

---

# PROPOSED VALIDATION STANDARD VS-2

## *Computer-Related System Validation*

### AUTHORS

**Lead  
Author**

*Barbara Mullendore*  
AstraZeneca

*Kenneth G. Chapman*  
Drumbeat Dimensions, Inc.

### REVIEWERS

*Robert W. Stotz, Ph.D.*  
Validation Technologies, Inc.

*Jay H. King*  
LifeScan, a Johnson & Johnson Company

### Introduction

This Preamble by the **Institute of Validation Technology Standards Committee (IVT/SC)** introduces the second in a series of new proposed validation standards that are available to reviewers of manuscripts intended for publication in the *Journal of Validation Technology* and the *Journal of GXP Compliance* (formerly the *Journal of cGMP Compliance*). It will also be useful to practitioners worldwide who develop, implement, validate, and maintain systems used to automate manufacturing processes, or to otherwise influence the ultimate quality, safety, or efficacy of drug substances or drug products. The focus of this proposed standard is the pharmaceutical industry.

#### *Regulations, Guidance Documents, and Standards*

What are the differences between regulations, guidance documents, and standards? In the United States, current Good Manufacturing Practice (GMP) regulations evolve only through due process and are considered binding and legally substantive, which means that violation represents a criminal act. Food and Drug Administration (FDA) guidance documents and guidelines do not necessarily evolve through due process and are no more legally binding than are industrial guidance documents. Rules Governing Medicinal Products in the European Community (EC), counterpart of U.S. GMPs, are also portrayed as non-binding; however, such rules in the European Union (EU) and, after a few years, FDA Guidance Documents and Guidelines in the U.S. all commonly become treated as de facto law.

In the directly related subject area of software validation, professional organizations like the Institute of Electrical and Electronics Engineers (IEEE) have demonstrated the value of setting standards. Rapid evolution and implementation of computer technology in today's pharmaceutical operations call for considerable focus on the validation of computer-related systems. As with process validation, numerous guidance documents, guidelines, published articles, and even regulations have appeared in recent years on the subject of computer-related system validation, most of which have relied on IEEE standards for the software portion of this important subject.

#### *Style of the IVT Proposed Validation Standard*

A fundamental need the **IVT/SC** intends to meet with its new proposed standards stems from the fact that most regulations today call for written policies and procedures to address their every aspect. Thus, the **IVT** proposed validation standards format includes statements that can be excised and used directly, or with minor editing in company policies and Standard Operating Procedures (SOPs). All **IVT** proposed standards are available on the company's web site at [www.ivthome.com](http://www.ivthome.com).

---

Most pharmaceutical firms like to have lists of succinct, unambiguous, and specific rules about quality assurance against which to audit. It is preferable for such rules to contain imperative verbs like “shall,” “will,” and “must” rather than passive verbs like “should,” “may,” and “can” to avoid interpretive debates with auditees. Standards usually satisfy this need, whereas guidance documents often do not. However, it is also important for those who are to follow the rules to have access to some interpretive documents that accompany and explain the rules. Thus, FDA provides a Preamble to each of its regulations. Similarly, the **IVT/SC** plans to accompany each proposed validation standard with a Preamble like this one, to amplify the rationale behind the rules contained.

As will be explained, many finalized and draft standards/guidelines covering validation of computer-related systems have emerged in the past 20 years. Why is this proposed standard needed? The **IVT/SC** believes VS-2 is needed and will be potentially useful for the following reasons. VS-2:

- Is designed to be comprehensive, contemporary, and consistent in its technical content as well as in its updating and optimization of the use and definition of key terms
- Uniquely separates its succinct standards statements from preamble-type explanation and elaboration about what those standards mean and how they were derived
- Addresses all three GXP components (GMP, GLP, and GCP), rather than just one or two
- Provides commonality of terms and principles with other **IVT/SC** proposed validation standards, promoting a more cohesive understanding and approach to validation of all types

#### ***Contents of the Proposed Validation Standard***

Each **IVT** proposed validation standard is separate from its Preamble and contains six sections:

- I. Policy Standards – Statements that indicate what is required
- II. Practice Standards – Statements that describe how to achieve requirements
- III. Acronyms – Definition of each acronym used in the document
- IV. Glossary – Definition of key terms, which are highlighted and asterisked (\*) when first used in the proposed validation standard
- V. Regulatory Excerpts – Regulatory language related to each standard
- VI. Useful References – Bibliography of selected technical references

#### ***Future Proposed Validation Standards by IVT/SC***

The **IVT/SC** authors plan to deliver several new sets of **IVT** proposed standards for publication in the *Journal of Validation Technology* over the next few years. Future proposed standards in preparation or under consideration include the following (not necessarily in the order of proposed publication):

- Validation of Analytical Test Methods
- Aseptic Pharmaceutical Process Validation
- Biopharmaceutical Process Validation
- Medical Device Process Validation
- Equipment Cleaning Validation
- Water Treatment System Validation
- Terminal Sterilization Validation

Already published was the Proposed Validation Standard VS-1: Non-Aseptic Pharmaceutical Processes.<sup>1</sup>

---

## Preamble

When FDA's GMPs were proposed in 1977, two of its chief architects, Bud Loftus and Ted Byers, lectured that the GMPs were designed to reflect what the "better-managed" (not the "best-managed") firms were already doing. Their point was clear: FDA did not want its proposed regulations to demand practices that were out of reach for most firms at that time. The **IVT/SC** has taken note of that successful experience and will attempt to structure all its proposed validation standards to reflect practices that are reasonable, achievable, and verifiable. Where cutting edge technology or practice comes to bear, the merits of such technology or practice will be discussed in this accompanying Preamble, but not in the proposed validation standards.

### *Some Specific Points About the Proposed Computerized System Validation Standard*

#### ■ On the Subject of GXP

Just about every school of thought relative to validation includes the standard approach of Installation Qualification (IQ), Operational Qualification (OQ), and Performance Qualification (PQ). This approach is primarily pharmaceutical GMP-driven and is appropriate for process, cleaning, utility, and other types of validation, as well as computer system validation in a production setting where automated systems are used to control operating processes and are validated within the larger context of the entire automated system. In some cases however, there may be difficulty in applying the IQ/OQ/PQ methodology to information systems in a non-shop-floor environment, such as the pharmaceutical research arena. An additional complicating factor is added to the computer validation process when these information systems are developed internally rather than purchased, either as a whole or in part. Additionally, many commercial software packages require extensive configuration. In an attempt to address the factor of internal development and configuration, some companies have borrowed from the medical device arena by including a design qualification or Design Verification and Review (DVR) in their computer system validation methodology.<sup>2</sup> Lastly, since the use of information systems is often not a part of repeatable production processes, the PQ portion of the standard methodology often does not really fit. (This statement excludes such things as Programmable Logic Controllers (PLCs) and embedded chips that are normally validated along with the equipment they control, and for which the IQ/OQ/PQ approach is appropriate.)

The terms IQ, OQ, and PQ are used in this standard for consistency with other **IVT** proposed standards, and also because these terms are the most widely used in Industry. It may be appropriate, however, to build flexibility into the testing methodology and protocols that accommodate non-shop-floor information systems.

Although the basic principles of computer validation and associated activities apply across all regulatory arenas, they are more firmly established within the GMP arena at present. Therefore, there is typically a slant toward GMP with respect to guidance regarding the execution of these basic principles.

#### ■ On the Subject of Part 11

The broad topic and details associated with 21 CFR Part 11, Electronic Records/Electronic Signatures are beyond the scope of this proposed standard. However, since most GXP requirements include records and signatures, and since Part 11 includes validation of all automated systems concerned as its first requirement, it appears axiomatic that the two subjects are about to merge into one. The **IVT/SC** will consider publishing a future proposed validation standard, if it appears needed.

