

Alan Goldhammer, PhD
ASSOCIATE VICE PRESIDENT
US REGULATORY AFFAIRS



3740 02 MAR -8 P2 25
March 8, 2002

Dockets Management Branch
Food and Drug Administration
5 130 Fishers Lane
Rockville, MD 20852

Re: Docket Number OOD-1538; Draft Guidance for Industry, 21 CFR Part 11; Electronic Records; Electronic Signatures Validation; (66 Federal Register 48886; 24 September 2001)

The following comments on the above cited draft guidance are submitted on behalf of the Pharmaceutical Research and Manufacturers of America (PhRMA). PhRMA represents the country's leading research-based pharmaceutical and biotechnology companies, which are devoted to inventing medicines that allow patients to lead longer, healthier and more productive lives. Investing over \$30 billion this year in discovering and developing new medicines, PhRMA companies are leading the way in the search for cures. Our member companies are a leading source of new drug research and development.

PhRMA welcomes the opportunity to comment on this draft guidance. As the FDA is well aware, full compliance with 21 CFR Part 11 is going to be time consuming and costly for PhRMA member companies. It will have an impact on every segment of the drug development process, from the acquisition of clinical and laboratory data on through to the manufacturing of approved pharmaceutical products. PhRMA's general and specific comments follow. In some cases our comments reference specific line numbers of the draft guidance. PhRMA has enclosed a copy of the guidance with line numbers so that the FDA can readily refer to the exact text under discussion.

General Comments:

00D-1538
FDA should develop one validation guidance document that will cover all relevant issues regardless of the type of product that is being regulated. PhRMA recommends that the FDA CDRH Draft Guidance Version 1.1 "General Principles of Software Validation" be incorporated into this 21 CFR Part 11 guidance. Critical to finalization of this guidance is a sound definition of the concept of validation, reflecting the one found in the companion Glossary of Terms draft guidance document (66 Federal Register 48886). PhRMA believes that rather than having a free standing Glossary of Terms, all relevant terms that have a crucial bearing on interpretation should be defined within the individual guidances. This Guidance document does not clearly define validation. Some sections indicate that validation covers the entire system life cycle. For example, requirements, specifications, program build testing, change control, configuration management, and revalidation are all discussed. However, the description of documentation of validation

C29

00D-1538

Pharmaceutical Research and Manufacturers of America

C29

activity (section 5.2) gives the impression that validation consists of a validation protocol (procedures), a validation report, and a validation plan. In contrast, the companion Glossary document defines Computer Systems Validation as, "Confirmation by examination and provision of objective evidence that computer system specifications conform to user needs and intended uses, and that all requirements can be consistently fulfilled."

In August 1995 FDA issued a Glossary of Computerized System and Software Development Terminology, which contains a list of initialisms and glossary of several hundred terms. The definitions include seven "validation" terms (e.g., validation, process validation, prospective validation, validation protocol, retrospective validation, software validation, and validation, verification, and testing.) In addition, several international consensus documents contain terminology and definitions agreed by subject matter experts. PhRMA recommends FDA should use available international standards and maintain consistency with agreed definitions whenever possible in its guidance documents. In addition, PhRMA recommends FDA make a concerted effort to reconcile the various Glossary documents.

PhRMA recommends that the guidance include a section that clearly states that systems which were validated prior to the issuance of the guidance do not need to be re-validated to meet the exact requirements of the guidance if the standard operating procedures used to validate the system have equal merit in meeting the intended validation objectives.

PhRMA urges FDA to provide additional guidance on the validation of security. In the "supplementary information" to the Part 11 regulation (sections F and G) the agency comments on the fact that virtually no security model is perfect and the intention of the applicable CFR parts is to "make it difficult to execute falsification by mishap or casual misdeed." FDA also notes that firms must rely largely on the "integrity of their employees." PhRMA suggests that FDA provide additional guidance on what this means regarding the perceived requirement to impose stronger user authentication and other techniques on Part 11-related information, and how rigorous the testing and validation of security components need to be.

PhRMA urges FDA to provide input on how to approach legacy versus new systems. This guidance appears to be written largely to discuss what the industry should be doing with new development but not how far or deep to go back and deal with legacy systems. Many processes within the industry use a mixture of new and legacy systems that will result in a complicated implementation of the Part 11 regulations.

Like most industries, the pharmaceutical industry is moving away from the custom development of IT systems to the use of commercial packages. Much of the validation guidance was developed at a time when custom development was common within the industry and it would be useful for guidance to place a greater emphasis on the use of commercial software where, in many cases, the industry has little ability to influence the design of the product.

PhRMA notes that several issues of consistency in the document need to be addressed. FDA should settle on using either “user” or “end-user,” but not both. There is some confusion as to whether they are being used interchangeably. In addition, the phrases “system requirements specifications,” “end-user requirements” and “end-user requirements specifications” are used interchangeably. Sentences containing “we” and “you” should be rewritten, as these words do not clearly identify the intended party and are not consistent with broadly used styles of technical writing. The 1st letter of “Part 11” should be capitalized. This change would enhance consistency throughout the document, as well as reflect the accepted style for use of an abbreviated term to reference a longer term.

Specific Comments:

Section 2:

The first paragraph of this section should be moved to the Purpose section of the document, as it appears to address purpose rather than scope.

