Risk Based Approach to Software Quality and Validation

By Praxis Life Sciences
Risk Based Approach to Software Quality and Validation

Your Praxis Facilitator

- Debra Bartel, MBA, CQA, PMP
- Partner, Praxis Life Sciences
- 30 years experience specializing in software quality assurance, validation and regulatory compliance, Information Systems project management, and process design.
- Prior to joining Praxis, held management positions in the pharmaceutical industry in both Quality Assurance and Information Systems organizations
- Active member of American Society for Quality (ASQ), Northeastern Illinois Section, Software Division
Intro to Praxis Life Sciences

Target Audience

Industries
- Pharmaceutical & Biologics
- Medical Device
- Clinical Studies
- Blood Products

Regions
- Operating in the US
- Selling to the US Market

Personnel
- IT Personnel and Managers
- Software Quality Personnel and Managers
- Auditors and Audit Managers
Have you ever heard…

- Computer System Validation is a waste of time
- It's just a bunch of paperwork
- It doesn't find the bugs
- We just repeated everything the vendor already did

Webinar Outline

1. Validation & Risk Framework
2. Risk Assessment
3. Risk Mitigation
4. FDA Leadership by Example
Part 1: Validation & Risk Framework

Section Overview

- Validation Terminology
- Validation Process
- Validation Roles & Responsibilities
- Risk Terminology
- Risk Process
**Terminology**

**VALIDATION**
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 software can be consistently fulfilled.

**VERIFICATION**
...consistency, completeness, and correctness of the software and its supporting documentation, ....

**QUALIFICATION**
Formal testing to demonstrate that the software meets its specified requirements.

**Validation Life Cycle**

**Planning**
- Specification
- Build, Purchase/Configure

**Verification**
- Build, Purchase/Configure
- Specification

**Reporting**
- Specification
- Build, Purchase/Configure

**GENERAL APPROACH**
Validation Life Cycle

NON-CONFIGURED PRODUCT APPROACH

CONFIGURED PRODUCT APPROACH
Validation Life Cycle

Planning
- User Requirement Specification
- Functional Specification
- Design Specification

Reporting
- Requirement Testing
- Functional Testing
- Integration Testing
- Module (Unit) Testing

CUSTOM CODED PRODUCT APPROACH

Validation Roles

Business Process Owner
- Manages the business process that uses the computer system
- Ensures that the system is appropriate for the business process
- Assigns Subject Matter Experts (SMEs) to participate in requirements definition and verification
Validation Roles

Business Process Owner

- Manages the implementation and support of the computer system
- Ensures that the system is available to support the business process
- Assigns technical experts to participate in all phases of the validation life cycle

Technology Owner

Validation Roles

Business Process Owner

- Ensures that the computer system meets all internal standards
- Ensures that the computer system meets all applicable regulations
- Ensures that the computer system is ready for inspection

Quality Assurance

Technology Owner
**Basic Risk Terminology**

**Hazard**
A potential source of harm

**Risk**
The combination of the probability of occurrence of a harm and the severity of the harm
Basic Risk Terminology

Hazard  A potential source of harm
Risk    Harm severity and probability

Risk Assessment
A comprehensive evaluation of risks and associated impacts

Severity:
A. [Image]
B. [Image]
C. [Image]

Probability:
A. 5 vehicles per hour
B. 1 vehicle per minute
C. 1 vehicle per second
Basic Risk Terminology

Hazard A potential source of harm
Risk Harm severity and probability
Risk Assessment Evaluation of risk and impact
Risk Mitigation Actions taken to reduce the risk

Basic Risk Terminology

Hazard A potential source of harm
Risk Harm severity and probability
Risk Assessment Evaluation of risk and impact
Risk Mitigation Action to reduce impact

Risk Management A systematic approach to assessment and mitigation of risks throughout the system life cycle
Risk Management Framework

Risk Management Process

<table>
<thead>
<tr>
<th>Risk Assessment</th>
<th>SOP System Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Mitigation</td>
<td>SOP Risk Based Validation</td>
</tr>
<tr>
<td></td>
<td>SOP Audit Trails</td>
</tr>
<tr>
<td></td>
<td>SOP System Security</td>
</tr>
<tr>
<td></td>
<td>SOP User Training</td>
</tr>
<tr>
<td></td>
<td>SOP Incident Management</td>
</tr>
<tr>
<td></td>
<td>SOP System Backup</td>
</tr>
<tr>
<td></td>
<td>SOP Software Vendor Assessment</td>
</tr>
<tr>
<td></td>
<td>Etc.</td>
</tr>
</tbody>
</table>

Risk Assessment

Part 2
Part 2: Risk Assessment

Section Overview

- Regulatory Guidance
- Risk Assessment Process
- Documentation

Risk = A measure of the probability and severity of undesired effects. Often taken as the simple product of probability and consequence. (Source: IEEE)

Risk Assessment = A comprehensive evaluation of the risk and its associated impact. (Source: DOD)

FDA 21 CFR 820 Quality System Regulation (Medical Device GMP)

- Design validation shall include software validation and risk analysis, where appropriate.

FDA Guidance: Off-The-Shelf Software Use in Medical Devices

- Existing international standards indicate that the estimation of risk should be considered as the product of the severity of harm and the probability of occurrence of harm.
- It is more appropriate to manage software safety risk based on the severity of harm rather than the software failure rates.
ICH Q9, Quality Risk Management

Risk assessment consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards.

