Applying Risk Management to Computer System Validation

Presented by:

April 20, 2010



Focus Compliance & Validation Services





Your Presenters



Tom Busmann



Mark Walker





Agenda

- Overview of Computer Systems Validation
- Definitions and Terminology
- FDA Regulations and Guidance Documents
- Benefits of Risk Management to Computer
 Systems Validation
- Approach to Risk Management
- Roles and Responsibilities
- Tools available for RA
- Levels of Risk and Risk Matrix
- What is a Hazard
- What are Mitigations
- Traceability Matrix



POLL

2010 Focus Compliance & Validation Services and SyberWorks, Inc.



"Software is often an integral part of MEDICAL DEVICE technology. Establishing the SAFETY and effectiveness of a MEDICAL DEVICE containing software requires knowledge of what the software is intended to do and demonstration that the implementation of the software fulfils those intentions without causing any unacceptable RISKS."



"It is important to understand that software is not itself a HAZARD, but software may contribute to HAZARDOUS SITUATIONS. Software should always be considered in a SYSTEM perspective and software RISK MANAGEMENT cannot be performed in isolation from the SYSTEM."



"Complex software designs can permit complex sequences of events which may contribute to HAZARDOUS SITUATIONS. Much of the TASK of software RISK MANAGEMENT consists of identifying those sequences of events that can lead to a HAZARDOUS SITUATION and identifying points in the sequences of events at which the sequence can be interrupted, preventing HARM or reducing its Probability."



"Since it is very difficult to estimate the probability of software ANOMALIES that could contribute to HAZARDOUS SITUATIONS, and since software does not fail randomly in use due to wear and tear, the focus of software aspects of RISK ANALYSIS should be on identification of potential software functionality and ANOMALIES that could result in HAZARDOUS SITUATIONS - not on estimating probability. RISKS arising from software ANOMALIES need most often to be evaluated on the SEVERITY of the HARM alone."



What Types of Computer Systems Are Regulated By The FDA?

Regulatory Governeg













Design Validation Risk Analysis Device Software



Quality System Software Design Tool Software Testing Software CAPA Software Validation

@ 2010 Focus Compliance & Validation Services and SyberWorks, Inc.

Computer System Projects Take Many Forms

- MS Excel[™] Spreadsheet or Minitab[™] Project
- Quality System including CAPA Tracking System, Document Management, or Training
- Software that is a Medical Device
- Software Embedded in a Medical Device
- Controls Software for the Production of Active Pharmaceutical Ingredient, Biologic or Medical Device
- Laboratory Information Management System (LIMs)
- Automated Testing Systems



POLL



What Are some of the Applicable Regulations and Guidance?

- The FDA guidance document entitled, "General Principles of Software Validation; Final Guidance for Industry and Staff," which was issued on January 11, 2002
- The PIC/S guidance document entitled, "Good Practices for Computerised Systems in Regulated GxP Environments," which was issued on September 25, 2007
- 21 CFR Part 820 Quality System Regulations
- 21 CFR Part 11 Electronic Records / Electronic Signatures, where applicable

Overview of the Approach to Computer Systems Validation

- Project Planning
- Validation Procedures, Deviations, Change Control Document Management, Training
- Validation Master Plan
- Design Requirements and Specifications
- Risk Assessment
- Vendor Selection / Audits
- Validation Activities
 - IQ/OQ/PQ
 - Test Plan
- Validation Report
- Validation after a Change
- Retirement of Computer System



Risk Management Standards and Guidance

- ICH Q9 for pharmaceuticals was adopted by FDA (CDER and CBER) as a guidance document
- ISO 14971 is an FDA-recognized consensus standard (CDRH)
- ANSI/AAMI/ISO 14971:2007
- ANSI/AAMI/IEC TIR80002-1:2009
- Guidance for the Content of Premarket Submissions
 for Software Contained in Medical Devices
- Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices

ISO 14971:2007 RISK MANAGEMENT PROCESS

The MANUFACTURER shall establish, document and maintain throughout the LIFE-CYCLE an ongoing PROCESS for identifying HAZARDS associated with a MEDICAL DEVICE, estimating and evaluating the associated RISKS, controlling these RISKS, and monitoring the effectiveness of the controls. This PROCESS shall include the following elements:

RISK ANALYSIS;

RISK EVALUATION;

RISK CONTROL;

Production and POST-PRODUCTION information.