#### ■ Overview of Computer-Related Systems Validation

Since 1983, many useful guidance documents, books, and technical articles, plus a limited number of regulations, have appeared addressing Computer-Related Systems Validation (CRSV). One of the earliest addressed specifically to the pharmaceutical industry was *The Bluebook* by Rick Garwood and Paul Motise in 1983.<sup>3</sup> *The Bluebook* emphasized software validation and software quality, subjects that have received considerable attention in most subsequent CRSV guidance documents.

---

IEEE's software standards present a comprehensive set of logically devised and ordered standards for developing and maintaining software and systems via good quality engineering practices and adequate checks and balances throughout the lifecycle.<sup>4</sup> Prior to this lifecycle perspective, computer system validation (as well as validation in general) was largely considered to be solely an exercise in testing the resulting software or system. IEEE's approach helped to advance the understanding that the process of actually developing the software and system must include good quality practices as well, otherwise testing would simply reveal problems and initiate rework, resulting in a "patchwork quilt" of mended code and configuration. Likewise, these good quality practices must continue into the maintenance phase of the system to ensure that its stable state is retained, and that the system remains robust and maintainable. Thus, IEEE's treatment of software testing, quality, and validation, including use of the lifecycle approach, has contributed substantially to the development of subsequent CRSV guidelines and standards.

### ***The Validation Master Plan***

The system-specific Validation Master Plan (VMP) is a master document that begins with the initiation of any computer system validation project. Although the VMP is specifically called for by most contemporary draft and approved validation guidelines, it has become a confusing term because two basic definitions exist; both are used by different (and sometimes even the same) regulatory officials. One definition calls for the VMP to be project-oriented, as in this and other **IVT** proposed validation standards. The other definition describes a more global document embracing a firm's overall validation philosophy.

Most pharmaceutical firms use policies and/or SOPs to address such global matters individually. **IVT/SC** finds the second (global) VMP definition workable, but cumbersome and inefficient. To minimize confusion, a firm should clearly define its use of the term VMP (e.g., by written policy or SOP), while ensuring that global and project-related matters are both adequately covered in some way. For firms preferring the global VMP, a term such as "Validation Project Plan" can be used in place of the VMP defined in VS-2.

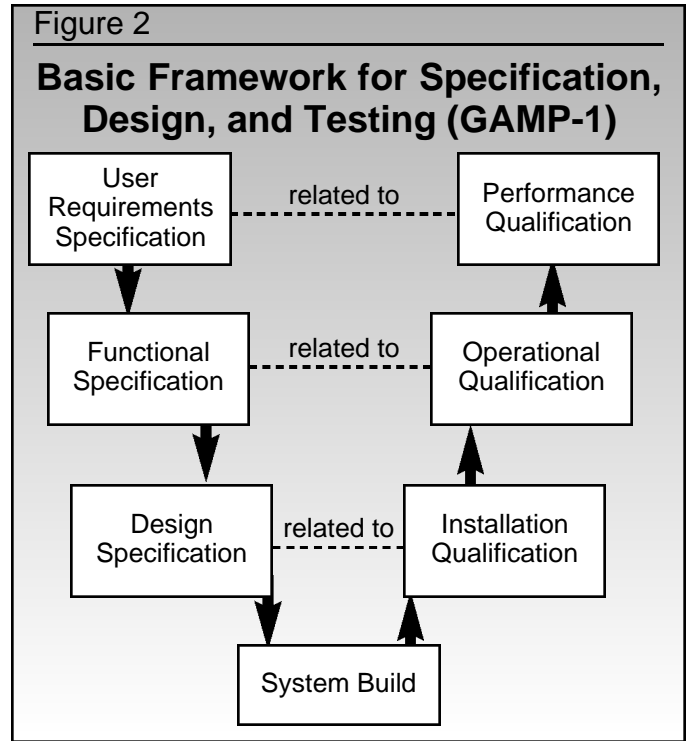
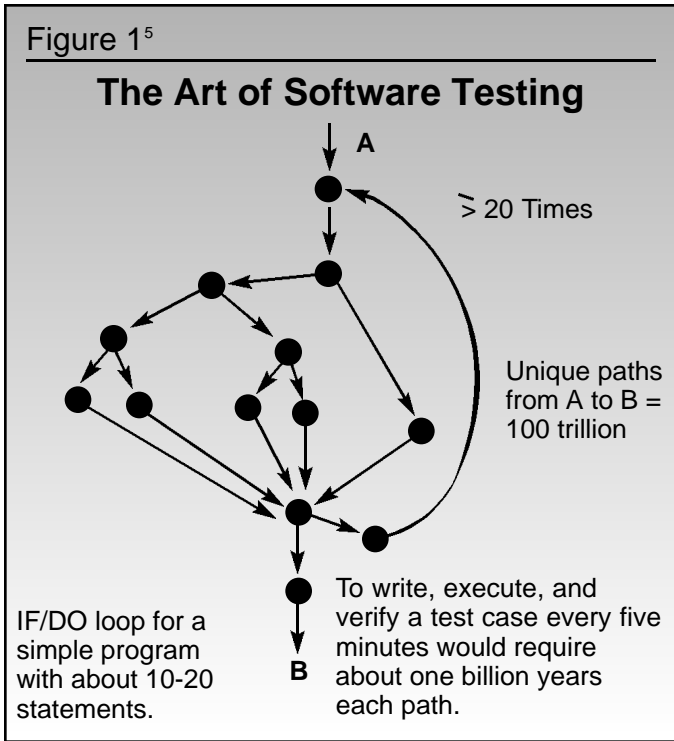
### ***The Source Code Controversy and Dynamic Path Analysis***

FDA's initial insistence upon the user firm possessing copies of original source code presumably stemmed from the stance that source code equals procedures, and must therefore be in the total control of the user firm. Having the source code on hand may be useful in instances where the supplier goes out of business or otherwise can no longer support the software. In this case, possessing the source code could enable the user firm to troubleshoot, modify, and otherwise maintain the software until a viable replacement could be implemented. Of course, this assumes the available expertise to do so.

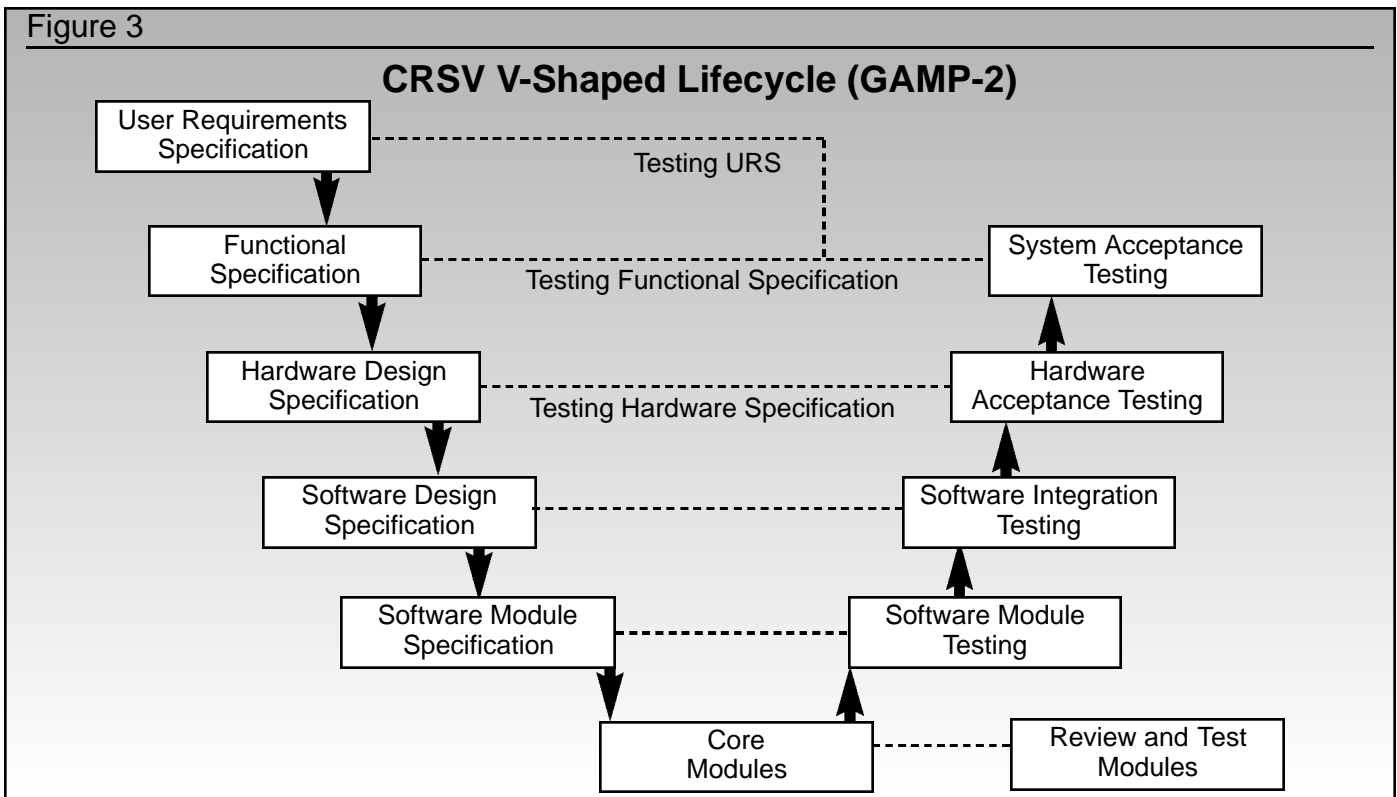
However, this assurance can also be accomplished by other means, such as maintaining source code availability via use of an escrow account or other similar arrangement, affording the same protection with a more feasible (and less costly) solution. This option also allows for the available code to be kept current, without additional cost and logistical complications. In any case, most software suppliers are not willing to provide copies of source code unless the software is developed expressly for a given firm. A review of more recent computer-related FDA observations reveals that this "pseudo-requirement" of actual possession of the code is no longer expected. An exception obviously being if the code is actually developed by, or customized for, the user firm, in which case the firm would possess it, and the code must be adequately documented.