Three fundamental questions:
1. What might go wrong?
2. What is the likelihood (probability) it will go wrong?
3. What are the consequences (severity)?
Risk Assessment
Regulated users should be able to justify and defend their standards, protocols, acceptance criteria, procedures, and records in the light of their own documented risk and complexity assessments.

The risk assessment and the results including the reasons for the ranking as either: ‘critical’ or ‘not critical’ should be documented.

The URS (User Requirements Specs) should form the basis of a risk assessment of the system for GxP compliance requirements, in addition to other risks, such as safety. The risk analysis may be based on the FS (Functional Spec), which is related to the URS.

The risk assessment should identify critical features.

Validation Scope & Approach
It is important to acknowledge that the scope and level of documentation and records needed to formalize and satisfy basic project management requirements for critical systems will be dependent on:

• The complexity of the system and variables
• The need to ensure data integrity
• The level of risk associated with its operation
• The GxP areas impacted
Risk Management Framework

Risk Management Process

- **Risk Assessment**
  - SOP System Risk Assessment

- **Risk Mitigation**
  - SOP Risk Based Validation
  - SOP Audit Trails
  - SOP System Security
  - SOP Software Vendor Assessment
  - SOP User Training
  - SOP Incident Management
  - SOP System Backup
  - SOP Business Continuity
  - Etc.

Risk Assessment Roles

- **Quality Assurance**
  - Evaluate any risks associated with regulatory compliance and company policies

- **Business Process Owner**
  - Identify, Evaluate, and Classify Risks

- **Technology Owner**
  - Provide information on how the software works and where it could fail
When does risk assessment take place?

High-Level

- Planning
- Specification
- Verification
- Reporting
- Purchase, Coding, and/or Configuration

Detailed

- Planning
- Specification
- Verification
- Reporting
- Purchase, Coding, and/or Configuration
Risk Assessment Steps

**Identification**
Determine and document the hazards associated with use of the system.

**Evaluation**
Assess the severity and probability of the identified hazards.

**Classification**
Categorize the risks according to severity and probability.
Document the classifications.

Hazard Identification

**Identification**
How are hazards identified?

- **Key Question**
  - What might go wrong with this system?

- **Areas of focus**
  - Feature or functions that would negatively impact
    - Patient safety
    - Product quality
    - The integrity of associated data
Example System

Laboratory Management System

Module “A”
Instrument Control & Test Result Tracking

Module “B”
Lab Analyst Training Management & Tracking

Module “C”
Test Charge Accounting

Example Hazards

Identification

What might go wrong?

<table>
<thead>
<tr>
<th>User Requirement</th>
<th>Identified Hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Send test instructions to lab instruments and receive test result data from the instrument</td>
<td>An instrument interface problem could result in an incorrect reading from equipment</td>
</tr>
<tr>
<td>2. Calculate whether a test passes or fails using input from the lab instruments and analyst entries</td>
<td>An incorrect laboratory calculation could provide a passing test result when it should have failed</td>
</tr>
<tr>
<td>3. Assign analysts to perform tests based on training</td>
<td>A data integrity error in the training module could show that a lab analyst was trained when she was not</td>
</tr>
<tr>
<td>4. Calculate the charges for testing for each product line</td>
<td>There could be a calculation error in the Test Charge module</td>
</tr>
</tbody>
</table>
Hazard Evaluation

How are hazards evaluated?

Risk Definition
The combination of the probability of occurrence of a hazard and the severity of the hazard

Key Questions
- What are the consequences (severity) of the hazard?
- What is the likelihood (probability) the hazard will occur?

Areas of focus
- Features or functions that could lead to
  - Patient death or injury
  - Product failure or quality issue
  - Compromised integrity of the associated data
Hazard Evaluation

Severity Evaluation

How are hazards evaluated?

Risk Definition

The combination of the probability of occurrence of a hazard and the severity of the hazard

Risk Component 1

Risk Component 2

Severity of Harm

Probability of Occurrence

Measured as Criticality

Measured as Complexity

Hazard Evaluation Examples

Severity Evaluation

How are hazards evaluated?

<table>
<thead>
<tr>
<th>URS</th>
<th>Identified Hazard</th>
<th>Evaluation of Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An instrument interface problem could result in an incorrect reading from equipment</td>
<td>Could result in an impure batch of product</td>
</tr>
<tr>
<td>2</td>
<td>An incorrect laboratory calculation could provide a passing test result when it should have failed</td>
<td>Could result in death of a patient (if too potent) or failure to cure a patient (if not potent enough)</td>
</tr>
<tr>
<td>3</td>
<td>A data integrity error in the training module could show that a lab analyst was trained when she was not</td>
<td>Could result in a lab analyst being assigned to run a lab test without proper training</td>
</tr>
<tr>
<td>4</td>
<td>There could be a calculation error in the Test Charge module</td>
<td>Could result in a manufacturing department being overcharged</td>
</tr>
</tbody>
</table>
Severity Classification

How is severity classified?