Risk Management is a Process



@ 2010 Focus Compliance & Validation Services and SyberWorks, Inc.



POLL

2010 Focus Compliance & Validation Services and SyberWorks, Inc.



Definitions

- **Hazard** A possible source of danger or a condition which could result in human injury.
- Hazard Analysis Identification of hazards and their initiating causes.
- Hazard Mitigation Reduction in the severity of the hazard, the likelihood of the occurrence, or both.



- **Risk Analysis** Investigation of available information to identify hazards and to estimate risks. [ISO DIS 14971]
- **Risk Control** the process through which decisions are reached and implemented for reducing risks to, or maintaining risks within, specified limits. [ISO DIS 14971]

Serious Injury – as adopted from the Medical Device Reporting (MDR) regulation in the Code of Federal Regulations 21 CFR 803.3 (aa), means an injury or illness that:

- 1. is life threatening,
- 2. results in permanent impairment of a body function or permanent damage to a body structure, or
- necessitates medical or surgical intervention to preclude permanent impairment of a body function or permanent damage to a body structure.



 Minor Level of Concern – The Level of Concern is minor if failures or latent design flaws would not be expected to result in any injury to the patient, operator, and/or bystander.



Moderate Level of Concern – The Level of Concern is moderate if the operation of the software associated with device function directly affects the patient, operator, and/or bystander so that failures or latent design flaws could result in non-serious injury to the patient, operator, and/or bystander, or if it indirectly affects the patient, operator, and/or bystander (e.g., through the action of the care provider) where incorrect or delayed information could result in nonserious injury of the patient, operator, and/or bystander.



Major Level of Concern – The Level of Concern is major if operation of the software associated with device function directly affects the patient, operator, and/or bystander so that failures or latent flaws could result in death or serious injury to the patient, operator, and/or bystander, or if it indirectly affects the patient, operator, and/or bystander (e.g., through the action of care provider) such that incorrect or delayed information could result in death or serious injury to the patient, operator, and/or bystander.



• **Permanent** – for the purpose of this subpart, permanent means irreversible impairment or damage to a body structure or function excluding trivial impairment or damage.



Benefit of Risk Management

- Prevent, reduce, avoid or mitigate conditions leading to a hazardous event or situation
- Severity lowered
- Probability reduced
- Concentrate limited resources on the highest risk items



Risk Analysis - Purpose

• The purpose of this is to:

Determine Hazards, their Mitigations, and their
 Traceability to Requirements and to Test Protocols
 for a Computer System Development Project



Forming a Risk Management Team

- Each team requires someone to fill a minimum of 3 functions:
 - Leader
 - Scribe
 - Expert
- A single individual can perform more than one function
- The scribe function can be rotated



POLL

2010 Focus Compliance & Validation Services and SyberWorks, Inc.



Forming a Risk Management Team

• The team leader:

- Is usually the person who has the most experience using the chosen tool
- Assembles materials (data, templates)
- Negotiates schedule
- Reserves meeting rooms
- Organizes site visits
- Drives decision making



Team Leader Responsibilities

- Ensure that the risk assessment tool(s) are properly applied
- Maintain objectivity, impartiality, honesty, and ethics
- Summarize issues to facilitate compromise and consensus, and drive decision-making.



Forming a Risk Management Team

- The core team should include individuals with expertise in the process/product under analysis.
- To keep the team size manageable, involve additional SMEs with very deep knowledge in particular areas of concern as needed.