In the early stages, the FDA expected suppliers and user firms to perform dynamic path analysis on all code, which has been proven to be mathematically impossible (see *Figure 1*).<sup>5</sup> It is since understood that quality must be built into the software and cannot be tested in, no matter how many paths are documented and analyzed.

These new understandings came largely from a paradigm shift that occurred from the early 1980s to the early 1990s. During this time, the software industry proved sensitive to the functional needs of its clients in the pharmaceutical industry and migrated steadily from mostly customized source code to mostly Commercial Off-the-Shelf (COTS) software. With this transition, the emphasis of software vendor quality audits also shifted subtly from dwelling on details of how specific programs were developed to focusing on the supplier's basic software



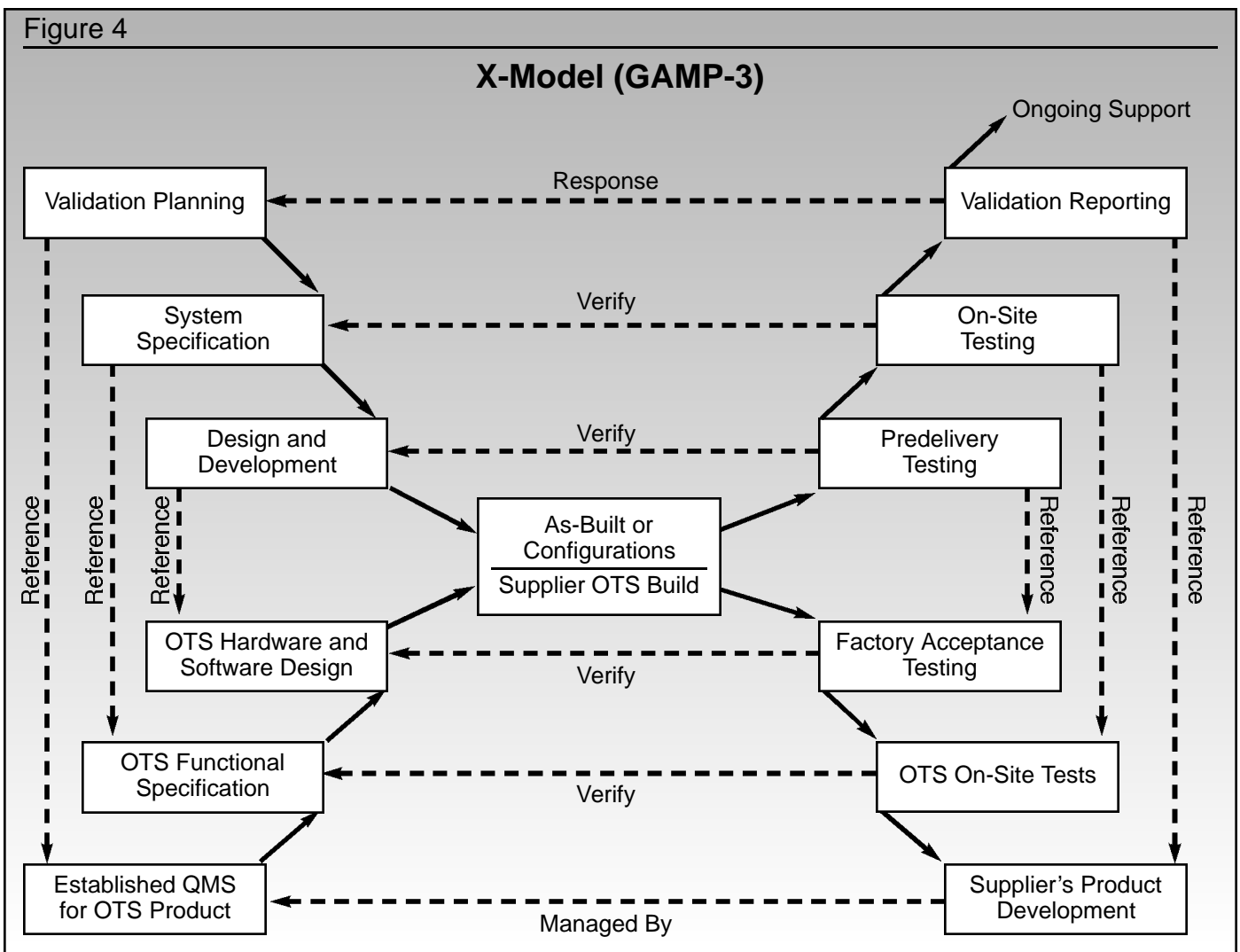
development process itself. When a supplier is producing hundreds or even thousands of the same version of a configurable program annually, users no longer need, nor have the opportunity, to inspect each line of code. Instead, the emphasis must be redirected to judging market performance and system functionality, including reliability of all relevant configuration options. Audits of the software producer, when it is possible to conduct such audits, now commonly involve ensuring that reliable software development practices, including change controls, exist and are being followed.



During the same transition era, the need to, the practicality of, and the rationale for possessing a supplier's source code diminished. Having access to all original and customized source code remained vital to a sound validation program; but even suggesting that Bill Gates should share his source code with customers worldwide would earn only a chuckle.

In 1986, taking a leaf from IEEE, the Pharmaceutical Manufacturers Association (PMA) incorporated a waterfall lifecycle to portray validation of computerized systems in its *Validation Concepts for Computer Systems Used in the Manufacture of Drug Products*.<sup>6</sup> Nine years later, the Parenteral Drug Association (PDA) included an enhanced waterfall lifecycle in its Technical Report No. 18.<sup>7</sup> In 1996, the GAMP Forum published the *GAMP Supplier Guide, Version 2*<sup>8</sup> which added a V-shaped lifecycle to waterfall versions. The V-shaped lifecycle adds the powerful feature of associating test plans directly with functional specifications as those specifications are created (see *Figure 2*). The *GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture, Version 3.0*<sup>9</sup> appeared in 1998 offering an enhanced V-shaped lifecycle (see *Figure 3*) plus a new X-shaped lifecycle (see *Figure 4*) that associates supplier activities with user activities in the validation process.

