

RAMP (Risk Assessment and Management Process): An Approach to Risk-Based Computer System Validation and Part 11 Compliance

Richard M. Siconolfi, MS
Computer System Validation
and System Lifecycle
Management, Information &
Decision Solutions, Research
& Development, Procter &
Gamble Pharmaceuticals,
Inc., Mason, Ohio

Suzanne Bishop, MA
Pharmaceutical Computer
Applications Consultant,
Lebanon, New Jersey

Risk-based computer system validation is a process many companies developed long before the August 2003 Guidance for Industry document on Part 11 Scope and Application was issued by the US Food and Drug Administration. The main differences between prior-existing risk models and this guidance is the emphasis on patient and product safety, product quality, and record integrity, as required in the Part 11 Scope and Application Guidance.

When computerized systems are used to collect data on which decisions are made on drug efficacy and patient safety or are used to control the quality of drug during a manufacturing process, the point of focus has to change. This article outlines a consistent and justifiable method for determining the risk of a computerized system with the emphasis on patient and product safety, product quality, and record integrity.

Key Words

Risk assessment; Risk
Management, Part 11; ERES;
System validation

Correspondence Address

Richard M. Siconolfi, The
Procter & Gamble Company,
8700 Mason-Montgomery
Road,
Mason, OH 45040-9462
(e-mail:
siconolfi.rm@pg.com).

INTRODUCTION

The Food and Drug Administration's (FDA's) 21 CFR Part 11 Guidance on Scope and Application (1) allowed the regulated industry a chance to reduce the extent that we validate computerized systems, manage audit trails, and retain our records by using a justifiable risk assessment-based approach. This approach must provide proof that it is adequately assessing risk of the computerized system and adequately addressing risk reduction through system validation, record audit trails, and record retention. However, the FDA did not relax any predicate rules. First, the regulated industry is still required to follow and obey the regulations FDA promulgates and approves.

This article outlines a consistent, painless, and justifiable method for determining the risk of a computerized system. While it is based on industry-accepted models, the main differences between prior-existing risk models and this methodology is the emphasis on patient and product safety, product quality, and record integrity as required in the Part 11 Scope and Application Guidance. By using this method, one is guided through the regulations and led to a consistent and justifiable conclusion regarding the potential level of risk posed by this comput-

erized application and the steps required to mitigate this risk. When a person knowledgeable with a computerized system performs this risk assessment and management process (RAMP), it will take from 15 to 45 minutes to complete. This methodology can reduce the time spent analyzing system risk and focus system development and validation efforts.

REGULATIONS, DIRECTIVE, AND GUIDELINES: THE KEY

The FDA's mission is described as follows:

The FDA is responsible for protecting the public health by assuring the safety, efficacy, and security of human and veterinary drugs, biological products, medical devices, our nation's food supply, cosmetics, and products that emit radiation. The FDA is also responsible for advancing the public health by helping to speed innovations that make medicines and foods more effective, safer, and more affordable; and helping the public get the accurate, science-based information they need to use medicines and foods to improve their health. (2)

In following this mission, the Scope and Application Guidance stresses "the need to base your approach on a justified and documented risk assessment and a determination of the potential

of the system to affect product quality and safety and record integrity” (1).

Procter & Gamble (P&G) started developing a risk model by reviewing two available assessment tools that showed some promise: the Society of Quality Assurance Computer Validation Initiative Committee’s article on risk assessment and validation priority setting (3) and International Society for Pharmaceutical Engineering’s (ISPE’s) guidelines posted on their Web page (4). We realized that neither of these models addressed two of the three key objectives of the guidance: product quality and safety (of the product and patients). The third key objective is record integrity. To ensure we addressed these objectives, we listed the FDA predicate rules and guidances in our model. This led us to expand our development team to include experts from all the good (regulatory) practice (GxPs), regulatory submission creation, and information technology (IT) areas.

To develop our RAMP model, we used our regulatory, IT, and quality assurance (QA) experts to ensure the regulations and guidances promulgated by FDA and other regulatory authorities were properly interpreted and applied.

