Develop a Roadmap for the Implementation of a Global CSV Program

Eileen Cortes
April 26, 2017
Agenda

- CSV Regulation Principles
- CSV Lifecycle Approach
- CSV and Quality Management
- Governance Program and CSV Standardization
- IT vs. CSV
- Supplier Qualification Program
- Open Discussion
CSV Regulation Principles – New Trends and Updates
Computer System Validation

• What is Computer System Validation (CSV)?
  • Provide high degree of assurance that a specific process, in this case Computer System, will consistently produce a product (control information or data) which meets predetermined specifications and quality attributes.

• Why is needed?
  • Reduces Risk and Legal Liability
  • Adherence to GMP’s
CSV Regulation Principles

• **Computer System Validation and Medical Device**
  • Two Major Cases or Scenarios

A
- Medical Device as Instrument/Equipment
- Validation of Hardware and Software per Specification

B
- Medical Device manufactured by a Computer System
- Validation of the Computer System
CSV Regulation Principles

- **CSV Medical Device Regulations - Guidance**
  - GAMP5 – Manufacturing and Process Control
  - FDA – General Principles of Software Validation
  - FDA – Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices

  - Device Hazard Analysis
    - Inclusion of Software related hazards
    - Identification of the Hazard
    - Severity of the Hazard
    - Cause of the Hazard
    - Method Control (i.e. hardware, software, alarms)
    - Corrective Measures (i.e. eliminate, reduce, warn)
    - Verification (did I make the *product right*?)
    - Validation (did I make the *right product*?)

- **Design Control**  
  21 CFR 820.30

- **Production and Process Controls**  
  21 CFR 820.70

- **Electronic Records & Signatures**  
  21 CFR Part 11
CSV Regulation Principles

• CSV Medical Device Regulations - Guidance
  • Software “Level of Concern”
    • Identification of the Severity of Injury that a device failure or latent design flaw could permit or inflict (direct or indirect)
      • Major: could directly result in death or serious injury
      • Moderate: could directly result in minor injury
      • Minor: unlikely to cause any injury

NOTE: Documentation recommended for and FDA Submission depends on the level of concern
CSV Regulation Principles

- CSV Medical Device Regulations - Guidance
  - Software Related Documentation
    - Describe the device design
    - Describe how the design was implemented
    - Demonstrate how the design was tested
    - Demonstrate identification of hazards and management of risk associated
    - Provide Traceability to link the design, implementation, testing and risk management

Verification and Validation
V&V Model
CSV Regulation Principles

Verification and Validation V&V Model

- **Major**
  - V&V Activities at the unit, integration, and system level
  - System level test protocols
  - Pass / Fail Criteria
  - Test Results

- **Moderate**
  - V&V Activities at the unit, integration, and system level
    - System level test protocols
    - Pass / Fail Criteria
    - Test Results

- **Minor**
  - V&V Activities
    - Software functional test plan
    - Pass / Fail Criteria
    - Test Results
CSV Regulation Principles

- **CSV Medical Device Regulations - Standard**
  - ISO 13485 – Quality Management System
  - ISO 62304 – Life cycle requirements for Medical Device Software
    - SW Development
    - SW Maintenance
    - SW Risk Management
    - SW Configuration Management
    - SW Problem Resolution
CSV Regulation Principles

• Medical Devices Challenges
  • ISO 13485 2016 Version
    • More emphasis on Risk Management
    • Increased expectation for documentation
  • Increased use of Software
    • From on and off and display readings to complex software functions
      • Interfaces
      • Communication Protocols
      • Traceability

• Compliance
  • Increased expectation for documentation
  • Integration of Quality Systems and Quality Risk Management Tools
CSV Lifecycle
CSV Life Cycle

• Highlight...
  • Neither ISO 13485, nor ISO 62304 nor GAMP®5 prescribe how code should be structured, what language it is written in, what hardware should be used;
  • That’s the purpose of CSV
    • to prove that the software and hardware operate as per specification
  • Recommendation
    • to design, manufacture and code in a structured and organized way using best practice, otherwise you are going to have a maintenance problem
CSV Life Cycle

• Which should we follow...
  • ISO 62304, GAMP5 or ISO 13485???

ANSWER: ALL OF THEM

The real question is which is more useful and which one is going to get you through an audit...