All of the above guidelines originated by Industry have contributed significantly to understanding, by pharmaceutical firms and by suppliers, of how to cope with validation requirements for systems that are based on swiftly-evolving new technology. Although variations exist, all versions of the lifecycle modules involve the same fundamentals and are compatible with each other.



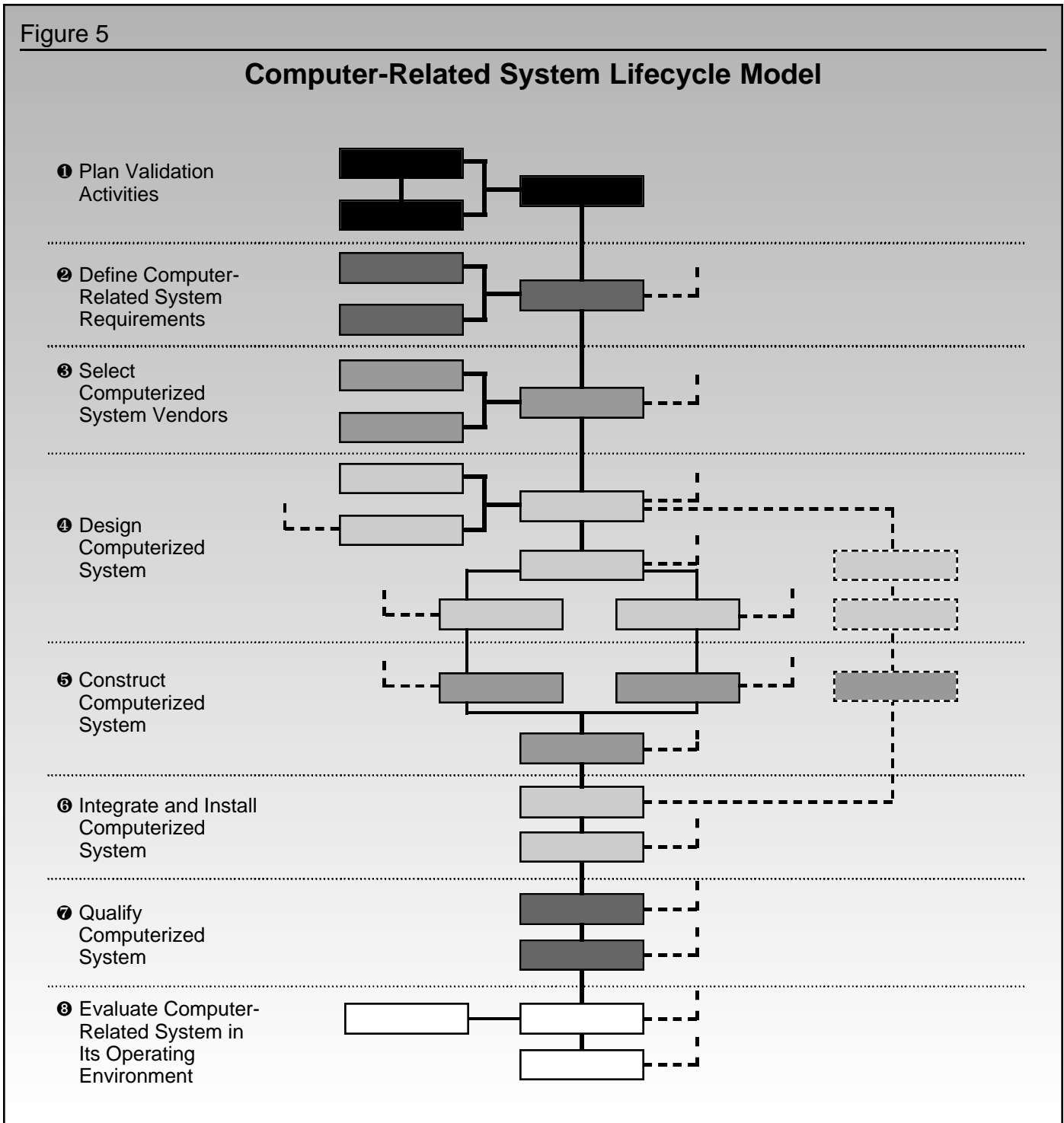
QMS: Quality Management System

OTS: Off-the-Shelf

**The Phases of a Typical Waterfall Lifecycle Model**

A System Lifecycle (SLC) is composed of phases during which a computer system is conceptualized, created, implemented, maintained, and finally retired (see *Figure 5*). Each phase will yield key deliverables. It is important to acknowledge that when iterative development, Rapid Application Development (RAD), or prototyping techniques, are used within a project, there may be overlap, merging, or repetition of phases, sometimes resulting in a model referred to as the spiral. However, the basic requirements of the SLC must not change.

The following are typical SLC phases:

