

Risk-Based Validation of Computer Systems Used In FDA-Regulated Activities

Purpose

This document provides a summary of the requirements relating to use of computer-based systems in activities that are regulated by the FDA. The relevant FDA and industry guidance for complying with these requirements is also summarized. Finally, the approach proposed by MPR for system validation/qualification is discussed. The MPR approach uses risk-based prioritization to identify and address the most critical systems and functions first. For complex distributed systems, MPR's approach is to segment the system on a functional basis. This can be used, for example, to divide network systems into functional components that can then be prioritized based on risk and validated.

Relevant FDA Requirements

FDA regulations that specify controls on activities related to the manufacturing, processing, and distribution of drug, medical device, and blood-related products are specified in several sections of the Code of Federal Regulations, including:

- 21 CFR Part 211, *Current Good Manufacturing Practice for Finished Pharmaceuticals*
- 21 CFR Part 606, *Current Good Manufacturing Practice for Blood and Blood Components*
- 21 CFR Part 820, *Quality System Regulation*

There are many similarities in these regulations in the requirements for design, documentation, and validation of computer-based systems and equipment. Fundamentally, FDA requires that systems used to perform or support regulated activities be controlled, maintained, and qualified. Key requirements include:

- Written procedures are required to control changes to hardware and software.
- Written procedures are required for operation and maintenance.
- Systems are required to be validated to demonstrate that the intended functions will consistently be performed accurately and reliably.
- Controls must be provided to backup and ensure security of computer records.

In addition to the specific requirements that are specified in the “predicate” regulations listed above, additional requirements apply if a computer system is used to either store or maintain

electronic records, or implement electronic signatures to authenticate records. These requirements are specified in 21 CFR Part 11, *Electronic Records; Electronic Signatures*.

Recently, FDA issued revised guidance which states that the Part 11 rules are intended to be applied only to a “narrow scope” of applications. Companies are expected to establish the applicability of the Part 11 rules to their systems using a risk-based analysis to identify the most critical electronic records. Further, the draft guidance indicates that FDA will exercise “enforcement discretion” with respect to implementation of the rules. This new interpretation will provide relief for application of the Part 11 rules.

FDA and Industry Guidance

In addition to the regulations listed above, regulatory expectations relating to the implementation of these regulations are discussed in various FDA guidance documents, including the following:

- *Guideline on General Principles of Process Validation*, May 1987, which covers general expectations for validation of processes and equipment.
- *General Principles of Software Validation*, January 2002, which provides specific guidance for computer-controlled equipment. While specifically intended to cover software related to medical devices, the principles apply to software in other applications.
- *Draft Guideline for the Validation of Blood Establishment Computer Systems*, September 1993, which describes expectations relating to documentation, procedures, and validation of computer systems used in blood product processing.

Due to the widespread use of automated and computer-controlled equipment in regulated health care applications, the industry, including the International Society of Pharmaceutical Engineers (ISPE) and the Parenteral Drug Association (PDA), have developed more specific guidance. Key industry guidance documents include:

- Good Automated Manufacturing Practice (GAMP), *GAMP Guide for Validation of Automated Systems*. This guidance focuses on quality control processes applied in the design of process equipment. Specifications, design documents, systematic software development, acceptance testing, use of procedures, configuration management, and other quality controls are required. One of the key elements of the GAMP guidance is a risk-based approach to validation. The guideline identifies various categories of software and provides graded levels of validation activities depending on risk.
- PDA, *Report on the Validation of Computer-Related Systems*, PDA Technical Report No. 18. This document presents a methodical approach to computer systems validation, describing what the validation effort should entail. It provides guidance on definition of requirements, evaluation of software system vendors, software development process issues, and methods for software testing.

Technical reports, such as References (7) and (8), provide additional guidance and methodologies for validation of distributed computing systems and network systems.

These and other guidance documents clearly establish use of risk in determining both the scope and extent of validation for computer-based systems. Current industry efforts are focused on developing better definition of risk analysis methodologies. Little guidance is currently available concerning the engineering judgment needed to determine the likelihood and consequences of computer system failures.

Typical Elements of Computer Systems Validation

Computer system validation typically involves the following elements. A Master Validation Plan is typically prepared to identify the responsibilities, activities to be performed, and documents to be prepared in the validation effort. The Master Validation Plan describes how these elements will be addressed.

