Conducting Effective Validations of Computer-Related Systems: *How Much is Enough?*

By Leonard A. Grunbaum
META Solutions, Inc.

So how much validation is enough? While not rising to the metaphysical heights of the great questions puzzling humankind, such as: "Why is the sky blue?" or "How many angels dance on the head of a pin," this is a question frequently posed by upper management. The concern, of course, is that "too much" validation costs too much money with no added value, while insufficient validation puts the company at risk.

The answer depends on how much risk you're willing to accept. From a business standpoint, inappropriately developed, tested, and/or implemented computer systems will usually result in improper, inefficient, inconsistent, and occasionally even unnecessary processing. In the short-term, this increases the cost of doing business. In the long-term, this will adversely affect the company's ability to compete and expand. From a regulatory standpoint, upper management is expected to exercise appropriate controls to help to ensure compliance with good ethical as well as business practices. These expectations are codified in 21 Code of Federal Regulations (CFR) Part 11 (Electronic Records and Signatures).[1] They are further explained in the guidance document *Computerized Systems Used in Clinical Trials*.[2] This article will focus on the value of system validation principles as a business model that will result in regulatory compliance in an efficient manner. The specific objectives are to:

"From a regulatory standpoint, upper management is expected to exercise appropriate controls to help to ensure compliance with good ethical as well as business practices."

- Identify good and practical validation practices
- Understand how validation represents good business practice
- Understand the risks of not following these practices
- Make knowledgeable decisions regarding how much computer validation is enough

Good and Practical Validation Practices

Let's start with the basics. For our purposes, validation will be defined as: "*... confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through the software can be consistently fulfilled.*"[3] Validation practices, in turn, are those conventions/methods utilized to help ensure that the respective system con-

Figure 1

Validation-Related Control Objectives and Related Disciplines

Control Objectives	Disciplines
Ensure that the system meets the business needs	• Pre-determined and formal (i.e., approved) functional requirements to identify what needs to be done (i.e., reports, capacity, performance, quality) • Formal specifications (i.e., hardware, software, communications) to identify how it will be done • Formal testing at a detailed and functional level to confirm that the system actually does what it is intended to do
Ensure that the system is developed and implemented in a quality manner	• Formal development methodology to provide the policy and general instructions (i.e., phases, deliverables, documentation requirements) for the development, implementation, and production control of computer systems, and to ensure that a consistent approach to computer system validation is established and followed • Programming standards to provide requirements (i.e., structured programming techniques, standardization, naming conventions, commented source code) designed to promote good programming practices, consistency across programs and programmers, and understanding on the part of a reviewer • Testing standards to provide requirements (i.e., formal test plans, documentation of test results, formal summary reporting) designed to provide complete documented evidence of testing • Appropriate hiring and training policies and procedures, including documented training records, designed to ensure that only qualified staff are involved in the development process • Due diligence (i.e., vendor audit) re: software developed by a third-party to ensure that the development was conducted in a qualified manner
Ensure that the system continues to meet business function appropriately	Formal policies and procedures (i.e., Standard Operating Procedures [SOPs]) designed to ensure the following: • Changes to the system (i.e., bug fixes, enhancements) are appropriate, tested, and documented • Security over programs and data are adequate to prevent and detect unauthorized access to system resources • Backup and recovery procedures are appropriate to ensure that data can be backed up and recovered without loss of data integrity • Contingency planning procedures are appropriate to ensure that alternative hardware and software can be employed should computing resources be lost for a protracted period of time • Training procedures are appropriate to ensure that staff that use and support the system are adequately trained in system operations (functional and technical) and that training documentation is retained • Hardware and software maintenance is performed according to a formal method and that documentation is retained i.e., what was done, why, who did it, and when.

forms to user needs and intended uses, and that the respective requirements can be consistently fulfilled. These practices consist of two basic elements: control objectives (the parameters within which company operations should function) and disciplines (the rules/methods designed to achieve the control objectives). *Figure 1* provides the relationship between validation-related control objectives and related disciplines designed to achieve the respective objective.