Based on experience, we conclude that:

ISO 62304 ➔ What are the must do’s

FDA Guidance

GAMP5 ➔ How to do it
GAMP5

• **GAMP Objectives**
  • Aims to achieve computerized systems that are fit for intended use and meet current regulatory requirements, by building upon existing industry good practice in an efficient and effective manner

PATIENT SAFETY
PRODUCT QUALITY
DATA INTEGRITY
GAMP 5 Drivers

- Focus on Patient Safety, Product Quality, and Data Integrity
- Life Cycle Approach within QMS
- Science Based Quality Management of Risks
- Scaleable Approach to GxP Compliance
- Effective Governance to Achieve and Maintain GxP Compliance
- Quality by Design (QbD)
- Continuous Improvement within QMS
- Critical Quality Attributes (CQA)
- Improving GxP Compliance Efficiency
- Use of Existing Documentation and Knowledge
- Configurable Systems and Development Models
- Effective Supplier Relationships

Source: Figure 1.1, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.
GAMP5 Key Concepts

Product and Process Understanding

Life Cycle Approach within a QMS
Scaleable Life Cycle Activities
Science Based Quality Risk Management

Leverage Supplier Involvement

Source: Figure 2.1, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org.
Computerized System Lifecycle
Computerized System Lifecycle

- Composed of all activities from **Initial Concept** to **Retirement**

- 4 Major Phases
  1. Concept
     - Business decision of Automate or integrate to their Processes a computerized system based on business needs and benefits
     - KEY POINTS
       - Initial Requirements
       - Initial Understanding of scope, costs and benefits
       - A DECISION is made to proceed with the PROJECT
Computerized System Lifecycle

2. **Project**
   - Stages includes Planning, Assessments, Selection of Supplier or Vendor, Specifications and Configuration Requirements
   - **KEY POINTS**
     - Risk Assessment
     - Specifications
     - Verification
     - Acceptance and Release
3. **Operation**
   - Longest phase, managed by Standard Operating Procedures
     - KEY POINTS
       - Control
       - Fitness for Intended Use
       - Compliance
Computerized System Lifecycle

4. **Retirement**
   - Business decision of system decommission
     - **KEY POINTS**
       - Plan/Documentation of Decisions
       - Data Retention
       - Data Migration
       - Destruction
Life Cycle Phases - Summary

* - This could be a complex supply chain
  - Supplier may provide knowledge, experience, documentation, and services throughout lifecycle

Source: Figure 3.2, GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, © Copyright ISPE 2008. All rights reserved. www.ISPE.org
CSV Lifecycle

New System Introduction → System Classification: Direct Impact → Yes
→ Software/Hardware Categorization → Supplier Assessment
→ No Validation Required

Validation Planning

URS → Risk Assessment → FRS → HDS → SDS → DQ → Software Coding

Risk Assessment → IQ (Hardware/Software Installation) → No Validation Impact/Minor Impact

FAT → SAT → Engineering Change Management

Validation Plan → IQ Report → OQ Report → PQ Report → RTM → VSR

PQ → Protocol Deviation Management

Change Control → Code Review / Functional Test

Major Impact to Validated State of the System

Decommissioning Plan → System Retirement

Supplier Assessment

System Acceptance and Commissioning

Decommissioning

Major Impact to Validated State of the System

Change Control

System Retirement
CSV and Quality Management
CSV & QMS

- Integration of Quality Systems or Quality Management Tools into the Computer System Validation Scope
  - Performance Monitoring
  - Security and System Administration
  - Training
  - Record Management
  - Computer Change Management
    - Change Control
    - Deviations
    - CAPAs
  - Computer System Validation
  - Quality Risk Management – ICH Q9
Quality Risk Management
Step 1: Initial Risk Assessment

**Inputs**
- URS
- GxP Regulations
- Gap Assessments

**Outputs**
- GxP Criticality
- Risks Considered
- Overall Risk
Quality Risk Management
Step 2: Functions with GxP Impact

Inputs

- Specifications
- System Architecture
- Categorization of Components

Outputs

- List of Functions to be Evaluated

Diagram:

1. Step 1: Perform Initial Risk Assessment and Determine System Impact
2. Step 2: Identify Functions with Impact on Patient Safety, Product Quality, and Data Integrity
3. Step 3: Perform Functional Risk Assessments and Identify Controls
4. Step 4: Implement and Verify Appropriate Controls
5. Step 5: Review Risks and Monitor Controls
Quality Risk Management
Step 3: Functional Risk Assessment