1. Defined Development Process – It is generally accepted that a well-defined software development process is important to produce software of sufficient quality to merit its use in critical applications. In addition, a key product of a good software development process is design documentation, which is a necessary input to the overall validation process. For example, a software specification is needed to define the software's functions, allowing test procedures to be prepared to confirm those functions perform as required. For software developed out-of-house, the adequacy of this documentation is generally assessed in a supplier evaluation. Of course, the ability to examine the development process and have access to key design documents is not always achievable for commercial off-the-shelf products. In these cases, the user must generally provide some justification for acceptance of the product. Regardless, detailed documentation of the as-installed configuration is necessary.
2. Procedures and Documentation – Compliance with FDA regulations requires documented evidence of control, and this includes written procedures for use, maintenance, and control of computer-based systems. Types of procedures that are expected include:
 - System operation for normal use.
 - System management, installation, maintenance, and updates.
 - Access control (e.g., creation and maintenance of user ID's and passwords).
 - Security (e.g., levels of access and write/edit/delete authorization).
 - Data archiving, backup, and restoration.
 - Periodic monitoring of system performance.
 - Disaster recovery.

The validation process must include activities to assure that these procedural controls are defined and documented. It is also appropriate to confirm that personnel are properly trained in these procedures.

3. Change Control – A prerequisite to validation is procedural controls to assure that any changes to a system are first documented and evaluated prior to being implemented. The change control process must assure that re-validation is performed when necessary.
4. Equipment Qualification – One of the key elements of validation is qualification of the equipment. For corporate computer systems, it is standard industry practice to separate the network infrastructure from the applications that run on the infrastructure. Traditionally, equipment qualification includes the following:
 - Installation qualification, in which installation and/or configuration in accordance with the design documents is verified.
 - Operational qualification, in which adequate system operation at the boundaries of normal operating conditions is verified.
 - Performance qualification, in which adequate system performance under normal operating conditions is verified.

The Master Validation Plan defines the specific requirements for each phase of equipment qualification. Often, the installation and operational qualification phases are combined.

Note that for suppliers with acceptable design, testing, and documentation practices, work done during a factory acceptance test can be credited for providing some of the data needed for qualification activities.

5. On-Going Maintenance – Processes and procedures must be established to periodically monitor and maintain the system to assure that its condition and performance remain in the same condition as when it was qualified.

MPR Validation Approach

Validation should be a “life cycle” activity which is integral with the design, installation, operation, and maintenance of a system. When it is performed in this way, the documentation required to provide satisfactory evidence that the system will perform as required is generated while development activities are completed. However, when a system is deployed and put into operation without validation, a plan for “retrospective” validation is needed.

MPR’s approach is to examine the specific system, its use, available documentation, and the customer’s business constraints to prepare a strategic plan for system validation. For complex distributed systems, MPR segments the system into functional units. This could include individual software applications, process equipment, and/or supporting network infrastructure (see Figure 1).

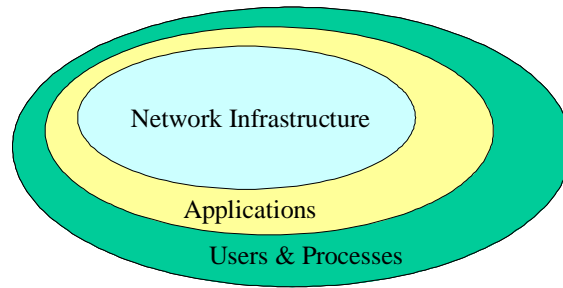


Figure 1. Top-Level Segmentation of Complex Computer System

Networks can often be treated as a supporting “utility” system that provides generic capabilities and functions used by one or more processes or functions. They too can be segmented by functional units (see Table 1).

Table 1. Examples of Network Functional Units

<i>Hardware</i>	<i>Software</i>
Routers	Applications
Gateways	Operating Systems
Workstations	Drivers and Services
Network-enabled Devices	User Interface

MPR’s strategic, risk-based approach to computer systems validation includes the following main steps. This approach is also summarized in Figure 2.

1. Define the System Inventory

Determine the “inventory” of systems, equipment and software.