- **Common Classification Method**
  - **Classification by Criticality**
  - 3 Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Expanded Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Criticality</td>
<td>Direct control of: • Manufacturing • Labeling • Distribution • Product Testing • Product Release • Clinical Trials Direct impact on: • Product Quality • Patient Safety • Study Outcomes</td>
</tr>
<tr>
<td>Medium Criticality</td>
<td>Indirect impact on patient safety, product quality, study outcomes, or the integrity of associated data</td>
</tr>
<tr>
<td>Low Criticality</td>
<td>No impact on patient safety, product quality, study outcomes, or the integrity of associated data</td>
</tr>
</tbody>
</table>

**Examples**
- Health product software
- Manufacturing controls
- Automated product inspection
- Label management & automation
- Distribution tracking to enable recalls
- Laboratory test results
- Adverse event tracking
- Clinical trial results
- Patient medical records
- Product quality status management
### Severity Classification

<table>
<thead>
<tr>
<th>Level</th>
<th>Expanded Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Criticality</td>
<td>Direct impact on patient safety, product quality, study outcomes, or the integrity of associated data</td>
</tr>
<tr>
<td>Medium Criticality</td>
<td>Indirect involvement in: Manufacturing, Labeling, Distribution, Product Testing &amp; Release, Clinical Trials</td>
</tr>
<tr>
<td>Low Criticality</td>
<td>No impact on patient safety, product quality, study outcomes, or the integrity of associated data</td>
</tr>
</tbody>
</table>

**Examples**
- Calibration tracking
- Validation tracking
- Document management
- Training tracking
- Corrective/Preventive action tracking
- System access tracking
- Electronic submissions to regulatory agencies
- Product work order management
- Deviation tracking
- Audit tracking
- Approved Supplier Tracking

**Severity Classification**

<table>
<thead>
<tr>
<th>Level</th>
<th>Expanded Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Criticality</td>
<td>Direct impact on patient safety, product quality, study outcomes, or the integrity of associated data</td>
</tr>
<tr>
<td>Medium Criticality</td>
<td>Indirect impact on patient safety, product quality, study outcomes, or the integrity of associated data</td>
</tr>
<tr>
<td>Low Criticality</td>
<td>Any function not already identified as “High Criticality” or “Medium Criticality”</td>
</tr>
</tbody>
</table>

**Examples**
- Manufacturing cost reports
- Turnaround time reports
Severity Classification Examples

<table>
<thead>
<tr>
<th>URS</th>
<th>Identified Hazard</th>
<th>Evaluation of Severity</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>An instrument interface problem could result in an incorrect reading from equipment</td>
<td>Could result in an impure batch of product</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td>An incorrect laboratory calculation could provide a passing test result when it should have failed</td>
<td>Could result in death of a patient or failure to cure a patient</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>A data integrity error in the training module could show that a lab analyst was trained when she was not</td>
<td>Could result in a lab analyst being assigned to run a lab test without proper training</td>
<td>Medium</td>
</tr>
<tr>
<td>4</td>
<td>There could be a calculation error in the Test Charge module</td>
<td>Could result in a manufacturing department being overcharged</td>
<td>Low</td>
</tr>
</tbody>
</table>

Probability Evaluation

How are hazards evaluated?

Risk Definition
The combination of the probability of occurrence of a hazard and the severity of the hazard

Risk Component 1
Severity of Harm
Measured as Criticality

Risk Component 2
Probability of Occurrence
Measured as Complexity
Probability Assessed as “Complexity”

The selection of validation activities should be commensurate with the complexity of the software and the risk associated with use of the software for its specific intended use.

Validation coverage should be based on the software' complexity and safety risk.

The scope and level of documentation and records needed to formalize and satisfy basic project management requirements for critical systems will be dependent on the complexity of the system.

Probability Classification

How can probability be classified?

<table>
<thead>
<tr>
<th>Validation Approach</th>
<th>Complexity Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Standard, non-configured functions within off-the-shelf purchased systems</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>Configured functions within off-the-shelf purchased systems</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>Custom developed functions within either purchased or custom systems</td>
</tr>
</tbody>
</table>
## Probability Classification

<table>
<thead>
<tr>
<th>Complexity Level</th>
<th>Definition</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Standard, non-configured functions within off-the-shelf purchased systems</td>
<td>• Standard test result report within an off-the-shelf laboratory system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Standard data entry screen in a medical records system</td>
</tr>
<tr>
<td>Medium</td>
<td>Configured functions within off-the-shelf purchased systems</td>
<td>• Report configured with an off-the-shelf query tool</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Calculation configured in a laboratory system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Calculation configured in an off-the-shelf spreadsheet tool</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Product release algorithm configured in an off-the-shelf inventory control system</td>
</tr>
<tr>
<td>High</td>
<td>Custom developed functions within either purchased or custom systems</td>
<td>• Custom accounting report developed in COBOL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Custom code developed to send e-mail notification from an off-the-shelf training management system</td>
</tr>
</tbody>
</table>

### Probability Classification Example

**Laboratory Management System**

- **Module “A”**
  - Instrument Control & Test Result Tracking
- **Module “B”**
  - Lab Analyst Training Management & Tracking
- **Module “C”**
  - Test Charge Accounting
Probability Classification Example