Risk Management Teams

- The exact makeup of any team depends on:
 - Process/product being analyzed
 - Stage of process/product lifecycle
 - Objectives of the analysis
 - Which risk assessment tool(s) are used
 - What resources are available



Candidates for Risk Management Teams

- Chemist/biochemist
- Safety Engineer/Manager
- Construction representative
- Electrical engineer
- Hazard evaluation expert
- Human factors specialist
- Shift supervisor
- Mechanical Engineer
- Process Engineer
- Process Designer
- Operations supervisor
- Operator/Technician

- Project Engineer
- Process control programmer
- R&D engineer/scientist
- Shift supervisor
- QC/QA analyst
- Toxicologist
- Vendor representative
- Mechanic/pipefitter/electrician
- Maintenance supervisor
- Instrumentation engineer/tech
- Outside Consultant



Forming a Risk Management Team

• The scribe:

- Typically someone with basic experience or training in risk management, but not as much as the team leader
- Should have good writing and organization skills

! Using extremely junior or non-technical personnel as scribes has a pitfall. Scribes with more experience can better sort out what needs to be documented from what does not.



POLL

2010 Focus Compliance & Validation Services and SyberWorks, Inc.



Steps for Performing a Computer Systems Risk Assessment

- Risk Management Plan
- Risk Analysis
 - Define Hazards, Levels of Concern, and Mitigations
- Risk Assessment Report



Elements of the Risk Management Plan

- Purpose
- Scope
- Timing
 - Study dates
 - Limitations on resource availability
- Activities and Deliverables
 - Tool(s) to be used and rationale
 - Milestones
 - Type and frequency of review
 - A report will always be a deliverable



Elements of the Risk Management Plan

Risk Criteria

- Define the criteria to be used for estimating and evaluating risk
- Use standardized scales unless otherwise warranted
- Provide a rationale for whatever technique you use
- Risk Communication
 - Describe how concerns that arise will be communicated to stakeholders (internal or external)
- Review and Approval
 - The Risk Management Plan must be reviewed and approved before you start the risk assessment.

Performing a Risk Assessment



Risk Assessment

- When performing a risk assessment, you must:
 - Identify and document foreseeable hazards associated with the product or process
 - Estimate the risk associated with each hazard
 - Evaluate the risks against given criteria.



Hazard Identification

- Systematically use available information to identify hazards related to your problem or scope.
 - Asks "what might go wrong?
 - Includes identifying potential consequences
 - Provides the foundation for all subsequent risk management activities



Risk Analysis

- Risk analysis is the estimation of the risk associated with the identified hazards.
 - Can be qualitative or quantitative
 - Links the severity and likelihood of harm together
 - The ability to detect a Hazard may also be factored into risk estimation



Risk Evaluation

- Each identified risk must be compared against your pre-established acceptability criteria to determine whether the risk:
 - Is acceptable
 - Should be controlled or mitigated



Risk Estimation

• There is no "standard" for estimating risk (severity, likelihood, detection).

Therefore....

 Any system used for qualitative or quantitative categorization of probability or severity of harm must be recorded in the risk management file. (ISO 14971)



Risk Estimation

- Specificity must be balanced with standardization
 - The scales and scores you use have to make sense in the context of YOUR particular risk assessment
 - If emphasis on standardization is too great, scales will be used inappropriately and assessment results will be misleading



Risk Estimation: Example

Likelihood	Guideline	Score
Very High (expected)	Expected to occur at least several times every year	10
High (very likely)	Expected to occur once per year	8
Medium (likely)	Expected to occur once per decade	6
Low (unlikely but possible)	Expected to occur once per 10-100 years. Unusual. Known to have happened in the company, locally, or multiple times industry-wide	4
Very Low (unlikely)	Expected to occur less than once per century. Known to have happened.	2



