A Case Study in Implementing an Effective CSV Program

Chris Reid, Integrity Solutions Limited

PO Box 71,
Middlesbrough, UK TS7 0BW
creid@integrity-solutions.co.uk

Agenda

I. The Quality System
   - Management support and of the functional areas
   - Effective training and communication
   - Self audits and customer focus

II. The CSV Methodology
   - Validation model and lifecycle
   - Effective SOPs
   - Key elements s and deliverables

III. Spreadsheets and Queries
   - Single-use and multi-use
   - Verification versus validation

IV. Roles and Responsibilities
   - Defining the responsibilities
   - Team concept
   - Who is involved in the validation?

V. How to Overcome Common Problems
   - Audit bias
   - Poor documentation practices
   - Do what you say you will do
   - Design does not meet requirements
   - Objective evidence
As with anything in life, resistance to change makes implementation of a CSV program much more difficult.

Culture

National Cultures
Organisational Cultures
Project Cultures
Functional Cultures

Delivering sustainable risk based solutions
Engage your “Users” in order to gain “buy in”

Communicate Risks and Benefits

- Patient Safety
- “Real” lifecycle costs reduced
- Reduced Operation and Support Cost
- System Stability
- Compliance Reputation
- Fitness for Purpose
- License To operate
Key Principles – Risk Based Approach

- The old perception at many firms*
  Impact Analysis Must Be Shifted to Reflect True Risk

- Analysis will bring us here*
  Impact Analysis Must Be Shifted to Reflect True Risk

*Dictated by long-standing conservative approaches to compliance (zero-risk was the ultimate goal).

*The new risk management mindset permits efficient allocation of resources to achieve an appropriate level of control that aims for low risk — not no risk.

Delivering sustainable risk-based solutions

Key Concepts – Risk Based Approach

Current Situation
- Standard Validation Approach
- Focus ERES/CSV Controls
- Current State
  - High
  - Medium
  - Low

Future Situation
- Risk Based Approach
- Focus ERES/CSV Controls
- Future State
  - High
  - Medium
  - Low

Delivering sustainable risk-based solutions
Key Concepts – Validation Built on GITP / GEP Foundation

Good IT / Engineering Practice

- Requirements
- Specification and Design
- Verification
- Acceptance Testing and Release

Risk Management

- Design Review

Change Management

Delivering sustainable risk based solutions

Key Concepts – Transition of Accountability

Business

IT

Vendor

Supplier

Delivering sustainable risk based solutions

Who owns docs & records

Who owns decision

Who leads

Who reviews
Key Concepts – Greater Complexity, Greater Effort

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Infrastructure Software</td>
<td>Operating system, database manager, statistical programming tool, network monitoring s/w, anti-virus</td>
</tr>
<tr>
<td>2</td>
<td>No longer used</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Non-Configured Products</td>
<td>Used ‘out-of-the-box’ with default configuration or cannot be configured. Firmware-based apps, instruments</td>
</tr>
<tr>
<td>4</td>
<td>Configured Products</td>
<td>ERP, LIMS, CDS, EDMS, ADR</td>
</tr>
<tr>
<td>5</td>
<td>Custom Applications</td>
<td>Internally &amp; externally developed custom applications, sometimes to modify an otherwise configured product</td>
</tr>
</tbody>
</table>

Key Concepts - Scalability

Software Complexity: L, M, H

GAMP Category: 1, 2, 3, 4, 5
Key Concepts - Scalability

System Impact

System Complexity, Increasing Rigour

Key Concepts – Leverage Vendor Support

Requirements  | Risk Assessment  | Planning

Design  | Testing  | Data Migration

Delivering sustainable risk based solutions
Key Concepts – Set scope

Key Principles – Transition of Accountability

Delivering sustainable risk based solutions
### Key Principles – Greater Complexity, Greater Effort