**Probability Classification**

<table>
<thead>
<tr>
<th>URS</th>
<th>Requirement</th>
<th>Criticality</th>
<th>Technology</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Send test instructions to lab instruments and receive test result data from the instrument</td>
<td>High</td>
<td>Configured using the out-of-the-box instrument interface tool</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>Calculate whether a test passes or fails using input from the lab instruments and analyst entries</td>
<td>High</td>
<td>Custom code</td>
<td>High</td>
</tr>
<tr>
<td>3</td>
<td>Assign analysts to perform tests based on training</td>
<td>Medium</td>
<td>Out-of the box functionality</td>
<td>Low</td>
</tr>
<tr>
<td>4</td>
<td>Calculate the charges for testing for each product line</td>
<td>Low</td>
<td>Custom report developed in house</td>
<td>High</td>
</tr>
</tbody>
</table>

**Classification Levels**

<table>
<thead>
<tr>
<th>Requirement Level Criticality</th>
<th>Requirement Level Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 High</td>
<td>Medium</td>
</tr>
<tr>
<td>2 High</td>
<td>High</td>
</tr>
<tr>
<td>3 Medium</td>
<td>Low</td>
</tr>
<tr>
<td>4 Low</td>
<td>High</td>
</tr>
</tbody>
</table>

System level criticality is the same as the highest requirement level criticality.
Risk Assessment Documentation

Where should the risk assessment be documented?

**System Level**
- Validation Master Plan (VMP)
- Stand-alone, Risk Assessment

**Requirement Level**
- Requirements Specification
- Stand-alone, Risk Assessment

---

**System and Requirement Risk Assessment**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Criticality Level</th>
<th>Rationale for Criticality Level</th>
<th>Complexity Level</th>
<th>Rationale for Complexity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instrument control</td>
<td>High</td>
<td>An incorrect lab instrument reading could result in an impure batch of product.</td>
<td>Medium</td>
<td>Configured with system’s instrument interface tool</td>
</tr>
<tr>
<td>Test pass/fail determination</td>
<td>High</td>
<td>A calculation error could result in patient death or injury, failure to cure a patient.</td>
<td>High</td>
<td>Custom Code</td>
</tr>
<tr>
<td>Analyst assignment based on training</td>
<td>Medium</td>
<td>A data integrity issue in this function could result in a lab analyst being assigned to run a lab test without proper training.</td>
<td>Low</td>
<td>Standard system functionality without modification</td>
</tr>
<tr>
<td>Testing charges for each product</td>
<td>Low</td>
<td>This function has no impact on patient safety or product quality.</td>
<td>High</td>
<td>Custom code</td>
</tr>
</tbody>
</table>
Part 3: Risk Mitigation

Section Overview

- Risk Mitigation Timing and Activities
- Regulatory Guidance
- Risk Mitigation via Risk Based Validation
- Vendor Documentation and Testing
- Risk Mitigation via Risk Based Software Quality Procedures
Risk Mitigation Definition

Risk Mitigation
Actions taken to reduce the risk

When does Risk Mitigation Take Place?

Validation

Planning → Reporting

Specification → Verification

Purchase, Coding, and/or Configuration

Retirement
What are Risk Mitigation Activities?

Risk Mitigation
Actions taken to reduce the impacts of risks

Activities that reduce the likelihood of system failure:
- 2nd person verification of data entry, calculations, increased user training, etc.

Activities that increase the likelihood of detection of system failure before harm:
- frequent audits of data integrity, back-up tapes, etc.

Activities that reduce the likelihood of system failure:
- design changes, design reviews, code walkthroughs, testing, etc.

Mitigation during Design Stage

FDA Guidance General Principles of Software Validation
Software design specification should include software risk analysis.

ICH Q9 Quality Risk Management
Leverage Risk Assessment:
A. To select the design of computer hardware and software

PIC/S PI 011 Good Practices for Computerised Systems Used in Regulated “GXP” Environments
System Design & Development
Structural integrity and the application of good software and engineering practices are important for critical systems.

Extra benefits may be achieved by code walk-throughs including evaluation of critical algorithms and routines, prior to testing.

Risk reduction measures may need to be incorporated into the system’s design and operation.
Mitigation during Design Stage

**Part 11 Approach:** We [FDA] recommend that you base your approach [to part 11] on a justified and documented risk assessment and a determination of the potential of the system to impact product quality and safety, and record integrity.

**Audit Trails:** We recommend that you base your decision on whether or not to apply audit trails, or other appropriate measures, on the need to apply with predicate rule requirements, a justified and documented risk assessment, and a determination of the potential effect on product quality and safety, and record integrity.

**Audit Trails:** The need for audit trails should be determined based on a justified and documented risk assessment that takes into consideration circumstances surrounding system use, the likelihood that information might be compromised, and any system vulnerabilities.

Mitigation during Vendor Selection

**Vendor Audits:** Depending upon the device risk involved, the device manufacturer should consider auditing the vendor’s design and development methodologies used in the construction of the OTS software and should assess the development and validation documentation generated for the OTS software.

**Supplier Audits and Approval:** The need to perform a supplier audit should be linked to the regulated user’s risk assessment and quality assurance standards.

For GxP regulated applications it is essential for the regulated user to define a requirement specification prior to selection and to carry out a properly documented supplier assessment and risk analysis for the various system options. Information for such exercises may come from supplier audits and research into the supplier’s product versions in the user community and literature.
Validation Center™ © 2019 Praxis Life Sciences

Mitigation during Validation Planning

**FDA Guidance General Principles of Software Validation**

**Validation Planning:** The quality plan should identify the role that risk (hazard) management will play.

**Tracing:** A software requirements traceability analysis should be conducted to trace software requirements to (and from) system requirements and the risk analysis results.