**Inputs**
- Functions from Step 2
- SME Experience
- Scenarios
- Possible Hazards

**Outputs**
- Breakdown of Risks
- Mitigation for High Risks
Quality Risk Management
Step 3: Controls

Inputs

- High Risk from Functional Analysis

Outputs

- Mitigation Strategies
  - Process change
  - Design change
  - Procedures
Quality Risk Management
Step 4: Implement & Verify Controls

- Verification Activity should demonstrate that the controls are effective in performing the required risk reduction.
Quality Risk Management

Step 5: Review Risks/Monitor Controls

- Establish Periodic Review of Control Effectiveness
- Apply Risk Process in Change Management Activities
QMS – Risk Procedure

Requirement Risk Assessment Procedure shall identify the following:

• **Assessment Participants:**
  - Roles and Responsibilities

• **Risk Assessment Levels:**
  - Business process, user requirement, or functional requirement levels

• **RRA Process:**
  - Primary risk scenario: “failure of the system to perform the desired activity or function”
  - Determine requirement **severity**
  - Determine **probability of occurrence**
  - Calculate **risk class**
  - Determine (CS failure) **detectability**
  - Calculate **risk priority** for each requirement or business process
  - Summarize RRA process and include justifications for low/medium risk priority items, and mitigations (e.g., procedural/technical controls)

• **SOP Output(s):**
  - RRA summary

• **Provides Input(s) to:**
  - CSV Validation Procedure
# CSV Lifecycle & QMS Summary

## Procedures (SOPs)
- Handover
- Performance Monitoring
- Incident Mgmt.
- CAPA Mgmt.
- Change & Configuration Mgmt.
- Periodic Review
- Document Mgmt.
- Data Mgmt.
  - Security
  - Backup & Restore
  - Business Continuity
  - System Administration
  - Archiving & Retrieval

## Risk-Based approach
- Identify risks
- Analyze
- Evaluate
- Control
- Review

## Governance
- Policies
- Standards
- Documentation
- Roles & Responsibilities
IT vs. CSV
IT vs. CSV

• Procedures that define or provide tools to assess applicability are Highly recommended
  • Proper documentation of **applicability** of computerized systems
    • GxP
    • Infrastructure
  • Computer System is categorized as CAT 1, then:
    • Applicable Test or Verification via an *IT Infrastructure Compliance and Control Life Cycle procedure*
      • Network Protocols
      • Virtualization
      • Servers
IT Qualified Infrastructure

- Risk Analysis
  - Specifications of equipment/hardware/software
  - Users experience with the same equipment already installed
  - Users experience with similar network equipment
  - IT staff experience with the same or similar network equipment
  - Network qualification and system qualification reports
  - Internal and external supplier or quality audit results.
  - Inputs can come from operators, the validation/qualification group, IT administrators, or from QA personnel, (e.g., as a result of findings from internal or external audits, etc).
IT Qualified Infrastructure

• Challenges
  • Typical problems and harms with network infrastructure with possible impact on compliance risks include, but are not limited to, the following:
    • Inadequate or absent verification of the accuracy of a file transfer can cause inaccurate results
    • Inadequate or absent verification of security access functions can result in unauthorized access to the network
    • An insufficient or absent plan for system back-up can result in data loss in case of system failure.
    • An insufficient or absent plan for rollbacks if updates don't work as expected may cause severe infrastructure downtime through reinstallation and reconfiguration.
    • Inadequate corporate quality assurance policies and procedures, or inadequate reviews may result if procedures are implemented and followed.
IT Qualified Infrastructure

- In Summary, minimize or avoid:
  - Regulatory compliance issue
  - Data integrity compromise or data leakage
  - System unavailable
IT Qualified Infrastructure

• Risk Evaluation
  • This phase is used to categorize and prioritize the risk in business and compliance / health risks.

• Risk Mitigation
  • This phase covers what is documented to mitigate risks. There are different methods and approaches to mitigate risks. They can range from process and system design changes to personnel training. Typically, the most effective methods are also the most expensive and take the longest amount of time.

