQ) and performance qualification (PQ). Definitions of these terms and additional information regarding IQ/OQ/PQ may be found in FDA's *Guideline on General Principles of Process Validation*, dated May 11, 1987 [available at: `http://www.fda.gov/cdrh/ode/425.pdf`], and in FDA's *Glossary of Computerized System and Software Development Terminology* [available at: `http://www.fda.gov/ora/inspect_ref/igs/gloss.html`], dated August 1995.

While IQ/OQ/PQ terminology has served its purpose well and is one of many legitimate ways to organize software validation tasks at the user site, this terminology may not be well understood among many software professionals, and it is not used elsewhere in this document. However, both FDA personnel and device manufacturers need to be aware of these differences in terminology as they ask for and provide information regarding software validation.

3.2. Software development as part of system design

The decision to implement system functionality using software is one that is typically made during system design. Software requirements are typically derived from the overall system requirements and design for those aspects in the system that are to be implemented using software. There are user needs and intended uses for a finished device, but users typically do not specify whether those requirements are to be met by hardware, software, or some combination of both. Therefore, software validation must be considered within the context of the overall design validation for the system.

A documented requirements specification represents the user's needs and intended uses from which the product is developed. A primary goal of software validation is to then demonstrate that all completed software products comply with all documented software and system requirements. The correctness and completeness of both the system requirements and the software requirements should be addressed as part of the design validation process for the device. Software validation includes confirmation of conformance to all software specifications and confirmation that all software requirements are traceable to the system specifications. Confirmation is an important part of the overall design validation to ensure that all aspects of the medical device conform to user needs and intended uses.

3.3. Software is different from hardware

While software shares many of the same engineering tasks as hardware, it has some very important differences. For example:

- The vast majority of software problems are traceable to errors made during the design and development process. While the quality of a hardware product is highly dependent on design, development and manufacture, the quality of a software product is dependent primarily on design and development with a minimum concern for software manufacture. Software manufacturing consists of reproduction that can be easily verified. It is not difficult to manufacture thousands of program copies that function exactly the same as the original; the difficulty comes in getting the original program to meet all specifications.
- One of the most significant features of software is branching, i.e., the ability to execute alternative series of commands, based on differing inputs. This feature is a major contributing factor for another characteristic of software – its complexity. Even short programs can be very complex and difficult to fully understand.
- Typically, testing alone cannot fully verify that software is complete and correct. In addition to testing, other verification techniques and a structured and documented development process should be combined to ensure a comprehensive validation approach.
- Unlike hardware, software is not a physical entity and does not wear out. In fact, software may improve with age, as latent defects are discovered and removed. However, as software is constantly updated and changed, such improvements are sometimes countered by new defects introduced into the software during the change.
- Unlike some hardware failures, software failures occur without advanced warning. The software’s branching that allows it to follow differing paths during execution, may hide some latent defects until long after a software product has been introduced into the marketplace.
- Another related characteristic of software is the speed and ease with which it can be changed. This factor can cause both software and non-software professionals to believe that software problems can be corrected easily. Combined with a lack of understanding of software, it can lead managers to believe that tightly controlled engineering is not needed as much for software as it is for hardware. In fact, the opposite is true. *Because of its complexity, the development process for software should be even more tightly controlled than for hardware, in order to prevent problems that cannot be easily detected later in the development process.*

- Seemingly insignificant changes in software code can create unexpected and very significant problems elsewhere in the software program. The software development process should be sufficiently well planned, controlled, and documented to detect and correct unexpected results from software changes.
- Given the high demand for software professionals and the highly mobile workforce, the software personnel who make maintenance changes to software may not have been involved in the original software development. Therefore, accurate and thorough documentation is essential.
- Historically, software components have not been as frequently standardized and interchangeable as hardware components. However, medical device software developers are beginning to use component-based development tools and techniques. Object-oriented methodologies and the use of off-the-shelf software components hold promise for faster and less expensive software development. However, component-based approaches require very careful attention during integration. Prior to integration, time is needed to fully define and develop reusable software code and to fully understand the behavior of off-the-shelf components.

For these and other reasons, software engineering needs an even greater level of managerial scrutiny and control than does hardware engineering.

3.4. Benefits of software validation

Software validation is a critical tool used to assure the quality of device software and software automated operations. Software validation can increase the usability and reliability of the device, resulting in decreased failure rates, fewer recalls and corrective actions, less risk to patients and users, and reduced liability to device manufacturers. Software validation can also reduce long term costs by making it easier and less costly to reliably modify software and revalidate software changes. Software maintenance can represent a very large percentage of the total cost of software over its entire life cycle. An established comprehensive software validation process helps to reduce the long-term cost of software by reducing the cost of validation for each subsequent release of the software.

3.5 Design review

Design reviews are documented, comprehensive, and systematic examinations of a design to evaluate the adequacy of the design requirements, to evaluate the capability of the design to meet these requirements, and to identify problems. While there may be many informal technical reviews that occur within the development team during a software project, a formal design review is more structured and includes participation from others outside the development team. Formal design reviews may reference or include results from other formal and informal reviews. Design reviews may be conducted separately for the software, after the software is integrated with the hardware into the system, or both. Design reviews should include examination of development plans, requirements specifications, design specifications, testing plans and procedures, all other documents and activities associated with the project, verification results from each stage of the defined life cycle, and validation results for the overall device.

Design review is a primary tool for managing and evaluating development projects. For example, formal design reviews allow management to confirm that all goals defined in the software validation plan have been achieved. The Quality System regulation requires that at least one formal design review be conducted during the device design process. However, it is recommended that multiple design reviews be conducted (e.g., at the end of each software life cycle activity, in preparation for proceeding to the next activity). Formal design review is especially important at or near the end of the requirements activity, before major resources have been committed to specific design solutions. Problems found at this point can be resolved more easily, save time and money, and reduce the likelihood of missing a critical issue.

Answers to some key questions should be documented during formal design reviews. These include:

- Have the appropriate tasks and expected results, outputs, or products been established for each software life cycle activity?
- Do the tasks and expected results, outputs, or products of each software life cycle activity:
  - Comply with the requirements of other software life cycle activities in terms of correctness, completeness, consistency, and accuracy?
  - Satisfy the standards, practices, and conventions of that activity?
  - Establish a proper basis for initiating tasks for the next software life cycle activity?

Section 4. Principles of software validation

This section lists the general principles that should be considered for the validation of software.

4.1. Requirements

A documented software requirements specification provides a baseline for both validation and verification. The software validation process cannot be completed without an established software requirements specification (Ref: 21 CFR 820.3(z) and (aa) and 820.30(f) and (g)).

4.2. Defect prevention

Software quality assurance needs to focus on preventing the introduction of defects into the software development process and not on trying to “test quality into” the software code after it is written. *Software testing is very limited in its ability to surface all latent defects in software code.* For example, the complexity of most software prevents it from being exhaustively tested. Software testing is a necessary activity. However, in most cases software testing by itself is not sufficient to establish confidence that the software is fit for its intended use. In order to establish that confidence, software developers should use a mixture of methods and techniques to prevent software errors and to detect software errors that do occur. The “best mix” of methods depends on many factors including the development environment, application, size of project, language, and risk.

4.3. Time and effort

To build a case that the software is validated requires time and effort. Preparation for software validation should begin early, i.e., during design and development planning and design input. The final conclusion that the software is validated should be based on evidence collected from planned efforts conducted throughout the software lifecycle.

4.4. Software life cycle

Software validation takes place within the environment of an established software life cycle. The software life cycle contains software engineering tasks and documentation necessary to support the software validation effort. In addition, the software life cycle contains specific verification and validation tasks that are appropriate for the intended use of the software. This guidance does not recommend any particular life cycle models – only that they should be selected and used for a software development project.

4.5. Plans

The software validation process is defined and controlled through the use of a plan. The software validation plan defines “what” is to be accomplished through the software validation effort. Software validation plans are a significant quality system tool. Software validation plans specify areas such as scope, approach, resources, schedules and the types and extent of activities, tasks, and work items.

4.6. Procedures

The software validation process is executed through the use of procedures. These procedures establish “how” to conduct the software validation effort. The procedures should identify the specific actions or sequence of actions that must be taken to complete individual validation activities, tasks, and work items.

4.7. Software validation after a change

Due to the complexity of software, a seemingly small local change may have a significant global system impact. When any change (even a small change) is made to the software, the validation status of the software needs to be re-established. *Whenever software is changed, a validation analysis should be conducted not just for validation of the individual change, but also to determine the extent and impact of that change on the entire software system.* Based on this analysis, the software developer should then conduct an appropriate level of software regression testing to show that unchanged but vulnerable portions of the system have not been adversely affected. Design controls and appropriate regression testing provide the confidence that the software is validated after a software change.

4.8. Validation coverage

Validation coverage should be based on the software’s complexity and safety risk – not on firm size or resource constraints. The selection of validation activities, tasks, and work items should be commensurate with the complexity of the software design and the risk associated with the use of the software for the specified intended use. For lower risk devices, only baseline validation activities may be conducted. As the risk increases additional validation activities should be added to cover the additional risk. Validation documentation should be sufficient to demonstrate that all software validation plans and procedures have been completed successfully.

4.9. Independence of review

Validation activities should be conducted using the basic quality assurance precept of “independence of review.” Self-validation is extremely difficult. When possible, an independent evaluation is always better, especially for higher risk applications. Some firms contract out for a third-party independent verification and validation, but this solution may not always be feasible. Another approach is to assign internal staff members that are not involved in a particular design or its implementation, but who have sufficient knowledge to evaluate the project and conduct the verification and validation activities. Smaller firms may need to be creative in how tasks are organized and assigned in order to maintain internal independence of review.

4.10. Flexibility and responsibility

Specific implementation of these software validation principles may be quite different from one application to another. The device manufacturer has flexibility in choosing how to apply these validation principles, but retains ultimate responsibility for demonstrating that the software has been validated.