FDA should provide guidance on how to deal with validating hybrid systems. The reality is that most companies adopted some form of hybrid approach and, in view of the large number of systems concerned, it will be some time before they can all be upgraded or replaced. Even if such a system cannot be fully compliant, FDA should provide alternative solutions allowing the validation of such systems.

On Page 2, line 13; the phrase “compatible with FDA’s public health responsibilities” should be replaced with “generally equivalent to paper records and handwritten signatures executed on paper.”

Page 2, line 17; states that the guidance is “not intended to cover everything that computer systems validation should encompass in the context of electronic record/electronic signature systems.” However the guidance does not explain what criteria were used to determine what went into the guidance and what didn’t. Therefore, the guidance does not make clear what might not be covered.

Page 2, lines 21-26; PhRMA recommends that a statement be included to recognize the distinction between independent programs and the electronic record systems and processes of which they may be a part. In addition, FDA should recognize that requirements for testing and documentation vary for programs that are either independent of systems or system components as opposed to complete systems. Substantially, only parts of the requirements will reasonably be applicable to independent programs and “stand alone” system modules.

PhRMA notes that the same argument can be made with respect to system complexity. Smaller systems that might consist of only a very few programs or modules, where there are only a few options, should not need all validation and test components expressed as

“Key Principles.” For a system that is normally specified with only a few user options or composed of only a few programs (perhaps 10 or fewer), 1) procedures need not include both dynamic and static results and 2) reports for tests conducted at all levels (structural, functional, and module tests) may not provide significant additional assurance that program operations are correct.

After the first sentence under section 2.1 Applicability, which ends “...or any FDA regulation,” insert, “ Since Part 11 also applies to records submitted under the requirements of the Act or the PHS Act, even if those records are not specifically identified in agency regulations, this draft guidance has broad applicability.” After the last sentence under section 2.1 Applicability, which ends, “...post marketing submissions and reports,” insert the following: “Examples of submitted records that are subject to Part 11, even though they are not specifically identified in regulations, are SAS transport files, data definition files, and patient profiles submitted with an NDA.”

Section 3:

Several terms in this draft guidance remain undefined, even in the accompanying guidance on Glossary of Terms. PhRMA recommends FDA review all terms in the draft validation guidance for understandability and consistency with the draft Glossary of Terms guidance and with previously issued international consensus documents (e.g., publications of the International Organization for Standardization, Institute of Electrical and Electronic Engineers, National Institute of Standards and Technology, etc. Consensus process and independent subject matter experts should be used to define outstanding terms in the validation guidance.

Section 4:

Page 3-4, lines 43-48; at the end of section 4, PhRMA recommends that FDA add the following: “Validation means establishing documented evidence which provides a high degree of assurance that a specific process will consistently perform to predetermined specifications and quality attributes. A key part of system validation is for the system owner or user to define the acceptable performance characteristics of procedures and controls for validation.”

Section 5:

PhRMA asserts that this section needs to be revised to provide an overall framework for the guidance. Validation should be better defined to bring out the concept that it is a continuous process that follows the life cycle of a system from requirement definition through retirement. Thus, validation activities closely parallel the development cycle. It would also be useful to reorganize the sections so they are in chronological order. In particular, the section on “Equipment Installation” should go before “Validation Activity.”

Page 4, lines 52-61; for some projects, user “requirements documentation” may be effectively combined (wholly or partially) with “system or program description documentation.” For software engineering projects managed by using a rapid application development (RAD), waterfall or “generate-evaluate-correct” methodology programs and their descriptive documentation are the expression of cumulatively evaluated user requirements. For these types of projects, user evaluations of acceptability and requirement satisfaction are expressed as corrections to trial programs. PhRMA notes that for systems built according to these principles, the additional requirement for explicitly maintaining distinct user requirements documentation (other than the collectively accepted application or program descriptions) is of little value. Therefore PhRMA recommends that the guidance recognize that “requirements specifications” could take a number of different forms, included user-accepted programs or system description documents.

“Traceable to system design requirements and specifications” implies that FDA is requiring a Traceability Matrix. While some good software vendors have this validation deliverable, purchasers of these systems do not and may have to invest time, money and resources to develop their own. The clients that purchase these systems can only develop a matrix, which links the user requirement to the user acceptance testing. The vendor must be responsible to develop and maintain a traceability matrix used on the quality system or development life cycle.

Page 5, lines 71-83; PhRMA suggest three changes:

- a) change the first sentence of the 2nd paragraph under section 5.1 to read, “Other factors not specifically addressed in Part 11 may also impact electronic record trustworthiness, integrity, and reliability; intended system performance should also be considered.”;
- b) delete the second sentence of the 2nd paragraph under section 5.1, which begins, “You should consider these ...”; and
- c) change “system performance” under the three bullets to read “intended system performance.”

Page 5, line 79; in the 2nd bullet regarding “scalability,” replace the word “Scalability” with “Scale.” One can establish a requirement for scale, but not scalability.

Page 5, line 81; It is implausible to ask for the establishment of specific requirements for RF interference, temperature/humidity, and electrical power fluctuations, unless the intent is to test for these either system-by-system (not possible) or as part of a facility commissioning or routine inspection. Determining a test to conduct for any of these is extremely difficult without some quantifiable benchmark of acceptance criteria to go against. PhRMA recommends that FDA understand and document these prior to inclusion in a final guidance.