- a) System Boundaries – Define the boundaries of the computer system, including network systems and applications that use the network. At the highest level, system boundaries can be defined as illustrated in Figure 1.
- b) Document Process – Define and document the business processes that use the applications and the network system. Identify specifications that describe the required systems and functions and written procedures that control these processes.
- c) Define Functions – Define the functions performed by the network system and the associated applications to support the business processes. Note that only a subset of all functions that can be performed might be identified as ones that must be qualified.

- d) Identify Data – Define the data that is used, manipulated, or created in each step of the process. Determine which electronic data are required to demonstrate compliance with FDA regulations (and which may therefore be subject to Part 11 rules).
- e) Identify Existing Controls – Identify any existing procedural controls on changes, access, security, etc.

2. Risk Assessment

Perform the risk assessment to identify functions and/or data that are critical to maintain public health. The risk assessment process asks the following questions:

- What are the functions performed or data used?
- What is affected by the function?
- How can it fail?
- What is the likelihood of failure (considering the vendor’s development process, system complexity, and experience)?
- What are the consequences of failure (focusing on the risk to public health)?
- How likely is failure to be detected (by the system design or by established controls)?

The risk assessment is performed in accordance with a written procedure that includes forms and checklists to support documentation of the results. Results are typically documented in a matrix format, much like a failure modes and effects analysis.

Using the likelihood and consequences of failure, a level of risk is assigned as follows:

Likelihood Consequences	High (credible/likely)	Moderate (credible/not likely)	Low (highly unlikely)
High (Serious Injury)	<i>High</i>	<i>High</i>	<i>Moderate</i>
Moderate (Non-Serious Injury)	<i>High</i>	<i>Moderate</i>	<i>Minor</i>
Minor (No Human Injury)	<i>Moderate</i>	<i>Minor</i>	<i>Minor</i>

The validation plan uses the risk assessment results to drive the scope and extent or rigor of validation activities.

3. Gap Analysis

Using the results of the risk assessment, a gap analysis is performed to identify shortcomings in the existing design and/or procedural controls. Where shortcomings are identified, strategies are developed to mitigate unacceptable risks. For example, lack of a specification for a given function or system would create a risk that adequate testing

cannot be performed. This risk would be mitigated by preparation of the needed specification. Recommended system improvements could involve architecture, hardware, or software upgrades. Process improvements could require enhanced change control procedures, use of automated system monitoring tools, or improved SOPs.

4. Prioritized Validation Plan

As noted above, the Master Validation Plan defines the detailed activities to be performed during the qualification/validation effort. The plan must be developed in consideration of the state of system development so that the necessary level of compliance is achieved. To keep the validation effort focused, priorities must be established on the basis of risk.

For complex computer systems, the Validation Plan becomes the basis for the interface between system stakeholders, including Operations, Engineering, IT, and QA groups. It is important, therefore, that the plan consider the processes and procedures employed by these organizations.

In addition, for a large and dynamic system such as an enterprise network, the plan must include provisions to accommodate changes. Using the risk-based approach with a rigorous change control process, the plan can provide:

- Triggers for appropriate re-qualification activities when network infrastructure elements are modified.
- Requirements for different levels of documentation associated with qualification (or re-qualification) commensurate with risk level of impacted elements.
- Use of online and in-process re-qualification where possible.

The plan should also include standardized procedures for hardware and software testing. These procedures would be executed during qualification and re-qualification to assure proper operation with respect to functional requirements and identified failure modes.

5. Execute Plan

Once approved, the validation plan is implemented, including preparation of procedural controls as necessary, retrospective development of system design documentation if necessary, and validation. High-priority systems or functions are validated first (this could include the network infrastructure as appropriate). Implementation of the plan establishes the baseline for maintaining continuous qualification of the system as it changes and evolves over time.

6. Training

Personnel must be trained to following the procedural controls that have been established to maintain the system in the validated state.