Software is designed, developed, validated, and regulated in a wide spectrum of environments, and for a wide variety of devices with varying levels of risk. FDA regulated medical device applications include software that:

- Is a component, part, or accessory of a medical device;
- Is itself a medical device; or
- Is used in manufacturing, design and development, or other parts of the quality system.

In each environment, software components from many sources may be used to create the application (e.g., in-house developed software, off-the-shelf software, contract software, shareware). In addition, software components come in many different forms (e.g., application software, operating systems, compilers, debuggers, configuration management tools, and many more). The validation of software in these environments can be a complex undertaking; therefore, it is appropriate that all of these software validation principles be considered when designing the software validation process. The resultant software validation process should be commensurate with the safety risk associated with the system, device, or process.

Software validation activities and tasks may be dispersed, occurring at different locations and being conducted by different organizations. However, regardless of the distribution of tasks, contractual relations, source of components, or the development environment, the device manufacturer or specification developer retains ultimate responsibility for ensuring that the software is validated.

Section 5. Activities and tasks

Software validation is accomplished through a series of activities and tasks that are planned and executed at various stages of the software development life cycle. These tasks may be one time occurrences or may be iterated many times, depending on the life cycle model used and the scope of changes made as the software project progresses.

5.1. Software life cycle activities

This guidance does not recommend the use of any specific software life cycle model. Software developers should establish a software life cycle model that is appropriate for their product and organization. The software life cycle model that is selected should cover the software from its birth to its retirement. Activities in a typical software life cycle model include the following:

- Quality Planning
- System Requirements Definition
- Detailed Software Requirements Specification
- Software Design Specification
- Construction or Coding
- Testing
- Installation
- Operation and Support
- Maintenance
- Retirement

Verification, testing, and other tasks that support software validation occur during each of these activities. A life cycle model organizes these software development activities in various ways and provides a framework for monitoring and controlling the software development project. Several software life cycle models (e.g., waterfall, spiral, rapid prototyping, incremental development, etc.) are defined in FDA's *Glossary of Computerized System and Software Development Terminology* [available at: http://www.fda.gov/ora/inspect_ref/igs/gloss.html], dated August 1995. These and many other life cycle models are described in various references listed in "Appendix A - References" on page 426.

5.2. Typical tasks supporting validation

For each of the software life cycle activities, there are certain "typical" tasks that support a conclusion that the software is validated. However, the specific tasks to be performed, their order of performance, and the iteration and timing of their performance will be dictated by the specific software life cycle model that is selected and the safety risk associated with the software application. For very low risk applications, certain tasks may not be needed at all. However, the software developer should at least consider each of these tasks and should define and document which tasks are or are not appropriate for their specific application. The following discussion is generic and is not intended to prescribe any particular software life cycle model or any particular order in which tasks are to be performed.

5.2.1. Quality planning

Design and development planning should culminate in a plan that identifies necessary tasks, procedures for anomaly reporting and resolution, necessary resources, and management review requirements, including formal design reviews. A software life cycle model and associated activities should be identified, as well as those tasks necessary for each software life cycle activity. The plan should include:

- The specific tasks for each life cycle activity;
- Enumeration of important quality factors (e.g., reliability, maintainability, and usability);
- Methods and procedures for each task;
- Task acceptance criteria;
- Criteria for defining and documenting outputs in terms that will allow evaluation of their conformance to input requirements;
- Inputs for each task;
- Outputs from each task;
- Roles, resources, and responsibilities for each task;
- Risks and assumptions; and
- Documentation of user needs.

Management must identify and provide the appropriate software development environment and resources. (See 21 CFR §820.20(b)(1) and (2).) Typically, each task requires personnel as well as physical resources. The plan should identify the personnel, the facility and equipment resources for each task, and the role that risk (hazard) management will play. A configuration management plan should be developed that will guide and control multiple parallel development activities and ensure proper communications and documentation. Controls are necessary to ensure positive and correct correspondence among all approved versions of the specifications documents, source code, object code, and test suites that comprise a software system. The controls also should ensure accurate identification of, and access to, the currently approved versions.

Procedures should be created for reporting and resolving software anomalies found through validation or other activities. Management should identify the reports and specify the contents, format, and responsible organizational elements for each report. Procedures also are necessary for the review and approval of software development results, including the responsible organizational elements for such reviews and approvals.

Typical tasks – Quality planning

- Risk (Hazard) Management Plan
- Configuration Management Plan
- Software Quality Assurance Plan
  - Software Verification and Validation Plan
    - Verification and Validation Tasks, and Acceptance Criteria
    - Schedule and Resource Allocation (for software verification and validation activities)
    - Reporting Requirements
  - Formal Design Review Requirements
  - Other Technical Review Requirements
- Problem Reporting and Resolution Procedures
- Other Support Activities

5.2.2. Requirements

Requirements development includes the identification, analysis, and documentation of information about the device and its intended use. Areas of special importance include allocation of system functions to hardware/software, operating conditions, user characteristics, potential hazards, and anticipated tasks. In addition, the requirements should state clearly the intended use of the software.

The software requirements specification document should contain a written definition of the software functions. It is not possible to validate software without predetermined and documented software requirements. Typical software requirements specify the following:

- All software system inputs;
- All software system outputs;
- All functions that the software system will perform;
- All performance requirements that the software will meet, (e.g., data throughput, reliability, and timing);
- The definition of all external and user interfaces, as well as any internal software-to-system interfaces;
- How users will interact with the system;
- What constitutes an error and how errors should be handled;
- Required response times;
- The intended operating environment for the software, if this is a design constraint (e.g., hardware platform, operating system);
- All ranges, limits, defaults, and specific values that the software will accept; and
- All safety related requirements, specifications, features, or functions that will be implemented in software.

Software safety requirements are derived from a technical risk management process that is closely integrated with the system requirements development process. Software requirement specifications should identify clearly the potential hazards that can result from a software failure in the system as well as any safety requirements to be implemented in software. The consequences of software failure should be evaluated, along with means of mitigating such failures (e.g., hardware mitigation, defensive programming, etc.). From this analysis, it should be possible to identify the most appropriate measures necessary to prevent harm.

The Quality System regulation requires a mechanism for addressing incomplete, ambiguous, or conflicting requirements. (See 21 CFR 820.30(c).) Each requirement (e.g., hardware, software, user, operator interface, and safety) identified in the software requirements specification should be evaluated for accuracy, completeness, consistency, testability, correctness, and clarity. For example, software requirements should be evaluated to verify that:

- There are no internal inconsistencies among requirements;
- All of the performance requirements for the system have been spelled out;
- Fault tolerance, safety, and security requirements are complete and correct;
- Allocation of software functions is accurate and complete;
- Software requirements are appropriate for the system hazards; and
- All requirements are expressed in terms that are measurable or objectively verifiable.

A software requirements traceability analysis should be conducted to trace software requirements to (and from) system requirements and to risk analysis results. In addition to any other analyses and documentation used to verify software requirements, a formal design review is recommended to confirm that requirements are fully specified and appropriate before extensive software design efforts begin. Requirements can be approved and released incrementally, but care should be taken that interactions and interfaces among software (and hardware) requirements are properly reviewed, analyzed, and controlled.

Typical tasks – Requirements

- Preliminary Risk Analysis
- Traceability Analysis
  - Software Requirements to System Requirements (and vice versa)
  - Software Requirements to Risk Analysis
- Description of User Characteristics
- Listing of Characteristics and Limitations of Primary and Secondary Memory
- Software Requirements Evaluation
- Software User Interface Requirements Analysis
- System Test Plan Generation
- Acceptance Test Plan Generation
- Ambiguity Review or Analysis

5.2.3. Design

In the design process, the software requirements specification is translated into a logical and physical representation of the software to be implemented. The software design specification is a description of what the software should do and how it should do it. Due to complexity of the project or to enable persons with varying levels of technical responsibilities to clearly understand design information, the design specification may contain both a high level summary of the design and detailed design information. The completed software design specification constrains the programmer/coder to stay within the intent of the agreed upon requirements and design. A complete software design specification will relieve the programmer from the need to make ad hoc design decisions.

The software design needs to address human factors. Use error caused by designs that are either overly complex or contrary to users' intuitive expectations for operation is one of the most persistent and critical problems encountered by FDA. Frequently, the design of the software is a factor in such use errors. Human factors engineering should be woven into the entire design and development process, including the device design requirements, analyses, and tests. Device safety and usability issues should be considered when developing flowcharts, state diagrams, prototyping tools, and test plans. Also, task and function analyses, risk analyses, prototype tests and reviews, and full usability tests should be performed. Participants from the user population should be included when applying these methodologies.

The software design specification should include:

- Software requirements specification, including predetermined criteria for acceptance of the software;
- Software risk analysis;
- Development procedures and coding guidelines (or other programming procedures);
- Systems documentation (e.g., a narrative or a context diagram) that describes the systems context in which the program is intended to function, including the relationship of hardware, software, and the physical environment;
- Hardware to be used;
- Parameters to be measured or recorded;
- Logical structure (including control logic) and logical processing steps (e.g., algorithms);
- Data structures and data flow diagrams;
- Definitions of variables (control and data) and description of where they are used;
- Error, alarm, and warning messages;
- Supporting software (e.g., operating systems, drivers, other application software);
- Communication links (links among internal modules of the software, links with the supporting software, links with the hardware, and links with the user);
- Security measures (both physical and logical security); and
- Any additional constraints not identified in the above elements.

The first four of the elements noted above usually are separate pre-existing documents that are included by reference in the software design specification. Software requirements specification was discussed in the preceding section, as was software risk analysis. Written development procedures serve as a guide to the organization, and written programming procedures serve as a guide to individual programmers. As software cannot be validated without knowledge of the context in which it is intended to function, systems documentation is referenced. If some of the above elements are not included in the software, it may be helpful to future reviewers and maintainers of the software if that is clearly stated (e.g., There are no error messages in this program).