Page 6, lines 84-102; All 3 subsections of this section indicate that review and approval is a management responsibility. However, management is undefined, and business SOPs could assign this responsibility to people not defined as “management” in the

organization. In addition, the guidance does not address responsibilities for creation/preparation and execution are not addressed. It is not clear from this Guidance document if validation is intended to discuss all activities during the system life cycle. PhRMA recommends that this section of the guidance clarify that the level of detail in the validation plan and the volume of the supporting evidence should be in proportion to *the size, complexity and regulatory sensitivity of the system*. This re-enforces Section 5.6, "Extent of Validation." PhRMA suggests that FDA (a) clarify the expectations regarding preparation, authorization, and execution of the plan and (b) clarify the extent to which the entire system life cycle should be addressed and when it might be appropriate to do so. The sentence starting on line 95: "It should describe the computer system..." as criteria for testing and configuration management are covered elsewhere in the guidance document; inclusion of this sentence may lead the reader to infer that only procedures for system configuration/testing are necessary.

Section 5.2.3

PhRMA notes that the validation report, as described here, is redundant with current practice and thus unnecessary. It states that test results should be expressed in quantifiable terms rather than pass/fail. Manufacturers protocols already state the expected outcome and in most cases the tester will be duplicating the expected outcome almost verbatim in the result. In addition, screen prints and reports are attached, demonstrating the results. Calculation checks are done on worksheets or some other hard copy documentation, all of which are attached to the executed protocol.

Section 5.3

Page 7, lines 103-106; PhRMA recommends that FDA replace the phrase "you should confirm that all hardware and software are properly installed" with the phrase "qualified personnel should document that all hardware and software are properly installed." FDA should provide more detail regarding IQ, OQ and PQ. Equipment installation should require documentation rather than just confirmation. FDA expectations for documentation in these areas need to be more clearly defined. The guidance is confusing with regard to "validation," verification and "qualification" activities.

Section 5.4

PhRMA recommends this section be modified as follows:

- a) expand this section to provide additional descriptive information and examples for each test condition listed,
- b) provide examples of differences between test environments and production environments and their potential impact on acceptability of results of dynamic testing,
- c) clarify whether user-site tests are equivalent to user acceptance testing and whether production data should be used in such testing,
- d) clarify whether the agency intends to include "branch testing, path testing, statement testing," etc. as part of structural testing,

- e) replace the words “software creator” in the third sentence after the first bullet in section 5.4.2 with “software programmer, coder, or developer.”,
- f) clarify the relationship of the August 1995 glossary to the draft validation guidance and review use and intended meaning of the term “functional testing” for consistency with previously issued international consensus documents, and
- g) provide examples of test results and expectations regarding documentation.

Page 7, line 111; in the 1st bullet regarding “test conditions,” FDA should replace the phrase “unexpected data entries” with “non-standard data entries.”

Page 7, line 112; FDA should provide examples to clarify what is meant by “branches, data flow and combinations of inputs” or eliminate the terms.

Page 7, lines 113-114; FDA should delete the second bullet regarding “simulation tests” because the issue of whether such a test is used is not a regulatory issue. Furthermore, PhRMA recommends that FDA recognize that stress tests cannot be exhaustive, and that stress condition testing recommendations should be bounded by good judgment. FDA should consider the incremental confidence in reliability or accuracy contributed by any test. FDA should not require manufacturers to select stress tests for inputs that are extraordinarily unlikely. For example, there is no value for most software systems in examining whether a system fails gracefully when ambient temperature is near 0 degrees Kelvin.

Page 7, line 115; FDA should eliminate the term “off-line” and replace it by “conducted in an environment that is separate from the actual users computing environment.” PhRMA members assume that this is a test in a mimic environment and not in the production environment.

Page 7, lines 116-119; FDA should require users to perform testing that simulates the work process, and that this testing should include realistic error scenarios. However, PhRMA notes that in a pre-production environment, it is difficult to continuously operate a computer system long enough to catch unforeseen faults. PhRMA suggests that FDA permit a performance verification step post-production that would identify and correct any problems that weren't apparent during testing. This would not be a substitute for user testing. In addition, PhRMA suggests ending the sentence after “... latent faults.”

Section 5.4.2

Page 8, Lines 121-133; PhRMA notes that bullet 1 “Structural testing” and Bullet 3 “Program build testing” are not possible for end-users to do with commercial software, even though the guidance later states in section (6.1.3.) that Bullet 2 “Functional testing” is not adequate for such software. “Program build testing” is not a widely recognized term. Its meaning in this section is unclear. PhRMA recommends that FDA include a complete definition in the glossary of terms.

Section 5.4.3

Page 8, lines 135-7; Testing a complex system requires hundred of steps, often automated, as in the case of regression tests. PhRMA notes that requiring tester comments on all test results, especially for tests that have passed, greatly decreases the productivity of the tester and adds little value to the quality of the end product. Given the thousand of comments that a tester would need to record, the inevitable tendency would be for the tester to write standard phrases with no meaning, but which satisfy the letter of the guidance. PhRMA suggests that the following sentence: “Quantifiable test results should be recorded in quantified rather than qualified (e.g., pass/fail) terms.” be replaced with the following: “Whenever possible, test results should be expressed in greater detail rather than stated as “pass/fail.”