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Infrastructure Software</td>
<td>Operating system, database manager, statistical programming tool, network monitoring s/w, anti-virus</td>
</tr>
<tr>
<td>2</td>
<td>No longer used</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Non-Configured Products</td>
<td>Used 'out-of-the-box' with default configuration or cannot be configured. Firmware-based apps, instruments</td>
</tr>
<tr>
<td>4</td>
<td>Configured Products</td>
<td>ERP, LIMS, CDS, EDMS, ADR</td>
</tr>
<tr>
<td>5</td>
<td>Custom Applications</td>
<td>Internally &amp; externally developed custom applications, sometimes to modify an otherwise configured product</td>
</tr>
</tbody>
</table>

### Key Principles - Scalability

![Diagram showing software complexity and GAMP category]

- **GAMP Category**: 1, 2, 3, 4, 5
- **Software Complexity**: Low (L), Medium (M), High (H)
- **System Complexity, Increasing Rigour**: 1, 3, 4, 5

*Delivering sustainable risk based solutions*
Key Principles - Scalability

System Impact

System Complexity, Increasing Rigour

Key Principles – Risk Based Approach

Current Situation

Standard Validation Approach

Future Situation

Risk Based Approach

Delivering sustainable risk based solutions
Key Principles – Risk Based Approach

• The old perception at many firms*
  Impact Analysis Must Be Shifted to Reflect True Risk

  *Dictated by long-standing conservative approaches to compliance (zero risk was the ultimate goal)

• Analysis will bring us here*
  Impact Analysis Must Be Shifted to Reflect True Risk

  *The new risk management mindset permits efficient allocation of resources to achieve an appropriate level of control that aims for low risk — not no risk

Delivering sustainable risk based solutions

Key Principles – Leverage Vendor / Project Team Support

Requirements Risk Assessment Planning

Design Testing Data Migration

Delivering sustainable risk based solutions
What is a Computerized System?

SOFTWARE

HARDWARE

COMPUTER SYSTEM

OPERATING PROCEDURES

EQUIPMENT (OPTIONAL)

CONTROLLED FUNCTION

COMPUTERIZED SYSTEM

OPERATING ENVIRONMENT
What is a Computerized System?

Key Concepts – Cradle to Grave

* = Event
" = Period
Lifecycles

Primary Responsibility
Regulated Company
User Requirements Specification
Requirements Testing
Design Specification
Functional Specification
Functional Testing
Code Modules Specification Verification
Supplier Supplier QMS
Integration Testing Module (Unit) Specification
Module (Unit) Testing
Delivering sustainable risk based solutions

Integrated Lifecycles

Validation is integrated
Defines good project management activities also
Scaled according to risk

Delivering sustainable risk based solutions
**Planning Risk Assessment Activities and Objectives**

- **Initial Risk Assessment**: Initial determination of project risks, regulatory risks (GxP, SOX, Data Privacy). Determines whether the application or infrastructure has any impact or not (but not scope of impact).
- **Vendor Assessment**: Need for, and rigor of, vendor assessment. Role of vendor based on outcome of assessment e.g. use of vendor documentation, use of vendor’s input into activities.
- **Validation Planning**: Determining activities, deliverables and responsibilities. Planning Risk Assessment and Management activities.
- **Business Process Risk Assessment**: Identify criticality of business processes, adequacy of process definition and controls.
- **User Requirements**: Identify Business, Safety/Health/Environment and Regulatory requirements.
- **Functional Risk Assessment**: Identify criticality of functional design, adequacy of design and controls requirements.
- **Electronic Records Risk Assessment**: Identify criticality of electronic records and associated electronic signatures maintained by the computerized system.
- **Requirements Traceability**: Determines deviations between requirements, design and testing.
- **Validation Reporting**: Assessment of deviations from Validation Plan and Lifecycle Activities.