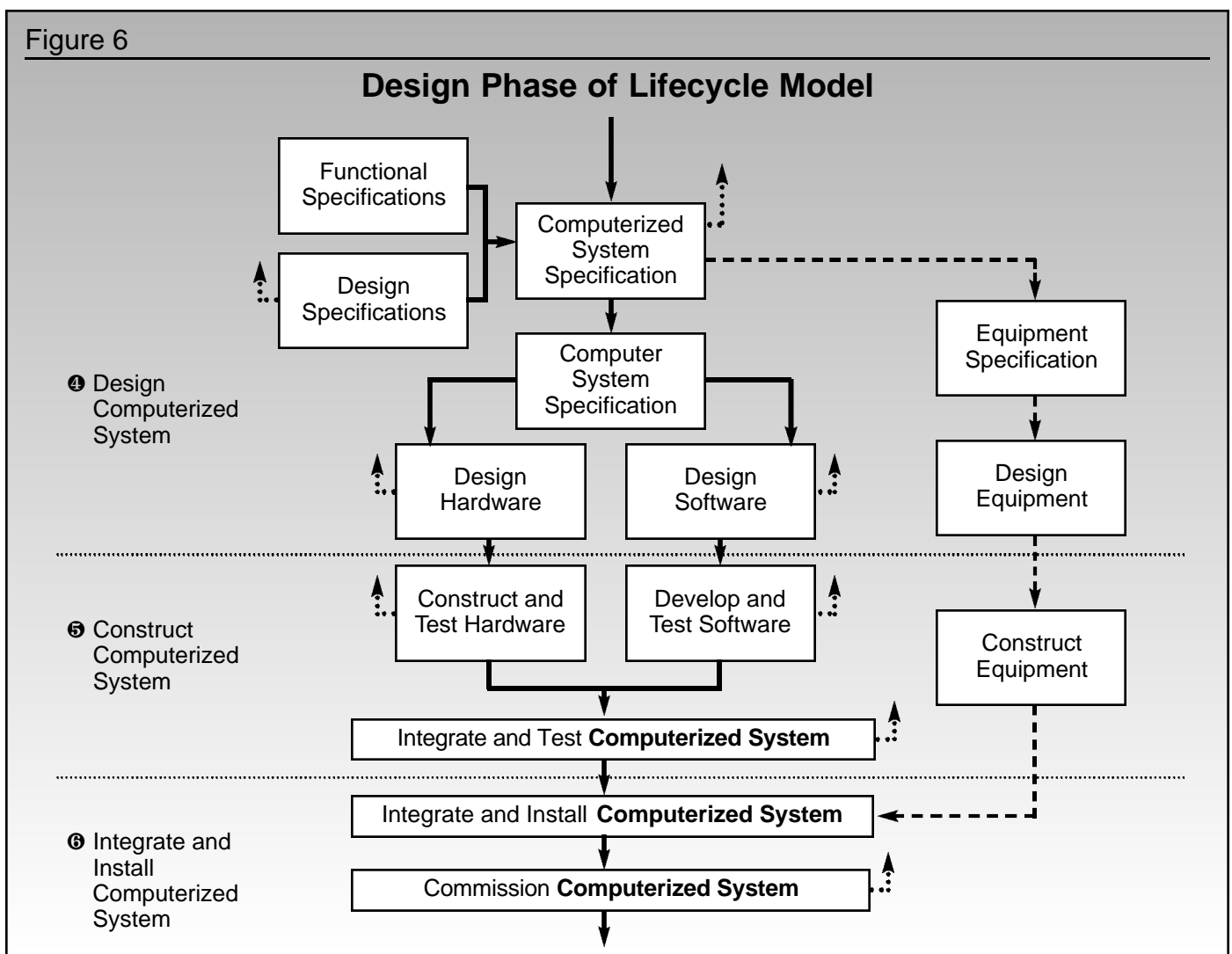


## 1 Planning

The planning phase is the initial phase of a project. The need for a system is identified, and there must be an understanding of the business case and processes that will be supported by the system. The scope of the project, the risks involved, business benefits, alternate approaches, and current technologies are examined. A high-level conceptual design of the proposed system is developed. The required resources for the project are estimated in a work plan for the computer system/application initiative. The current experience and training of all project team participants should be verified. The regulatory impact of the system must be understood, and validation activities must be included in the planning phase for regulated systems. Key deliverables yielded from the planning phase typically include a business case, project work plan, and project quality plan. If the system is regulated, the system validation plan is typically started in this phase, but cannot be completed until system requirements are fully defined.

## 2 Requirements Analysis

The requirements analysis phase encompasses both the functional requirements of the system from the users' perspective and the technical requirements from the developers and implementers' perspective. Functional requirements identify the expected capabilities of the system, capturing what the system will do without defining how it will do it. Technical requirements identify the technical conditions necessary for proper operation of the system. Key deliverables yielded from the requirements analysis phase typically



---

include the functional requirements specification and the technical requirements specification. Failure to adequately define the functional requirements at the beginning of a project is universally recognized as the most frequent reason for failure involving computer system design and/or validation.

### ③ Design

The intent of the design phase is to capture how the requirements will be met (see *Figure 6*). The functional and technical requirements identified during the requirements analysis phase are translated so that the proposed system can be described in terms of physical components, such as database tables and program components (i.e., windows, buttons, etc.). All of the application prompts, events, constraints, and actions are designed. All reports and business forms are designed. Program modules, messages, and interfaces are designed. In a client-server system, application partitioning is defined. The data requirements identified in the requirements analysis phase are transformed into logical and physical structures to be used by developers and database administrators, which include the database tables, views, and constraint definitions. The physical database design includes creating indexes, laying out files, de-normalizing tables (when applicable), and developing replication, as well as backup and recovery strategies. The physical characteristics of the database are captured in the Data Definition Language (DDL) that is used to create the physical structures. To accomplish this definition, the design document typically includes both text and diagrams.

If a vendor-supplied application is chosen, detailed design documentation can be limited to aspects constructed or configured by the user firm, although the complete design documentation should be verified during the supplier audit. Key deliverables yielded from the design phase typically include the detailed design specification. Additionally, a draft of the technical operations manual for the system is often started during this phase.

### ④ Development

Construction of the software takes place in the development phase. All work units (modules, windows, reports, etc.) are fully developed. Each piece of code created as part of the application is debugged so that processing or logic errors, as well as invalid or inefficient designs, can be identified and corrected. Work units are integrated, resulting in a fully functional application, which is then configured in an environment that is representative of the target production environment. The key deliverable yielded from the development phase is the application source code or supplier's application code customized/configured with the user firm's parameters.

### ⑤ Testing

During the testing phase, verification is performed to ensure that the application flow, user and system interfaces, controls, and error processing are technically correct and in alignment with functional requirements. Testing is documented via organized test protocols, and a final report of the test results is produced. Testing documentation is signed and dated by the tester(s). Key deliverables yielded from the testing phase typically include the executed technical/functional test protocols and a final report.

### ⑥ Implementation

The implementation phase comprises the activities required to coordinate the controlled and successful roll-out of the system into the production computing environment. Training takes place for technical support personnel, as well as the users of the system. Service level agreements are established with technical infrastructure personnel with respect to system availability, backup, and restoration, etc. Installation and data migration/conversion plans are developed. The implementation takes place, and a post-implementation review is conducted. Key deliverables yielded from the implementation phase typically include a production version of the application code, implementation instructions, training materials and records, service level agreements, system release authorization, and finalized user and operations manuals.

---

## 7 Maintenance

The maintenance phase spans the duration of time between the initial production implementation and the retirement of the system. The validated state of the system is preserved during this phase via use of good change control and configuration management practice, as well as a robust problem reporting and resolution process. A change history is maintained for the system and revalidation/requalification takes place when required. Key deliverables yielded from the maintenance phase typically include the system change history and associated documentation, problem logs, maintenance logs, security logs, and system logs.

## 8 Retirement

The retirement phase addresses the retirement of a system from active use by the firm. When a system is retired, consideration must be given to the application source code concerning how it will be phased out, how data will be converted if applicable, how it will be stored, and how it will be available for retrieval if required. Key deliverables yielded from the retirement phase typically include documentation covering the storage requirements for application source code and data, the retrieval process to be followed, and any hardware or other software dependencies, as well as the process by which the application will be removed from operational status including any data conversion activity, along with a schedule of execution dates and approval.

### *Traceability Between Phase Deliverables*

There should be a correlation between the elements of the various phase deliverables/validation documents; for example, the correlation between the functional requirements and the test cases that challenge them. This correlation can be demonstrated by using a traceability matrix. This matrix facilitates maintenance of the cross-referencing between requirements, the corresponding design elements, and the test cases that challenge them, as well as between the design and the code.<sup>10</sup> During the design phase, the traceability matrix can help facilitate design review since correlation of requirements to design can unearth mismatches and omissions. Additionally, completing the traceability matrix can help ensure adequate test coverage in the testing phase. In the system's maintenance phase, if any of the requirements or design elements need to be updated due to a change, it is easy to determine what other documents are affected and/or what tests must be re-executed once the change takes place. In short, the usefulness of the traceability matrix cannot be overstated.

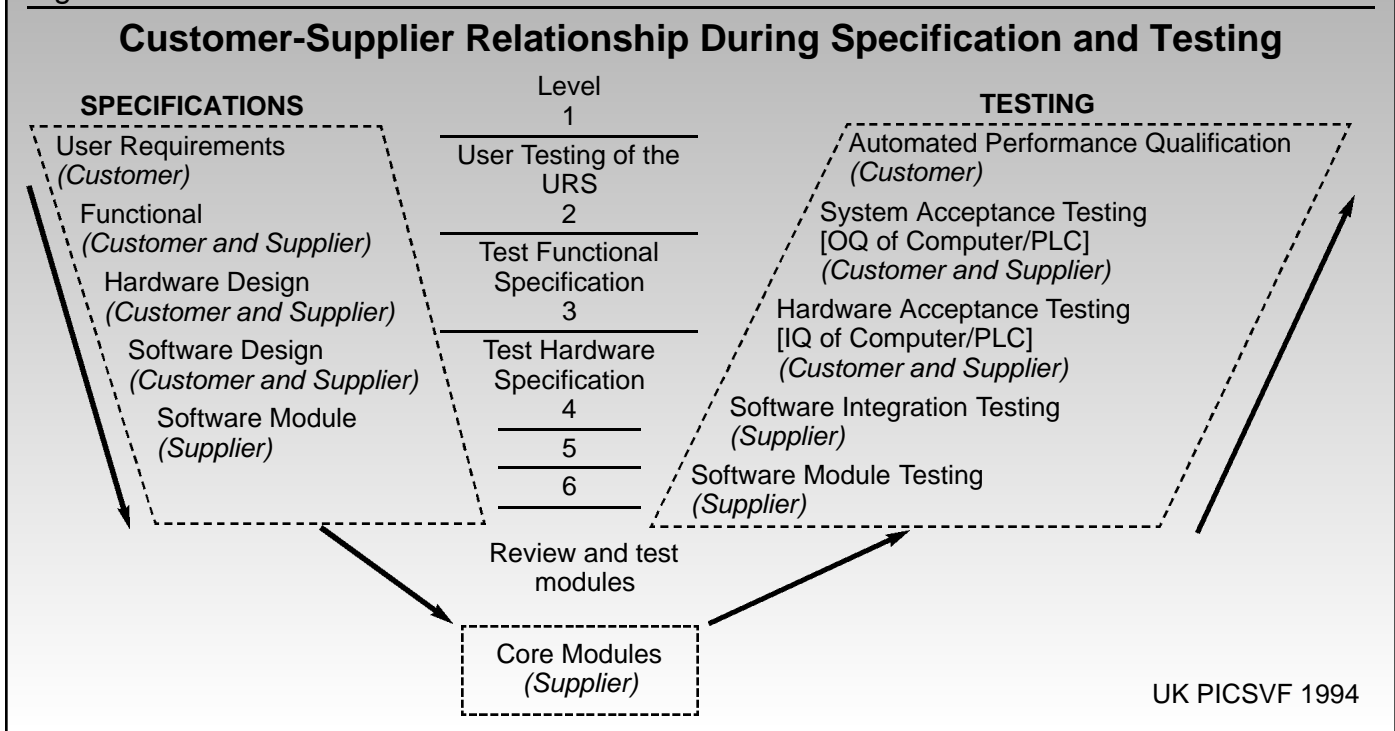
### *Qualification and Change Control of Infrastructure Architecture*