The activities that occur during software design have several purposes. Software design evaluations are conducted to determine if the design is complete, correct, consistent, unambiguous, feasible, and maintainable. Appropriate consideration of software architecture (e.g., modular structure) during design can reduce the magnitude of future validation efforts when software changes are needed. Software design evaluations may include analyses of control flow, data flow, complexity, timing, sizing, memory allocation, criticality analysis, and many other aspects of the design. A traceability analysis should be conducted to verify that the software design implements all of the software requirements. As a technique for identifying where requirements are not sufficient, the traceability analysis should also verify that all aspects of the design are traceable to software requirements. An analysis of communication links should be conducted to evaluate the proposed design with respect to hardware, user, and related software requirements. The software risk analysis should be re-examined to determine whether any additional hazards have been identified and whether any new hazards have been introduced by the design.

At the end of the software design activity, a Formal Design Review should be conducted to verify that the design is correct, consistent, complete, accurate, and testable, before moving to implement the design. Portions of the design can be approved and released incrementally for implementation; but care should be taken that interactions and communication links among various elements are properly reviewed, analyzed, and controlled.

Most software development models will be iterative. This is likely to result in several versions of both the software requirement specification and the software design specification. All approved versions should be archived and controlled in accordance with established configuration management procedures.

Typical tasks – Design

- Updated Software Risk Analysis
- Traceability Analysis - Design Specification to Software Requirements (and vice versa)
- Software Design Evaluation
- Design Communication Link Analysis
- Module Test Plan Generation
- Integration Test Plan Generation
- Test Design Generation (module, integration, system, and acceptance)

5.2.4. Construction or coding

Software may be constructed either by coding (i.e., programming) or by assembling together previously coded software components (e.g., from code libraries, off-the-shelf software, etc.) for use in a new application. Coding is the software activity where the detailed design specification is implemented as source code. Coding is the lowest level of abstraction for the software development process. It is the last stage in decomposition of the software requirements where module specifications are translated into a programming language.

Coding usually involves the use of a high-level programming language, but may also entail the use of assembly language (or microcode) for time-critical operations. The source code may be either compiled or interpreted for use on a target hardware platform. Decisions on the selection of programming languages and software build tools (assemblers, linkers, and compilers) should include consideration of the impact on subsequent quality evaluation tasks (e.g., availability of debugging and testing tools for the chosen language). Some compilers offer optional levels and commands for error checking to assist in debugging the code. Different levels of error checking may be used throughout the coding process, and warnings or other messages from the compiler may or may not be recorded. However, at the end of the coding and debugging process, the most rigorous level of error checking is normally used to document what compilation errors still remain in the software. If the most rigorous level of error checking is not used for final translation of the source code, then justification for use of the less rigorous translation error checking should be documented. Also, for the final compilation, there should be documentation of the compilation process and its outcome, including any warnings or other messages from the compiler and their resolution, or justification for the decision to leave issues unresolved.

Firms frequently adopt specific coding guidelines that establish quality policies and procedures related to the software coding process. Source code should be evaluated to verify its compliance with specified coding guidelines. Such guidelines should include coding conventions regarding clarity, style, complexity management, and commenting. Code comments should provide useful and descriptive information for a module, including expected inputs and outputs, variables referenced, expected data types, and operations to be performed. Source code should also be evaluated to verify its compliance with the corresponding detailed design specification. Modules ready for integration and test should have documentation of compliance with coding guidelines and any other applicable quality policies and procedures.

Source code evaluations are often implemented as code inspections and code walkthroughs. Such static analyses provide a very effective means to detect errors before execution of the code. They allow for examination of each error in isolation and can also help in focusing later dynamic testing of the software. Firms may use manual (desk) checking with appropriate controls to ensure consistency and independence. Source code evaluations should be extended to verification of internal linkages between modules and layers (horizontal and vertical interfaces), and compliance with their design specifications. Documentation of the procedures used and the results of source code evaluations should be maintained as part of design verification.

A source code traceability analysis is an important tool to verify that all code is linked to established specifications and established test procedures. A source code traceability analysis should be conducted and documented to verify that:

- Each element of the software design specification has been implemented in code;
- Modules and functions implemented in code can be traced back to an element in the software design specification and to the risk analysis;
- Tests for modules and functions can be traced back to an element in the software design specification and to the risk analysis; and
- Tests for modules and functions can be traced to source code for the same modules and functions.

Typical tasks – Construction or coding

- Traceability Analyses
  - Source Code to Design Specification (and vice versa)
  - Test Cases to Source Code and to Design Specification
- Source Code and Source Code Documentation Evaluation
- Source Code Interface Analysis
- Test Procedure and Test Case Generation (module, integration, system, and acceptance)

5.2.5. Testing by the software developer

Software testing entails running software products under known conditions with defined inputs and documented outcomes that can be compared to their predefined expectations. It is a time consuming, difficult, and imperfect activity. As such, it requires early planning in order to be effective and efficient.

Test plans and test cases should be created as early in the software development process as feasible. They should identify the schedules, environments, resources (personnel, tools, etc.), methodologies, cases (inputs, procedures, outputs, expected results), documentation, and reporting criteria. The magnitude of effort to be applied throughout the testing process can be linked to complexity, criticality, reliability, and/or safety issues (e.g., requiring functions or modules that produce critical outcomes to be challenged with intensive testing of their fault tolerance features). Descriptions of categories of software and software testing effort appear in the literature, for example:

- NIST Special Publication 500-235, *Structured Testing: A Testing Methodology Using the Cyclomatic Complexity Metric*;

- NUREG/CR-6293, *Verification and Validation Guidelines for High Integrity Systems*; and
- IEEE Computer Society Press, *Handbook of Software Reliability Engineering*.

Software test plans should identify the particular tasks to be conducted at each stage of development and include justification of the level of effort represented by their corresponding completion criteria.

Software testing has limitations that must be recognized and considered when planning the testing of a particular software product. Except for the simplest of programs, software cannot be exhaustively tested. Generally it is not feasible to test a software product with all possible inputs, nor is it possible to test all possible data processing paths that can occur during program execution. There is no one type of testing or testing methodology that can ensure a particular software product has been thoroughly tested. Testing of all program functionality does not mean all of the program has been tested. Testing of all of a program's code does not mean all necessary functionality is present in the program. Testing of all program functionality and all program code does not mean the program is 100% correct! Software testing that finds no errors should not be interpreted to mean that errors do not exist in the software product; it may mean the testing was superficial.

An essential element of a software test case is the expected result. It is the key detail that permits objective evaluation of the actual test result. This necessary testing information is obtained from the corresponding, predefined definition or specification. A software specification document must identify what, when, how, why, etc., is to be achieved with an engineering (i.e., measurable or objectively verifiable) level of detail in order for it to be confirmed through testing. The real effort of effective software testing lies in the definition of what is to be tested rather than in the performance of the test.

A software testing process should be based on principles that foster effective examinations of a software product. Applicable software testing tenets include:

- The expected test outcome is predefined;
- A good test case has a high probability of exposing an error;
- A successful test is one that finds an error;
- There is independence from coding;
- Both application (user) and software (programming) expertise are employed;
- Testers use different tools from coders;
- Examining only the usual case is insufficient;
- Test documentation permits its reuse and an independent confirmation of the pass/fail status of a test outcome during subsequent review.

Once the prerequisite tasks (e.g., code inspection) have been successfully completed, software testing begins. It starts with unit level testing and concludes with system level testing. There may be a distinct integration level of testing. A software product should be challenged with test cases based on its internal structure and with test cases based on its external specification. These tests should provide a thorough and rigorous examination of the software product's compliance with its functional, performance, and interface definitions and requirements.

Code-based testing is also known as structural testing or “white-box” testing. It identifies test cases based on knowledge obtained from the source code, detailed design specification, and other development documents. These test cases challenge the control decisions made by the program; and the program's data structures including configuration tables. Structural testing can identify “dead” code that is never executed when the program is run. Structural testing is accomplished primarily with unit (module) level testing, but can be extended to other levels of software testing.

The level of structural testing can be evaluated using metrics that are designed to show what percentage of the software structure has been evaluated during structural testing. These metrics are typically referred to as “coverage” and are a measure of completeness with respect to test selection criteria. The amount of structural coverage should be commensurate with the level of risk posed by the software. Use of the term “coverage” usually means 100% coverage. For example, if a testing program has achieved “statement coverage,” it means that 100% of the statements in the software have been executed at least once. Common structural coverage metrics include:

- **Statement Coverage** – This criteria requires sufficient test cases for each program statement to be executed at least once; however, its achievement is insufficient to provide confidence in a software product's behavior.
- **Decision (Branch) Coverage** – This criteria requires sufficient test cases for each program decision or branch to be executed so that each possible outcome occurs at least once. It is considered to be a minimum level of coverage for most software products, but decision coverage alone is insufficient for high-integrity applications.
- **Condition Coverage** – This criteria requires sufficient test cases for each condition in a program decision to take on all possible outcomes at least once. It differs from branch coverage only when multiple conditions must be evaluated to reach a decision.
- **Multi-Condition Coverage** – This criteria requires sufficient test cases to exercise all possible combinations of conditions in a program decision.
- **Loop Coverage** – This criteria requires sufficient test cases for all program loops to be executed for zero, one, two, and many iterations covering initialization, typical running and termination (boundary) conditions.
- **Path Coverage** – This criteria requires sufficient test cases for each feasible path, basis path, etc., from start to exit of a defined program segment, to be executed at least once. Because of the very large number of possible paths through a software program, path coverage is generally not achievable. The amount of path coverage is normally established based on the risk or criticality of the software under test.
- **Data Flow Coverage** – This criteria requires sufficient test cases for each feasible data flow to be executed at least once. A number of data flow testing strategies are available.