• Design Process Change
  • This could entail installing new types of equipment, such as servers having higher capacity and new functionality. Typically, this requires expenditures for purchasing, installation, qualification, and familiarization. It also may require development of new SOPs and additional training.
IT Qualified Infrastructure

- Extended Testing
  - This does not remove the problematic network component, but shows weaknesses of the component and conditions under which component failures can be identified. This only helps if procedures and workaround solutions can be developed and implemented to avoid known critical conditions. A typical example would be to test a system under increasingly high loads, and to always operate the system below the point when it started to fail in the test phase. It is suggested that a development or test environment be available for such exercises.
IT Qualified Infrastructure

- Training
  - Purpose:
    - to avoid risk situations that are caused by human errors.
  - Alternatives:
    - training existing staff
    - hire additional personnel with experience
IT Qualified Infrastructure

• Control
  • Effectiveness of the plan should be monitored and adjusted, if necessary.
  • The risk monitoring program should also help to identify previously unrecognized issues. These could have been introduced by changing processes or introducing new technologies.
  • The risk monitoring program should check to determine if risk factors have changed to either higher or lower values. If factors exceed the previous specified risk limits, mitigation strategies should be reevaluated. If higher risk values decrease below the threshold of acceptable risk levels, further mitigation may not be necessary.
IT Qualified Infrastructure

- Documentation
  - Lists with description of risk categories, ranking criteria, and results of ranking.
  - Justification for mitigation strategies.
  - Risk mitigation plan. Includes actions with time tables, deliverables, and responsibilities.
IT Qualified Infrastructure

- Infrastructure risk management demands are best supported by good IT practices and standards such as Information Technology Infrastructure Library (ITIL®), International Organization for Standardization (ISO) and Good Automated Manufacturing Practices (GAMP®). Key aspects include:
  - Specification and verification of IT infrastructure components or services
  - Management of IT infrastructure risks
  - Change and configuration management
  - Incident and problem management
  - Security management in relation to access controls, availability of services and data integrity
  - Availability and performance monitoring
  - Controls and quality assurance
  - Backup, restore and disaster recovery
  - Archiving

*The sum of these procedures in place gives a level of confidence that the IT managed infrastructure is under control, secure and data integrity is well-looked-after.*
Computer System Validation
CSV Process

• Computer System Validation process (how and minimum requirements) must be documented at:
  • Procedures (SOP)
  • CSV Master Plan
    • Or Both...

• CSV Procedure
  • Validation Planning
    • System Classification (direct, indirect impact)
    • Software and Hardware Categories
    • Vendor Audit
    • Deliverables
    • Validation Strategy
CSV Process

- CSV Procedure
  - System Development
    - URS
    - QRA
    - 21 CFR Part 11 / EU Annex 11 Assessment
    - FRS
    - SDS
    - DQ
  - System Acceptance and Commissioning
    - FAT
    - SAT
  - Qualification
    - IQ
    - OQ
    - PQ
CSV Process

- CSV Procedure
  - Requirement Traceability Matrix
  - Validation Summary Report
- Others
  - Leverage
  - Data Migration
  - Validation Maintenance (Periodic Reviews)
  - Validation Impact Assessments
  - Decommissioning / Retirement
GAMP5 Model

Life Cycle Model for Process Control Systems

Quality Plan Validation Master Plan
→ User Requirement Specification
→ Control System Functional Specification
→ Software Module Design Specification
→ Design Review

Performance Qualification (PQ)
→ Installation & Operational Qualification (IQ & OQ)
→ Software Site Acceptance Test
→ Software Factory Acceptance Test
→ Software Module & Integration Tests
→ Source Code Review

Mechanical & Electrical Build
→ System Software Development & Code

Design
→ Build
→ Verify
Supplier Qualification Program
Supplier Qualification – Good Practices

<table>
<thead>
<tr>
<th>Practice</th>
<th>Description</th>
</tr>
</thead>
</table>
| Establish QMS                 | The supplier QMS should:  
1. Provide a documented set of procedures and standards  
2. Ensure activities are performed by suitably competent and trained staff  
3. Provide evidence of compliance with the documented procedures and standards  
4. Enable and promote continuous improvement |
| Establish Requirements         | The supplier should ensure that clear requirements are defined or provided by the regulated company                                                                                                           |
| Quality Planning               | The supplier should define how their QMS will be implemented for a particular product, application, or service.                                                                                               |
| Assessments of Sub-Suppliers   | Suppliers should formally assess their sub-suppliers as part of the process of selection and quality planning                                                                                                 |
| Produce Specifications         | The supplier should specify the system to meet the defined requirements.                                                                                                                                     |
| Perform Design Review          | The design of the system should be formally reviewed against requirements, standards, and identified risks to ensure that the system will meet its intended purpose and that adequate controls are established to manage the risks. |
| Software Production/ Configuration | Software should be developed in accordance with defined standards, including the use of code review processes. Configuration should follow any pre-defined rules or recommendations and should be documented |
| Perform Testing                | The supplier should test the system in accordance with approved test plans and test specifications.                                                                                                           |
| Commercial Release of the System | System release to customers should be performed in accordance with a formal process. (note: this is not the release into the GxP environment, which is a regulated activity.)                                                   |
| Provide User Documentation and Training | The supplier should provide adequate system management documentation, operational documentation, and training in accordance with agreed contracts.                                                             |
| Support and Maintain the System in Operation | The supplier should support and maintain the system in accordance with agreed contracts. The process for managing and documenting system changes should be fully described.                                      |
| System Replacement and Retirement | The supplier should manage the replacement or withdrawal of products in accordance with a documented process and plan. The supplier also may support the regulated company with the retirement of computerized systems in accordance with regulated company procedures. |
Leverage of Supplier – Main Areas