**Risk Management Log**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient Validation Resources</td>
<td>System not adequately tested</td>
<td>Business and Compliance</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Recruit additional resources</td>
<td>CR 12/1 10/29</td>
</tr>
</tbody>
</table>

**Delivering sustainable risk based solutions**
Risk Determination

Risk Likelihood

High
Medium
Low

Low 1 2
Medium 2 3
High 3

Probability of Detection

Low
Medium
High

N
H
L

Severity of Impact

Level ONE
Level TWO
Level THREE

Low
Medium
High

Delivering sustainable risk based solutions

System Inventory

<table>
<thead>
<tr>
<th>Field</th>
<th>Purpose / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>Descriptive Name of System e.g. Document Management System</td>
</tr>
<tr>
<td>System Reference</td>
<td>Unique System identification</td>
</tr>
<tr>
<td>System Description</td>
<td>Brief Description of System Use (e.g. business processes supported)</td>
</tr>
<tr>
<td>Computerized System Version</td>
<td>Version of main application / system software component</td>
</tr>
<tr>
<td>Location</td>
<td>Location where application installed / deployed.</td>
</tr>
<tr>
<td>Business System Owner</td>
<td>Name of System Owner (may be multiple for business applications)</td>
</tr>
<tr>
<td>Technical System Owner</td>
<td>Name of the Technical System Owner (normally IT Manager)</td>
</tr>
<tr>
<td>Regulated Status</td>
<td>GxP, HIPAA, SOX, non regulated, etc</td>
</tr>
<tr>
<td>Primary GAMP Category*</td>
<td>GAMP software category 1 – 5</td>
</tr>
<tr>
<td>Validation Status*</td>
<td>Not Required, Not Validated, Ongoing, Validated (including date of Validation Report sign off)</td>
</tr>
<tr>
<td>Electronic Records &amp; Electronic Signatures</td>
<td>Indication of whether system holds regulated electronic regulated records</td>
</tr>
<tr>
<td>Date of last Periodic Review*</td>
<td>Date when last period review report approved</td>
</tr>
<tr>
<td>Periodic Review Frequency*</td>
<td>1, 3 or 5 years</td>
</tr>
<tr>
<td>Date of next Periodic Review*</td>
<td>Date of next periodic review (last review date + frequency)</td>
</tr>
</tbody>
</table>
Documentation Considerations

- Documentation requirements may be satisfied by alternative documentation providing the requirements of the CSV policy are met e.g.
  - Supplier documentation

- For less complex systems, documentation may be combined e.g.
  - Development and Acceptance test documents
  - Functional and detailed design

- Additional documentation may be generated for more complex systems.

Initial Risk Assessment – Project Risk Summary

<table>
<thead>
<tr>
<th>IMPACT RESULTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS THE PROJECT SIZE ACCEPTABLE AND MANAGABLE?</td>
</tr>
<tr>
<td>IS THE PROJECT DEFINITION CLEAR AND ACCEPTABLE?</td>
</tr>
<tr>
<td>IS PROJECT SPONSORSHIP AND COMMITMENT CLEAR AND ACCEPTABLE?</td>
</tr>
<tr>
<td>IS THE IMPACT ON USER ORGANIZATION CLEAR AND ACCEPTABLE?</td>
</tr>
<tr>
<td>IS THE PROPOSED TECHNOLOGY MANAGEABLE WITH CURRENT SKILLS SET?</td>
</tr>
<tr>
<td>IS THERE AN ADEQUATE PROJECT TEAM THAT IS AVAILABLE TO FULFILL DEFINED ROLES?</td>
</tr>
<tr>
<td>IS THE PROJECT MANAGER EXPERIENCED, SKILLED AND ABLE TO MEET PROJECT DEMANDS?</td>
</tr>
</tbody>
</table>
Initial Risk Assessment – Regulatory Impact Summary

<table>
<thead>
<tr>
<th>IMPACT RESULTS</th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS THE SYSTEM SUBJECT TO ANY GLOBAL HEALTHCARE REGULATIONS?</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>IS THE SYSTEM SOX / PCI / HIPAA REGULATED?</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>DOES THE SYSTEM HOLD, CREATE, MODIFY, DELETE OR DISTRIBUTE REGULATED ELECTRONIC RECORDS?</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>IF THE SYSTEM IS A LEGACY SYSTEM AND MANAGES HEALTHCARE REGULATED ELECTRONIC RECORDS, HAS AN ELECTRONIC RECORDS AND ELECTRONIC SIGNATURE ASSESSMENT BEEN CONDUCTED?</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>DOES THE SYSTEM EXECUTE ELECTRONIC SIGNATURES TO REGULATED ELECTRONIC RECORDS</td>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>