Definition-based or specification-based testing is also known as functional testing or “black-box” testing. It identifies test cases based on the definition of what the software product (whether it be a unit (module) or a complete program) is intended to do. These test cases challenge the intended use or functionality of a program, and the program's internal and external interfaces. Functional testing can be applied at all levels of software testing, from unit to system level testing.

The following types of functional software testing involve generally increasing levels of effort:

- **Normal Case** – Testing with usual inputs is necessary. However, testing a software product only with expected, valid inputs does not thoroughly test that software product. By itself, normal case testing cannot provide sufficient confidence in the dependability of the software product.
- **Output Forcing** – Choosing test inputs to ensure that selected (or all) software outputs are generated by testing.
- **Robustness** – Software testing should demonstrate that a software product behaves correctly when given unexpected, invalid inputs. Methods for identifying a sufficient set of such test cases include Equivalence Class Partitioning, Boundary Value Analysis, and Special Case Identification (Error Guessing). While important and necessary, these

techniques do not ensure that all of the most appropriate challenges to a software product have been identified for testing.

- **Combinations of Inputs** – The functional testing methods identified above all emphasize individual or single test inputs. Most software products operate with multiple inputs under their conditions of use. Thorough software product testing should consider the combinations of inputs a software unit or system may encounter during operation. Error guessing can be extended to identify combinations of inputs, but it is an ad hoc technique. Cause-effect graphing is one functional software testing technique that systematically identifies combinations of inputs to a software product for inclusion in test cases.

Functional and structural software test case identification techniques provide specific inputs for testing, rather than random test inputs. One weakness of these techniques is the difficulty in linking structural and functional test completion criteria to a software product's reliability. Advanced software testing methods, such as statistical testing, can be employed to provide further assurance that a software product is dependable. Statistical testing uses randomly generated test data from defined distributions based on an operational profile (e.g., expected use, hazardous use, or malicious use of the software product). Large amounts of test data are generated and can be targeted to cover particular areas or concerns, providing an increased possibility of identifying individual and multiple rare operating conditions that were not anticipated by either the software product's designers or its testers. Statistical testing also provides high structural coverage. It does require a stable software product. Thus, structural and functional testing are prerequisites for statistical testing of a software product.

Another aspect of software testing is the testing of software changes. Changes occur frequently during software development. These changes are the result of 1) debugging that finds an error and it is corrected, 2) new or changed requirements (“requirements creep”), and 3) modified designs as more effective or efficient implementations are found. Once a software product has been baselined (approved), any change to that product should have its own “mini life cycle,” including testing. Testing of a changed software product requires additional effort. Not only should it demonstrate that the change was implemented correctly, testing should also demonstrate that the change did not adversely impact other parts of the software product. Regression analysis and testing are employed to provide assurance that a change has not created problems elsewhere in the software product. Regression analysis is the determination of the impact of a change based on review of the relevant documentation (e.g., software requirements specification, software design specification, source code, test plans, test cases, test scripts, etc.) in order to identify the necessary regression tests to be run. Regression testing is the rerunning of test cases that a program has previously executed correctly and comparing the current result to the previous result in order to detect unintended effects of a software change. Regression analysis and regression testing should also be employed when using integration methods to build a software product to ensure that newly integrated modules do not adversely impact the operation of previously integrated modules.

In order to provide a thorough and rigorous examination of a software product, development testing is typically organized into levels. As an example, a software product's testing can be organized into unit, integration, and system levels of testing.

1. Unit (module or component) level testing focuses on the early examination of sub-program functionality and ensures that functionality not visible at the system level is examined by testing. Unit testing ensures that quality software units are furnished for integration into the finished software product.
2. Integration level testing focuses on the transfer of data and control across a program's internal and external interfaces. External interfaces are those with other software (including operating system software), system hardware, and the users and can be described as communications links.

3. System level testing demonstrates that all specified functionality exists and that the software product is trustworthy. This testing verifies the as-built program's functionality and performance with respect to the requirements for the software product as exhibited on the specified operating platform(s). System level software testing addresses functional concerns and the following elements of a device's software that are related to the intended use(s):
   - Performance issues (e.g., response times, reliability measurements);
   - Responses to stress conditions, e.g., behavior under maximum load, continuous use;
   - Operation of internal and external security features;
   - Effectiveness of recovery procedures, including disaster recovery;
   - Usability;
   - Compatibility with other software products;
   - Behavior in each of the defined hardware configurations; and
   - Accuracy of documentation.

Control measures (e.g., a traceability analysis) should be used to ensure that the intended coverage is achieved.

System level testing also exhibits the software product's behavior in the intended operating environment. The location of such testing is dependent upon the software developer's ability to produce the target operating environment(s). Depending upon the circumstances, simulation and/or testing at (potential) customer locations may be utilized. Test plans should identify the controls needed to ensure that the intended coverage is achieved and that proper documentation is prepared when planned system level testing is conducted at sites not directly controlled by the software developer. Also, for a software product that is a medical device or a component of a medical device that is to be used on humans prior to FDA clearance, testing involving human subjects may require an Investigational Device Exemption (IDE) or Institutional Review Board (IRB) approval.

Test procedures, test data, and test results should be documented in a manner permitting objective pass/fail decisions to be reached. They should also be suitable for review and objective decision making subsequent to running the test, and they should be suitable for use in any subsequent regression testing. Errors detected during testing should be logged, classified, reviewed, and resolved prior to release of the software. Software error data that is collected and analyzed during a development life cycle may be used to determine the suitability of the software product for release for commercial distribution. Test reports should comply with the requirements of the corresponding test plans.

Software products that perform useful functions in medical devices or their production are often complex. Software testing tools are frequently used to ensure consistency, thoroughness, and efficiency in the testing of such software products and to fulfill the requirements of the planned testing activities. These tools may include supporting software built in-house to facilitate unit (module) testing and subsequent integration testing (e.g., drivers and stubs) as well as commercial software testing tools. Such tools should have a degree of quality no less than the software product they are used to develop. Appropriate documentation providing evidence of the validation of these software tools for their intended use should be maintained (see section 6 of this guidance).

Typical tasks – Testing by the software developer

- Test Planning
- Structural Test Case Identification

- Functional Test Case Identification
- Traceability Analysis - Testing
  - Unit (Module) Tests to Detailed Design
  - Integration Tests to High Level Design
  - System Tests to Software Requirements
- Unit (Module) Test Execution
- Integration Test Execution
- Functional Test Execution
- System Test Execution
- Acceptance Test Execution
- Test Results Evaluation
- Error Evaluation/Resolution
- Final Test Report

5.2.6. User site testing

Testing at the user site is an essential part of software validation. The Quality System regulation requires installation and inspection procedures (including testing where appropriate) as well as documentation of inspection and testing to demonstrate proper installation. (See 21 CFR §820.170.) Likewise, manufacturing equipment must meet specified requirements, and automated systems must be validated for their intended use. (See 21 CFR §820.70(g) and 21 CFR §820.70(i) respectively.)

Terminology regarding user site testing can be confusing. Terms such as beta test, site validation, user acceptance test, installation verification, and installation testing have all been used to describe user site testing. For purposes of this guidance, the term “user site testing” encompasses all of these and any other testing that takes place outside of the developer’s controlled environment. This testing should take place at a user's site with the actual hardware and software that will be part of the installed system configuration. The testing is accomplished through either actual or simulated use of the software being tested within the context in which it is intended to function.

Guidance contained here is general in nature and is applicable to any user site testing. However, in some areas (e.g., blood establishment systems) there may be specific site validation issues that need to be considered in the planning of user site testing. Test planners should check with the FDA Center(s) with the corresponding product jurisdiction to determine whether there are any additional regulatory requirements for user site testing.

User site testing should follow a pre-defined written plan with a formal summary of testing and a record of formal acceptance. Documented evidence of all testing procedures, test input data, and test results should be retained.

There should be evidence that hardware and software are installed and configured as specified. Measures should ensure that all system components are exercised during the testing and that the versions of these components are those specified. The testing plan should specify testing throughout the full range of operating conditions and should specify continuation for a sufficient time to allow the system to encounter a wide spectrum of conditions and events in an effort to detect any latent faults that are not apparent during more normal activities.

Some of the evaluations that have been performed earlier by the software developer at the developer's site should be repeated at the site of actual use. These may include tests for a high volume of data, heavy loads or stresses, security, fault testing (avoidance, detection, tolerance, and recovery), error messages, and implementation of safety requirements. The developer may be able to furnish the user with some of the test data sets to be used for this purpose.

In addition to an evaluation of the system's ability to properly perform its intended functions, there should be an evaluation of the ability of the users of the system to understand and correctly interface with it. Operators should be able to perform the intended functions and respond in an appropriate and timely manner to all alarms, warnings, and error messages.

During user site testing, records should be maintained of both proper system performance and any system failures that are encountered. The revision of the system to compensate for faults detected during this user site testing should follow the same procedures and controls as for any other software change.

The developers of the software may or may not be involved in the user site testing. If the developers are involved, they may seamlessly carry over to the user's site the last portions of design-level systems testing. If the developers are not involved, it is all the more important that the user have persons who understand the importance of careful test planning, the definition of expected test results, and the recording of all test outputs.

Typical tasks – User site testing

- Acceptance Test Execution
- Test Results Evaluation
- Error Evaluation/Resolution
- Final Test Report

5.2.7. Maintenance and software changes

As applied to software, the term maintenance does not mean the same as when applied to hardware. The operational maintenance of hardware and software are different because their failure/error mechanisms are different. Hardware maintenance typically includes preventive hardware maintenance actions, component replacement, and corrective changes. Software maintenance includes corrective, perfective, and adaptive maintenance but does not include preventive maintenance actions or software component replacement.