Validation as Good Business Practice

Let's return to a portion of our definition of validation: *"...that software specifications conform to user needs and intended uses, and that the particular requirements implemented through the software can be consistently fulfilled."* In other words, the system does what we need and it will continue to do so. And what are our basic needs? The answer is summarized in the following three words: bigger, better, and faster. We need to be able to:

- Minimize processing time (i.e., minimizing redundant processes, data handling, bottlenecks, the need for reprocessing) from initial data entry to ultimate endpoint (i.e., application, submission)
- Maximize knowledge management capability by making all pertinent information available to decision makers
- Maximize speed (i.e., timely delivery of information to allow for expeditious decision-making)
- Maximize application of quality measures (i.e., edits, authority and sequence checking, consistency checking)
- Maximize capacity (i.e., customers, users, studies)

The main objective here, of course, is to be profitable. Unprofitable companies don't survive.

The alternative is a situation in which the system doesn't do what we need and never will. Given this alternative, what remediation needs to be done? You guessed it – reengineer the system with a host of bug fixes and enhancements, go back to the drawing board (i.e., implement a new system), or do the "work-around waltz" (i.e., implement Byzantine alternative procedures to accomplish what should have been effectively accomplished in the first place). All of these options have something in common, they result in additional costs and serve to reduce profitability.

Therefore, validation is a good business practice because it promotes efficiency. Validation practices allow you to "do it right the first time" – while promoting increased quality of information and decision-making. Specifically properly developed systems:

- Meet business needs, work as intended, work consistently, and are relatively easy to maintain
- Continue to meet business needs, work as intended, work consistently, and be relatively easy to maintain
- Reduce bottlenecks with qualified staff and effective documentation, promote proper actions/activities and promote consistency among individuals

Risks

Business Risk

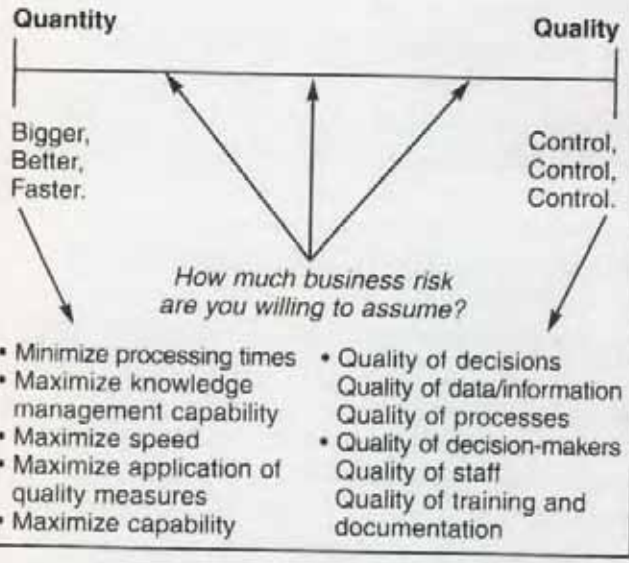
There is a counter-weight to the concept of "bigger ... better ... faster," and that is the concept of "control ... control ... control." We are in a regulated industry after all. The purpose of the regulations is to help ensure the quality of decisions (a result of the quality of the data/information plus the quality of the processes that generated the data/information) and quality of the decision-makers (a result of the quality of the staff plus the quality of the training/documentation). Policies and procedures (i.e., reviews and approvals, standardization, and documentation) are required to help ensure that the system produces a quality product in a quality manner. The concept of "control ... control ... control," therefore, is contrary to the concept of "bigger... better... faster." So the dilemma is this; too much "bigger... better... faster" and not enough control can result in a diminished quality of the work product, while the too much control and not enough "bigger... better... faster" can result in a diminished quantity of the work product. *Figure 2* illustrates the concept of "business risk" and poses the question: How much business risk are you willing to assume?

System Risk and Audit Risk

Business risk, in turn, is the result of evaluating "system risk" (the likelihood that a given system contains quality problems that cause the company to be

Figure 2

The Concept of Business Risk

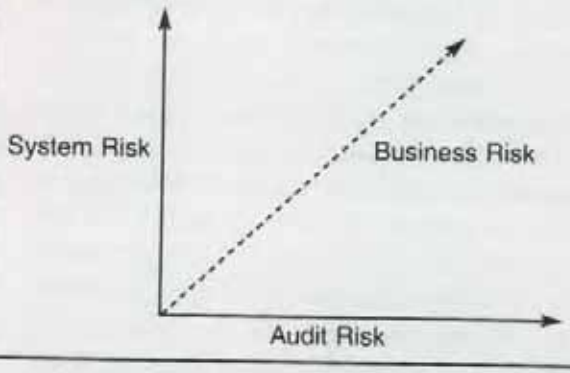


out of regulatory compliance, or jeopardizes the ability of the company to function effectively) against the "audit risk" (the likelihood that you will be audited – by the Food and Drug Administration [FDA], a sponsor company, a prospective client/customer, etc. – and thus be susceptible to having your quality problems identified). The business risk aspect comes into play due to having your quality problems identified and can cause a loss of clients/customers, rejection of submissions, a poor reputation in industry and, in extreme cases, recalls and shutdowns. The relationship between system and audit risk is illustrated in *Figure 3*. This figure demonstrates how the business risk increases as the likelihood exists that a problematic critical system will be audited.