Validation Planning

- Vendor Risks
- Requirements Criticality
- Size and Complexity
- Standard vs Bespoke
- Innovative or Routine
- Single Site/ Multiple Sites
- Resource Skills And Availability
- Validation Approach
- Leverage Supplier Work
- In-source / Outsource
- Team Org. Roles & Responsibilities
- Documentation Requirements, Org. Ownership
- V. Plan Roles and Resp Approach Deliverables Etc Etc

Delivering sustainable risk based solutions
## Validation Planning

- **Validation Plans define:**
  - System Implementation and site quality assurance approach
  - Organization, Roles and Responsibilities
  - SOPs governing lifecycle activities
  - Documentation and other Deliverables
  - Risks and Risk Management Plans
  - Relationships with vendor activities and documentation
  - System / Project Acceptance criteria

### Influence of Risk on Validation Planning

<table>
<thead>
<tr>
<th>Risk Area</th>
<th>Determined from</th>
<th>Validation Strategy Decisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criticality of the Computerized</td>
<td>Business Process Risk Assessment</td>
<td>Degree of effort required in documentation and testing</td>
</tr>
<tr>
<td>System</td>
<td>Requirements categorization</td>
<td>Need to engage Business QA in the project</td>
</tr>
<tr>
<td></td>
<td>Electronic Records and Electronic Signatures Risk</td>
<td>Need and approach to vendor assessment</td>
</tr>
<tr>
<td></td>
<td>Assessment</td>
<td>Need for in project audits</td>
</tr>
<tr>
<td>Resource availability and skills</td>
<td>Initial Risk Assessment</td>
<td>Need to procure additional / specialist resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Need to phase project</td>
</tr>
<tr>
<td>System Complexity:</td>
<td>Validation and Project Planning</td>
<td>System Development / Implementation Lifecycle</td>
</tr>
<tr>
<td>• Level of configuration required</td>
<td></td>
<td>Expanded or condensed documentation set</td>
</tr>
<tr>
<td>• Level of customization required</td>
<td></td>
<td>Need for design reviews and functional risk assessments</td>
</tr>
<tr>
<td>• Size</td>
<td></td>
<td>Need for in project audits</td>
</tr>
<tr>
<td>• Number of users</td>
<td></td>
<td>Roll out planning</td>
</tr>
<tr>
<td>• Interfaces to other systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Novelty of solution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor Capability</td>
<td>Vendor Assessment</td>
<td>Effort that can be leveraged from vendor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Documentation that can be leveraged from vendor</td>
</tr>
<tr>
<td>Legacy system implications</td>
<td>Validation and Project Planning</td>
<td>Need for System Retirement Planning and Data Migration Planning</td>
</tr>
</tbody>
</table>

*Delivering sustainable risk based solutions*
### Validation Planning

<table>
<thead>
<tr>
<th>Infrastructure Software</th>
<th>Document Management Plan</th>
<th>Configuration Plan</th>
</tr>
</thead>
</table>

### Document Management Plan

**Attachment 1 - Validation Document Set**

Any document number not yet assigned (NYA) will be documented in the Final Validation Report. Documents identified in the table as "A" are applicable for all Waves and sites. Documents identified in the table as "B" are only applicable to a particular Wave or site.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;SYSTEM&gt;-System Validation Plan (SVP)</td>
<td>A</td>
<td>A</td>
<td>Validation Specialist(s)</td>
<td>Global IT, Global IT Governance and Compliance</td>
<td>System Owner(s), Quality System Owner, Global Software Validation, Validation Project Manager</td>
<td></td>
</tr>
<tr>
<td>&lt;SYSTEM&gt;-Document Management Plan (DMP)</td>
<td>A</td>
<td>A</td>
<td>Validation Specialist(s)</td>
<td>Global IT, Global IT Governance and Compliance</td>
<td>System Owner(s), Quality System Owner, Global Software Validation, Validation Project Manager</td>
<td></td>
</tr>
<tr>
<td>&lt;SYSTEM&gt;-System Description (DS)</td>
<td>A</td>
<td>A</td>
<td>Validation Specialist(s)</td>
<td>Global IT, Global IT Governance and Compliance</td>
<td>System Owner(s), Quality System Owner, Global Software Validation, Validation Project Manager</td>
<td></td>
</tr>
<tr>
<td>Vendor Audit Report(s)</td>
<td>A</td>
<td>A</td>
<td>Validation Specialist(s)</td>
<td>Global IT, Global IT Governance and Compliance</td>
<td>System Owner(s), Quality System Owner, Global Software Validation, Validation Project Manager</td>
<td></td>
</tr>
</tbody>
</table>
Vendor Assessment