Changes made to correct errors and faults in the software are corrective maintenance. Changes made to the software to improve the performance, maintainability, or other attributes of the software system are perfective maintenance. Software changes to make the software system usable in a changed environment are adaptive maintenance.

When changes are made to a software system, either during initial development or during post release maintenance, sufficient regression analysis and testing should be conducted to demonstrate that portions of the software not involved in the change were not adversely impacted. This is in addition to testing that evaluates the correctness of the implemented change(s).

The specific validation effort necessary for each software change is determined by the type of change, the development products affected, and the impact of those products on the operation of the software. Careful and complete documentation of the design structure and interrelationships of various modules, interfaces, etc., can limit the validation effort needed when a change is made. The level of effort needed to fully validate a change is also dependent upon the degree to which validation of the original software was documented and archived. For example, test documentation, test cases, and results of previous verification and validation testing need to be archived if they are to be available for performing subsequent regression testing. Failure to archive this information for later use can significantly increase the level of effort and expense of revalidating the software after a change is made.

In addition to software verification and validation tasks that are part of the standard software development process, the following additional maintenance tasks should be addressed:

- **Software Validation Plan Revision** - For software that was previously validated, the existing software validation plan should be revised to support the validation of the revised software. If no previous software validation plan exists, such a plan should be established to support the validation of the revised software.
- **Anomaly Evaluation** – Software organizations frequently maintain documentation, such as software problem reports that describe software anomalies discovered and the specific corrective action taken to fix each anomaly. Too often, however, mistakes are repeated because software developers do not take the next step to determine the root causes of problems and make the process and procedural changes needed to avoid recurrence of the problem. Software anomalies should be evaluated in terms of their severity and their effects on system operation and safety, but they should also be treated as symptoms of process deficiencies in the quality system. A root cause analysis of anomalies can identify specific quality system deficiencies. Where trends are identified (e.g., recurrence of similar software anomalies), appropriate corrective and preventive actions must be implemented and documented to avoid further recurrence of similar quality problems. (See 21 CFR 820.100.)
- **Problem Identification and Resolution Tracking** - All problems discovered during maintenance of the software should be documented. The resolution of each problem should be tracked to ensure it is fixed, for historical reference, and for trending.
- **Proposed Change Assessment** - All proposed modifications, enhancements, or additions should be assessed to determine the effect each change would have on the system. This information should determine the extent to which verification and/or validation tasks need to be iterated.
- **Task Iteration** - For approved software changes, all necessary verification and validation tasks should be performed to ensure that planned changes are implemented correctly, all documentation is complete and up to date, and no unacceptable changes have occurred in software performance.
- **Documentation Updating** – Documentation should be carefully reviewed to determine which documents have been impacted by a change. All approved documents (e.g., specifications, test procedures, user manuals, etc.) that have been affected should be updated in accordance with configuration management procedures. Specifications should be updated before any maintenance and software changes are made.

Section 6. Validation of automated process equipment and quality system software

The Quality System regulation requires that “when computers or automated data processing systems are used as part of production or the quality system, the [device] manufacturer shall validate computer software for its intended use according to an established protocol.” (See 21 CFR §820.70(i)). This has been a regulatory requirement of FDA’s medical device Good Manufacturing Practice (GMP) regulations since 1978.

In addition to the above validation requirement, computer systems that implement part of a device manufacturer’s production processes or quality system (or that are used to create and maintain records required by any other FDA regulation) are subject to the Electronic Records; Electronic Signatures regulation. (See 21 CFR Part 11.) This regulation establishes additional security, data integrity, and validation requirements when records are created or maintained electronically. These additional Part 11 requirements should be carefully considered and included in system requirements and software requirements for any automated record `keeping systems. System validation and software validation should demonstrate that all Part 11 requirements have been met.

Computers and automated equipment are used extensively throughout all aspects of medical device design, laboratory testing and analysis, product inspection and acceptance, production and process control, environmental controls, packaging, labeling, traceability, document control, complaint management, and many other aspects of the quality system. Increasingly, automated plant floor operations can involve extensive use of embedded systems in:

- Programmable logic controllers;
- Digital function controllers;
- Statistical process control;
- Supervisory control and data acquisition;
- Robotics;
- Human-machine interfaces;
- Input/output devices; and
- Computer operating systems.

Software tools are frequently used to design, build, and test the software that goes into an automated medical device. Many other commercial software applications, such as word processors, spreadsheets, databases, and flowcharting software are used to implement the quality system. All of these applications are subject to the requirement for software validation, but the validation approach used for each application can vary widely.

Whether production or quality system software is developed in-house by the device manufacturer, developed by a contractor, or purchased off-the-shelf, it should be developed using the basic principles outlined elsewhere in this guidance. The device manufacturer has latitude and flexibility in defining how validation of that software will be accomplished, but validation should be a key consideration in deciding how and by whom the software will be developed or from whom it will be purchased. The software developer defines a life cycle model. Validation is typically supported by:

- Verifications of the outputs from each stage of that software development life cycle; and
- Checking for proper operation of the finished software in the device manufacturer's intended use environment.

6.1. How much validation evidence is needed

The level of validation effort should be commensurate with the risk posed by the automated operation. In addition to risk other factors, such as the complexity of the process software and the degree to which the device manufacturer is dependent upon that automated process to produce a safe and effective device, determine the nature and extent of testing needed as part of the validation effort. Documented requirements and risk analysis of the automated process help to define the scope of the evidence needed to show that the software is validated for its intended use. For example, an automated milling machine may require very little testing if the device manufacturer can show that the output of the operation is subsequently fully verified against the specification before release. On the other hand, extensive testing may be needed for:

- A plant-wide electronic record and electronic signature system;
- An automated controller for a sterilization cycle; or

- Automated test equipment used for inspection and acceptance of finished circuit boards in a life-sustaining/life-supporting device.

Numerous commercial software applications may be used as part of the quality system (e.g., a spreadsheet or statistical package used for quality system calculations, a graphics package used for trend analysis, or a commercial database used for recording device history records or for complaint management). The extent of validation evidence needed for such software depends on the device manufacturer's documented intended use of that software. For example, a device manufacturer who chooses not to use all the vendor-supplied capabilities of the software only needs to validate those functions that will be used and for which the device manufacturer is dependent upon the software results as part of production or the quality system. However, high risk applications should not be running in the same operating environment with non-validated software functions, even if those software functions are not used. Risk mitigation techniques such as memory partitioning or other approaches to resource protection may need to be considered when high risk applications and lower risk applications are to be used in the same operating environment. When software is upgraded or any changes are made to the software, the device manufacturer should consider how those changes may impact the "used portions" of the software and must reconfirm the validation of those portions of the software that are used. (See 21 CFR §820.70(i).)

6.2. Defined user requirements

A very important key to software validation is a documented user requirements specification that defines:

- The "intended use" of the software or automated equipment; and
- The extent to which the device manufacturer is dependent upon that software or equipment for production of a quality medical device.

The device manufacturer (user) needs to define the expected operating environment including any required hardware and software configurations, software versions, utilities, etc. The user also needs to:

- Document requirements for system performance, quality, error handling, startup, shutdown, security, etc.;
- Identify any safety related functions or features, such as sensors, alarms, interlocks, logical processing steps, or command sequences; and
- Define objective criteria for determining acceptable performance.

The validation must be conducted in accordance with a documented protocol, and the validation results must also be documented. (See 21 CFR §820.70(i).) Test cases should be documented that will exercise the system to challenge its performance against the pre-determined criteria, especially for its most critical parameters. Test cases should address error and alarm conditions, startup, shutdown, all applicable user functions and operator controls, potential operator errors, maximum and minimum ranges of allowed values, and stress conditions applicable to the intended use of the equipment. The test cases should be executed and the results should be recorded and evaluated to determine whether the results support a conclusion that the software is validated for its intended use.

A device manufacturer may conduct a validation using their own personnel or may depend on a third party such as the equipment/software vendor or a consultant. In any case, the device manufacturer retains the ultimate responsibility for ensuring that the production and quality system software:

- Is validated according to a written procedure for the particular intended use; and
- Will perform as intended in the chosen application.

The device manufacturer should have documentation including:

- Defined user requirements;
- Validation protocol used;
- Acceptance criteria;
- Test cases and results; and
- A validation summary

that objectively confirms that the software is validated for its intended use.

6.3. Validation of off-the-shelf software and automated equipment

Most of the automated equipment and systems used by device manufacturers are supplied by third-party vendors and are purchased off-the-shelf (OTS). The device manufacturer is responsible for ensuring that the product development methodologies used by the OTS software developer are appropriate and sufficient for the device manufacturer's intended use of that OTS software. For OTS software and equipment, the device manufacturer may or may not have access to the vendor's software validation documentation. If the vendor can provide information about their system requirements, software requirements, validation process, and the results of their validation, the medical device manufacturer can use that information as a beginning point for their required validation documentation. The vendor's life cycle documentation, such as testing protocols and results, source code, design specification, and requirements specification, can be useful in establishing that the software has been validated. However, such documentation is frequently not available from commercial equipment vendors, or the vendor may refuse to share their proprietary information.

Where possible and depending upon the device risk involved, the device manufacturer should consider auditing the vendor's design and development methodologies used in the construction of the OTS software and should assess the development and validation documentation generated for the OTS software. Such audits can be conducted by the device manufacturer or by a qualified third party. The audit should demonstrate that the vendor's procedures for and results of the verification and validation activities performed the OTS software are appropriate and sufficient for the safety and effectiveness requirements of the medical device to be produced using that software.