• **Activities**
  - Requirements Identification
  - Risk Assessments
  - Functional Specifications
  - Configuration Specifications
  - Testing
  - Support and Maintenance

• **Principles**
  - Assessment
    - Suitability
    - Accuracy
    - Completeness
  - Flexibility
    - Format
    - Structure
Application of Risk and use of SME Knowledge are keys to Success

- Validation of computer systems should be done keeping in mind the intended use of the system.
- Implementing a Systems Integration Lifecycle when it is better-suited to COTS software than the traditional Software Development Lifecycle makes sense.
- GxP for Computer System Validation: It should employ a risk-based approach efficiently, in which it gives greater attention to elements that can be bracketed as causing high risk.
- This should be done in accordance with the resources and strengths the organization has.
- The organization implementing GxP in computer system validation should be diligent in having its documentation done, preferably from audited vendors.
Q&A
Open Discussion
Thank You!
Backup Slides
ISO 14971 Risk Management

ISO 14971 – Risk management

Risk = \text{combination of the likelihood (L) of occurrence of harm and the severity (S) of that harm [ISO 14971]}

(ALARP = As Low As Reasonable Practical)
ISO 62304 Risk Management

- same principle for HW and electronic Design-FMEA
- identify software items contributing to hazardous situation
- requires knowledge of architecture

![Diagram of ISO 62304 Risk Management with a grid for risk analysis, severity, likelihood, and risk control measures.]

- Risk Analysis
  - Severity
    - 3: 1
    - 16: 7
    - 18: 5
    - 20: 8
  - Likelihood
    - 1: 58
    - 2: 34
    - 7: 3
    - 8: 1
- Risk Control Measures
### ISO 62304: Quality Management

<table>
<thead>
<tr>
<th>Process</th>
<th>SOP/Process Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW development process</td>
<td>SOP Software Life Cycle</td>
</tr>
<tr>
<td>SW maintenance process</td>
<td>SOP Change Management Process / CAPA process</td>
</tr>
<tr>
<td>SW risk management process</td>
<td>SOP Risk Management Process</td>
</tr>
<tr>
<td>SW configuration management process</td>
<td>SOP SCCS</td>
</tr>
<tr>
<td>SW problem resolution process</td>
<td>During development ➔ SOP Issues Management</td>
</tr>
<tr>
<td></td>
<td>After release ➔ SOP Change Management / CAPA</td>
</tr>
</tbody>
</table>
CSV Life Cycle Documentation

- **Software Validation Protocol (Validation Plan)**
  - This document outlines the project deliverables and responsibilities.
- **System /Software Requirements Specification**
  - This document details system requirements. However, this is more than just a list of functional requirements; it also should capture a good description of the various components that make up the system so that everyone has a clear understanding of what this system involves. The Requirements Specification also needs to include information around physical hardware requirements, physical software requirements, client user requirements, training requirements and detail about any customizations or integration with other systems.
- **Network Diagram**
  - This required document provides a visual layout of how the system is configured on the network. It serves to demonstrate that you understand how your system is configured for your implementation. Note: this diagram may be included as an attachment to the (Software Requirements Specification)
- **Risk Analysis**
  - This document evaluates application safety and identifies potential hazards, the causes and the effect that each hazard has on the application safety and use. Because this is a business system the risk assessment should focus on the business processes being managed by the system vs. a more traditional FMEA risk assessment for software programs which are part of a device and pose direct patient risk. Not all risks will be solely mitigated by the software, some risks are mitigated procedurally.
- **21 CFR Part 11 Compliance Analysis**
  - This document evaluates system applicability/requirements for the use of electronic signature as required by the FDA in 21 CFR, Part 11.
- **Design Specification**
  - Typically a design specification is not required for a purchased configurable business quality system. In the event that major integration or customization is to be performed as part of the project this document may be added as deemed appropriate by the project team and quality reviewer.
CSV Life Cycle Documentation

• **Verification Protocol (Test Plan)**
  - This document defines the type of testing to be completed along with the procedures and schedules for those tests.