<table>
<thead>
<tr>
<th>QUALITY ORGANIZATION</th>
<th>Vendor A</th>
<th>Vendor B</th>
<th>Vendor C</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUALITY SYSTEM EXISTS</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>QUALITY SYSTEM APPLIED</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>QUALITY SYSTEM MAINTAINED</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>TECHNICAL COMPETENCE</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>PHARMA EXPERIENCE</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>SUPPORT INFRASTRUCTURE</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>COMMERCIAL ROBUST</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

Method | Typical Criteria for Method
--- | ---
Postal Audit Questionnaire / Desktop Audit | Non patient safety related processes
Identifying areas to focus on during site audits
Filtering vendors during product and vendor selection processes
Follow-up of observations from previous audits
Surveillance audits
Site Audit | Patient Critical Systems
Complex and / or Custom Systems
Performance Review | Existing vendors / service providers where experience of actual working practices and experience is at hand
Interview | Where individuals are supplied from a company to work to internal procedures.
Vendor Assessment

- Planning Considerations:
  - Scope and criticality of system / service use
  - Whether a managed solution / service is to be provided or whether external resources shall work to internal’s procedures under internal management
  - The extent to which the system / service is used in industry and evidence that problems raised by customers are addressed
  - Whether there has been a significant change in scope of systems / services provided or whether there have been significant changes in regulatory requirements since previous assessments
  - Is there confidence in the Vendor based on previous experience?
  - System maturity
  - Complexity of system (e.g. will validation itself fully prove the system is fit for intended use)
  - Is the system based on new and relatively unproven technologies?

Delivering sustainable risk based solutions

Vendor Assessment

- Background and Audit Purpose
- Details of Audit
- Name of Organization being audited
- Date of Audit
- Audit Location
- Audit Team
- Vendor Team
- Summary of Observations & Risks
- Detailed Explanation of Findings (strengths and weaknesses)
- Recommendations for selection, rejection, corrective action and follow up
- Identification of responsibilities for actions identified.

- Deficiencies discovered and corrected during the audit
- Confidential information without express permission of organization
- Subjective opinion or ambiguous statements
- Antagonistic words or phrases

Delivering sustainable risk based solutions
Vendor Assessment

- Observations
  - Critical: A finding that would disqualify a facility, a study or portion thereof or significantly jeopardize patient safety or accuracy of reported regulatory data
  - Major: Non-compliance against internal policies, external regulations, internal protocols, Standard Operating Procedure, Statement of Work or other contractual agreement or obligation
  - Minor: A finding which may not affect operations or conclusion of a study or does not meet the current acceptable standards or practice.

Business Processes

- Business processes:
  - Identify main process steps
  - Highlight computerized system interactions with the process
  - Identify process interfaces
  - Identify critical data flows
  - Identify process inputs and outputs
  - Identify manual interventions
Delivering sustainable risk based solutions