Some vendors who are not accustomed to operating in a regulated environment may not have a documented life cycle process that can support the device manufacturer's validation requirement. Other vendors may not permit an audit. Where necessary validation information is not available from the vendor, the device manufacturer will need to perform sufficient system level "black box" testing to establish that the software meets their "user needs and intended uses." For many applications black box testing alone is not sufficient. Depending upon the risk of the device produced, the role of the OTS software in the process, the ability to audit the vendor, and the sufficiency of vendor-supplied information, the use of OTS software or equipment may or may not be appropriate, especially if there are suitable alternatives available. The device manufacturer should also consider the implications (if any) for continued maintenance and support of the OTS software should the vendor terminate their support.

For some off-the-shelf software development tools, such as software compilers, linkers, editors, and operating systems, exhaustive black-box testing by the device manufacturer may be impractical. Without such testing – a key element of the validation effort – it may not be possible to validate these software tools. However, their proper operation may be satisfactorily inferred by other means. For example, compilers are frequently certified by independent third-party testing, and commercial software products may have "bug lists", system requirements and other operational information available from the vendor that can be compared to the device manufacturer's intended use to help focus the "black-box" testing effort. Off-the-shelf operating systems need not be validated as a separate program. However, system-level validation testing of the application software should address all the operating system services used, including maximum loading conditions, file operations, handling of system error conditions, and memory constraints that may be applicable to the intended use of the application program.

For more detailed information, see the production and process software references in Appendix A - References.

Appendix A - References

Food and Drug Administration references

Design Control Guidance for Medical Device Manufacturers, Center for Devices and Radiological Health, Food and Drug Administration, March 1997 [available at: http://www.fda.gov/cdrh/comp/designgd.html].

Do It by Design, An Introduction to Human Factors in Medical Devices, Center for Devices and Radiological Health, Food and Drug Administration, March 1997 [available at: http://www.fda.gov/cdrh/humfac/doit.html].

Electronic Records; Electronic Signatures Final Rule, 62 Federal Register 13430 (March 20, 1997).

Glossary of Computerized System and Software Development Terminology, Division of Field Investigations, Office of Regional Operations, Office of Regulatory Affairs, Food and Drug Administration, August 1995 [available at: http://www.fda.gov/ora/inspect_ref/igs/gloss.html].

Guidance for the Content of Pre-market Submissions for Software Contained in Medical Devices, Office of Device Evaluation, Center for Devices and Radiological Health, Food and Drug Administration, May 1998 [available at: http://www.fda.gov/cdrh/ode/57.html].

Guidance for Industry, FDA Reviewers and Compliance on Off-the-Shelf Software Use in Medical Devices, Office of Device Evaluation, Center for Devices and Radiological Health, Food and Drug Administration, September 1999 [available at: http://www.fda.gov/cdrh/ode/1252.html].

Guideline on General Principles of Process Validation, Center for Drugs and Biologics, & Center For Devices and Radiological Health, Food and Drug Administration, May 1987 [available at: http://www.fda.gov/cdrh/ode/425.pdf].

Medical Devices; Current Good Manufacturing Practice (CGMP) Final Rule; Quality System Regulation, 61 Federal Register 52602 (October 7, 1996).

Reviewer Guidance for a Pre-Market Notification Submission for Blood Establishment Computer Software, Center for Biologics Evaluation and Research, Food and Drug Administration, January 1997 [available at: http://www.fda.gov/cber/gdlns/swreview.txt].

Student Manual 1, Course INV545, Computer System Validation, Division of Human Resource Development, Office of Regulatory Affairs, Food and Drug Administration, 1997.

Technical Report, Software Development Activities, Division of Field Investigations, Office of Regional Operations, Office of Regulatory Affairs, Food and Drug Administration, July 1987.

Other government references

W. Richards Adrion, Martha A. Branstad, John C. Cherniavsky. *NBS Special Publication 500-75, Validation, Verification, and Testing of Computer Software*, Center for Programming Science and Technology, Institute for Computer Sciences and Technology, National Bureau of Standards, U.S. Department of Commerce, February 1981.

Martha A. Branstad, John C Cherniavsky, W. Richards Adrion, *NBS Special Publication 500-56, Validation, Verification, and Testing for the Individual Programmer*, Center for Programming Science and Technology, Institute for Computer Sciences and Technology, National Bureau of Standards, U.S. Department of Commerce, February 1980.

J.L. Bryant, N.P. Wilburn, *Handbook of Software Quality Assurance Techniques Applicable to the Nuclear Industry*, NUREG/CR-4640, U.S. Nuclear Regulatory Commission, 1987.

H. Hecht, et.al., *Verification and Validation Guidelines for High Integrity Systems*. NUREG/CR-6293. Prepared for U.S. Nuclear Regulatory Commission, 1995.

H. Hecht, et.al., *Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems, Final Report*. NUREG/CR-6463. Prepared for U.S. Nuclear Regulatory Commission, 1996.

J.D. Lawrence, W.L. Persons, *Survey of Industry Methods for Producing Highly Reliable Software*, NUREG/CR-6278, U.S. Nuclear Regulatory Commission, 1994.

J.D. Lawrence, G.G. Preckshot, *Design Factors for Safety-Critical Software*, NUREG/CR-6294, U.S. Nuclear Regulatory Commission, 1994.

Patricia B. Powell, Editor. *NBS Special Publication 500-98, Planning for Software Validation, Verification, and Testing*, Center for Programming Science and Technology, Institute for Computer Sciences and Technology, National Bureau of Standards, U.S. Department of Commerce, November 1982.

Patricia B. Powell, Editor. *NBS Special Publication 500-93, Software Validation, Verification, and Testing Technique and Tool Reference Guide*, Center for Programming Science and Technology, Institute for Computer Sciences and Technology, National Bureau of Standards, U.S. Department of Commerce, September 1982.

Delores R. Wallace, Roger U. Fujii, *NIST Special Publication 500-165, Software Verification and Validation: Its Role in Computer Assurance and Its Relationship with Software Project Management Standards*, National Computer Systems Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, September 1995.

Delores R. Wallace, Laura M. Ippolito, D. Richard Kuhn, NIST *Special Publication 500-204, High Integrity Software, Standards and Guidelines*, Computer Systems Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, September 1992.

Delores R. Wallace, et.al. *NIST Special Publication 500-234, Reference Information for the Software Verification and Validation Process*. Computer Systems Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, March 1996.

Delores R. Wallace, Editor. *NIST Special Publication 500-235, Structured Testing: A Testing Methodology Using the Cyclomatic Complexity Metric*. Computer Systems Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, August 1996.

International and national consensus standards

ANSI/ANS-10.4-1987, *Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry*, American National Standards Institute, 1987.

ANSI/ASQC Standard D1160-1995, *Formal Design Reviews*, American Society for Quality Control, 1995.

ANSI/UL 1998:1998, *Standard for Safety for Software in Programmable Components*, Underwriters Laboratories, Inc., 1998.

AS 3563.1-1991, *Software Quality Management System, Part 1: Requirements*. Published by Standards Australia [Standards Association of Australia], 1 The Crescent, Homebush, NSW 2140.

AS 3563.2-1991, *Software Quality Management System, Part 2: Implementation Guide*. Published by Standards Australia [Standards Association of Australia], 1 The Crescent, Homebush, NSW 2140.

IEC 60601-1-4:1996, *Medical electrical equipment, Part 1: General requirements for safety, 4. Collateral Standard: Programmable electrical medical systems*. International Electrotechnical Commission, 1996.

IEC 61506:1997, I*ndustrial process measurement and control – Documentation of application software*. International Electrotechnical Commission, 1997.

IEC 61508:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems*. International Electrotechnical Commission, 1998.

IEEE Std 1012-1986, *Software Verification and Validation Plans*, Institute for Electrical and Electronics Engineers, 1986.

IEEE Standards Collection, Software Engineering, Institute of Electrical and Electronics Engineers, Inc., 1994. ISBN 1-55937-442-X.

ISO 8402:1994, *Quality management and quality assurance – Vocabulary*. International Organization for Standardization, 1994.

ISO 9000-3:1997, *Quality management and quality assurance standards - Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software*. International Organization for Standardization, 1997.

ISO 9001:1994, Quality systems – *Model for quality assurance in design, development, production, installation, and servicing*. International Organization for Standardization, 1994.

ISO 13485:1996, *Quality systems – Medical devices – Particular requirements for the application of ISO 9001*. International Organization for Standardization, 1996.

ISO/IEC 12119:1994, *Information technology – Software packages – Quality requirements and testing*, Joint Technical Committee ISO/IEC JTC 1, International Organization for Standardization and International Electrotechnical Commission, 1994.

ISO/IEC 12207:1995, *Information technology – Software life cycle processes*, Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 7, International Organization for Standardization and International Electrotechnical Commission, 1995.

ISO/IEC 14598:1999, *Information technology – Software product evaluation*, Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 7, International Organization for Standardization and International Electrotechnical Commission, 1999.

ISO 14971-1:1998, *Medical Devices – Risk Management – Part 1: Application of Risk Analysis*. International Organization for Standardization, 1998.

Software Considerations in Airborne Systems and Equipment Certification. Special Committee 167 of RTCA. RTCA Inc., Washington, D.C. Tel: 202-833-9339. Document No. RTCA/DO-178B, December 1992.

Production process software references

The Application of the Principles of GLP to Computerized Systems, Environmental Monograph #116, Organization for Economic Cooperation and Development (OECD), 1995.

George J. Grigonis, Jr., Edward J. Subak, Jr., and Michael Wyrick, "Validation Key Practices for Computer Systems Used in Regulated Operations," *Pharmaceutical Technology*, June 1997.

Guide to Inspection of Computerized Systems in Drug Processing, Reference Materials and Training Aids for Investigators, Division of Drug Quality Compliance, Associate Director for Compliance, Office of Drugs, National Center for Drugs and Biologics, & Division of Field Investigations, Associate Director for Field Support, Executive Director of Regional Operations, Food and Drug Administration, February 1983.

Daniel P. Olivier, "Validating Process Software", *FDA Investigator Course: Medical Device Process Validation*, Food and Drug Administration.