Another important aspect of a comprehensive system validation is the qualification and continuous stable state of the infrastructure architecture on which the system resides and depends (eg., servers, network, communications devices, etc.) Since these are typically housed in a data center and maintained by infrastructure operations personnel, it can be easy to neglect them; however, they are integral parts of the overall system and therefore must be included in the lifecycle validation activities. Since the infrastructure architecture often supports many systems, rather than performing qualifications associated with each system, it can be beneficial to perform them centrally on a regular basis (supported by change control) and reference the infrastructure qualification in each system validation package.

It is essential that good communication, effective technology transfer, and support transition measures exist between those who develop software and those who are to later manage and control it.

FDA and Industry have agreed from the beginning that CRSV should be regarded as continuing throughout the lifecycle of a system until its eventual retirement. With the primary focus on critical system functionality and availability, statistical trend analyses and trend controls can be useful, especially in the first year of active use by the firm. During the maintenance phase of the system, the periodic assessments, change control, and revalidation maintain the stable state of the system to ensure its stability, robustness, and ongoing proper functionality.

Figure 7



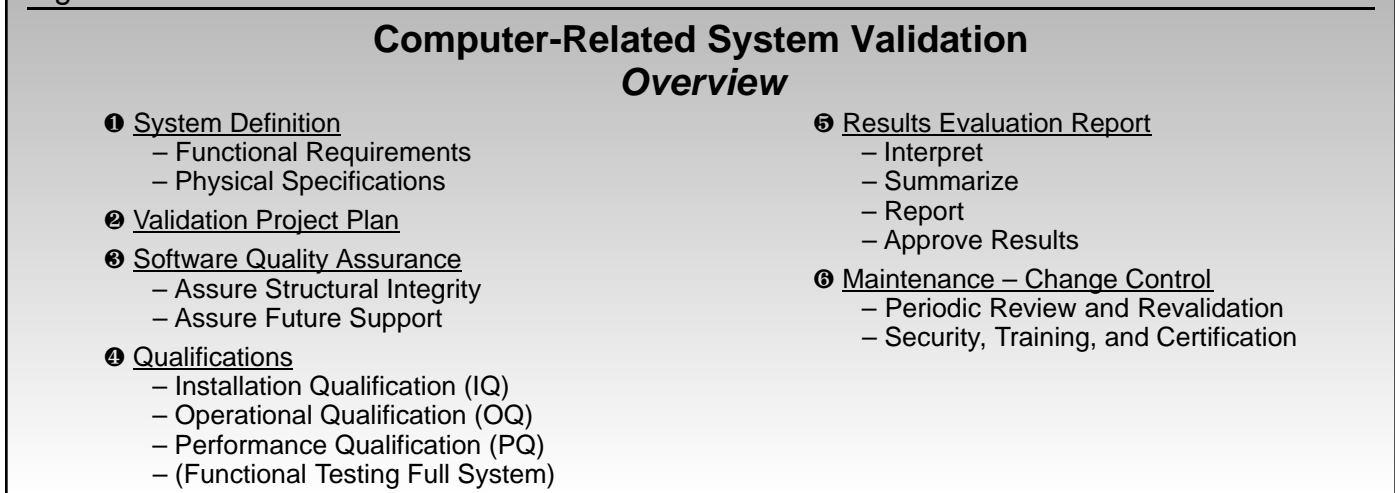
**Acronym Definitions and Glossary**

Computer system validation has proven to be a complex subject, a clear understanding of which depends largely on use of a common language by everyone concerned. Thus, the authors have attempted to provide a glossary that reflects the clearest and most accurate possible contemporary definitions. Moreover, the definition of each term has been developed in a way that will enable the term to have the identical meaning when it is used in any IVT proposed validation standard.

**Conclusion**

See Figure 7 for the details of the customer-supplier relationship during specification and testing. For a computer-related system overview, see Figure 8. As with all of its proposed validation standards, the **Institute of Validation Technology** invites questions and comments from our readers.

Figure 8



---

## References

1. Proposed Validation Standard VS-1: Non-Aseptic Pharmaceutical Processes. *Journal of Validation Technology*. Vol. 6, No. 2. pp. 502-521. Feb. 2000.
2. *Medical Devices: Current Good Manufacturing Practice (CGMP) Final Rule; Quality System Regulation*. 1996.
3. Garwood, R. and Motise, P. *FDA's Guide to Inspection of Computerized Systems in Drug Processing*. Reference Materials and training aids for investigators. (*The Blue Book*). Feb. 2000.
4. Institute of Electrical and Electronics Engineers. *IEEE Standards Collection: Software Engineering*. 1994 Edition.
5. Myers, G.J., Ed. "The Art of Software Testing." John Wiley & Sons: New York. 1979.
6. Pharmaceutical Manufacturers Association. "Validation Concepts for Computer Systems Used in the Manufacture of Drug Products." *Pharmaceutical Technology*. Vol. 10(5). 1987. pp. 24-34.
7. Parenteral Drug Association. "Validation of Computer-Related Systems: Technical Report No. 18." *Journal of Pharmaceutical Technology*. Vol. 49(S1). S1-S17.
8. GAMP Forum. "Supplier Guide: Version 2.0." May 1996.
9. International Society of Pharmaceutical Engineering. "GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture: Version 3.0." Vols. 1-2. March 1998.
10. FDA. *Guidance for Industry: General Principles of Software Validation*. Draft Guidance Version 1.1. June 9, 1997.

## Suggested Reading

- TickIT. A Guide to Software Quality Management System (Using 9001:1994) – The TickIT Guide. ISBN 0-580, Issue 3.0, 1994.
- Parenteral Drug Association. "Validation of Computer-Related Systems: Technical Report #18." *PDA Journal of Pharmaceutical Science and Technology*. 49 (S1), S1-S17.
- International Society for Pharmaceutical Engineering. *GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture*. 1 (1) User Guide. Mar. 1998.
- International Society for Pharmaceutical Engineering. *GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture*. 1 (2) Supplier Guide. Mar. 1998.
- International Society for Pharmaceutical Engineering. *GAMP Guide for Validation of Automated Systems in Pharmaceutical Manufacture*. Vol. 2. Best Practice for Users and Suppliers. Mar. 1998.
- Parenteral Drug Association. "Validation and Qualification of Computerized Laboratory Data Acquisition Systems, Technical Report #31." *PDA Journal of Pharmaceutical Science and Technology*. 53 (4).