• **Test Specifications (Test Cases)**
  - This document contains the system level test cases, based on the functional requirements set forth in the Requirements Specification. If these are separate or maintained as an attachment to the Verification Protocol it makes it easier to add modules or new phases to the validation package while limiting revision time. Plus they are easier to format and work with testing wise.

• **Requirements Traceability Matrix**
  - This matrix details all system requirements including Requirements ID, and links them to the Test Case IDs. This is a required document that can be helpful going forward when a change occurs, as it makes it easier to assess and identify where there is impact.

• **Final Validation Report**
  - The validation report should provide a summary of all documentation associated with the validation of the software and test case results. This report should include both a summary of all the validation activities and define how the system will be managed in production. Information such as what work instructions are used to train users to use the system, what system support is available, how the system will be backed up, and how change control will be managed are extremely important elements captured in this document. In essence it puts a bow on the validation package.
CSV Life Cycle Documentation

- **Purchase of Validation Documentation?**

The FDA requires that verification and validation activities cover how a system is configured in the customer’s environment so there is no “one size fits all” validation. Many times software vendors will try to sell prepackaged validation documentation. Because a vendor selling a prepackaged validation does not know your requirements they try and list every functionality that the system has and let you whittle down the list of requirements based on your use of the system. Since they do not know exactly which requirements you are going to keep and which requirements you are going to throw out they can’t group the test cases to contain multiple requirements. Again, it looks like a great deal because they can show you all of these test cases that you are going to get with their packaged validation. What they aren’t telling you is that sorting out which ones you want and don’t want takes a lot of time (possibly weeks) that your team might not have.

- Everyone’s business is a little different so software manufacturers, have developed highly configurable systems that can be set up to manage your business processes electronically. Even if you don’t need to validate your system from a regulatory standpoint, methodical documentation and testing of your configuration is a good business function. It’s risky not to be sure (with documentation) that important activities are being handled electronically the way you think they are.
## Software Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Software</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Infrastructure Software</td>
<td>Layered software (i.e. upon which applications are built)</td>
<td>Operating systems, database engines, middleware, programming languages, statistical packages, spreadsheets, network monitoring tools, scheduling tools, version control tools</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software used to manage the operating environment</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Firmware</td>
<td>This is no longer to be used as a separate category. Firmware shall be categorized, depending on the nature of the embedded software, into any of the remaining categories.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Non-Configured</td>
<td>Run-time parameters may be entered and stored, but the software cannot be configured to suit the business process</td>
<td>Firmware-based applications, COTS software, instruments</td>
</tr>
<tr>
<td>4</td>
<td>Configured</td>
<td>Software, often very complex, that can be configured by the user to meet the specific needs of the user’s business process. Software code is not altered.</td>
<td>Data acquisition systems, SCADA, DCS, Building Management Systems, Spreadsheets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: The system type examples provided may contain custom elements that shall be categorized separately.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Custom</td>
<td>Software custom designed and coded to suit the business process.</td>
<td>Internally and externally developed process control applications, custom ladder logic, custom firmware, spreadsheet macros</td>
</tr>
</tbody>
</table>


# CSV Requirements - Example

<table>
<thead>
<tr>
<th>Document Type</th>
<th>Category 1</th>
<th>Category 3</th>
<th>Category 4</th>
<th>Category 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation Plan</td>
<td>X</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Requirements Specification</td>
<td>X</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Design Specification</td>
<td>X</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Design Qualification</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>R</td>
</tr>
<tr>
<td>Requirements Traceability Matrix</td>
<td>X</td>
<td>X</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Installation Qualification</td>
<td>X</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Operational Qualification</td>
<td>X</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Performance Qualification</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>R</td>
</tr>
<tr>
<td>Validation Summary Report</td>
<td>X</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
</tbody>
</table>