*GAMP Guide For Validation of Automated Systems in Pharmaceutical Manufacture, Version V3.*0, Good Automated Manufacturing Practice (GAMP) Forum, March 1998:
Volume 1, Part 1: User Guide, Part 2: Supplier Guide. Volume 2: Best Practice for User and Suppliers.

Technical Report No. 18, Validation of Computer-Related Systems. PDA Committee on Validation of Computer-Related Systems. PDA Journal of Pharmaceutical Science and Technology, Volume 49, Number 1, January-February 1995 Supplement.

Validation Compliance Annual 1995, International Validation Forum, Inc.

General software quality references

Boris Beizer, *Black Box Testing, Techniques for Functional Testing of Software and Systems*, John Wiley & Sons, 1995. ISBN 0-471-12094-4.

Boris Beizer, *Software System Testing and Quality Assurance*, International Thomson Computer Press, 1996. ISBN 1-85032-821-8.

Boris Beizer, *Software Testing Techniques*, Second Edition, Van Nostrand Reinhold, 1990. ISBN 0-442-20672-0.

Richard Bender, *Writing Testable Requirements*, Version 1.0, Bender & Associates, Inc., Larkspur, CA 94777, 1996.

Frederick P. Brooks, Jr., *The Mythical Man-Month, Essays on Software Engineering*, Addison-Wesley Longman, Anniversary Edition, 1995. ISBN 0-201-83595-9.

Silvana Castano, et.al., *Database Security*, ACM Press, Addison-Wesley Publishing Company, 1995. ISBN 0-201-59375-0.

Computerized Data Systems for Nonclinical Safety Assessment, Current Concepts and Quality Assurance, Drug Information Association, Maple Glen, PA, September 1988.

M. S. Deutsch, *Software Verification and Validation*, Realistic Project Approaches, Prentice Hall, 1982.

Robert H. Dunn and Richard S. Ullman, *TQM for Computer Software*, Second Edition, McGraw-Hill, Inc., 1994. ISBN 0-07-018314-7.

Elfriede Dustin, Jeff Rashka, and John Paul, *Automated Software Testing – Introduction, Management and Performance*, Addison Wesley Longman, Inc., 1999. ISBN 0-201-43287-0.

Robert G. Ebenau and Susan H. Strauss, *Software Inspection Process*, McGraw-Hill, 1994. ISBN 0-07-062166-7.

Richard E. Fairley, *Software Engineering Concepts*, McGraw-Hill Publishing Company, 1985. ISBN 0-07-019902-7.

Michael A. Friedman and Jeffrey M. Voas, *Software Assessment - Reliability, Safety, Testability*, Wiley-Interscience, John Wiley & Sons Inc., 1995. ISBN 0-471-01009-X.

Tom Gilb, Dorothy Graham, *Software Inspection*, Addison-Wesley Publishing Company, 1993. ISBN 0-201-63181-4.

Robert B. Grady, *Practical Software Metrics for Project Management and Process Improvement,* PTR Prentice-Hall Inc., 1992. ISBN 0-13-720384-5.

Les Hatton, *Safer C: Developing Software for High-integrity and Safety-critical Systems*, McGraw-Hill Book Company, 1994. ISBN 0-07-707640-0.

Janis V. Halvorsen, *A Software Requirements Specification Document Model for the Medical Device Industry*, Proceedings IEEE SOUTHEASTCON '93, Banking on Technology, April 4th -7th, 1993, Charlotte, North Carolina.

Debra S. Herrmann, *Software Safety and Reliability: Techniques, Approaches and Standards of Key Industrial Sectors*, IEEE Computer Society, 1999. ISBN 0-7695-0299-7.

Bill Hetzel, *The Complete Guide to Software Testing*, Second Edition, A Wiley-QED Publication, John Wiley & Sons, Inc., 1988. ISBN 0-471-56567-9.

Watts S. Humphrey, *A Discipline for Software Engineering*. Addison-Wesley Longman, 1995. ISBN 0-201-54610-8.

Watts S. Humphrey, *Managing the Software Process*, Addison-Wesley Publishing Company, 1989. ISBN 0-201-18095-2.

Capers Jones, *Software Quality, Analysis and Guidelines for Success*, International Thomson Computer Press, 1997. ISBN 1-85032-867-6.

J.M. Juran, Frank M. Gryna, *Quality Planning and Analysis*, Third Edition, McGraw-Hill, 1993. ISBN 0-07-033183-9.

Stephen H. Kan, *Metrics and Models in Software Quality Engineering*, Addison-Wesley Publishing Company, 1995. ISBN 0-201-63339-6.

Cem Kaner, Jack Falk, Hung Quoc Nguyen, *Testing Computer Software*, Second Edition, Vsn Nostrand Reinhold, 1993. ISBN 0-442-01361-2.

Craig Kaplan, Ralph Clark, Victor Tang, *Secrets of Software Quality, 40 Innovations from IBM*, McGraw-Hill, 1995. ISBN 0-07-911795-3.

Edward Kit, *Software Testing in the Real World*, Addison-Wesley Longman, 1995. ISBN 0-201-87756-2.

Alan Kusinitz, "Software Validation", *Current Issues in Medical Device Quality Systems*, Association for the Advancement of Medical Instrumentation, 1997. ISBN 1-57020-075-0.

Nancy G. Leveson, *Safeware, System Safety and Computers*, Addison-Wesley Publishing Company, 1995. ISBN 0-201-11972-2.

Michael R. Lyu, Editor, *Handbook of Software Reliability Engineering*, IEEE Computer Society Press, McGraw-Hill, 1996. ISBN 0-07-039400-8.

Steven R. Mallory, *Software Development and Quality Assurance for the Healthcare Manufacturing Industries*, Interpharm Press, Inc., 1994. ISBN 0-935184-58-9.

Brian Marick, *The Craft of Software Testing*, Prentice Hall PTR, 1995. ISBN 0-13-177411-5.

Steve McConnell, *Rapid Development*, Microsoft Press, 1996. ISBN 1-55615-900-5.

Glenford J. Myers, *The Art of Software Testing*, John Wiley & Sons, 1979. ISBN 0-471-04328-1.

Peter G. Neumann, *Computer Related Risks*, ACM Press/Addison-Wesley Publishing Co., 1995. ISBN 0-201-55805-X.

Daniel Olivier, *Conducting Software Audits, Auditing Software for Conformance to FDA Requirements*, Computer Application Specialists, San Diego, CA, 1994.

William Perry, *Effective Methods for Software Testing*, John Wiley & Sons, Inc. 1995. ISBN 0-471-06097-6.

William E. Perry, Randall W. Rice, *Surviving the Top Ten Challenges of Software Testing*, Dorset House Publishing, 1997. ISBN 0-932633-38-2.

Roger S. Pressman, *Software Engineering, A Practitioner's Approach*, Third Edition, McGraw-Hill Inc., 1992. ISBN 0-07-050814-3.

Roger S. Pressman, *A Manager's Guide to Software Engineering*, McGraw-Hill Inc., 1993 ISBN 0-07-050820-8.

A. P. Sage, J. D. Palmer, *Software Systems Engineering*, John Wiley & Sons, 1990.

Joc Sanders, Eugene Curran, *Software Quality*, Addison-Wesley Publishing Co., 1994. ISBN 0-201-63198-9.

Ken Shumate, Marilyn Keller, *Software Specification and Design, A Disciplined Approach for Real-Time Systems*, John Wiley & Sons, 1992. ISBN 0-471-53296-7.

Dennis D. Smith, *Designing Maintainable Software*, Springer-Verlag, 1999. ISBN 0-387-98783-5.

Ian Sommerville, *Software Engineering*, Third Edition, Addison Wesley Publishing Co., 1989. ISBN 0-201-17568-1.

Karl E. Wiegers, *Creating a Software Engineering Culture*, Dorset House Publishing, 1996. ISBN 0-932633-33-1.

Karl E. Wiegers, *Software Inspection, Improving Quality with Software Inspections*, Software Development, April 1995, pages 55-64.

Karl E. Wiegers, *Software Requirements*, Microsoft Press, 1999. ISBN 0-7356-0631-5.

Appendix B - Development team

Center for Devices and Radiological Health

Office of Compliance
Stewart Crumpler

Office of Device Evaluation
James Cheng, Donna-Bea Tillman

Office of Health and Industry Programs
Bryan Benesch, Dick Sawyer

Office of Science and Technology
John Murray

Office of Surveillance and Biometrics
Howard Press

Center for Drug Evaluation and Research

Office of Medical Policy
Charles Snipes

Center for Biologics Evaluation and Research

Office of Compliance and Biologics Quality
Alice Godziemski

Office of Regulatory Affairs

Office of Regional Operations
David Bergeson, Joan Loreng

X

FDA guides to inspections

The FDA guides to inspections can be found on the FDA Web site at:

http://www.fda.gov/ora/inspect_ref/igs/iglist.html

Guides to inspections of:

- Biotechnology
- Biologics
- Computer Issues
- Devices
- Drugs
- Foods Cosmetics
- Miscellaneous

> **Note:** These documents are reference material for investigators and other FDA personnel. The documents do not bind FDA and do not confer any rights, privileges, benefits or immunities for or on any person(s). An alternative approach may be used if such an approach satisfies the applicable statutes, regulations or both.