**Validation Scope & Scale:** Validation coverage should be based on the software’s complexity and safety risk. The selection of validation activities should be commensurate with the complexity of the software design and the risk associated with use of the software for its specific intended use. As the risk increases, additional validation activities should be added to cover the additional risk. For very low risk applications, certain tasks might not be needed at all.

---

PIC/S PI 011 Good Practices for Computerised Systems Used in Regulated “GXP” Environments

**Validation scope** should include GxP compliance criteria, ranked for all product/process quality and data integrity risk criticality, should the system fail or malfunction.

It is essential to assign priorities and attention to those systems (and features within systems) that represent the highest potential for disaster, should they malfunction or become inoperative.

**ICH Q9 Quality Risk Management**

Leverage Risk Assessment to determine the extent of validation, e.g.,
- identification of critical performance parameters
- selection of the requirements and design
- code review
- the extent of testing and test methods
- reliability of electronic records and signatures.
Mitigation during and after Validation

Testing: The amount of structural testing should be commensurate with the level of risk posed by the software. The amount of path coverage is normally established based on the risk or criticality of the software under test.

Validation Evidence: Document requirements and risk analysis of the automated process help to define the scope of the evidence needed to show that the software is validated for its intended use.

Mitigation during the Life of the System

Data Entry: Where applicable, there should be special procedures for critical data entry requiring and second check.

Back-Ups: The frequency of back-up is dependent on the computer system function and the risk assessment of the loss of data.

There should be procedures to assure routine back-up of data to a safe storage location, adequately separated from the primary storage location, and at a frequency based on the analysis of risk to GxP data.

Record Maintenance: We [FDA] suggest that your decision on how to maintain records be based on predicate rule requirements and that you base your decision on a justified and documented risk assessment and a determination of the value of the records over time.

Security: We [FDA] recommend that passwords or other access keys be changed at established intervals commensurate with a documented risk assessment.
Risk Mitigation Roles

**Business Process Owner**
Develop procedural mitigation approaches

**Technology Owner**
Develop technical mitigation approaches

**Quality Assurance**
Ensure mitigation approach meets expectations for regulatory compliance and company policies

Risk Mitigation Framework

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Risk Based Approach to Validation Testing

<table>
<thead>
<tr>
<th>Criticality</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements Coverage</td>
<td>All requirements, multiple data sets</td>
<td>All requirements, single data set</td>
<td>Sampling</td>
<td>All requirements, multiple data sets</td>
<td>All requirements, single data set</td>
<td>Sampling</td>
<td>All requirements, multiple data sets</td>
<td>All requirements, single data set</td>
<td>Sampling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path testing</td>
<td>All paths, multiple scenarios</td>
<td>All paths, single scenario</td>
<td>Sampling</td>
<td>All paths, multiple scenarios</td>
<td>All paths, single scenario</td>
<td>Sampling</td>
<td>All paths, multiple scenarios</td>
<td>All paths, single scenario</td>
<td>Sampling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boundary testing</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test case degree of detail and specificity</td>
<td>Specific, detailed</td>
<td>Medium detail</td>
<td>General</td>
<td>Specific, detailed</td>
<td>Medium detail</td>
<td>General</td>
<td>Specific, detailed</td>
<td>Medium detail</td>
<td>General</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test data similar to production data</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing evidence</td>
<td>Completed protocol, screen prints of test inputs and outputs</td>
<td>Completed protocol, screen prints of test outputs</td>
<td>Completed protocol</td>
<td>Completed protocol, screen prints of test inputs and outputs</td>
<td>Completed protocol, screen prints of test outputs</td>
<td>Completed protocol</td>
<td>Completed protocol, screen prints of test inputs and outputs</td>
<td>Completed protocol, screen prints of test outputs</td>
<td>Completed protocol</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User execution of validation tests</td>
<td>OQ &amp; PQ</td>
<td>Optional</td>
<td>PQ</td>
<td>Optional</td>
<td>PQ</td>
<td>Optional</td>
<td>PQ</td>
<td>Optional</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Risk Based Approach to Validation Documentation

<table>
<thead>
<tr>
<th>Criticality</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Med</td>
<td>Med</td>
<td>Med</td>
<td>Med</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Change Request</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation Plan</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Requirements (URS)</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Functional Specifications (FS)</td>
<td>Highly Detailed</td>
<td>Less Detailed</td>
<td>Optional</td>
<td>Highly Detailed</td>
<td>Less Detailed</td>
<td>Optional</td>
<td>Highly Detailed</td>
<td>Less Detailed</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Design: Architecture</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Design: Software</td>
<td>Highly Detailed</td>
<td>Less Detailed</td>
<td>Optional</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Design: Configuration</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test Plan/Design</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>Optional</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validation Protocols (IQ, OQ, PQ)</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>Optional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Required
### Risk Based Approach to Validation Documentation