Only you can determine which of your systems relate to regulatory compliance or continued effectiveness of the business. However, from a regulatory standpoint, computerized systems used to create, modify, maintain, archive, retrieve, or transmit clinical data intended for submission to FDA become mission-critical. It is this data that the Agency will review and decide upon the safety and efficacy of new human and animal drugs, biologics, medical devices, and certain food and color additives.[4] It is this criticality that also makes these systems more likely to be audited to ensure that the information, and the processes that generated the information, can be relied on. Other systems (i.e., payroll) are critical even if not directly involved in the clinical aspects of the business. A third class of systems (i.e., United Way) would not be considered critical.

Figure 3

System Risk Versus Audit Risk



You can't always predict when the FDA will audit you, but the following are indicators that should lead you to begin preparing:

- The company has a poor compliance history with FDA (i.e., deficiencies cited in the past)
- Remediation measures, regarding FD-483 or Warning Letter issues, remaining to be confirmed by FDA
- The company is a new company with no history with FDA
- The company is involved in a high profile study area, or has a submission under active consideration

If your company is a Contract Research Organization (CRO) conducting a clinical study for a sponsor, or is being considered for such a role, you can fully expect the sponsor to conduct a thorough audit of the processes and data relating to the respective study. Other suppliers of goods/services (i.e., software vendors, device manufacturers) can expect audits by clients/customers.

How Much Validation is Enough?

I can't tell you exactly how much validation is appropriate for your company, but this article offers a method to help you evaluate your needs. To do this, I will go back to our definition of validation: "... *con-*

firmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through the software can be consistently fulfilled." We've seen that the concepts of software specifications conforming to user needs, and that the requirements being consistently fulfilled, are standards to achieve. But how do we achieve them? By our definition, the answer is through confirmation by examination and provision of objective evidence. The question "how much validation is enough?" – or "how much business risk am I willing to assume?" – then becomes "how much examination is required and how much objective evidence is necessary?"

Examinations are audits to be conducted by an independent quality assurance group or other qualified auditing organization. With respect to clinical data and information management systems, the objective of such an effort is to evaluate the given operation and determine whether or not reliance can be placed on the process and the resulting information. The examiner has to examine something, and that something is the objective evidence (i.e., documentation) provided to demonstrate that the system does what it is intended to do, and that it will function properly on a consistent basis. Let's focus, then, on what documentation needs to be provided and how often it should be examined. In discussing this point, I postulate the following:

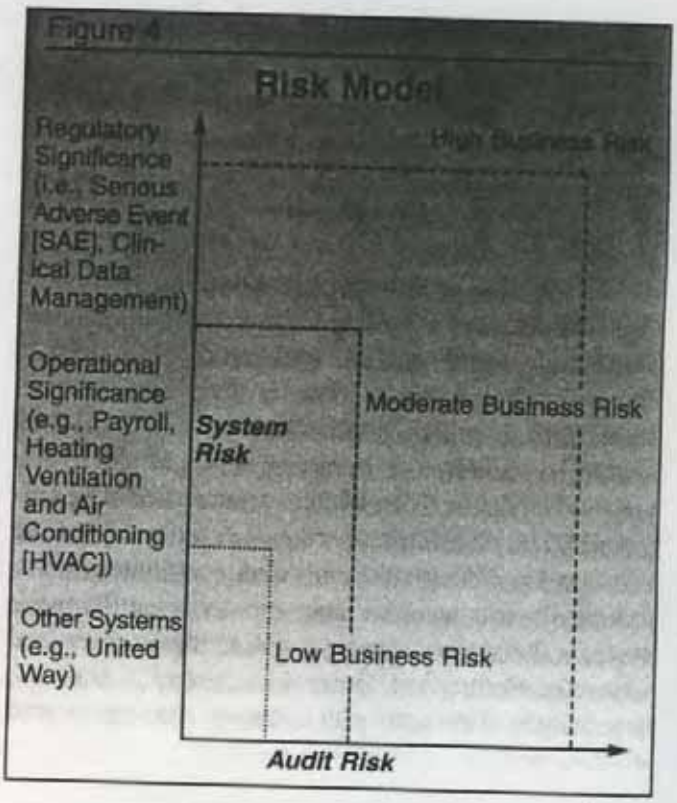
- In regards to regulated processes, you always have to be prepared for an audit so you have to assume that the audit risk is high
- Systems that are high risk, per the definition of "system risk" above, should have the full suite of documentation as described previously in *Figure 1*
- This documentation should be examined to the extent that the complexity and duration that the project warrants. This means that you have to
  - Identify all of your computerized systems
  - Determine which ones represent business risks and which do not
  - Stratify the systems that represent business risks into priority order (of course the priorities are company-specific) and ensure that the higher priority systems can withstand scrutiny