The three main regulations we reviewed were the Good Clinical Practice (GCP) regulations (21 CFR Part 312 [5] and the International Conference on Harmonisation [ICH] GCPs [6]), the Good Laboratory Practice (GLP) standards (21 CFR Part 58 [7]), and the Good Manufacturing Practice (GMP) regulations (21 CFR Parts 210 and 211 [8,9]) and the European Union’s (EU’s) Annex II (10). We also included the regulations from the Prescription Drug Marketing Act (PDMA [11]) and other FDA guidances, ICH

guidelines, and EU directives to ensure we had a global approach to risk assessment and mitigation.

To weave our way through all of these regulations, we developed a decision-tree branching method. The process is initiated by asking a series of questions, starting with those indicated in Table 1.

If the business and technical system owners performing the assessment know which regulations, directives, or guidelines apply to their application, they choose either of the first two answers and continue. If the owners are aware that the computerized systems do not handle any regulated data, then they must still verify and document that their computerized system meets business and financial objectives; however, they can exit the RAMP process. If the business and technical owners do not know whether regulations, directives, or guidelines apply, then the model guides them to a series of specific questions based directly on the regulations, directives, and guidelines to ascertain which may be relevant and whether a computerized system handles regulated data. For example, the first question in GMP determination asks:

Does your computerized system support the manufacturing, analytical determinations prior to, during, or after of the manufacturing, testing, packaging, or storing processes; or distribution of government regulated products, or are the records within the system kept in order to prove compliance with regulations, guidances, or directives on the manufacturing, testing, packaging, storing or distribution processes?

If they answer yes to this question, RAMP directs them to eight specific GMP questions to

TABLE 1

GxP Applicability	
Question 1: Which Regulation, Directive, or Guideline Applies to Your Computerized System?	
GxPs or PDMA	Go to Part 11 applicability
Submissions	Validation and Part 11 is required; go to risk identification
No GxP regulations	Computerized system does not handle regulated data; however, you must still verify and document that this computerized system meets business and financial objectives
Not sure	Go to GxP determination

TABLE 2

Part 11 Applicability	
Question 2: Does the Computerized System Create, Modify, Maintain, Archive, Retrieve, or Transmit Electronic Records?	
Yes	Go to question 3
No	These records will <i>not</i> trigger Part 11 compliance; however, validation is required; follow your validation SOP <i>Exit the process and document</i>
Question 3: Which Types of Records From This System Do You Rely on to Perform Your Regulated Activities?	
Both electronic and paper	You must <i>document</i> which record (electronic or paper) is relied on to perform regulated activities in your user requirements, functional specifications, SOP, change control log, equipment file, or site inspection file 21 CFR Part 11 applies to this system Go to risk identification
Electronic only	21 CFR Part 11 applies to this system Go to risk identification
Paper	21 CFR Part 11 <i>does not</i> apply. However, validation is required; follow your validation SOP <i>Exit the process and document.</i>
SOP, standard operating procedure.	

further ensure that GMPs apply. If they answer no to the above question or to all eight GMP-specific questions, then the computerized system does not handle any GMP-regulated data, and RAMP points them to general GLP or GCP questions—similar to the GMP question. Similar detailed questions were developed for GLPs (12 questions) and GCPs (9 questions) to ascertain whether the application handles any regulated data. If it is determined that the computerized system does not handle any GxP regulated data, then the owners are directed to verify and document that the computerized system meets its business and financial objectives, and they are done with the RAMP process. Otherwise, they move to determine whether Part 11 applies to this system.

ELECTRONIC RECORD PART 11 APPLICABILITY

Once it is determined that a system handles regulated data or controls a regulated process, Part 11 applicability is reduced to determining and understanding *how* that computerized system handles records or functions (Table 2).