Section 5.5

Page 9, lines 138-146; This guidance does not define static verification techniques and the guidance does not clearly define expectations around documentation and reproducibility of these verification steps. PhRMA recommends inserting the following after the 3rd sentence of section 5.5: “When static verification techniques are used, acceptable reproducibility and documentation thereof can be defined by the system owner or end user, as may be appropriate for the system.” In addition, FDA should add the following language to conclude this section: “These techniques require the availability of source code and its associated documentation. This is not normally available in the case of commercial software packages.”

Section 5.6

PhRMA recommends that FDA move this section in its entirety between section 5.1 System Requirements and section 5.2 Documentation of Validation Activity, to improve the context of the guidance.

Page 9, lines 147-155; FDA should reword the first two bullets as follows:

- “The risk that system failure or inadequate system design poses to product safety ...”
- “The risk that system failure or inadequate system design poses to data integrity ...”

These bullets address the risk that the system poses to the regulated article or to data. The recommended wording specifically cites the main issues.

Page 9, line 149; In the 1st bullet regarding “product safety...,” FDA should replace the phrase “product safety, efficacy, and quality” with “product identity, strength, quality and purity.” This recommended language uses the phrasing in the cGMP regulation, 21 CFR Part 211.22(c).

Page 9, line 152; In the 2nd bullet regarding “data integrity...,” PhRMA recommends replacing with the phrase “data integrity, authenticity, security and, if appropriate, confidentiality.” Security is an important component that should be included in determining the extent of validation. Likewise, confidentiality does not always need to be included in system validation.

Section 5.7

Page 10, lines 157-62; PhRMA recommends that FDA clarify those aspects of the computer system validation that must be performed by persons other than those responsible for building it. This guidance does not clearly set forth what aspects of validation or the system development life cycle warrant independent review. Secondly, PhRMA recommends “self-evaluation” in the first sentence of this section be changed to “review of one’s own work.” For certain types of testing (e.g., unit testing), it is neither plausible nor desirable for testing to be carried out by anyone other than the individual(s) who built it.

Section 5.8

PhRMA notes that change control is not equivalent to configuration management, and neither term is clearly defined in either the draft validation guidance or in the draft Glossary of Terms guidance. PhRMA recommends changing the title of this section to “5.8 Change Control and Configuration Management.” In addition, FDA should insert the following before the existing first sentence of section 5.8: “Change control represents the process(es), authority(ies) for, and procedure(s) to be used for all changes that are made to the computerized system and/or the system’s data. In contrast, configuration management represents application of technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verifying compliance with specified requirements.”

Page 10, lines 166-67; FDA should replace the last sentence in the first paragraph with the following: “Changes that cause the system to operate outside of previously validated operating limited would require more extensive revalidation.”

Page 11, line 175-76; PhRMA is uncertain about the meaning of the term re-validation. Is a system “re-validated” or is validation maintained via change control and appropriate testing? PhRMA recommends that the sentence in this line end at “assess the changes.”

Page 11, lines 177-182; PhRMA notes that the intended meaning of regression analysis is not clear. The draft Glossary of Terms guidance does not have a definition of regression analysis, but “regression analysis and testing” is defined as, “A software verification and validation task to determine the extent of verification and validation analysis and testing that must be repeated when changes are made to any previously examined software

products.” FDA should clarify whether the Agency wants simple “trend analysis” or whether manufacturers need to perform more detailed regression testing.

Section 6.1.1

Page 12, lines 196-197; It is unrealistic to assume that vendors will provide copies of developers’ requirement specifications to their customers. However, they may be willing to provide access to these requirements for review, during an onsite vendor audit. PhRMA recommends replacing the last sentence with the following: “If possible (e.g., during a vendor audit), the end user should review a copy of the developer’s requirements specifications for comparison.”

Section 6.1.2

Page 12-13, lines 199-218; Considering the complexity and size of today's code, PhRMA notes that it is not realistic to expect that source code review could accurately judge how good the code is, whether or not it will work, or how much testing must be done by purchaser. This section of the guidance assumes that software vendors would agree to disclose their software’s limitations and that their clients would disclose usage experiences with the software products when asked. This is a naïve assumption. For many broad-based software products, the pharmaceutical industry does not have enough influence to force providers to produce the desired information when it is not normally available. Other means, such as those mentioned in lines 201-208 and section 5.6 and 6.1.3, are more useful. Therefore, PhRMA recommends removing the implication that source code must be reviewed if available.

Page 12, line 200; FDA should change the end of the sentence from “by doing all of the following” to “by doing either or both of the following:”

Page 12, line 201; PhRMA recommends changing the language to: “Conducting research into the program’s use history whenever possible.”

Section 6.1.3

PhRMA recommends that FDA clarify the concept that more extensive functional testing may be warranted when users cannot “directly review the program source code or development documentation.” Conversely, the current draft guidance implies that less extensive testing might be appropriate for systems that are more transparent and when users are able to examine and evaluate the quality of source code and system documents. In effect, the guidance suggests that evaluation of code and documentation by qualified and knowledgeable users can be acceptably substituted for static verification techniques that might be performed by developers. Assuming a vendor audit showed adequate software testing by the developer, PhRMA recommends that FDA clarify how much of section 5.4 must be repeated by the purchasing company, especially around the considerations in lines 100-112.

Page 13, line 217; PhRMA recommends changing to: “Note, however, functional testing alone is not sufficient to establish software adequacy and needs to be supplemented with the other elements described in this section.” This is more conclusive than the original language.

