INTRODUCTION

This book offers a systematic, ten-step approach, from the decision to validate to the assessment of the validation outcome, for validating configurable off-the-shelf (COTS) computer software that generates data or controls information about products and processes subject to binding regulations. COTS software validation often is a time-consuming process in which a great deal of effort is spent determining the necessary validation tasks and the content and format of the validation documents. Ten Easy Steps for Risk-Based Software Validation provides the templates and explains how to get from start to “go live” in the most time-efficient way.

What exactly is COTS? The Food and Drug Administration (FDA) Glossary of Computerized Systems Software Development Terminology, published in 1995, defines COTS as “configurable, off-the-shelf software,” but within regulated industries the c also is understood to mean “commercial.” FDA now simply identifies software as off-the-shelf (OTS) only (FDA, Jan. 11, 2002).

COTS software is vendor-supplied and designed to comply with industry requirements and standards for managing systems and processes related to product design, development, manufacturing, packaging, distribution, and monitoring within the marketplace. Software developers validate these systems to make sure they meet the industry standards. But COTS software also must undergo validation by the end users. As more software to improve these systems and processes becomes available, a consistent process for validation becomes invaluable for companies that use COTS software.

RISK-BASED VALIDATION

In accord with FDA's focus on high-risk systems, this book promotes a risk-based approach to Title 21 of the Code of Federal Regulations (CFR) Part 11, Electronic Records; Electronic Signatures. Part 11 has been in effect for almost ten years, yet most companies still are not compliant. The two primary areas of focus for compliance are the Standard Operating Procedure (SOP) infrastructure and validation. FDA expects all companies to have SOPs to address computer security, data transfer, audit trails, electronic signatures, validation, and training. The second area is much larger because it deals with validation of new computer systems and existing legacy systems. FDA understands that companies have limited resources, so the risk-based approach is just a common sense way to approach the problem.

The risk-based approach starts by identifying the computer systems to validate first. New systems, lacking performance history data, present unknown risks and therefore must be validated first. Furthermore, Part 11 requires users to validate prospectively all systems that manage good industry practice (GxP) data, meaning that validation must be undertaken before going live into production use. The selection of new systems must be based on user requirements that address Part 11 features, such security and audit trails.

Next to be validated are upgrades to existing systems. The last systems to undergo validation are the legacy systems. All electronic systems that already are in operation or that a company introduces are subject to rigorous validation in compliance with either Part 11 or the predicate rules.

INDUSTRY BEST PRACTICES

Professionals in regulated industries worldwide carefully scrutinize COTS validation processes. The Pharmaceutical Industry Systems Validation Forum in the United Kingdom developed the Good Automated Manufacturing Practice (GAMP) Supplier Guide to help software developers implement quality management systems. The GAMP Guide has evolved to define best practices for these systems, providing category summaries (one through five) that capture the breadth of activities involved in software validation. The ten-step validation process in this book satisfies categories three and four of the Good Automated Manufacturing Practices (GAMP) guidelines.

> Category 3: This category includes standard software packages such as databases and spreadsheets. Validation of the software itself is not a requirement, but validation of applications made with the software is.

> **Category 4:** This category includes COTS software packages intended for specific use, such as Laboratory Information Management Systems (LIMS) or document management.

The GAMP guidelines, in total, base validation on the installation qualification (IQ), operation qualification (OQ), and process or performance qualification (PQ), with process validation usually occurring in tandem with process qualification. This IQ/OQ/PQ model works well for automated equipment. It is not, however, the best system for computer systems validation because it does not address the configurations to satisfy the end-user requirements, the hazards and mitigations, the training, or the infrastructure of Standard Operating Procedures (SOPs) that must be in place.

Before computer systems were in widespread use, hardware such as equipment and instruments were qualified using the IQ/OQ/PQ model. This model involves the creation of a protocol that describes the qualification tasks. Once the protocol is approved, it is executed, and the results are recorded in a report. Sometimes the protocol and report are combined into one document in which space is reserved to record results for each step of the protocol. This compound document has two sets of signatures to reflect approval before and after execution.

The IQ component provides installation instructions and verification that the installation is correct with respect to manufacturer specifications; OQ presents verification that the operation of the equipment meets manufacturer specifications; and PQ gives verification that the operation meets user requirements over the entire range of operation, including stress conditions.

Computer hardware initially was regarded as equipment. Early computer systems did little more than emulate hardware but over time have evolved to perform increasingly complex functions. IQ/OQ/PQ, already well established at the onset of the growing software industry, naturally became adopted for computer system validation (CSV). Because IQ/OQ/PQ was developed for dedicated hardware, though, it focuses on a single device rather than on the process of implementing an entire system. IQ/OQ/PQ isn't comprehensive enough to address the complexities of software, and this shortcoming has posed a critical problem for industry. Whereas IQ/OQ/PQ is insufficient for validating computer systems themselves, it does offer underlying validation principles to apply.

Although the process laid out in Ten Easy Steps for Risk-Based Software Validation is compatible with the GAMP guidelines, it is more thorough. This book specifically helps companies ensure that their COTS software systems fully demonstrate “fitness for purpose” by providing an easy and systematic process to address the needs of end users as well as the system’s suitability to meet those needs.

VALIDATION EQUALS GOOD BUSINESS PRACTICES

No single validation process ever duplicates another; each validation is unique. Even a validation for software that is identical to a product already in place may have a different user base, a distinct intended application of the package, a broader or narrower scope, or be subject to updated regulations. The validation process must take all of these factors into account. Further, validation of a specific software package is rarely a one-time occurrence. When software is updated, revalidation is essential. When systems are modified through change control, partial or full revalidation may be necessary. Software validation is thus an ongoing, evolving process that helps companies remain current.