RISK IDENTIFICATION

If Part 11 does apply to the application, then the next step is to conduct the risk assessment. The goal of risk identification is to help the owner manage the impact of that risk on the three key areas of concern: patient and product safety, product quality, and record integrity. We call this risk identification the *overall computerized system risk level*. It is the *potential* risk that could be posed to records handled by this system and is based on the

- types of data it handles (record criticality)
- types of functions it performs
- likelihood of exposure to user actions that may identify system errors and trigger system correction and maintenance

Each of these areas will be rated high, moderate, or low, and the combination of these ratings will produce the overall computerized system risk level. The risk level indicates what level of susceptibility may exist toward patient and product safety, product quality, or record integrity if something should go wrong with a system. Based on this indication, recommendations will be made on how to control this risk such that the system as put into production *does*

TABLE 3

GxP Record Criticality		
Does Your Computerized System Handle the Following Data or Information?		
GMPs (including distribution and sampling) <ul style="list-style-type: none"> • GMP master, batch production, and control records • Specifications • SOPs • Methods • Process validation records • Product release/stability data, component and labeling records • Equipment cleaning and use logs • Return drug product or salvaging records • Distribution records • Other data/documents used to make product quality decisions, complaint records, and variance reports 	GLPs <ul style="list-style-type: none"> • Protocols • Amendments • SOPs • Raw data • Final reports • Individual scientist reports • Sample chain of custody • Test and control article: accountability, characterization, concentration, formulation 	GCPs (including submissions) <ul style="list-style-type: none"> • Electronic records from NDA/BLA submissions • Adverse event report/submissions • Patient data from pivotal safety and efficacy studies (eg, phase IIb and phase III clinical studies) • Patient data from PK drug labeling clinical studies and PK drug-drug interaction studies
If yes to one of these records, then your criticality is <i>HIGH</i>		
If no, continue ...		
Does Your Computerized System Handle the Following Data or Information?		
GMPs (including distribution and sampling) <ul style="list-style-type: none"> • Inventory records • Equipment calibration and maintenance logs • Consultant records • Annual product reviews 	GLPs <ul style="list-style-type: none"> • Archive indices • Audit reports • Deviation reports and memos • Equipment calibration and maintenance logs • Master schedule • Quality assurance statement • Study director correspondence • Test and control article distribution • Test system: accountability, distribution, maintenance 	GCPs (including submissions) <ul style="list-style-type: none"> • Patient data from nonpivotal clinical studies • Patient data from all PK studies except as noted for high records of criticality
If yes to one of these records, then your criticality is <i>MODERATE</i>		
If no, continue ...		

not pose a risk to patient and product safety, product quality, or record integrity (eg, these recommendations could run from stringent automated checking controls for a *high* system to manual or process controls for a *low* system).

GxP RECORD CRITICALITY

The criticality of a record is the extent to which a record is crucial to patient health, drug safety,

quality, and efficacy and drug manufacturing process or the ability to reconstruct a regulated process. Each system must be rated for the most critical records it handles. The questions for GMP, GLP, and GCP are similar but are specific to the types of electronic records in each regulated area. The RAMP model presents the assessor(s) with only the questions pertaining to their identified area (Table 3).

TABLE 3

<i>Continued</i>		
Does Your Computerized System Handle the Following Data or Information?		
<p>GMPs (including distribution and sampling)</p> <ul style="list-style-type: none"> • Validation records • Training records and CVs • Facilities records • Report formatting records, etc • Other records 	<p>GLPs</p> <ul style="list-style-type: none"> • Validation records • Training records and CVs • Facilities records • Report formatting records • Test system ordering, etc • Other records 	<p>GCPs (including submissions)</p> <ul style="list-style-type: none"> • Financial disclosure statements • Investigator CVs • Validation records • Training records and CVs • Facilities records • Report formatting records • Protocols • Protocol amendments • Form FDA 1572 • Drug inventory records (receipt, distribution, accountability) • Internal review board/ethics board documents • Investigator's brochure • Sponsor SOPs • Other records
<p>If yes to one of these records, then your criticality is <i>LOW</i></p>		
<p>If not on list, please contact your QA department to discuss</p>		
<p><small>SOP, standard operating procedure, NDA, New Drug Application; BLA, Biologic License Application; PK, Pharmacokinetics.</small></p>		

COMPUTERIZED SYSTEM ISSUES

System functionality and system distribution together produce an overall effect on the risk level of a system. Each area is scored, and then the scores are combined to determine high, moderate, or low risk posed by computerized system issues. This will then be combined with the record criticality risk to determine the overall computerized system risk level.