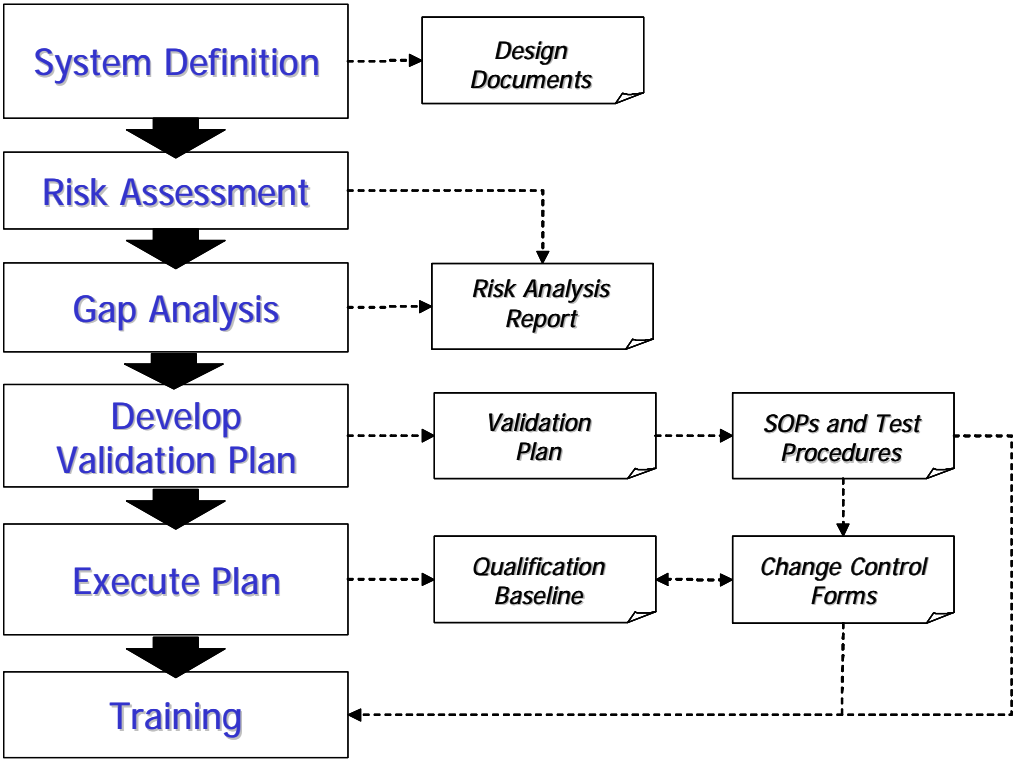


Figure 2. Simplified Illustration of Risk-Based Validation Approach and Associated Output Documents

References

1. Food and Drug Administration, “Guidance for Industry, Part 11, Electronic Records; Electronic Signatures — Scope and Application,” August 2003.
2. Food and Drug Administration, “General Principles of Software Validation; Final Guidance for Industry and FDA Staff,” January 11, 2002.
3. Food and Drug Administration, “Guideline on General Principles of Process Validation,” May 1987.
4. Food and Drug Administration, “Draft Guideline for the Validation of Blood Establishment Computer Systems,” September 1993.
5. International Society of Pharmaceutical Engineers, “Good Automated Manufacturing Practice, GAMP Guide for Validation of Automated Systems,” (GAMP 4), December 2001.
6. Parenteral Drug Association, “Report on the Validation of Computer-Related Systems,” PDA Technical Report No. 18, October 1994.
7. Lopez, Orlando, “Qualification of Computer Networks,” Horwood Publishing, 2002. [Available through PDA.]
8. Wingate, Guy, “Validating Corporate Computer Systems: Good IT Practice for Pharmaceutical Manufacturers,” Interpharm Press, 2000.



About the Authors

This paper was prepared by Eric Claude and Chris Rice of MPR Associates, Inc. For more information about this paper or MPR Associates, please contact:

Eric Claude
Phone: 703-519-0535
Email: eclau@mpr.com

The address at our Alexandria headquarters is:

MPR Associates, Inc.
320 King Street
Alexandria, VA 22314

Phone: 703-519-0200
Fax: 703-519-0224

MPR Associates is an engineering and consulting firm founded in 1964 and headquartered in Alexandria, Virginia. MPR provides technology development solutions for life science firms, with a focus on product design (instruments, delivery systems, devices), manufacturing process development, training, and validation. Key expertise is available in process engineering, mechanical design, materials science, electronics, controls, software, and GMP compliance.

Please also refer to the “Technology” section of our web site at www.mpr.com for additional information.