<table>
<thead>
<tr>
<th>Complexity</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation Incident Reports</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>Trace Matrix – URS to FS</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>Trace Matrix – FS to Design</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>Trace Matrix – URS to PQ</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>Trace Matrix – FS to OQ</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>OQ, PQ Trace To Test Step</td>
<td>Test</td>
<td>Step</td>
<td>Optional</td>
<td>Test</td>
<td>Step</td>
<td>Test</td>
<td>Case</td>
<td>Optional</td>
<td>Test</td>
<td>Step</td>
</tr>
</tbody>
</table>

- Required

---

### Risk Based Approach to Verification Activities

<table>
<thead>
<tr>
<th>Complexity</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Assessment</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>Unit Testing</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Code Review</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Design Review</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>Part 11 Compliance Assessment</td>
<td>✓</td>
<td>✓</td>
<td>n/a</td>
<td>✓</td>
<td>✓</td>
<td>n/a</td>
<td>✓</td>
<td>✓</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Verification of System Use and Support SOPs **</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>✓</td>
<td>Optional</td>
<td>Optional</td>
<td>✓</td>
<td>✓</td>
<td>Optional</td>
<td>Optional</td>
</tr>
</tbody>
</table>

- Required

** System Use and Support SOPs include: Back-up, Recovery, Security and Access, Training Requirements, Incident Handling, Change Management, Technical Operation and Routine Maintenance, User Operation.
### Risk Based Validation Example

**Examples from Laboratory Management System**

<table>
<thead>
<tr>
<th>Function</th>
<th>Criticality</th>
<th>Technology</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong> Interface to a lab instrument to control instrument and read results</td>
<td>High</td>
<td>Configured using the out-of-the-box instrument interface screen</td>
<td>Medium</td>
</tr>
</tbody>
</table>

**Document Requirements**
- User Requirements
- Detailed Functional Specs
- Design Documentation (Architecture + Software)
- Test Plan/Design
- Protocols (IQ, OQ, PQ)
- Trace Matrices (URS → FS, FS → Design, URS → PQ, FS → OQ)

**Testing Requirements**
- All requirements, multiple data sets
- All paths, 1 scenario
- Boundaries
- Realistic test data
- Screen prints of inputs and outputs
- Users execute PQ, may delegate OQ execution

**Additional Verifications**
- Design Review
- Part 11 Compliance Assessment
- SOPs for system use and support

---

<table>
<thead>
<tr>
<th>Function</th>
<th>Criticality</th>
<th>Technology</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>B</strong> Calculation of batch pass/fail based on lab test results</td>
<td>High</td>
<td>Custom code</td>
<td>High</td>
</tr>
</tbody>
</table>

**Document Requirements**
- User Requirements
- Detailed Functional Specs
- Design Documentation (Architecture + Software)
- Test Plan/Design
- Protocols (IQ, OQ, PQ)
- Trace Matrices (URS → FS, FS → Design, URS → PQ, FS → OQ)
- Unit Test Report
- Code Review Report

**Testing Requirements**
- All requirements, multiple data sets
- All paths, multiple scenarios
- Boundaries
- Realistic test data
- Screen prints of inputs and outputs
- Users execute both OQ and PQ

**Additional Verifications**
- Design Review
- Part 11 Compliance Assessment
- SOPs for feature use
- Unit Testing
- Code Review
### Risk Based Validation Example

#### Examples from Laboratory Management System

<table>
<thead>
<tr>
<th>Function</th>
<th>Criticality</th>
<th>Technology</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>C</strong> Entry of training dates</td>
<td>Medium</td>
<td>Out-of-the-box functionality</td>
<td>Low</td>
</tr>
</tbody>
</table>

#### Required Documents
- User Requirements
- Functional Specs
  (can be less detailed)
- Design Documentation
  (Architecture only)
- Protocols (IQ, OQ, PQ)
- Trace Matrices (URS → FS, URS → PQ, FS → OQ)

#### Optional Documents
- Test Plan/Design
- Trace from FS → Design

#### Testing Requirements
- All requirements, single data set
- Sample of paths
- Screen prints of outputs
  (no screen prints of inputs)

#### Testing Options
- Boundary testing
- Realistic test data
- Users may delegate both OQ & PQ execution

#### Additional Verifications
- Part 11 Compliance Assessment
- SOPs for feature use

---

### Risk Based Validation Example

#### Examples from Laboratory Management System

<table>
<thead>
<tr>
<th>Function</th>
<th>Criticality</th>
<th>Technology</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>D</strong> Reporting of test charges for a department</td>
<td>Low</td>
<td>Custom report developed in house</td>
<td>High</td>
</tr>
</tbody>
</table>

#### Optional Documents
- User Requirements
- Functional Specs
- Design Documentation
- Test Plan
- Protocols (IQ, OQ, PQ)
- Trace Matrices
- Unit Test Report
- Code Review Report

#### Testing Requirements
- Sample of requirements
- Sample of paths

#### Testing Options
- Boundary testing
- Realistic test data
- Users may delegate both OQ & PQ execution

#### Optional Verifications
- Part 11 Compliance Assessment
- SOPs for feature use
- Design Review
- Code Review
- Unit Testing
### Can we leverage the vendor’s work?