All GxP systems are evaluated by the same functionality grid to assess the main function performed by the computerized system and the degree to which associated tasks have the ability to effect the integrity of the critical records. If a computerized system performs more than one of these functions (Table 4), then the highest score is used to assess the risk.

All GxP systems are evaluated by the same distribution grid to assess the extent to which an application is used in industry, in academia, or by the government. Risk is reduced with broader distribution due to the “stability” of the software (Table 5).

Combining the scores for functionality and

distribution, we can assign the following scores for computerized systems issues: 7 or 8 = High; 4, 5, or 6 = Moderate; 2 or 3 = Low.

OVERALL COMPUTERIZED SYSTEM RISK LEVEL

The overall computerized system risk level indicates the potential risk a system may pose but does *not* indicate what risks actually exist with this system (only a Part 11 gap analysis will indicate areas of the system that truly pose a risk and the amount of remediation to be performed to mitigate this risk). This overall system risk level is the justified risk assessment allowed in the 21 CFR Part 11 Scope and Application Guidance (1). It is based on the combination of risk identified for record criticality and system issues (Table 6).

RISK MANAGEMENT AND PART 11 GAP ANALYSIS

The completion of a gap analysis shows whether the system complies with Part 11 or if remediation is necessary. Risk management in the areas

TABLE 4

Computerized System Functionality		
What Function Does This Computerized System Perform?		
Main System Function	Description	Score
Electronic data capture	Systems that facilitate the electronic capture of data	3
Data entry/modifications	Systems used to enter, modify, or delete electronic data records	3
Data calculations, transformation, or derivation	Systems used to create new <i>stored</i> data by changing the data format (ie, changing an alpha to a numeric) or by deriving it from other stored data <i>Note:</i> If there is a significant impact on patient health or product safety based on the type of data being transformed or derived, increase this value to 3	2
Data analysis—reporting	Systems used to analyze data—output may be in the form of data sets or listings, graphs, reports	2
Submission creating	Systems used to collate and publish a regulatory submission or report	2
Data transport	Systems used to move electronic records from one platform to another	1
Data browsing	Systems used to interrogate data for accuracy, quality, and reliability or other preanalysis purposes; output would not be used for any regulated activity	1
Data/document storage and distribution	Systems used to facilitate storage of data/documents required to be retained	1

of validation, audit trail, and record retention is part of the gap analysis process. The gap analysis follows the requirements listed in 21 CFR Part 11 (12) and was modified according to the recommendations in the Guidance for Scope and Application (1). We have interpreted this guidance to consolidate or reduce validation

deliverables and testing commensurate with an overall computerized system risk level and complexity. Each system is assessed against each of the 25 requirements of Part 11. On the basis of the justified assessment, this model instructs by providing specific remediation requirements for each risk level.

TABLE 5

Computerized System Distribution		
How Is This Computerized System Distributed?		
System Distribution	Description	Score
Custom-designed, highly configured or contains OSS	System was designed, developed, or highly configured for or by user organization or application is or contains OSS	5
Multi-industry limited use	System was designed and developed for general purposes across many industries, academia, or government but is not widely used	4
Regulated industry limited use	System was designed and developed for regulated purposes (eg, pharmaceutical industry) but is not widely used	3
Regulated industry broad use	System was designed and developed for regulated purposes (eg, pharmaceutical industry) and is widely used	2
Multi-industry broad use	System was designed and developed for general purposes across many industries, academia, or government and is widely used	1

OSS, Open Source software.

- *High-risk systems* will be validated and tested to ensure compliance with all aspects of Part II and applicable predicate rules, directives, and guidelines.
- *Moderate-risk systems* will be allowed to reduce some Part II requirements for record retention, audit trails, and validation. Some testing will be reduced commensurate with this risk level.
- *Low-risk systems* will be allowed to reduce further some of the Part II requirements for record retention, audit trails, validation. Testing will be reduced commensurate with this risk level.

