Certified Software Solutions Quality Forum
November, 2003 Vol.1 No. 7

Use of Risk Management Principles to Satisfy Part 11 Requirements

By: Curtis Egan and Dan Olivier

The focus of this paper is the use of risk assessment techniques to address the three Part 11 requirements explicitly identified in the FDA's August 2003 Part 11 Guidance. In the Guidance for Part 11 Scope and Application, the FDA recommends use of a risk assessment to determine applicable requirements for validation (21 CFR Part 11.10(a)), record retention (21 CFR Part 11.10(c)), and for audit trails (21 CFR Part 11.10(e)).[1] Application of risk assessment to address these particular requirements is the focus of this paper. The August 2003 Part 11 Guidance is one of many documents that the FDA has recently published that increasingly refer to the to risk management techniques including the approach for the new Pharmaceutical GMP and the Quality Systems Inspection Technique (QSIT) audit methodology.[2,3]

What is a Risk Assessment Approach?

Although risk assessment normally implies an evaluation of risk as a combination of severity and likelihood of occurrence, this risk assessment model is difficult to apply to the elements of the Part 11 regulation that are referred to in the FDA Guidance. In general, failure to adequately conduct validation, implement audit trails, and/or to properly conduct record retention procedures all could result in severe risk conditions. In support of the use of risk assessment for these requirements an alternate risk assessment strategy is needed.

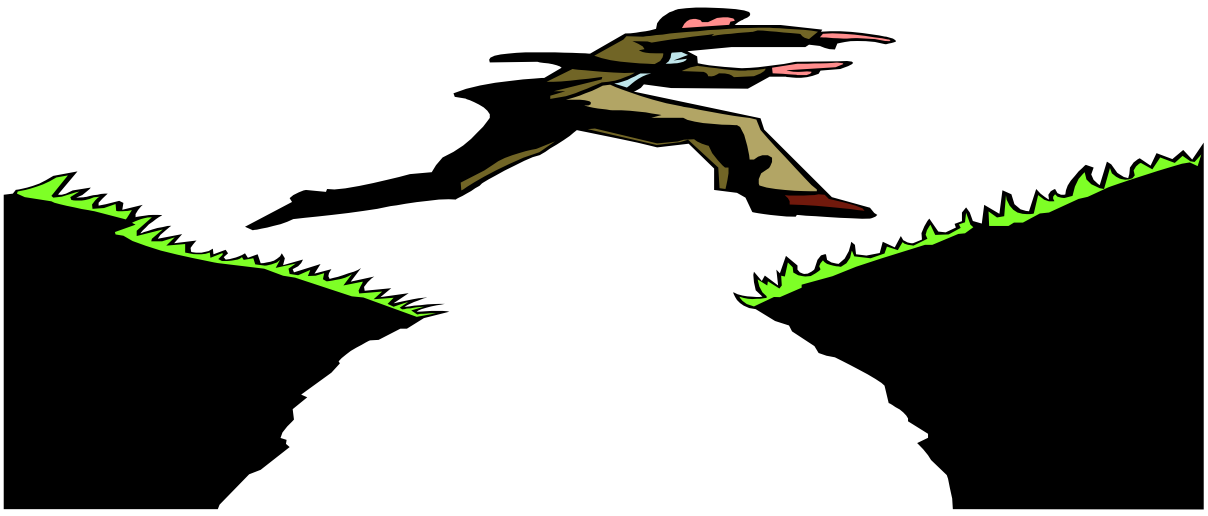
Instead of the severity and likelihood evaluation, we propose a risk assessment at a functional level of quality systems, to identify the selected functions that would be subject to these specific regulatory requirements. In this case the risk is not applied to the entire system, but to individual functions of the system that would introduce risk if not adequately validated, if the functions failed to provide audit trails, or if the records produced were not properly retained. Examples of a risk assessment applied to each of these three Part 11 requirements follow.

Part 11 Scope

As stated in the FDA Guidance, "Part 11 will be interpreted narrowly; we are now clarifying that fewer records will be considered subject to part 11." The Guidance further states that "when persons choose to use records in electronic format in place of paper format, part 11 would apply." This means that it is up to the manufacturer to identify what systems (paper based or automated) are used to address the requirements of the predicate rules (requirements defined in regulations other than Part 11). The guidance goes on to state that the Agency "intends to exercise enforcement discretion with respect to all part 11 requirements for systems that otherwise were operational prior to August 20, 1997". As a result of these statements the manufacturer must first identify the systems that are then subject to Part 11 compliance, and then address use of a risk assessment to determine the requirements that are necessary to support compliance with the validation, audit trail, and record retention requirements of the Part 11 regulation.