Risk Evaluation

- Risks must be evaluated against pre-established criteria such as:
 - A matrix (table) showing which combinations of severity and likelihood are acceptable/unacceptable
 - Can be further subdivided to indicate risks that are negligible, acceptable with mitigation, or required to be reduced
 - Threshold values for numeric Risk Priority Numbers or Relative Risk indices



Prol

Occ

Re

Probability of Occurrence

Risk Matrix

Severity of Harm

	Negligible	Moderate	Serious	Critical
bable	Low	Medium	High	High
asional	Low	Medium	Medium	High
note	Low	Low	Medium	High



Risk Estimation and Evaluation

- Standardization is good for maintaining comparability across different assessments for the same product/process over its life cycle
- Over-standardization can give a false impression of comparing "apples to apples" across different products/processes



Risk Control



Risk Control

- Part of the Risk Management Team's job is to make recommendations for controlling risks that were identified in the risk assessment. Control can take the form of:
 - Risk reduction
 - Risk acceptance



Risk Control

- When making recommendations for risk control, consider:
 - Is the risk above an acceptable level?
 - What can be done to reduce or eliminate the risk?
 - What is the appropriate balance among risks, benefits, and resources?
 - Does the control introduce new risks?



Risk Acceptance

- Risk acceptance can be a formal decision
 - Decided and documented case-by-case
- Risk acceptance can be passive
 - Automatic acceptance based on pre-defined criteria



Risk Reduction

- Risk can be reduced by:
 - Mitigating the severity of harm
 - Reducing the likelihood of harm
 - Improving the detectability of hazards



Risk Control Recommendations

• The risk management team should

- Make recommendations for risk control, including risk acceptance and risk reduction
- Estimate the residual risk that will remain if the recommended controls are implemented



Risk Analysis Tools

- PrHA
- FMEA/FMECA
- HAZOP
- FTA
- HACCP

- LOPA
- ETA
- Checklist
- What If
- HHE



Details of Conducting Software System Risk Analysis

- Hazards Analysis
- Assignment of Risk
- Mitigations
- Traceability Matrix



What are Hazards

(1 of 3)

- **System Requirement ID** Requirement ID
- Hazard ID A Sequence Number that uniquely identifies the Hazard (e.g., HA001, HA002)
- User Exposure Risk is the requirement used by a user?
 - If "Not Used," enter the value of one (1).
 - If "Infrequently," enter the value of one (1).
 - If "Occasionally," enter the value of four (4).
 - If "Frequently," enter the value of ten (10).
 - If "Insufficient Information," enter the value of ten (10).
- **Regulatory Risk** is data resulting from, or managed by, the function derived from the requirement is governed by GxP?
 - If "No," enter the value of zero (0).
 - If "Yes," enter the value of twelve (12).
 - If "Insufficient Information," enter the value of twelve (12).

System Requirement ID	Hazard ID	User Exposure Risk	Regulatory Risk	Override Capability	Technical Risk	Security Risk	Consequence of Failure	Sum Value	Risk Assessment



Potential Software Hazards

- Unexpected results
- External interface faults
- Software design
- User input
- Security
- Interface with other software or hardware systems

Hazards (2 of 3)

- **Override Capability** Could the function derived from the requirement be carried out by an alternative means?
 - If "No," enter the value of zero (0).
 - If "Yes," enter the value of ten (10).
 - If "Insufficient Information," enter the value of ten (10).
- **Technical Risk** Would the failure of the function derived from the requirement directly impact overall reliability of the system?
 - If "No Possibility," enter the value of one (1).
 - If "Low Possibility," enter the value of one (1).
 - If "Moderate Possibility," enter the value of four (4).
 - If "High Possibility," enter the value of ten (10).
 - If "Insufficient Information," enter the value of ten (10).
- **Security Risk** Would the function derived from the requirement be controlled and secured through a user-ID and password and/or supervisory intervention?
 - If "No Possibility," enter the value of one (1).
 - If "Low Possibility," enter the value of one (1).
 - If "Moderate Possibility," enter the value of four (4).
 - If "High Possibility," enter the value of ten (10).
 - If "Insufficient Information," enter the value of ten (10).