Business Process Risk Assessment

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>QU003 – QA Release (including CoA Generation)</td>
<td>N/A</td>
<td>N/A</td>
<td>GXP Incorrect results entered</td>
<td>H</td>
<td></td>
<td></td>
<td>Test: Verifies that correct results have been entered (PRA SOP Ref 6.9.3)</td>
</tr>
<tr>
<td>Enter results into QMS</td>
<td>N/A</td>
<td>N/A</td>
<td>GXP Incorrect results entered</td>
<td>H</td>
<td></td>
<td></td>
<td>Test: Ensures that results cannot be entered against wrong item (i.e. invalid test spec for item) (PRA Test Ref 6.9.3)</td>
</tr>
<tr>
<td>Step 1: QMS updates lot status</td>
<td>N/A</td>
<td>N/A</td>
<td>GXP Incorrect lot status assigned based on comparison of results to specification</td>
<td>H</td>
<td></td>
<td></td>
<td>Test: Confirm that results out side of each defined test limit result in failed test status (PRA Test Ref 6.9.4)</td>
</tr>
<tr>
<td>Step 2: Create and Print CoA by authorised person</td>
<td>N/A</td>
<td>N/A</td>
<td>GXP CoA not printed</td>
<td>H</td>
<td></td>
<td></td>
<td>Test: CoA printed and contains correct information (PRA Test Ref 6.9.5)</td>
</tr>
<tr>
<td>Step 3: Warehouse transfer to write off materials</td>
<td>N/A</td>
<td>N/A</td>
<td>GXP CoA contains incorrect information</td>
<td>H</td>
<td></td>
<td></td>
<td>Test: Ensure that the correct status is assigned, as entered by the QP. (PRA Test Ref 6.9.6)</td>
</tr>
<tr>
<td>Step 4: QP changes the lot status to approved or reject depending on test outcome</td>
<td>N/A</td>
<td>N/A</td>
<td>GXP Approved status is assigned from a failed test status</td>
<td>H</td>
<td></td>
<td></td>
<td>Test: Confirm that approved status cannot be assigned if the test failed (PRA Test Ref 6.9.7)</td>
</tr>
<tr>
<td>QP signs CoA (as printed from the system)</td>
<td>N/A</td>
<td>N/A</td>
<td>GXP Unauthorised person approves material</td>
<td>H</td>
<td></td>
<td></td>
<td>Test: Ensure only QP can approve material (PRA Test Ref 6.9.8)</td>
</tr>
</tbody>
</table>

Delivering sustainable risk based solutions

Requirements

<table>
<thead>
<tr>
<th>Req. No.</th>
<th>Description</th>
<th>Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>x.0</td>
<td>Security Requirements</td>
<td></td>
</tr>
<tr>
<td>x.1</td>
<td>Access Control/Security Hierarchy</td>
<td></td>
</tr>
<tr>
<td>x.1.1</td>
<td>System security must allow for the following user types: a.) System Administrator</td>
<td>RC</td>
</tr>
<tr>
<td>x.1.2</td>
<td>System must provide System Administrator with authorities as defined in the Security Hierarchy Matrix. (Appendix x)</td>
<td>RC</td>
</tr>
<tr>
<td>x.1.3</td>
<td>System must provide Production Supervisor with authorities as defined in the Security Hierarchy Matrix. (Appendix x)</td>
<td>RC</td>
</tr>
<tr>
<td>x.1.4</td>
<td>System must provide Production Operator with authorities as defined in the Security Hierarchy Matrix. (Appendix x)</td>
<td>RC</td>
</tr>
<tr>
<td>x.1.5</td>
<td>System must provide Data Reviewer with authorities as defined in the Security Hierarchy Matrix. (Appendix x)</td>
<td>RC</td>
</tr>
<tr>
<td>x.2</td>
<td>Password Expiration</td>
<td></td>
</tr>
<tr>
<td>x.2.1</td>
<td>Passwords must expire every 90 days</td>
<td>RC</td>
</tr>
<tr>
<td>x.2.2</td>
<td>Upon expiration of the password, the user must be prompted to reassign a new password</td>
<td>RC</td>
</tr>
<tr>
<td>x.2.3</td>
<td>The user must be granted three grace log-ins after initial expiry notification</td>
<td>RC</td>
</tr>
<tr>
<td>x.2.4</td>
<td>The system must not allow the reassignment of previously used passwords</td>
<td>RC</td>
</tr>
</tbody>
</table>
### Roles