Definition of Risk

Before we begin the risk assessment, a definition of risk is appropriate. In the instances where the FDA recommends a risk assessment in the Part 11 Guidance, the reference defines risk as "a determination of the potential of the system to affect product quality and safety, and record integrity". Table 1 provides an example of the types of risk that can be associated with the three Part 11 requirements for which use of a risk assessment method is recommended.



Requirement	Examples of Potential Risks
11.10(a) Validation	• Incorrect data for determination of product release such as data for: test results, equipment operation (calibration and maintenance data), environmental monitoring, laboratory test results, etc. • Improper manufacturing due to equipment not validated • Incorrect specifications used for production or design • Improper failure analysis due to incorrect complaint/service records (records not complete, not correct, traceability incorrect, etc.) • Manufacturing processes not correctly monitored • Use of unqualified components (improper status, expired, supplier not qualified, etc.) • Unqualified operators/users (training records incorrect)
11.10(c) Record retention	• Required records not available for defined retention period • Records retained but cannot be reliability retrieved and printed/copied
11.10(e) Audit trails	• Integrity of records in question due to ability of records to be changed without audit trail (records such as: results from clinical trials, manufacturing tests, design tests, complaint investigations, etc.)

Table 1 Part 11 Risk Identification Table

For purposes of this paper we will assume that these definitions of risk are appropriate without further discussion.

Risk Assessment for Validation

Validation is required for automated systems used in support of applicable FDA regulations even if electronic records are not used, this is not a requirement that is unique to the Part 11 regulation. Before a risk assessment can be conducted at this level, a review of the system must first be conducted to identify if it is subject to compliance with Part 11. What value is then provided through the use of a risk assessment approach for the evaluation of the need for validation? Where the risk assessment may yield value is in the selection of the specific functionality that is to be validated and the level of validation (thoroughness of testing) that is appropriate for these functions. So even though the use of a risk assessment does not eliminate the need for system validation, it can be a very valuable tool in reducing the scope and detail of validation activities that are required to ensure compliance. An example of how an assessment of risk for system validation may be applied at a functional level for a example set of system functional requirements is shown in Table 2 below.

	Function	Regulated Rqmt?	Quality Affect?	Validation Required
1.	Logon security	√	√	Yes
2.	Report generation	√	√	Yes
3.	Data entry	√	√	Yes
4.	Billing			No
5.	Accounts due reports			No
6.	Trending summary		√	Yes

Table 2 Analysis of System Functions for Validation Requirement

As a result of such a risk assessment, a reduced scope of system validation may be defended as acceptable to meet regulatory requirements. (This risk based approach to the definition of system functional validation requirements is also supported by the FDA's guidance on the use of a Hazards Analysis of Critical Control Points.[4])

Risk Assessment for Audit Trails

The need for "computer-generated time-stamped audit trials" (Part 11.10(e)) for electronic records is heightened for systems where the operator can change data and for systems where there is a motivation for changing data (for instances pressure to meet production schedules).[5] Using this as a basis, we can propose a risk assessment to identify where audit trails should be mandated for records where the operator is permitted to add, modify, or delete data. Lesser risk and therefore lesser need for audit trails may be appropriate for records where the operator cannot modify data through normal readily accessible means, this would include data that is automatically imported from another system and cannot be changed.

To apply a risk assessment for audit trails an analysis may be conducted of all of the records in the system that are applicable to the implementation of regulatory requirements. Once these records are identified, the level of operator accessibility can be evaluated to determine audit trail requirements. An example analysis is provide in Table 3 following.

	System Records	Regulated data?	Data can be edited?	Audit Trails Required
1.	Security records	√	√	Yes
2.	Batch history record data	√	√	Yes
3.	Automated test system results	√		No
4.	Billing records			No
5.	Complaint investigation test records	√	√	Yes
6.	Lot number record	√		No

Table 3 Analysis of System Records that Require Audit Trails

Risk Assessment for Record Retention

Record retention is not normally implemented as a system function but as a procedure, for instance a procedure to conduct back-ups at a predefined interval. In addition to the definition of the back up itself, established procedures should include other key requirements such as:

1. checks to ensure that the data that has been backed-up is easily accessible and readable (we all are aware of instances when the back-up records have been retrieved only to find that the data cannot be reloaded onto the system because it is corrupt, because the data format has changed, etc.);
2. ensure that the data is stored in a format that can be read in the future even if the application software has changed (a standard electronic file format is preferred such as PDF, or XML); and
3. ensure that data is stored to media that can reliably be used for the duration of the required retention period.