Section 6.2

Page 14, line 228; PhRMA recommends FDA add an additional bullet: “use of data encryption to ensure data integrity and high fidelity transfer of confidential data.” This is necessary as the Internet configuration is dynamic and additional examples will provide guidance as to other measures the FDA expects the user to implement.

Page 14, line 229; after measures, FDA should add “(both technical and procedural)”

Page 14, line 235; at the end of sentence “Examples of such measures include:” FDA should add “but are not limited to:”

Page 14, line 236; FDA should add “Validated” to beginning of sentence. This will add additional clarification.

Page 14, line 238; FDA should add “For measures that cannot be validated, delivery acknowledgments can be used such as...”

Appendix A References, pages 18-21; PhRMA believes that the entire General Software Quality References section should be deleted. Objective references, e.g., governmental and international /national standards and documents, are useful and should be included. However, the General software Quality References section is less appropriate due to its general nature.

PhRMA trusts that these comments are useful to FDA as this guidance is finalized. Please do not hesitate to contact me if any of these points require clarification.

Sincerely,



Draft Guidance for Industry - Not For Implementation

Guidance for Industry

21 CFR Part 11; Electronic Records; Electronic Signatures

Validation

Draft Guidance

This guidance document is being distributed for comment purposes only.

Comments and suggestions regarding this draft document should be submitted within 90 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit comments to Dockets Management Branch (HFA-305), Food and Drug Administration, 5630 Fishers Lane, room 1061, Rockville, MD 20852. All comments should be identified with the docket number OOD-1538.

For questions regarding this draft document contact Paul J. Motise, Office of Enforcement, Office of Regulatory Affairs, 301-827-0383, e-mail: pmotise@ora.fda.gov.

U.S. Department of Health and Human Services
Food and Drug Administration
Office of Regulatory Affairs (ORA)
Center for Biologics Evaluation and Research (CBER)
Center for Drug Evaluation and Research (CDER)
Center for Devices and Radiological Health (CDRH)
Center for Food Safety and Applied Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
August 2001

Draft Guidance for Industry - Not For Implementation

Guidance For Industry

21 CFR Part 11; Electronic Records;

Electronic Signatures

Validation

Additional copies of this draft guidance document are available from the Office of Enforcement, HFC-200, 5600 Fishers Lane, Rockville, MD 20857; Internet http://www.fda.gov/ora/compliance_ref/part11.htm

U.S. Department of Health and Human Services
Food and Drug Administration
Office of Regulatory Affairs (ORA)
Center for Biologics Evaluation and Research (CBER)
Center for Drug Evaluation and Research (CDER)
Center for Devices and Radiological Health (CDRH)
Center for Food Safety and Applied Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
August 2001

Guidance For Industry

21 CFR Part 11; Electronic Records; Electronic Signatures

Validation

Table of Contents

1. Purpose.....	1
2. Scope.....	1
2.1 Applicability.....	2
2.2 Audience.....	3
3. Definitions and Terminology	3
4. Regulatory Requirements; What Does Part 11 Require?	3
5. Key Principles.....	4
5.1 System Requirements Specifications.....	4
5.2 Documentation of Validation Activity	6
5.2.1 Validation Plan.....	6
5.2.2 Validation Procedures.....	6
5.2.3 Validation Report.....	6
5.3 Equipment Installation	7
5.4 Dynamic Testing.....	7
5.4.1 Key Testing Considerations	7
5.4.2 Software testing should include:	8
5.4.3 How test results should be expressed.	8
5.5 Static Verification Techniques	9
5.6 Extent of Validation	9
5.7 Independence of Review.....	10
5.8 Change Control (Configuration Management)	10
6. Special Considerations	11
6.1 Commercial, Off-The-Shelf Software.....	11
6.1.1 End User Requirements Specifications.....	12
6.1.2 Software Structural Integrity.....	12
6.1.3 Functional Testing of Software	13
6.2 The Internet.....	13
6.2.1 Internet Validation.....	13
Appendix A - References	15

Guidance For Industry¹

21 CFR Part 11; Electronic Records; Electronic Signatures Validation

This draft guidance, when finalized, will represent the Food and Drug Administration's (FDA'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 FDA or the public. An alternative approach may be used if such approach satisfies the requirements of applicable statutes and regulations.

1. Purpose

1 The purpose of this draft guidance is to describe the Food and Drug Administration's
2 (FDA's) current thinking regarding considerations in meeting the validation requirements of
3 Part 11 of Title 21 of the Code of Federal Regulations; Electronic Records; Electronic
4 Signatures. It provides guidance to industry, and is intended to assist persons who are
5 subject to the rule to comply with the regulation. It may also assist FDA staff who apply
6 part 11 to persons who are subject to the regulation.

2. Scope

7 This draft guidance is one of a series of guidances about part 11. We intend to provide
8 information with respect to FDA's current thinking on acceptable ways of meeting part 11

9 ¹ This draft guidance was prepared under the aegis of the Office of Enforcement by the FDA Part 11
10 Compliance Committee. The committee is composed of representatives from each center within the Food
11 and Drug Administration, the Office of Chief Counsel and the Office of Regulatory Affairs.

Draft Guidance for Industry - Not For Implementation

12 requirements to ensure that electronic records and electronic signatures are trustworthy,
13 reliable, and compatible with FDA's public health responsibilities.