**LEGEND:**
- **R** = Required
- **X** = Not Required (optional)

**Notes:** Documents may be combined as determined by Validation.
Category 1 is typically handled by IT Infrastructure Procedures
## Validation Impact Assessment - Example

<table>
<thead>
<tr>
<th>Change</th>
<th>Validation Impact</th>
<th>Testing Required</th>
<th>Validation Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipe Parameters Value</td>
<td>None</td>
<td>No</td>
<td>Code Review</td>
</tr>
<tr>
<td>Configurable Parameter Value</td>
<td>None</td>
<td>No</td>
<td>Code Review</td>
</tr>
<tr>
<td>Modification of existing HMI screens</td>
<td>None</td>
<td>No</td>
<td>Code Review</td>
</tr>
<tr>
<td>Deleting or changing the location of screen objects</td>
<td>None</td>
<td>No</td>
<td>Code Review</td>
</tr>
<tr>
<td>Display existing PLC readings in a HMI screen</td>
<td>None</td>
<td>No</td>
<td>Code Review</td>
</tr>
<tr>
<td>Introduction of new Recipe Parameters for hard coded values currently used in the logic</td>
<td>Minor</td>
<td>Yes</td>
<td>Functional Test</td>
</tr>
<tr>
<td>Introduction of new Configurable Parameters for hard coded values currently used in the logic</td>
<td>Minor</td>
<td>Yes</td>
<td>Functional Test</td>
</tr>
<tr>
<td>Add instruction to Enable or disable alarms</td>
<td>Minor</td>
<td>Yes</td>
<td>Functional Test</td>
</tr>
<tr>
<td>Add instruction to Start/Stop/Reset timers</td>
<td>Minor</td>
<td>Yes</td>
<td>Functional Test</td>
</tr>
<tr>
<td>Add instruction to Start/Stop/Reset flow totalizers</td>
<td>Minor</td>
<td>Yes</td>
<td>Functional Test</td>
</tr>
<tr>
<td>Eliminate the need for Manual interventions</td>
<td>Minor</td>
<td>Yes</td>
<td>Functional Test</td>
</tr>
<tr>
<td>Merge existing recipes into a one recipe</td>
<td>Minor</td>
<td>Yes</td>
<td>Functional Test</td>
</tr>
<tr>
<td>Add existing and qualified phases into a recipe</td>
<td>Minor</td>
<td>Yes</td>
<td>Functional Test</td>
</tr>
<tr>
<td>Change the sequence of phases of an existing recipe</td>
<td>Minor</td>
<td>Yes</td>
<td>Functional Test</td>
</tr>
<tr>
<td>Major re-definition or modification of a phase that changes the sequence of logic due to a change in the process</td>
<td>Major</td>
<td>Yes</td>
<td>OQ Addendum</td>
</tr>
<tr>
<td>Automation of manual process</td>
<td>Major</td>
<td>Yes</td>
<td>OQ Addendum</td>
</tr>
<tr>
<td>New control and/or equipment module</td>
<td>Major</td>
<td>Yes</td>
<td>OQ Addendum</td>
</tr>
<tr>
<td>Introduction of new phases into an existing system</td>
<td>Major</td>
<td>Yes</td>
<td>OQ Addendum</td>
</tr>
<tr>
<td>Introduction of new recipes into an existing system</td>
<td>Major</td>
<td>Yes</td>
<td>OQ Addendum</td>
</tr>
</tbody>
</table>
## CSV Impact Assessment

<table>
<thead>
<tr>
<th>IF the change ...</th>
<th>THEN Validation Impact is ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>• is not the result of a User Requirement change or addition AND</td>
<td>None</td>
</tr>
<tr>
<td>• does not alter the operating sequence AND</td>
<td>(No Impact)</td>
</tr>
<tr>
<td>• is not critical or within a validated range or is configurable AND</td>
<td></td>
</tr>
<tr>
<td>• does not change functionality AND</td>
<td></td>
</tr>
<tr>
<td>• does not impact other software or modules</td>
<td></td>
</tr>
<tr>
<td>• is not the result of a User Requirement change or addition AND</td>
<td>Minor</td>
</tr>
<tr>
<td>• does not alter the operating sequence AND</td>
<td>(Impact)</td>
</tr>
<tr>
<td>• is not critical or is within a validated range or is configurable AND</td>
<td></td>
</tr>
<tr>
<td>• changes functionality AND</td>
<td></td>
</tr>
<tr>
<td>• does not impact other software or modules</td>
<td></td>
</tr>
<tr>
<td>• is the result of a User Requirement change or addition AND/OR</td>
<td>Major</td>
</tr>
<tr>
<td>• alters the operating sequence AND/OR</td>
<td>(Impact)</td>
</tr>
<tr>
<td>• is critical and not within a validated range or is configurable AND/OR</td>
<td></td>
</tr>
<tr>
<td>• changes functionality AND/OR</td>
<td></td>
</tr>
<tr>
<td>• impacts other software or modules</td>
<td></td>
</tr>
</tbody>
</table>
**Decommissioning Plan Requirements - Example**