So the first step in this assessment of risk is to ensure that adequate procedures are in place to support ongoing record retention requirements for automated systems that are used to support regulatory requirements.

In addition to verifying that adequate procedures are in place to specify data back-up requirements, it is also probably a good idea to examine record retention requirements. In many cases companies have established a product life that is very lengthy or failed to establish a product life resulting in extremely difficult record retention requirements (if no product life is established records must be retained indefinitely). For many companies the overhead and compliance risk associated with satisfying record retention requirements can be streamlined by reducing the duration of record retention requirements.

The risk for record retention comes into play in assessing current records that have been retained that may not be accessible for the required retention period because the media has deteriorated or because the data format cannot be read by the current software application. (If the data is corrupt or cannot be located there is not much that can be done to recover the data, this risk is not addressed in this paper.) The risk assessment for addressing Part 11 requirements can then be focused on whether archived records that exist are accessible and can be projected to be accessible for the required retention period. If these records exist, the durability of the storage media used and the accessibility to hardware and software systems that can retrieve the data should be reviewed to ensure access throughout the defined retention period. If these capabilities do not exist, then a risk assessment can be used to determine what remediation should be required for the existing records (for instance even though records are required to be retained for a period of ten years, a company may elect to only re-copy records for the last two years suggesting that the risk of needing older records for regulatory requirements is minimal).

Summary

In this issue we have discussed how risk assessment techniques can be used to address selected Part 11 requirements as recommended by the FDA in their guidance document. In addition to the specific use of a risk assessment for Part 11, we want to offer some additional observations.

1. Risk assessment can take on a different approach based on what is being analyzed. ISO 14971 advocates a risk assessment based on severity and likelihood of occurrence, we suggested a different approach for the assessment of Part 11 risks. Risk assessment methods should be tailored to the specific objectives being addressed.

2. Risk assessment methods are being increasingly encouraged by the FDA for use by investigators, in new regulations, and these techniques have also been encouraged for manufacturers. In light of this emphasis, we suggest that manufacturers increasingly use risk management methods for internal regulatory procedures as well.

3. We have only addressed the use of risk assessment from a regulatory perspective, it is also appropriate to recognize that risk assessment methods have significant potential business benefit. Optimal use of risk assessment methods provide an excellent strategy to streamline validation activities for products as well as processes and also offers a technique that can instill increased confidence in the safety of established products and processes.

The benefits obtained from use of risk management methods are becoming increasingly acknowledged by medical and pharmaceutical manufacturers as well as by regulatory bodies such as the FDA. Familiarity and competence in the conduct of risk management techniques is increasingly becoming a critical skill for all quality and regulatory processionals.

References:

1. Guidance for Industry: Part 11, Electronic Records; Electronic Signatures – Scope and Application, US Department of Health and Human Services, Food and Drug Administration, August 2003.
2. New drug GMP
3. Quality System Inspection Technique Handbook, Food and Drug Administration, Center for Devices and Radiological Health, August 1999.
4. Hazard Analysis of critical Control Points for Medical Devices, Food and Drug Administration, Center for Devices and Radiological Health, October 1997.
5. Electronic Records; Electronic Signatures, Title 21 Part 11, Federal Register, Vol. 62, No. 54, March 20, 1997.

CSS Quality Forum

Spotlight on Products: Executive Vision Quality Suite

Executive Vision

Executive Vision is a suite of Quality tools that help organizations monitor and improve their processes.

If you are concerned with product quality, Executive Vision provides the tool for continual improvement and tracking of your quality systems. Quality improvements can only be as good as the information on which they are based.

This system provides an answer to your measurement and improvement needs as defined in the ISO 9001: 2000 Standard. Quality should be more than troubleshooting. At many manufacturing companies, quality has become simple testing and inspection of parts to see if they meet product specifications.

Each application of the Executive Vision Suit is customizable by the user and validated to FDA and 21CFR part 11 regulations. On site training, customer support and maintenance agreements are also available.

Download a free demo of Executive Vision now:

simply go to **www.certifiedsoftware.com/products/vision.htm** and click on the Download Demo Version link.

Medical Community Articles by CSS

CSS also has a number of articles that discuss topics germane to the medical device industry. These articles can be downloaded at no cost at http://www.certifiedsoftware.com/news/articles.htm

The articles cover topics ranging from Software Safety, to Design Controls. They have been published in peridocals such as *Regulatory Affairs, Medical Device & Diagnostic Industry,* and *Regulatory Affairs Focus.*