The risk model, demonstrated in *Figure 4*, illustrates the concept of prioritization. In this example, systems of regulatory significance, such as Serious Adverse Event (SAE) reporting and clinical data management, are in the high-risk category because problems in these areas have the potential to adversely affect a company's ability to do business. The audit visibility is high and it is likely that the problems will be identified. Systems that have operational significance (e.g., payroll, Heating, Ventilation, and Air Conditioning [HVAC]) are labeled moderate risk because employee morale, for example, might be affected if these systems do not work properly, but they should not affect the long-term ability of the company to conduct business. Additionally, the audit risk is not high. Finally, systems such as United Way do not affect the company's operations and the risk of an audit is quite low.

Here is how you can decide how much validation is enough:

- Step 1 – Identify all computerized systems operating in your environment, all systems being developed, and all systems that support your business, but are operating in another environment (i.e., an application service provider environment).

Figure 4



- Step 2 – Plot each system on the "risk model" graph, identifying it as high-, moderate-, or low-risk.
- Step 3 – Ensure that each high-risk system has the full suite of validation documentation as previously shown in *Figure 1*.
  - If the system is operational, perform an assessment to ensure that all appropriate documentation exists, and address any remediation requirements as soon as possible.
  - If the system is currently being developed or to be developed, ensure that the development process is formal and will result in the suite of documentation described in *Figure 1*.
  - If the system is being operated in an outside environment, perform appropriate due diligence to ensure that the proper processes/documentation exist.
- Step 4 – Ensure that an effective quality assurance capability exists to perform periodic examinations of the high-risk system operations and resulting data. The nature, scope, and regularity of the examinations should be formalized and approved by company management.
- Step 5 – For each moderate-/low-risk system, determine the cost/benefit of developing a full suite of documentation and, if such documentation will not be provided, document the decision and rationale.

Conclusion

The question of how much validation is enough is typically asked of a particular system: for my clinical data management system, how much validation is enough? The author's view is that the question should be: given that systems covered by regulations should be validated to minimize any and all regulatory and business risks, which systems should be validated? You shouldn't try to save money by taking risks on the systems that fall under regulatory parameters. If you want to save money, identify those systems that do not present a risk to the business and adjust the elements of "control ... control ... control" accordingly. This approach is penny wise and pound wise as well. ❑

About the Author

Leonard A. Grunbaum is the President and Chief Operating Officer of META Solutions, Inc. He is responsible for all operational aspects of the company, and the management of all aspects of the validation consulting services to the pharmaceutical industry. Len has a B.A. and an M.B.A. from Long Island University. He was a Director of the Electronic Data Processing (EDP) Auditors Association and is a member of the Drug Information Association (DIA). Len is the author of "Do It Right The First Time: A Handbook for Controlling Technology Through Good Validation Practices," published in the February 2000 issue of the Journal of Validation Technology. He has also presented validation and audit-related training sessions to clients and professional groups. Len can be reached by phone at 732-845-4904, by fax at 732-845-4834, or by e-mail at len_g@metasol.com.

References

1. FDA Code of Federal Regulations, Title 21, Food and Drugs, Part 11. "Electronic Records; Electronic Signatures: Final Rule." *Federal Register*. Vol. 62. No. 54. Pp. 13429-13466. March 20, 1997.
2. FDA. Guidance for Industry: Computerized Systems Used in Clinical Trials. April 1999.
3. Ibid.
4. Ibid.