Validation is rarely a simple process, but it is one that makes sense not only because it is mandated but also because it is a good business practice. Getting a product to market is a laborious process having many starts and stops, and one that always relies on the generation, control, and retention of data. Increasingly, software programs are used to produce and control data. All computer software programs directly connected to these activities are prime for validation.

From a business perspective alone, validation can save companies money by discovering costly defects before a system goes live (that is, into production) and informing management of any associated risks so as to better understand and assess legal liability. Validation also increases the likelihood that a system will be implemented on schedule and within budget. Validation reduces labor costs by increasing employee efficiency and effectiveness as well. Perhaps most important, though, is the fact that validation is a requirement for regulatory compliance. Furthermore, customers and business partners often require validation. Every indication suggests that regulations increasingly will focus on electronic generation of data, data control, and data transfer.

Today, a paperless environment is possible with the electronic applications available to regulated industries. With electronic records, the ability to demonstrate traceability every step of the way—from discovery to product in the marketplace—is the benchmark. The systems that perform these functions are certain to be under scrutiny, given the critical nature of the data they contain.

THE REGULATIONS

Although some software programs do not require electronic signatures, inherent in much software validation is the concept of electronic signatures. In general, according to 21 CFR Part 11, Electronic Records; Electronic Signatures, companies can use electronic records and signatures in place of paper, provided such records are trustworthy and reliable. The regulation applies to all data reported to FDA and includes unreported supporting data as well. All GxP-critical stored electronic data is an electronic record and, according to 21 CFR Part 11, Subpart A 11.3, "electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system" (FDA, Mar. 20, 1997).

Electronic record and signature regulations, as delineated in 21 CFR 11, are not the single driving force behind configurable off-the-shelf (COTS) computer software validation. 21 CFR 11 also states that companies must adhere to the predicate rules—the binding regulations that drive the industry—such as FDA's 21 CFR 58 Good Laboratory Practices (GLPs), 21 CFR 211 Good Manufacturing Practices (GMPs), and 21 CFR 820 FDA Quality System Regulation, 1996, to name a few.

Implicit in the predicate rules that govern any facet of the manufacture of a drug, biologic, medical device, or cosmetic is that any system of control be confirmed as appropriate for the task at hand. Inherent in the term "control" is validation, if the process utilized is computerized.

FDA's Quality Systems Regulations—1996 21 CFR 820.70 [i] Automated processes—spell out the regulatory expectations for electronic systems:

> When computers or automated data processing systems are used as part of production or the quality system, the manufacturer shall validate computer software for its intended use according to an established protocol.

- All software changes shall be validated before approval and issuance.
- These validation activities and results shall be documented.

This requirement applies to any software used to automate device design, testing, component acceptance, manufacturing, labeling, packaging, distribution, complaint handling, or to automate any other aspect of the quality system. FDA does not restrict this rule solely to medical devices, however. The scope is much broader, because Part 820 provides a foundation for industry best practices that encompasses all therapeutic products.

The regulations for GMP explicitly call for tight control of computer systems; the following is an excerpt from 21 CFR 211.68(b) Automatic, mechanical, and electronic equipment:

> [A]ppropriate 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….

Similarly, the guideline for GCP from the International Conference on Harmonization (ICH) is clear in its directive about computer systems that handle electronic data for clinical trials. Sites must ensure and document that the electronic data processing systems conform to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance.

The International Organization for Standardization (ISO) also requires organizations to define their validation activities. For instance, the 2000 edition of the ISO 9001 guidance sub-clause 7.5.2 Validation of processes for production and service provision states the following:

> The organization shall establish arrangements for these processes, including, as applicable—
>
> a) defined criteria for review and approval of the processes,
>
> b) approval of equipment and qualification of personnel,
>
> c) use of specific methods and procedures,
>
> d) requirements for records…and
>
> e) revalidation.

In an ISO environment, all processes related to product quality that use COTS software must undergo validation. Although many countries embrace the standards set forth by ISO, most countries (for example, Australia, Canada, the United Kingdom, and Japan) also have additional governing regulations that cite the need for COTS validation.

THE BIG PICTURE

Validation is never a stand-alone event; it requires putting peripheral systems in place. Binding regulations say that systems used to create, modify, maintain, or transmit electronic records must include procedures and controls to validate that the systems are trustworthy and reliable. These procedures may involve Information Technology (IT) practices such as data backup, disaster recovery, event recording, and e-mail retention. Certainly procedures for the use and management of the system are necessary. Validation may extend to assessing controls such as facilities security and training records as well.

The regulations don't address the "how to" issues of validation, however. The regulations set forth what companies must do, not how to do it. That task is up to the companies to determine and implement, and that is what Ten Easy Steps for Risk-Based Software Validation can help companies do. This book provides templates to serve as the roadmap for navigating the validation process. In many processes, the creation of the templates and the determination of what they need to contain takes the lion's share of validation time, expense, and effort. Using the templates included here eliminates this step, making the process flow smoothly and efficiently from start to finish.

Moreover, this book focuses on user validation, which is the validation of a software application from the end users' perspective. Validation from this vantage point is what 21 CFR Part 11.10 calls for: "(a) Validation of the system to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records." The emphasis is on "intended performance," which is something only the end users of the COTS software can determine and thus validate.

Finally, Ten Easy Steps for Risk-Based Software Validation details the measures companies must take to ensure that systems remain compliant with the requirements of all good practice disciplines (GxP), from discovery to post-marketing.

There is no question that software packages are effective business tools. Indeed, the company that does not use software—much of it being the off-the-shelf kind—is uncommon. As more software integrates itself into the operations of individual companies, the need for validation escalates, which in turn translates to more people needing the skills to validate software. That's what this book is all about: It's a tool to help industry professionals effectively validate the systems they need to move their businesses forward.