Updated: April 2001

Guides to Inspections of:

- Biotechnology
  - *Biotechnology Inspection Guide* (11/91) [available at: http://www.fda.gov/ora/inspect_ref/igs/biotech.html]
- Biologics
  - *Blood Banks* (9/94) [available at: http://www.fda.gov/ora/inspect_ref/igs/blood.html]
  - *Source Plasma Establishments* (Rev 4/01) [available at: http://www.fda.gov/ora/inspect_ref/igs/Source_Plasma/default.htm]

- *Infectious Disease Marker Testing Facilities* (6/96) [available at: http://www.fda.gov/ora/inspect_ref/igs/infdis.html]
- *Viral Clearance Processes for Plasma Derivatives* [available at: http://www.fda.gov/ora/inspect_ref/igs/viralcl.html]

- Computer Issues
  - *Computerized Systems in Drug Establishments* (2/83) [available at: http://www.fda.gov/ora/inspect_ref/igs/csd.html]
  - *Computerized System in the Food Processing Industry* [available at: http://www.fda.gov/ora/inspect_ref/igs/foodcomp.html]
  - *Glossary Comp. Systems. Software Development Terminology* (8/95) [available at: http://www.fda.gov/ora/inspect_ref/igs/gloss.html]
- Devices
  - *Quality Systems* [available at: http://www.fda.gov/ora/inspect_ref/igs/qsit/qsitguide.htm]
  - *Electromagnectic Compatibility Aspects of Medical Device Quality Systems* [available at: http://www.fda.gov/ora/inspect_ref/igs/elec_med_dev/emc1.html]
  - *Bioresearch Monitoring Inspections of In Vitro Diagnostic Devices* [available at: http://www.fda.gov/ora/inspect_ref/igs/bimoivd.html]
  - *Mammography Quality Standards Act Auditor's Guide* [available at: http://www.fda.gov/ora/inspect_ref/igs/mqsa.html]
  - *Medical Device Manufacturers* [available at: http://www.fda.gov/ora/inspect_ref/igs/med_dev_mnfct/toc.html]
- Drugs
  - *Bulk Pharmaceutical Chemicals* (9/91) [available at: http://www.fda.gov/ora/inspect_ref/igs/bulk.html]
  - *High Purity Water Systems* (7/93) [available at: http://www.fda.gov/ora/inspect_ref/igs/high.html]
  - *Lyophilization of Parenterals* (7/93) [available at: http://www.fda.gov/ora/inspect_ref/igs/lyophi.html]
  - *Microbiological. Pharmaceutical Quality Control Labs* (7/93) [available at: http://www.fda.gov/ora/inspect_ref/igs/micro.html]
  - *Pharmaceutical Quality Control Laboratories* (7/93) [available at: http://www.fda.gov/ora/inspect_ref/igs/pharm.html]
  - *Validation of Cleaning Processes* (7/93) [available at: http://www.fda.gov/ora/inspect_ref/igs/valid.html]
  - *Dosage Form Drug Manufacturers - CGMP's* (10/93) [available at: http://www.fda.gov/ora/inspect_ref/igs/dose.html]
  - *Oral Solid Dosage Forms Pre/Post Appr. Issues* (1/94) [available at: http://www.fda.gov/ora/inspect_ref/igs/solid.html]
  - *Sterile Drug Substance Manufacturers* (7/94) [available at: http://www.fda.gov/ora/inspect_ref/igs/subst.html]
  - *Topical Drug Products* (7/94) [available at: http://www.fda.gov/ora/inspect_ref/igs/topic.html]
  - *Oral Solutions and Suspensions* (8/94) [available at: http://www.fda.gov/ora/inspect_ref/igs/oral.html]

- Foods Cosmetics
  - *Allergy Inspection Guide* (April, 2001) [available at: `http://www.fda.gov/ora/inspect_ref/igs/Allergy_Inspection_Guide.htm`]
  - *Nutritional Labeling and Education Act (NLEA) Requirements* (8/94-2/95) [available at: `http://www.fda.gov/ora/inspect_ref/igs/nleatxt.html`]
  - *Cosmetic Product Manufacturers* (2/95) [available at: `http://www.fda.gov/ora/inspect_ref/igs/cosmet.html`]
  - *Computerized Systems in the Food Processing Industry* [available at: `http://www.fda.gov/ora/inspect_ref/igs/foodcomp.html`]
  - *Grain Product Manufacturers* [available at: `http://www.fda.gov/ora/inspect_ref/igs/grain.html`]
  - *Interstate Carriers and Support Facilities* (4/95) [available at: `http://www.fda.gov/ora/inspect_ref/igs/icsf.html`]
  - *Dairy Product Manufacturers* (4/95) [available at: `http://www.fda.gov/ora/inspect_ref/igs/dairy.html`]
  - *Miscellaneous Food Products-Vol. 1* (5/95) [available at: `http://www.fda.gov/ora/inspect_ref/igs/foodsp.html`]
  - *Miscellaneous Food Products-Vol. 2* (9/96) [available at: `http://www.fda.gov/ora/inspect_ref/igs/foodsp2.html`]
  - *Low Acid Canned Food Manufacturers Part 1 - Administrative Procedures/Scheduled Processes* [available at: `http://www.fda.gov/ora/inspect_ref/igs/lacfpt1/lacfpt101.html`]
  - *Low Acid Canned Food Manufacturers Part 2 - Processes/Procedures* [available at: `http://www.fda.gov/ora/inspect_ref/igs/lacfpt2/lacfpt201.html`]
  - *Acidified Food Manufacturers* [available at: `http://www.fda.gov/ora/inspect_ref/igs/acidfgde.htm`]
  - *Traceback of Fresh Fruits and Vegetables Implicated in Epidemiological Investigations* [available at: `http://www.fda.gov/ora/inspect_ref/igs/epigde/epigde.html`]
- Miscellaneous
  - *Foreign Medical Device Manufacturers* (9/95) [available at: `http://www.fda.gov/ora/inspect_ref/igs/fordev.html`]
  - *Foreign Pharmaceutical Manufacturers* (5/96) [available at: `http://www.fda.gov/ora/inspect_ref/igs/fordrug.html`]

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

Other publications

These publications are also relevant as further information sources:

2105 Enterprise Storage Server

- *IBM TotalStorage Enterprise Storage Server Introduction and Planning Guide*, GC26-7444
- *IBM TotalStorage Enterprise Storage Server User's Guide*, SC26-7445
- *IBM TotalStorage Enterprise Storage Server Host Systems Attachment Guide*, SC26-7446
- *IBM TotalStorage Enterprise Storage Server Web Interface User's Guide*, SC26-7448
- *IBM TotalStorage Enterprise Storage Server Copy Services Command-Line Interface User's Guide*, SC26-7449
- *IBM TotalStorage Enterprise Storage Server Subsystem Device Driver User's Guide*, SC26-7478
- *IBM TotalStorage Enterprise Storage Server Configuration Planner for S/390 and IBM @server zSeries Hosts*, SC26-7476
- *IBM TotalStorage Enterprise Storage Server Configuration Planner for Open-Systems Hosts*, SC26-7477

3584 Linear Tape Open Library

- *IBM 3584 UltraScalable Tape Library Planning and Operator Guide*, GA32-0408
- *IBM Ultrium Device Driver Installation and User's Guide*, GA32-0430
- *Translated Safety Notices for External Storage Devices*, SA26-7197

7014 Rack

- *7014 Series Model T00 and T42 Installation and Service Guide*, SA38-0577

RS/6000 Enterprise Server

- *Enterprise Server Model H80 and pSeries 660 Model 6H1 Installation Guide*, SA38-0575
- *RS/6000 Enterprise Server Model H80 System Unit Safety Information*, SA23-2652

IBM @server pSeries 670

- *IBM @server pSeries 670 Installation Guide*, SA38-0613
- *RS/6000 and pSeries PCI Adapter Placement Reference*, SA38-0538
- *IBM @server pSeries 670 Installation Guide*, SA38-0613

IBM @server pSeries 690

- *IBM @server pSeries 690 Installation Guide*, SA38-0587
- *RS/6000 Enterprise Server Model H80 System Unit Safety Information*, SA23-2652

- *RS/6000 and pSeries PCI Adapter Placement Reference*, SA38-0538

AIX Version 4.3

- *AIX Version 4.3 Quick Installation and Startup Guide*, SC23-4111
- *AIX Version 4.3 Installation Guide*, SC23-4112
- *AIX Version 4.3 Network Installation Management Guide and Reference*, SC23-4113
- *AIX Version 4.3 Quick Beginnings*, SC23-4114
- *AIX Version 4.3.0 Release Notes*, GI10-0697

2031 McData Switch

- *McData Sphereon 4500 Fabric Switch Product Manager User Manual*, P/N 620158000-0000 Rev A

Online resources

These Web sites and URLs are also relevant as further information sources:

- The Food and Drug Administration Web site

  `http://www.fda.gov`

- FDA *Glossary of Computerized System and Software Development Terminology*

  `http://www.fda.gov/ora/inspect_ref/igs/gloss.html`

- The FDA guides to inspections

  `http://www.fda.gov/ora/inspect_ref/igs/iglist.html`

How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

IBM

Redbooks

Installation Qualification of IBM Systems and Storage for FDA Regulated Companies

(1.0” spine)
0.875”<->1.498”
460 <-> 788 pages

Installation Qualification of IBM Systems and Storage for FDA Regulated Companies

Demonstrates how the infrastructure of IBM TotalStorage, eServer pSeries, LTO, and SAN can facilitate regulatory compliance

Uses a sample method to help meet the qualification requirements of FDA 21 CFR Part 11

Shows sample documentation to help meet compliance standards

This IBM Redbook contains an Installation Qualification (IQ) executed at a pharmaceutical manufacturer with the help of IBM. The customer purchased IBM equipment to support a major new computerized system that came within the regulatory scope of FDA 21 CFR Part 11. This IQ was performed as one part of an overall systems validation, and a separate system requirements document contained the technical infrastructure requirements, including equipment.

The following IBM equipment was installed and qualified by the customer for this project:

- IBM @server pSeries 670 Server running AIX, HACMP, and LPARs
- IBM TotalStorage Enterprise Storage Server
- IBM LTO Tape Library
- IBM McData SAN Switches

The materials contained in this Installation Qualification include:

- Protocol
- Procedures
- Training materials
- Test scripts for the IBM equipment

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-6630-00 ISBN 0738454117