---

# PROPOSED VALIDATION STANDARD VS-2

## *Computer-Related System Validation*

The following proposed standard is intended to reflect desirable contemporary practices, are not binding in any way, and can be modified to suit a firm's specific needs. The proposed standard incorporates imperative verbs (e.g., shall, will, must) to provide users with unambiguous quality assurance auditing tools, and are prefaced by a Preamble that provides rationale for several of the more complex concepts. The proposed standard is also directed toward users that may, or may not, be part of a larger corporation.

Terms that are **bold** and asterisked (\*) the first time they are used are defined in Section IV – Glossary.

### I. POLICY STATEMENTS

#### POL 2.1

Every **Computerized System\*** with functions that can directly or indirectly affect product quality or cause product misshipments is to be identified as a **New System\*** or **Legacy System\*** and **Validated\***. Throughout these proposed validation standards, all references to computerized systems apply to such systems and include **Computer-Related Systems\***.

#### POL 2.2

One or more Computerized System Validation Team (CSVT) members shall be available to each site having one or more computerized system. The team shall define and direct validation-related Computerized System Validation (CSV) activities, have an identified team leader, and include **Qualified\*** representation from at least each of the following groups:

- The **Quality Authority\***
- Computer validation experts
- Computer hardware experts
- Software experts
- Users of the computerized system

#### POL 2.3

Responsibilities of the CSVT leader shall include ensuring that all outside consultants, hardware and software **Suppliers\***, and system integrators understand their responsibilities and provide documented credentials that are **Verified\***.

#### POL 2.4

A **System-Specific Validation Master Plan – (VMP)\*** is to be developed for each CSV project that describes, defines, or refers to documents that describe or define at least the following:

- System **Functional Requirements\***
- System **Functional Specifications\***
- System, hardware, and software design specifications
- Planned validation activities

- 
- Major resource requirements
  - Team member responsibilities
  - Validation document management plans including the use of a traceability matrix to ensure/document traceability between requirements, design, and testing
  - **Installation Qualification (IQ)\*** and **Operational Qualification (OQ)\*** reports covering all relevant software and hardware
  - Plans for updating all SOPs affected by the project
  - Change control procedures

### **POL 2.5**

Validation documents must all be approved by the quality authority and by an authorized representative from the business function (eg., Production) that the validated system will support.

### **POL 2.6**

There shall be written instructions (e.g., SOPs and/or policies) for computer and computer-related systems that are designed to:

- Ensure data input accuracy
- Establish the adequacy of both functional and structural quality of all software
- Provide documented **Performance Qualification (PQ)\*** of the installed system(s)
- Implement human and environmental system security
- Provide validated backup, contingency, error handling, and recovery plans
- Maintain ongoing change control to address all significant planned and unplanned changes to any part of the system

### **POL 2.7**

**Revalidation\*** procedures are to be established that: (1) include, as part of ongoing change control measures, assessments to determine when revalidation is required and (2) provide for documented annual reviews of each computerized system to further ensure that revalidation is conducted when required.

## **II. PROCEDURAL STATEMENTS**

### **PROC – 2.a [ref. POL 2.1]**

Amaster list is to be maintained that identifies every on-site computerized system and includes: (1) its classification as either new or legacy and (2) its validation status as either “validated” or “being validated.”

### **PROC – 2.b [ref. POL 2.6]**

Practices must be in place to verify or otherwise ensure that all critical quality-related data entries made by human beings are accurate.

### **PROC – 2.c [ref. POL 2.6]**

The following validation documents, company-wide and/or system-specific, are to be available and maintained that apply to every computerized system, whether new or legacy:

- System definition
- Corporate/enterprise-level master validation plan
- System-specific validation master plan
- Functional requirements

- 
- Performance qualification task report
  - System security plan – physical and electronic
  - Error-handling plan
  - Backup, contingency, and recovery plans
  - Change control and maintenance plans
  - Traceability matrix

**PROC – 2.d [ref. POL 2.6]**

The following validation documents shall also be available and maintained to cover every large, new computerized system:

- User requirements
- Computerized system design specifications
- Hardware design specifications
- Software design specifications
- Installation qualification
- Operational qualification

**PROC – 2.e [ref. POL 2.6]**

Documented system security measures must be established that protect the validated system against such actions as:

- Unauthorized access to computer hardware and software
- Unauthorized changes and damage to or loss of data
- Sharing of access rights, such as passwords

**PROC – 2.f [ref. POL 2.6]**

Written contingency, backup, and restoration plans are to be audited and/or tested periodically.

**PROC – 2.g [ref. POLs 2.3, 2.6]**

Outside services related to any computerized system must be covered by written contracts, under which contractors and other outside employees are subject to all internal security and change control measures identified in this proposed validation standard.

**PROC – 2.h [ref. POL 2.7]**

Revalidation of a computerized system shall consist of repeating any or all of the original validation processes and shall occur when need is indicated by: (1) results and review following any change to software, hardware, or procedures related to the system or (2) results of an annual or other review of the system.

### III. ACRONYMS

API	Active Pharmaceutical Ingredient
BPC	Bulk Pharmaceutical Chemical
COTS	Commercial-Off-The-Shelf
CRSV	Computer-Related System Validation
CSV	Computer System Validation
CSVT	Computer System Validation Team
IT	Information Technology
OQ	Operational Qualification

---

PQ	Performance Qualification
SLC	System Lifecycle
SOP	Standard Operating Procedure
VMP	Validation Master Plan (system-specific)
IQ	Installation Qualification

#### IV. Glossary

*Reference  
Standard  
Number*

- POL 2.1**     **Computerized System** – a computer system plus the controlled function that it operates or controls.
- POL 2.1**     **Computer-Related System** – one or more computerized system and the relevant operating environment.
- POL 2.4**     **Functional Requirements** – statements that describe the functions a computer-related system must be capable of performing (also referred to as User Requirements).
- POL 2.4**     **Functional Specifications** – statements of how the computerized system, including its software, will satisfy functional requirements of the computerized system.
- POL 2.4**     **Installation Qualification (IQ)** – documented verification that the equipment, system, or subsystem has been properly installed and adheres to applicable codes and approved design intentions: and that supplier recommendations have been suitably addressed.
- POL-2.1**     **Legacy System** – (as applied to Computerized Systems) a computerized system installed and successfully operated *prior* to a specific date identified by the firm.
- POL-2.1**     **New System** – (as applied to Computerized Systems) a computerized system installed on or *after* a specific date identified by the firm (see **Legacy System**).
- POL-2.4**     **Operational Qualification (OQ)** – documented verification that the equipment, system, or subsystem performs as specified throughout representative or anticipated operating ranges. (Note: Overlap between IQ and OQ often occurs and is considered allowable.)
- POL-2.6**     **Performance Qualification (PQ)** – documented evidence that the defined process or system functions as intended and produces intended results under normal operating conditions at simulated or actual commercial scale.
- POL-2.2**     **Qualified** – (when applied to a person) sufficiently trained in procedures and skills with documented evidence of competence to perform assigned tasks.
- POL-2.2**     **Quality Authority** – one or more persons who, collectively, have formal responsibilities for specified quality-related operations, such as approval of manufacturing materials, release of finished products for sale, review and approval of documents, adjudication of quality assurance

---

investigations, and review of certain records. Titles of Quality Authority principals vary throughout the world; for example, in the United States, the term “the q.c. unit” is all-embracing; in the EU and Canada, the head of Quality Control has some of the responsibilities, while a Qualified Person has others; terms such as Responsible Head (or Person) and Quality Assurance (and/or Control) Department are also used in other areas.

**POL-2.7**     **Revalidation** – repetition of the validation process or a specific portion of it, including total process/system review, and/or requalification of those portions of the automated process/system potentially affected by a change.

**POL-2.3**     **Supplier** – a merchant firm that manufactures or sells materials. For the purpose of the supplier approval process, each supplier site that produces the material of interest requires separate approval.