<table>
<thead>
<tr>
<th>IF the system ...</th>
<th>THEN the Decommissioning Plan must include requirements to ...</th>
</tr>
</thead>
</table>
| Stores electronic GMP records | • Identify records that need to be maintained.  
• Identify records that may be destroyed.  
• Define retention periods for the records to be maintained.  
• Establish the process for the retrieval of these records. This process must be available throughout the retention period. |
| Has data that will be migrated or archived | Verify and document this activity. |
| Has associated SOPs | • Obsolete any system-specific SOP.  
• Remove system references in any remaining SOP. |
| Has an active maintenance | Inactivate the system in applicable maintenance system. |
| Is access controlled | Remove access to the system. |
Change Management Principles

“It is not the strongest of the species that survive, nor the most intelligent, but the one most responsive to change”
Change Management Cycle

- Knowledge
- Risk Assessment
- Collect Data & Evaluate Variation
- Implement Change
- Monitor / Continuous Verification
# Application of Change Management through Lifecycle

<table>
<thead>
<tr>
<th>Pharmaceutical Development</th>
<th>Technology Transfer</th>
<th>Commercial Manufacturing</th>
<th>Product Discontinuation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change is an inherent part of the development process and should be documented; the formality of the change management process should be consistent with the stage of pharmaceutical development.</td>
<td>The change management system should provide management and documentation of adjustments made to the process during technology transfer activities.</td>
<td>A formal change management system should be in place for commercial manufacturing. Oversight by the quality unit should provide assurance of appropriate science- and risk-based assessments.</td>
<td>Any changes after product discontinuation should go through an appropriate change management system.</td>
</tr>
</tbody>
</table>
Regulations and Change Management

- ICH Q8 – Pharmaceutical Development
- ICH Q9 – Quality Risk Management
- ICH Q10 – Quality Systems

“Knowledge understanding - the use of quality risk management principles, supported by the implementation of ICH Q8, ICH Q9 and ICH Q10 principles provides the opportunity to be Science based and execute risk based post-approval changes. Drive innovation and Continuous improvement ICH Q10”
# Quality Manual

- Quality Management System

<table>
<thead>
<tr>
<th>QMS Subsystem</th>
<th>Key Components of Subsystem</th>
</tr>
</thead>
</table>
| **Quality**                 | • Incident Management
                               | • Change Management
                               | • Training
                               | • Audits
                               | • Document & Records Management
                               | • Regulatory Inspections
                               | • Escalation/FARs/Recalls
                               | • Product Complaints
                               | • CAPAs
                               | • Data Integrity
                               | • Risk Management
                               | • Management Review |
| **Laboratory Controls**     | • Lab Operations
                               | • Analytical Method Validation
                               | • Laboratory Investigations
                               | • Stability Program |
# Quality Manual

## QMS Subsystem

<table>
<thead>
<tr>
<th>QMS Subsystem</th>
<th>Key Components of Subsystem</th>
</tr>
</thead>
</table>
| **Production Controls**                   | • In Process Controls  
|                                          | • Process Validation  
|                                          | • Aseptic Process  
|                                          | • Cleaning Validation  
|                                          | • Master Batch Records  
|                                          | • Environmental Monitoring                                      |
| **Packaging and Labeling Controls**       | • Packaging Controls  
|                                          | • Labeling Controls                                              |
| **Material Controls**                     | • CMO/Supplier Management                                        |
|                                          | • Specification Setting                                         |
|                                          | • Specification Management                                     |
|                                          | • Distribution and Transport                                    |
| **Infrastructure**                        | • Computerized Systems                                          |
|                                          | • Computer System Validation                                    |
|                                          | • Organization Roles & Responsibilities                         |
| **Facilities, Equipment, and Utilities**  | • Equipment/Facility/Utilities Validation                        |
|                                          | • Calibration/Maintenance                                       |