<table>
<thead>
<tr>
<th>Complexity</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criticality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor Assessment</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>Required</td>
<td>Required</td>
<td>Optional</td>
<td>Required</td>
<td>Required</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Unit Testing</td>
<td>Required</td>
<td>Required</td>
<td>Optional</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Code Review</td>
<td>Required</td>
<td>Optional</td>
<td>Optional</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Part 11 Compliance Assessment</td>
<td>Required</td>
<td>Required</td>
<td>Optional</td>
<td>Required</td>
<td>Optional</td>
<td>Required</td>
<td>Required</td>
<td>Optional</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification of System Use and Support SOPs **</td>
<td>Required</td>
<td>Required</td>
<td>Optional</td>
<td>Required</td>
<td>Required</td>
<td>Optional</td>
<td>Required</td>
<td>Required</td>
<td>Optional</td>
<td></td>
</tr>
</tbody>
</table>

**Vendor Rating Impact to Validation Approach**

- **Full Approval**
  - Follow risk-based validation matrix
  - Internally review, approve vendor provided documents

- **Restricted Approval**
  - Use vendor documents with caution
  - Rating indicates increased risk, so additional validation required.
  - Approach validation as if 1 complexity level higher
    - If configured, approach as “custom”
    - If out-of-the-box, approach as “configured”

- **Not Approved**
  - Avoid reliance on vendor documents
  - Rating indicates increased risk, so additional validation required.
  - Approach validation as if “Custom”
Have You Ever Heard…

- Computer System Validation is a waste of time
- It's just a bunch of paperwork
- It doesn't find the bugs
- We just repeated everything the vendor already did

Risk Management Framework

Risk Management Process

<table>
<thead>
<tr>
<th>Risk Assessment</th>
<th>SOP System Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Mitigation</td>
<td>SOP Risk Based Validation</td>
</tr>
<tr>
<td></td>
<td>SOP Audit Trails</td>
</tr>
<tr>
<td></td>
<td>SOP System Security</td>
</tr>
<tr>
<td></td>
<td>SOP Software Vendor Assessment</td>
</tr>
<tr>
<td></td>
<td>SOP User Training</td>
</tr>
<tr>
<td></td>
<td>SOP Incident Management</td>
</tr>
<tr>
<td></td>
<td>SOP System Backup</td>
</tr>
<tr>
<td></td>
<td>SOP Business Continuity</td>
</tr>
<tr>
<td>Etc.</td>
<td></td>
</tr>
</tbody>
</table>
Risk Mitigation in ...

Vendor Assessment SOP example

<table>
<thead>
<tr>
<th>System Criticality Level</th>
<th>Vendor Assessment Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>On-site audit is the preferred method for highly critical software applications.</td>
</tr>
<tr>
<td>Medium</td>
<td>Questionnaire or phone interview assessment are the preferred methods for medium criticality software applications. An assessment purchased from a third-party software vendor assessment firm is also acceptable for this criticality level.</td>
</tr>
<tr>
<td>Low</td>
<td>Vendors of low criticality software applications do not require assessment.</td>
</tr>
</tbody>
</table>

Risk Mitigation in ...

Audit Trail SOP example

<table>
<thead>
<tr>
<th>Requirement Criticality Level</th>
<th>Audit Trail Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Audit trail is required for records associated with highly critical system functions</td>
</tr>
<tr>
<td>Medium</td>
<td>Audit trail is required for records associated with system functions of medium criticality</td>
</tr>
<tr>
<td>Low</td>
<td>Audit trail is not required for records associated with system functions of low criticality</td>
</tr>
</tbody>
</table>
Risk Mitigation in ...

System Security SOP *example*

<table>
<thead>
<tr>
<th>System Criticality Level</th>
<th>Password Change Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Every 90 days</td>
</tr>
<tr>
<td>Medium</td>
<td>Every 120 days</td>
</tr>
<tr>
<td>Low</td>
<td>Not required</td>
</tr>
</tbody>
</table>

User Training SOP *example*

<table>
<thead>
<tr>
<th>Requirement Criticality Level</th>
<th>Training Format</th>
</tr>
</thead>
</table>
| High                          | • Instructor Led Class  
|                               | • Hands-on Exercises  
|                               | • Competency Exam  
|                               | • Self-study Materials  
|                               | • Hands-on Exercises  
|                               | • Competency Exam  |
| Medium                        | • Instructor Led Class  
|                               | • Hands-on Exercises  
|                               | • Self-study Materials  |
| Low                           | • Self-study Materials  
|                               | • Hands-on Exercises  
|                               | • Self-study Materials  |
Risk Mitigation in ...

System Back-up SOP example

<table>
<thead>
<tr>
<th>System Criticality Level</th>
<th>Back-up Location</th>
<th>Back-up Media Audit Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Off-site Secure vault</td>
<td>Annual</td>
</tr>
<tr>
<td>Medium</td>
<td>Off-site Locked cabinet</td>
<td>Every 18 months</td>
</tr>
<tr>
<td>Low</td>
<td>Separate building</td>
<td>Not required</td>
</tr>
</tbody>
</table>

Risk Mitigation in ...