14 Electronic record and electronic signature systems consist of both manual procedural
15 controls and technical controls implemented through computer systems. This draft
16 guidance focuses on validation of computer systems. It identifies key validation principles
17 and addresses some frequently asked questions, but it is not intended to cover everything
18 that computer systems validation should encompass in the context of electronic
19 record/electronic signature systems. You can read more information about computer
20 systems validation in the documents listed in Appendix A - References.

2.1 Applicability

21 This draft guidance applies to electronic records and electronic signatures that persons
22 create, modify, maintain, archive, retrieve, or transmit under any records or signature
23 requirement set forth in the Federal Food, Drug, and Cosmetic Act (the Act), the Public
24 Health Service Act (PHS Act), or any FDA regulation. Any requirements set forth in the
25 Act, the PHS Act, or any FDA regulation, with the exception of part 11, are referred to in
26 this document as predicate rules. Most predicate rules are contained in Title 21 of the
27 Code of Federal Regulations. In general, predicate rules address the research, production,
28 and control of FDA regulated articles, and fall into several broad categories. Examples of
29 such categories include, but are not limited to, manufacturing practices, laboratory

Draft Guidance for Industry - Not For Implementation

30 practices, clinical and pre-clinical research, adverse event reporting, product tracking, and pre
31 and post marketing submissions and reports.

2.2 Audience

32 We intend this draft guidance to provide useful information and recommendations to:

- 33 • Persons subject to part 11;
- 34 • Persons responsible for validation of systems used in electronic recordkeeping;
- 35 • Persons who develop products or services to enable implementation of part 11
36 requirements; and,

37 This draft guidance may also assist FDA staff who apply part 11 to persons subject to the
38 regulation.

3. Definitions and Terminology

39 Unless otherwise specified below, all terms used in this draft guidance are defined in FDA's
40 draft guidance document, "Guidance For Industry, 21 CFR Part 11; Electronic Records;
41 Electronic Signatures, Glossary of Terms," a document common to the series of guidances
42 on part 11.

4. Regulatory Requirements; What Does Part 11 Require?

43 Section 11.10 requires persons to "employ procedures and controls designed to ensure the
44 authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to
45 ensure that the signer cannot readily repudiate the signed record as not genuine." To

46 satisfy this requirement persons must, among other things, employ procedures and controls
47 that include "[v]alidation of systems to ensure accuracy, reliability, consistent intended
48 performance, and the ability to discern invalid or altered records."

5. Key Principles

49 Here are some key principles you should consider when validating electronic recordkeeping
50 computer systems.

5.1 System Requirements Specifications

51 Regardless of whether the computer system is developed in-house, developed by a
52 contractor, or purchased off-the-shelf, establishing documented end user (i.e., a person
53 regulated by FDA) requirements is extremely important for computer systems validation.
54 Without first establishing end user needs and intended uses, we believe it is virtually
55 impossible to confirm that the system can consistently meet them. Once you have
56 established the end user's needs and intended uses, you should obtain evidence that the
57 computer system implements those needs correctly and that they are traceable to system
58 design requirements and specifications. It is important that your end user requirements
59 specifications take into account predicate rules, part 11, and other needs unique to your
60 system that relate to ensuring record authenticity, integrity, signer non-repudiation, and,
61 when appropriate, confidentiality. For example, as noted above, section 11.10 has a
62 general requirement that persons who use closed systems to create, modify, maintain, or
63 transmit electronic records must employ procedures and controls designed to ensure the

Draft Guidance for Industry - Not For Implementation

64 authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and
65 to ensure that signers cannot readily repudiate signed records as not genuine. In addition,
66 section 11.30 requires persons who use open systems to employ procedures and controls
67 identified in section 11.10, as appropriate; persons who use open systems must also
68 implement special procedures and controls, such as document encryption and use of digital
69 signature standards, as necessary under the circumstances, to ensure record authenticity,
70 integrity, and confidentiality.

71 Other factors not specifically addressed in part 11 may also impact on electronic record
72 trustworthiness, integrity and system performance. You should consider these factors and
73 establish appropriate requirements specifications for them, as well. Here are some
74 examples:

- 75 • Scanning processes: where a paper record is scanned to create an electronic
76 record, scanner resolution, scanning rates, color fidelity, and the type of
77 hardware interface may impact the accuracy and reliability of the electronic
78 record as well as system performance.
- 79 • Scalability: in a networked environment, system performance may be affected by
80 the number of workstations and bandwidth demands of file size and types.
- 81 • Operating environment: sources of electromagnetic interference, radio frequency
82 interference, temperature/humidity, and electrical power
83 fluctuations may affect system performance.

5.2 Documentation of Validation Activity

84 We consider thorough documentation to be extremely important to the success of your
85 validation efforts. Validation documentation should include a validation plan, validation
86 procedures, and a validation report, and should identify who in management is responsible for
87 approval of the plan, the procedures and the report.

88 5.2.1 Validation Plan

89 The validation plan is a strategic document that should state what is to be done, the scope
90 of approach, the schedule of validation activities, and tasks to be performed. The plan
91 should also state who is responsible for performing each validation activity. The plan
92 should be reviewed and approved by designated management.

93 5.2.2 Validation Procedures

94 The validation procedures should include detailed steps for how to conduct the validation.
95 It should describe the computer system configuration, as well as test methods and
96 objective acceptance criteria, including expected outcomes. The procedures should be
97 reviewed and approved by designated management.