Hazards (3 of 3)

- **Consequence of Failure** Would the failure of the function derived from the requirement endanger the user, patient, or facility?
 - If "No Possibility," enter the value of zero (0).
 - If "Low Possibility," enter the value of one (1).
 - If "Moderate Possibility," enter the value of eight (8).
 - If "High Possibility," enter the value of twenty (20).
 - If "Insufficient Information," enter the value of twenty (20).

• Sum Value –

 Add the values in columns, "User Exposure Risk," "Regulatory Risk," "Override Capability," "Technical Risk," "Security Risk," and "Consequence of Failure" columns, and enter the result in the "Sum Value" column

• Risk Assessment -

- If the value is greater than or equal to 36, enter the value of "Major."
- If the value is greater than or equal to 15 but less than 36, enter the value of "Moderate."
- If the value is greater than or equal to zero but less than 15, enter the value of "Minor."

System Requirement ID	Hazard ID	User Exposure Risk	Regulatory Risk	Override Capability	Technical Risk	Security Risk	Сосе	Sum Value	Risk Assessment



Prol

Occ

Re

Probability of Occurrence

Risk Matrix

Severity of Harm

	Negligible	Moderate	Serious	Critical
bable	Low	Medium	High	High
asional	Low	Medium	Medium	
note	Low	Low	Medium	High



Mitigations

- Hazard ID Hazard ID designated in Hazard Table
- Enter a Sequence Number that uniquely identifies the Mitigation (e.g., MIT001, MIT002) in the "Mitigation ID" column. could be many to one relationship
- Description Text that explains the "Major," "Moderate," or "Minor" assessment of the Hazard in the "Description" column:
 - If the Hazard is "Major," enter a brief narrative explaining how the Hazard will be Mitigated.
 - If the Hazard is "Moderate," enter a brief narrative explaining how the Hazard will be Mitigated.
 - If the Hazard is "Minor," enter "Hazard has been determined to be minor and will not be Mitigated."



Traceability Matrix Examples

Risk Analysis Report - Table A (Risk Analysis)

User Require- ment Specifi- cation No.	Requirement Title				Probability	Risk	Mitigation ID	Mitigation Description
URS-001		HAZ-002	Business risk	Negligible	Remote	LOW	MIT-001	LOW RISK - MITIGATION NOT REQUIRED
URS-002		HAZ-003		Serious	Remote	MEDIUM	MIT-002	

Protocol	Environment	Requirement(s)
P-001	Environment	URS-004
P-002	Environment	URS-058
P-003		URS-023



Risk Assessment Report

• Summarize Risk Analysis

- Table of Hazards with assigned Levels of Concern
- Table of Mitigations
- Traceability Matrix



Risk Management after Change

- Follow a Change Control Procedure
 - Procedure that defines when Risk Assessment process is necessary
 - Evaluate all changes to the Computer System
 - Identify new Hazards or changes to previously identified Hazards
 - Changes could impact previous mitigations
 - Control
 - Detectability
 - Full Risk Assessment might be necessary

Questions ??



Contact Information



Focus Compliance & Validation Services



9050 Executive Park Drive Suite A-202 Knoxville, TN 37923 USA E-mail: <u>focus@focuscvs.com</u> Office: (865) 694-7517 Fax: (865) 531-8854 411 Waverley Oaks Road Building 3, Suite 319 Waltham, MA 02452 E-mail: <u>mklofurno@syberworks.com</u> Office: 781-891-1999 Fax: 781-891-1999

www.focuscvs.com

www.syberworks.com

@ 2010 Focus Compliance & Validation Services and SyberWorks, Inc.