**POL-2.4**     **System-Specific Validation Master Plan (VMP)** – a comprehensive, project-oriented action plan that includes or references all protocols, key SOPs and policies, existing validation task reports, and other relevant materials on which the specific system or process validation effort will be based. The plan also identifies resources to be allocated, specific personnel training and qualification requirements if relevant, organizational structure and responsibilities of the validation team, and planned schedules. The validation project plan is subject to periodic revision and is maintained by the CSVT.

**POL-2.1**     **Validated** – the establishment of documented evidence, which provides a high degree of assurance, that a specific process will consistently produce a product meeting its predetermined specifications and quality characteristics.

**POL-2.3**     **Verified** – confirmed or authenticated by human review and inspection or by direct observation (dual witnessing). Human verification is not required when automated systems are provided and validated that achieve the verification function.

## V. REGULATORY EXCERPTS

AUS	Australia	EC	European Community
CAN	Canada	US	United States
ECAx11	European Community Annex 11	WHO	World Health Organization

### *Regulatory Reference*

AUS 900     Where a computer is used in connection with any procedure or process associated with the production of therapeutic goods, the computer system...should meet the requirements of this Code for those manual functions which it replaces.

AUS 903     The development, implementation, and operation of a computer system should be carefully documented...and each step proven to achieve its written objective...

AUS 903     Software development should follow the principles of Australian Standard AS 3563: Software Quality Management System...

---

AUS 905 A control document should be prepared specifying the objectives of a proposed computer system, the data to be entered and stored, the flow of data, the information to be produced, the limits of any variables and the operating...and test programs...

AUS 907 Any change to an existing computer system should be made in accordance with a defined change control procedure which should document the details of each change made, its purpose, and its date of effect, and should provide for a check to confirm that the change has been applied correctly.

AUS 908 Where development has progressed to a point, where the system cannot readily be assessed by reading the control, and development documents together, a new control document...should be prepared

AUS 908 Data collected directly from manufacturing or monitoring equipment should be checked by verifying circuits or software to confirm that it has been accurately and reliably transferred.

AUS 909 Similarly, data or control signals transmitted from a computer to equipment involved in the manufacturing process should be checked to ensure accuracy and reliability.

AUS 910 The entry of critical data...by an authorized person...should require independent verification and release for use by a second authorised person.

AUS 911 ...methods of preventing unauthorized entry should be available...

AUS 912 The computer system should create a complete record (“audit trail”) of all entries and amendments to the database.

AUS 913 The recovery procedure to be followed in the event of a system breakdown should be defined in writing...

AUS 914 The computer system should be able to provide printed copies of relevant data and information...

AUS 917 Records should be available for the following aspects of a computer system validation:

- Protocol for validation
- General description of the system, the components, and the operating characteristics
- Diagrams of hardware layout/interaction
- List of programs with a brief description of each
- System logic diagrams or other schematic form for software packages
- Current configuration for hardware and software
- Review of historical logs of hardware and software for development, start-up, and normal run periods
- Records of evaluation data to demonstrate system does as intended (verification stage and ongoing monitoring)
- Range of limits for operating variables
- Details of formal change control procedure
- Records of operator training
- Details of access security levels/controls
- Procedure for ongoing evaluation

---

CAN C.02.005  
C.02.005 [E]quipment...shall be...maintained...in a manner that...permits it to function in accordance with  
[i 5.4] its intended use.

**INTERPRETATION**

**5.4 [C]omputerized systems...are routinely calibrated, inspected, or checked according to a written program designed to assure proper performance...**

CAN C.02.004  
C.02.004 [P]remises...shall be designed, constructed and maintained in a manner that...permits the opera-  
[i 10] tions therein to be performed under...orderly conditions...

**INTERPRETATION**

**10 Where necessary, separate rooms are provided to protect analytical instruments and associated control systems from vibration, electrical interference, and contact with excessive moisture or other external factors.**

EC 4.26. There should be written procedures...for...validation...  
4.26

EC 4.9 Data may be recorded by electronic data processing systems, photographic, or other reliable  
4.9 means, but detailed procedures relating to the system in use should be available, and the accuracy of the records should be checked. If documentation is handled by electronic data processing methods, only authorized persons should be able to enter or modify data in the computer, and there should be a record of changes and deletions; access should be restricted by passwords or other means, and the result of entry of critical data should be independently checked. Batch records electronically stored should be protected by backup transfer on magnetic tape, microfilm, paper, or other means. It is particularly important that the data are readily available throughout the period of retention.

ECAx11 [E]quipment [should be sited]...where extraneous factors cannot interface with the system.  
Ax11-3

ECAx11 A written detailed description of the system should...[include] principles, objectives, security  
Ax11-4 measures... scope[,]...main features...and how it interacts with other systems and procedures.

ECAx11 ...The...software should [be] produced in accordance with a system of Quality Assurance.  
Ax11-5

ECAx11 The system should include...built-in checks of... correct entry and processing of data.  
Ax11-6

ECAx11 Before a system using a computer is...use[d], it should be...tested and confirmed as...achieving  
Ax11-7 the desired results. If a manual system is being replaced, the two should be run in parallel for a time, as a part of this testing and validation.

ECAx11 Data should only be entered or amended by [authorized persons]. [M]ethods of deterring unau-  
Ax11-8 thorized entry of data include the use of keys, pass cards, personal codes and restricted access to computer terminals. There should be a defined procedure for the issue, cancellation, and alter-

---

ation of authorization to enter and amend data, including the changing of personal passwords. Consideration should be given to systems allowing for recording of attempts to access by unauthorized persons.

ECAx11  
Ax11-9 When critical data are...entered manually...there should be an additional check [of] accuracy [which] may be...by a second operator or ...validated electronic means.

ECAx11  
Ax11-11 Alterations to a system or to a computer program should only be made in accordance with a defined procedure which should include provision for validating, checking, approval, and implementing the change. Such an alteration should only be implemented with the agreement of the person responsible for the part of the system concerned, and the alteration should be recorded. Every significant modification should be validated.

ECAx11  
Ax11-12 [I]t should be possible to obtain clear printed copies of electronically stored data.

ECAx11  
Ax11-13 Data should be secured by physical or electronic means against willful or accidental damage, in accordance with Item 4.9. of the Guide. Stored data should be checked for accessibility, durability, and accuracy. If changes are proposed to the computer equipment or its programs, the above mentioned checks should be performed at a frequency appropriate to the storage medium being used

ECAx11  
Ax11-14 Data should be protected by backing-up at regular intervals. Back-up data should be stored... at a separate[,] secure location.

ECAx11  
Ax11-15 There should be...adequate alternative (arrangements) for systems...in the event of a breakdown. The time required to bring [them] into use should be related to the...urgency of the need to use them...

ECAx11  
Ax11-16 [P]rocedures to be followed if the system fails or breaks down should be defined and validated. [F]ailures and remedial action taken should be recorded.

ECAx11  
Ax11-17 A procedure should be established to record and analyze errors and [effect] corrective action...

ECAx11  
Ax11-18 When outside agencies are used to provide a computer service, there should be a formal agreement including a clear statement of... responsibilities...

ECAx11  
Ax11-19 When the release of batches...[uses a] computerized system, the system should allow... only a Qualified Person to release the batches and... should clearly identify and record the person releasing the batches.

US

211.68(b) § 211.68 Automatic, mechanical, and electronic equipment

(b) 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 or data shall be checked for accuracy. 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.

11.10 (a) § 11.10 Controls for Closed Systems

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

WHO  
14.9

Data may be recorded by electronic data-processing systems, photographic, or other reliable means. Master formulae and detailed standard operating procedures relating to the system in use should be available, and the accuracy of the records should be checked. If documentation is handled by electronic data-processing methods, only authorized persons should be able to enter or modify data in the computer, and there should be a record of changes and deletions; access should be restricted by passwords or other means and the entry of critical data should be independently checked. Batch records electronically stored should be protected by backup transfer on magnetic tape, microfilm, paper print-outs, or other means. It is particularly important that, during the period of retention, the data is readily available.