98 5.2.3 Validation Report

99 The validation report should document detailed results of the validation effort, including test
100 results. Whenever possible, test results should be expressed in quantified terms rather
101 than stated as "pass/fail." The report should be reviewed and approved by designated
102 management.

5.3 Equipment Installation

103 Prior to testing, you should confirm that all hardware and software are properly installed
104 and, where necessary, adjusted and calibrated to meet specifications. User manuals, standard
105 operating procedures, equipment lists, specification sheets, and other documentation should
106 be readily accessible for reference.

5.4 Dynamic Testing

107 5.4.1 Key Testing Considerations

- 108 • Test conditions: test conditions should include not only "normal" or "expected"
109 values, but also stress conditions (such as a high number of users accessing a
110 network at the same time). Test conditions should extend to boundary values,
111 unexpected data entries, error conditions, reasonableness challenges (e.g.,
112 empty fields, and date outliers), branches, data flow, and combinations of inputs.
- 113 • Simulation tests: some testing may be performed using simulators, usually
114 conducted off-line outside of the actual user's computing environment.
- 115 • Live, user-site tests: these tests are performed in the end user's computing
116 environment under actual operating conditions. Testing should cover
117 • continuous operations for a sufficient time to allow the system to encounter a
118 wide spectrum of conditions and events in an effort to detect any latent faults that
119 are not apparent during normal activities.

120 5.4.2 Software testing should include:

- 121 • Structural testing: this testing takes into account the internal mechanism
122 (structure) of a system or component. It is sometimes referred to as "white
123 box" testing. Structural testing should show that the software creator followed
124 contemporary quality standards (e.g., consensus standards from national and
125 international standards development organizations, such as those listed in
126 Appendix A of this guidance). This testing usually includes inspection (or
127 walk-throughs) of the program code and development documents.
- 128 • Functional testing: this testing involves running the program under known
129 conditions with defined inputs, and documented outcomes that can be
130 compared to pre-defined expectations. Functional testing is sometimes called
131 "black box" testing.
- 132 • Program build testing: this testing is performed on units of code (modules), integrated
133 units of code, and the program as a whole.

134 5.4.3 How test results should be expressed.

135 Quantifiable test results should be recorded in quantified rather than qualified (e.g.,
136 pass/fail) terms. Quantified results allow for subsequent review and independent
137 evaluation of the test results.

5.5 Static Verification Techniques

138 While dynamic testing is an important part of validation, we believe that by using dynamic
139 testing alone it would be virtually impossible to fully demonstrate complete and correct system
140 performance. A conclusion that a system is validated is also supported by
141 numerous verification steps undertaken throughout the system development. These
142 include static analyses such as document and code inspections, walk-throughs, and
143 technical reviews. Where available, knowledge of these activities and their outcomes can help
144 to focus testing efforts, and help to reduce the amount of system level functional
145 testing needed at the user site in order to validate that the software meets the user's needs
146 and intended uses.

5.6 Extent of Validation

147 When you determine the appropriate extent of system validation, the factors you should
148 consider include (but are not limited to) the following:

- 149 • The risk that the system poses to product safety, efficacy, and quality; note that
150 product means the FDA regulated article (food, human or veterinary drug,
151 biological product, medical device, or radiological product);
- 152 • The risk that the system poses to data integrity, authenticity, and confidentiality;
153 and,
- 154 • The system's complexity; a more complex system might warrant a more
155 comprehensive validation effort.

5.7 Independence of Review

157 It is a quality assurance tenet that objective self-evaluation is difficult. Therefore, where
158 possible, and especially for higher risk applications, computer system validation should be
159 performed by persons other than those responsible for building the system. Two
160 approaches to ensuring an objective review are: (1) Engaging a third party; and, (2) dividing
161 the work within an organization such that people who review the system (or a portion of the
162 system) are not the same people who built it.

5.8 Change Control (Configuration Management)

163 Systems should be in place to control changes and evaluate the extent of revalidation that the
164 changes would necessitate. The extent of revalidation will depend upon the change's nature,
165 scope, and potential impact on a validated system and established operating conditions.
166 Changes that cause the system to operate outside of previously validated operating limits
167 would be particularly significant.

168 Contractor or vendor upgrades or maintenance activities, especially when performed remotely
169 (i.e., over a network), should be carefully monitored because they can introduce changes that
170 might otherwise go unnoticed and have an adverse effect on a validated system. Examples of
171 such activities include installation of circuit boards that might hold
172 new versions of "firmware" software, addition of new network elements, and software
173 "upgrades", "fixes" or "service packs." It is important that system users be aware of such

Draft Guidance for Industry - Not For Implementation

174 changes to their system. You should arrange for service providers to advise you regarding
175 the nature of such revisions so you can assess the changes and perform appropriate
176 revalidation.

177 We consider regression analysis to be an extremely important tool that should be used to
178 assess portions of a system that were themselves unchanged but are nonetheless
179 vulnerable to performance/reliability losses that the changes can cause. For instance, new
180 software might alter performance of other software on a system (e.g., by putting into place
181 new device drivers or other code that programs share.) Regression testing should be
182 performed based on the results of the regression analysis.