Table 7 shows our recommended controls for applications, based on their risk level for record retention, audit trails, and validation and testing.

BUSINESS PRIORITY RANKING

The business priority ranking (Table 8) is an optional activity. It takes into consideration government audit findings on this or similar computerized systems and the ability of the business to manage or tolerate the impact of system unavailability. Priority ranking indicates the significance an organization should place on providing resources toward any necessary remediation as determined by the gap analysis.

If an assessment is being done on a system prior to implementation, then there is no reason to identify a business priority ranking as any areas identified in the gap analysis will be addressed during system requirement analysis and implementation. While all areas determined by the gap analysis to be out of compliance must be corrected, in reality an organization may not have readily available resources to address all needs of all systems as soon as they are identified. In this case, the business priority ranking can help them determine the order to apply the limited resources.

The business priority rank focuses on regulatory experience and system vulnerability. Each of these areas is scored, and combining their scores provides a ranking number of 0 through 10. The ranking number determines appropriate priority for managing resources for multiple systems within a single risk category (high, moderate, low). A higher business priority rank indicates a higher urgency for the business to make

Overall Computerized System Risk Level		
Record Criticality	System Issues	Overall Computerized System Risk Level
High	High	High
High	Moderate	High
High	Low	Moderate
Moderate	High	High
Moderate	Moderate	Moderate
Moderate	Low	Moderate
Low	High	Moderate
Low	Moderate	Low
Low	Low	Low

TABLE 6

modifications to the system based on areas identified as out of compliance in the 21 CFR Part II gap analysis.

When a high-priority rank is determined, a system owner may want to use this to elevate the risk to the next higher level to justify following the more stringent guidelines for validation, record retention, and audit trailing. For example, a warning letter on a low-risk system would increase the business priority rank, and this could be used to justify elevating the system risk to require a more rigorous handling of this system.

Adding together these two values will give the *business priority rank* (a number from 0 to 10) for your application.

COMPLIANCE PLANNING

All systems that are in production and have areas out of compliance, as determined by the 21 CFR Part II gap analysis, must complete a compliance plan. A compliance plan consists of identifying discrepancies based on the 21 CFR Part II gap analysis, setting a priority to these systems, and scheduling appropriate resources and target completion dates to accomplish the required tasks. The business priority rank should be used to allocate resources within a compliance plan and for resources that cross over functional areas (eg, IT resources).

TABLE 7

Justified Risk Assessment Part 11 Gap Analysis		
Record Retention Risk		
System will comply with <i>predicate rule retention requirements</i> .		
<i>Note:</i> If the system is not responsible for record retention, then there must be another validated process or system in place to handle this requirement for the records generated by this system.		
High	Moderate	Low
Retention process preserves the content and meaning, provides for accurate retrieval, and is a part of the system validation plan	Retention process preserves the content and meaning, provides for accurate retrieval, and is a part of the system validation plan	Retention process preserves the content and meaning, provides for accurate retrieval, and is a part of the system validation plan
Records can be readily retrieved during retention period	Records can be readily retrieved during retention period	E-records are retained in human-readable format (ie, paper, microfiche) or in common e-format (ie, PDF)
E-records are retained in human-readable format	E-records are retained in human-readable format (ie, paper, microfiche) or in common e-format (ie, PDF)	
Associated audit trail is retained with e-record	Associated audit trail is retained with e-record	
Audit Trail Risk		
System will comply with <i>predicate rule retention requirements</i> .		
Computerized systems that do not modify or delete records are not required to have an audit trail.		
High	Moderate	Low
System has an <i>automated audit trail</i> as defined in 21 CFR Part 11: "Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying."	Physical record deletion is not allowed (but logical deletion is permissible) during the record retention period	System has control measures (automated or nonautomated)
	Changes to records do not obscure previous entries	
	Nonroutine "system repair" work that cannot be captured in an audit trail is documented using appropriate system change procedures	
Physical record deletion is not allowed (but logical deletion is permissible) during the record retention period		
Nonroutine "system repair" work that cannot be captured in an automated fashion is documented using appropriate system change procedures		