Business Continuity SOP example

<table>
<thead>
<tr>
<th>Requirement Criticality Level</th>
<th>Business Continuity Procedure Required</th>
<th>2nd Person Verification of Data Entry Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Medium</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Low</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
## SOP Incident Management Example

### Requirement Criticality Level

<table>
<thead>
<tr>
<th>Criticality Level</th>
<th>Users cannot perform job</th>
<th>Major Inconvenience</th>
<th>Minor Inconvenience</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
</tbody>
</table>

### FDA Leadership By Example

Part 4
Part 4: FDA Leadership by Example

Section Overview
- Warning Letter Data
- Warning Letter Examples

FDA Warning Letter Data

- Data Source
  - FDA Warning Letters related to Software and Computers
  - 3 Year Date Range: Q1-2015 through Q4-2017

- Summaries
  - By system type
  - By observation topic
    - By validation observation topics
FDA Warning Letter Example

Regulatory Reference

Finding

2. Your firm failed to exercise appropriate controls over computer or related systems to assure that only authorized personnel institute changes in master production and control records, or other records (21 C.F.R. §211.68(b)).

Your firm failed to have adequate procedures for the use of computerized systems in the quality control (QC) laboratory. Our inspection team found that current computer users in the laboratory were able to delete data from analyses. Notably, we also found that the audit trail function for the gas chromatograph (GC) and the X-Ray Diffraction (XRD) systems was disabled at the time of the inspection. Therefore, your firm lacks records for the acquisition, or modification, of laboratory data.

Moreover, greater than (b)(4) QC laboratory personnel shared (b)(6) login IDs for (b)(4) high performance liquid chromatographs (HPLC) units. In addition, your laboratory staff shared one login ID for the XRD unit. Analysts also shared the username and password for the Windows operating system for the (b)(4) GC workstations and no computer lock mechanism had been configured to prevent unauthorized access to the operating systems. Additionally, there was no procedure for the backup and protection of data on the GC standalone workstations.

Specific Observations

Summary

Software & Computer Warning Letters

3 Year Summary by System Type

- Device/product Software: 22%
- Laboratory Systems: 58%
- Manufacturing Control Software: 4%
- Complaints Systems: 4%
- Non-conformance Systems: 6%
- CAPA Systems: 1% each
- Inventory Control Systems: 1%
- Calibration Management: 1%
- Building Management: 1%
- CoA: 1%
- Others (< 1% each)

"Other" system types include systems for Labeling, Annual Product Review, Service Records, Livestock Tracking, Audit Management, Product Design Software, Equipment Tracking, Qualification Tracking, and Supplier Approval Tracking
Software & Computer Warning Letters

3 Year Summary by Observation Topic

*Other* observation topics include Suitability for Use, Data Accuracy, Vendor Management, Quality Oversight, Risk Analysis, Change Control, Electronic Signatures, Back-Ups, Internal Audits

Software & Computer Warning Letters

3 Year Summary by Validation Observation Details

*Other* observation validation topics include Inadequate Requirements, Incomplete Design Documentation, Went Live with Known Critical Defects, Inadequate Test Evidence, and Failure to Approve Release Notes
**Warning Letter Examples**

<table>
<thead>
<tr>
<th>Regulatory Reference</th>
<th>21 CFR 820 (Medical Devices)</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Type</td>
<td>Medical Device Software</td>
</tr>
<tr>
<td>FDA Branch or District</td>
<td>CDRH</td>
</tr>
</tbody>
</table>

**Failure to adequately establish and maintain procedures to control the design to ensure that requirements are met.**

- **Development of Key Functionality**, requires the firm to assess risk and re-assess risk as needed. Although XXXXXX was released on November 25, 2010, Software Risk Management Summary Doc. was not completed until July 14, 2011 and did not include an analysis of the risk specific to the intended use of XXXXXX.

**Failure to demonstrate that the device was developed in accordance with the design control requirements of the Quality System regulation.**

- Failure to have complete risk analyses in that 5 versions of risk analysis were not controlled documents.
- Risk analyses were not reviewed and approved.
- Risk analyses were not updated when a software issue was discovered that resulted in a software change.
Warning Letter Examples

<table>
<thead>
<tr>
<th>Regulatory Reference</th>
<th>21 CFR 820 (Medical Devices)</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Type</td>
<td>Medical Device Software</td>
</tr>
<tr>
<td>FDA Branch or District</td>
<td>Florida District</td>
</tr>
</tbody>
</table>

Failure to adequately establish and maintain procedures for validation.

- Firm’s Risk Analysis Report for software version 00, does not adequately assess the risk presented by the software controlling the X-Ray Unit XXX as a moderate risk to users and patients.
- For example, the report indicates a “No” to the questions:
  - “Could a malfunction of, or a latent design flaw in the Software Device lead to an erroneous diagnosis or a delay in delivery of appropriate medical care that would likely lead to Moderate Injury?”
  - “Does the Software Device control the delivery of potentially harmful energy that could result in death or serious injury?”

Conclusion
Next Steps

1. Review your regulations and guidelines
2. Identify your criticality levels and definitions
3. Define your complexity measures
4. Determine how you will apply complexity & criticality to validation and software quality practices
5. Write your policies and procedures
6. Train your staff

Need Help?

- ValidationCenter.com Library of SOPs and Template
- Online and Classroom CSV Training
- Software QA and Validation Program Implementation
- Validation Services
- Audit Readiness Assessments
Thank You!

• Thanks for your interest in Risk Based Approach to Software Quality & Validation.

• Any questions about what we have discussed today?
  • Please, feel free to contact me:

  Deb Bartel
  +1 (847) 295-7160
dbartel@PraxisLifeSciences.com

  ValidationCenter.com
  PraxisLifeSciences.com