6. Special Considerations

6.1 Commercial, Off-The-Shelf Software

183 Commercial software used in electronic recordkeeping systems subject to part 11 needs to
184 be validated, just as programs written by end users need to be validated. See 62 Federal
185 Register 13430 at 13444-13445 (March 20, 1997.) We do not consider commercial
186 marketing alone to be sufficient proof of a program's performance suitability. The end user
187 is responsible for a program's suitability as used in the regulatory environment. However,
188 the end user's validation approach for off-the-shelf software is somewhat different from
189 what the developer does because the source code and development documentation are
190 not usually available to the end user. End users should validate any program macros and

Draft Guidance for Industry - Not For Implementation

191 other customizations that they prepare. End users should also be able to validate off-the-shelf
192 software by performing all of the following:

193 6.1.1 End User Requirements Specifications

194 End users should document their requirements specifications relative to part 11
195 requirements and other factors, as discussed above. The end user's requirements
196 specifications may be different from the developer's specifications. If possible, the end
197 user should obtain a copy of the developer's requirements specifications for comparison.

198 6.1.2 Software Structural Integrity

199 Where source code is not available for examination, end users should infer the adequacy of
200 software structural integrity by doing all of the following:

- 201 • Conducting research into the program's use history. This research should
202 include: (1) Identifying known program limitations; (2) evaluating other end user
203 experiences; and, (3) identifying known software problems and their resolution;
204 and
- 205 • Evaluating the supplier's software development activities to determine its
206 conformance to contemporary standards. The evaluation should preferably be derived
207 from a reliable audit of the software developer, performed by the end
208 user's organization or a trusted and competent third party.

209 6.1.3 Functional Testing of Software

210 End users should conduct functional testing of software that covers all functions of the
211 program that the end user will use. Testing considerations discussed above should be applied.
212 When the end user cannot directly review the program source code or
213 development documentation (e.g., for most commercial off-the-shelf software, and for some
214 contracted software,) more extensive functional testing might be warranted than when such
215 documentation is available to the user. More extensive functional testing might also be
216 warranted where general experience with a program is limited, or the software performance
217 is highly significant to data/record integrity and authenticity. Note, however, we do not
218 believe that functional testing alone is sufficient to establish software adequacy.

6.2 The Internet

219 We recognize the expanding role of the Internet in electronic recordkeeping in the context
220 of part 11. Vital records, such as clinical data reports or batch release approvals, can be
221 transmitted from source to destination computing systems by way of the Internet.

222 6.2.1 Internet Validation

223 We recognize that the Internet, as computer system, cannot be validated because its
224 configuration is dynamic. For example, when a record is transmitted from source to destination
225 computers, various portions (or packets) of the record may travel along different

Draft Guidance for Industry - Not For Implementation

226 paths, a route that neither sender nor recipient can define or know ahead of time. In
227 addition, entirely different paths might be used for subsequent transfers.

228 The Internet can nonetheless be a trustworthy and reliable communications pipeline for
229 electronic records when there are measures in place to ensure the accurate, complete and
230 timely transfer of data and records from source to destination computing systems.

231 Validation of both the source and destination computing systems (i.e., both ends of the
232 Internet communications pipeline) should extend to those measures. We therefore
233 consider it extremely important that those measures are fully documented as part of the
234 system requirements specifications, so they can be validated. Examples of such measures
235 include:

- 236 • Use of digital signature technology to verify that electronic records have not
237 been altered and that the sender's authenticity is affirmed.
- 238 • Delivery acknowledgements such as receipts or separate confirmations
239 executed apart from the Internet (e.g., via fax or voice telephone lines.)

Appendix A - References

Much has been written about activities that support computer systems validation. You may find the following references useful to your validation efforts.

Food and Drug Administration References

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.

Guidance for Industry: Computerized Systems Used in Clinical Trials, Food and Drug Administration, April 1999.

Guidance for Industry and for FDA Staff: General Principles of Software Validation, Center for Devices and Radiological Health, Food and Drug Administration, Draft - June 1997.

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.

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.

Guideline on General Principles of Process Validation, Center for Drugs and Biologics, & Center For Devices and Radiological Health, Food and Drug Administration, May 1987.

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

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.

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, 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.

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 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/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.

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

Draft Guidance for Industry - Not For Implementation

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.

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.

Draft Guidance for Industry - Not For Implementation

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.

Janis V. Halvorsen, *A Software Requirements Specification Document Model for the Medical Device Industry*, Proceedings IEEE SOUTH EASTCON '93, Banking on Technology, April 4th -7th, 1993, Charlotte, North Carolina.

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.

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-

Draft Guidance for Industry - Not For Implementation

201-87756-2.

Alan Kusnitz, "Software Validation" ; *Current Issues in Medical Device Quality Systems*, Association for the Advancement of Medical Instrumentation, 1997. ISBN 1-57020-075-0.

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.

Glenford J. Myers, *The Art of Software Testing*, John Wiley & Sons, 1979. ISBN 0-471-04328-1.

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.

Draft Guidance for Industry - Not For Implementation

Karl E. Wieggers, *Creating a Software Engineering Culture*, Dorset House Publishing, 1996. ISBN 0-932633-33-1.

Karl E. Wieggers, *Software Inspection, Improving Quality with Software Inspections*, Software Development, April 1995, pages 55-64.

Karl E. Wieggers, *Software Requirements*, Microsoft Press, 1999. ISBN 0-7356-0631-5.

DocID Validation Draft.PostRES.doc 08/29/01