TABLE 7

<i>Continued</i>		
Validation Risk		
System is validated such that any potential risk is minimized.		
Only the depth and extent of the validation can be modified based on the justified risk.		
The amount of documentation should be commensurate with the complexity and risk of the application but ample to prove that the risk of such system can be minimized.		
It should be noted that, for small systems, these deliverables may be combined into a single document, while for large systems, there may be a document for each deliverable.		
High	Moderate	Low
Vendor audit or assessment has been performed; any outages uncovered during the audit or assessments are included in your validation plan	System is validated and documented with sufficient detail to at a minimum thoroughly discuss the following: Computerized system description	System is validated and documented with sufficient detail to at a minimum thoroughly discuss the following: Requirements
Validation deliverables must be based on your system life cycle or validation SOP	Requirements Traceability matrix (as determined by the complexity of the computerized system) Validation plans, protocols, and reports Vendor audit or assessment (optional)	Validation plans, protocols, and reports (executed and signed) Vendor audit or assessment (optional)
Testing	Testing	Testing
The amount of testing includes	The amount of testing can be limited to	The amount of testing can be limited to
User requirements Normal functionalities All business processes Regulatory requirements Robust and challenge testing	Critical functionalities All business objectives Regulatory requirements	Business objectives Regulatory requirements
PDF, portable document format; SOP, standard operating procedure.		

ASSESSMENT COMPLETION

The RAMP is completed by a signature from the assessor and system business owner. The completed and signed RAMP document is stored with the system validation documentation. It is appropriate to review the RAMP with subsequent system upgrades that require system revalidation.

SUMMARY

When computerized systems are used to collect data where decisions are made on drug efficacy and patient safety or are used to control the quality of drug during the manufacturing process, they must comply with applicable regulations and guidances, protect the public by fa-

cilitating approval of safe and effective drug products, and meet business objectives. FDA's Part 11 Final Rule on Electronic Records and Signatures (1997) (12) outlines stringent controls expected to ensure this public protection. The 2003 Guidance on Scope and Application of Part 11 (1) allows the regulated industry a chance to reduce how we manage the validation, audit trailing, and retention of our electronic records by developing a justifiable risk assessment-based approach and providing proof that, based on sound rationale, we are adequately assessing, documenting, and mitigating the risk of the computerized system.

The RAMP model developed by P&G is a methodical and logical risk assessment tool focus-

TABLE 8

Business Priority Ranking		
Regulatory Experience: Choose One Condition That Best Describes the Regulatory Experience of Your Application		
Condition	Definition	Value
Warning letter within the industry	Warning letter has been issued on this or similar computerized system here or within the industry	5
Critical Part 11 gap	21 CFR Part 11 gap analyses indicate a compliance outage in the system that could pose a risk of receiving a warning letter.	5
483 and EIR within the industry	483 observation and EIR with required action indicated has been issued on this or similar computerized system here or within the industry	4
Significant Part 11 gap	21 CFR Part 11 gap analyses indicate a compliance outage in the system that could pose a risk of receiving a 483 observation	4
System routinely inspected	FDA typically looks at records from this type of system during routine inspections	3
No information	No regulatory information available for this or similar computerized systems	3
No 483; voluntary action indicated in EIR	No 483 issued, comments made during debriefing; voluntary action indicated in EIR	2
Not routinely inspected or not inspected	FDA does not typically look at records from this type of system during inspections or has not performed an inspection on this system	1
No 483; no action indicated	FDA has inspected this system/records and made no comments or indicated no actions	0
Vulnerability: Choose One Condition That Best Describes the Business Tolerance of This Application Being Out of Production		
Condition	Definition	Value
Low tolerance of downtime (ie, less than a day)	If the system should go down for a short period of time, then there will be a negative impact on patient health, product quality, or business objectives	5
Low tolerance and contingency plan	Although there is a low tolerance of downtime, a tested contingency plan is in place	4
Moderate tolerance of downtime (ie, 2–4 days)	If the system should go down for a moderate period of time, then there will be moderate impact on patient health, product quality, or business objectives	3
Moderate tolerance and contingency plan	Although there is a moderate tolerance of downtime, a tested contingency plan is in place	2
High tolerance of downtime (ie, 5+ days)	If the system should go down for a long period of time, then there will be little impact on patient health, product quality, or business objectives	1
High tolerance and contingency plan	There is a high tolerance of downtime and a tested contingency plan is in place	0

EIR, establishment inspection report.

ing on patient safety and product safety and quality. An outcome of this assessment is an evaluation of a record's integrity and the type of testing, audit trailing, and records retention needed, commensurate with the justified risk. A further outcome is a guideline for prioritizing remediation work in identified areas. This process is consistent and justified, especially when it is coupled with a robust system life cycle management process.

Acknowledgment—We would like to thank the RAMP Development Team for their hard work and dedication during the 15-month development, pilot, and rollout of the model. The team members are Lori Carlson, Mark Gibbs, Dave Kunzinger, Andrew Linegang, Peter Passalacqua, Suzanne Bishop, and Richard Siconolfi.

REFERENCES

1. Food and Drug Administration, Center for Drug Evaluation and Research. Guidance for Industry, Part II, Electronic Records; Electronic Signatures—Scope and Application. August 2003. Available at: <http://www.fda.gov/cder/guidance/5667fnl.htm>. Accessed November 1, 2006.
2. Food and Drug Administration. FDA's Mission Statement. 2005. Available at: <http://www.fda.gov/opacom/morechoices/mission.html>. Accessed November 1, 2006.
3. Society of Quality Assurance Computer Validation Initiative Committee. Risk assessment/validation priority setting. *Qual Assurance Newsl.* 1998;14.
4. International Society for Pharmaceutical Engineers. Risk-Based Approach to 21 Part CFR Part II, via www.ispe.org. January 2003. [A six-page white paper on approaching risk assessment; no longer available on their Web site.]
5. Food and Drug Administration. 21 CFR Part 312, Investigation New Drug Application. Available at: <http://www.fda.gov/cder/Offices/DSI/goodClinPractice.htm>. Accessed November 1, 2006.
6. International Conference on Harmonisation. Good Clinical Practice: Consolidated Guideline. Available at: <http://www.ich.org/cache/compo/276-254-1.html>. Accessed November 1, 2006.
7. Food and Drug Administration. 21 CFR Part 58, Good Laboratory Practice for Nonclinical Laboratory Studies. Available at: <http://www.fda.gov/cder/Offices/DSI/regulations.htm>. Accessed November 1, 2006.
8. Food and Drug Administration. 21 CFR Part 210, Current Good Manufacturing Practice in Manufacturing, Processing, Packing, or Holding of Drugs; General. Available at: <http://www.fda.gov/cder/dmpq/cgmpregs.htm>. Accessed November 1, 2006.
9. Food and Drug Administration. 21 CFR Part 211, Current Good Manufacturing Practice for Finished Pharmaceuticals. Available at: <http://www.fda.gov/cder/dmpq/cgmpregs.htm>. Accessed November 1, 2006.
10. European Union Annex II. Commission Directive 2003/94/EC, 8 October 2003, Laying Down the Principles and Guidelines of Good Manufacturing Practice in Respect of Medicinal Products for Human Use and Investigational Medicinal Products for Human Use. Replacement of Commission Directive 91/356/EC, 13 June 1991, to Cover Good Manufacturing Practice of Investigational Medicinal Products. Available at: <http://ec.europa.eu/enterprise/pharmaceuticals/eudralex/homev4.htm>. Accessed November 1, 2006.
11. Food and Drug Administration. 21 CFR Parts 203 Prescription Drug Marketing Act (revised as of 1 April 2006). Available at: <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=203>. Accessed November 1, 2006.
12. Food and Drug Administration. 21 CFR Part II, Electronic Records; Electronic Signatures Final Rule. *Federal Register*, March 20, 1997. Available at: <http://www.fda.gov/cder/Offices/DSI/regulations.htm>.

Suzanne Bishop and Richard M. Siconolfi report no relationships to disclose.