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Knowledge</td>
<td>In order to identify key requirements of the system that are related to the business or manufacturing process</td>
</tr>
<tr>
<td>Business Knowledge</td>
<td>To ensure that requirements are challenged against business need and are realised</td>
</tr>
<tr>
<td>Ownership</td>
<td>To ensure clarity and understanding of stated requirements</td>
</tr>
<tr>
<td>Analytical</td>
<td>To ensure requirements are challenged to ensure they are accurate and complete</td>
</tr>
<tr>
<td>Technical/Product</td>
<td>To ensure that requirements are practical in terms of available technology</td>
</tr>
<tr>
<td>Process/Product Impact</td>
<td>To ensure requirements which impact the process or product are clearly identified</td>
</tr>
<tr>
<td>Technical Authorship</td>
<td>To ensure that requirements are written in concise, correct, and unambiguous language</td>
</tr>
</tbody>
</table>

### Requirements Specification Content

- Requirements Specifications shall be established in order to amplify business Process Steps and to define user, functional and technical requirements. Typically, Requirements Specifications shall address:
  - Process requirements
  - Process limits
  - User interface
  - System interface requirements
  - Data management
  - Electronic Records and Electronic Signatures requirements
  - Security controls
  - Health, Safety, Environmental requirements
  - Equipment needs
  - Operating context / environment
  - Regulations, internal and external standards to be met
  - Future development needs
Avoid Requirements that cannot be tested

- Provide *easy* navigation between screens
- Provide *periodic* auto-archival of data
- Allow deletion of data *when applicable*
- Provide *appropriate* security levels
- Generate the *required* reports

---

Design and Design Review

- Business Processes
- Requirements
  - Standard System Manuals (COTS)
  - Functional Specification
  - Hardware / Infrastructure Design
  - Software Specifications
  - Configuration Specifications
Infrastructure Design

- Business applications and processes
  - Enterprise Resource Planning
  - Laboratory Information
  - Adverse Event Reporting
  - Advance Planning
  - AV

- Infrastructure applications and processes
  - Configuration Management
  - Service Desk
  - Security Management
  - Virus Management
  - Backup and Restoration
  - Problem Management
  - Network Monitoring
  - etc

- Clients
  - IT Services (e.g., DBMS, F&P, Email)
  - Operating Systems
  - Server Hardware
  - Network Environment

Delivering sustainable risk based solutions

Functional Risk Assessment - BMS

<table>
<thead>
<tr>
<th>F/B Section</th>
<th>Function</th>
<th>Sub Function</th>
<th>RISK</th>
<th>Risk Scenarios</th>
<th>Impact</th>
<th>Collection</th>
<th>Priority</th>
<th>Mitigation Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1</td>
<td>TE04</td>
<td>None</td>
<td></td>
<td>TESI failed, no impact as this is only for visual monitoring of external air temperature</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>1. None</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.2</td>
<td>Inlet Flow Control</td>
<td>B</td>
<td>Fall open, required closed Heating and cooling units would freeze in winter if HVAC shutdown but FV01 remained open</td>
<td>M</td>
<td>H</td>
<td>L</td>
<td>1. Temperature alarm TZ01 would indicate that fluid is —ve temperature Interlock closes FV01 when fan TH2 not running – Verify that the interlock has been tested</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1.2</td>
<td>Pre-filtration</td>
<td>B</td>
<td>Pre-filtration blocks</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>1. Pre-filtration blocks</td>
<td>2. Pre-filters changed annually (SOP &lt;title and reference&gt;) 3. Pre-filters cleaned monthly (SOP &lt;title and reference&gt;) 4. Routine weekly check to ensure differential pressure is within limits (SOP &lt;title and reference&gt;)</td>
</tr>
</tbody>
</table>
Electronic Record Risk

Risk Vulnerability (Probability)

Calculating Record Risk
## Controls based on criticality of record

<table>
<thead>
<tr>
<th>Impact</th>
<th>Records that may directly affect either:</th>
<th>E.g. but not limited to:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td>• Patient safety</td>
<td>Bill of Materials</td>
</tr>
<tr>
<td></td>
<td>• Product quality, safety, identity, or efficacy</td>
<td>Design History File</td>
</tr>
<tr>
<td></td>
<td>• Data integrity for regulatory submission</td>
<td>Recall Records</td>
</tr>
<tr>
<td></td>
<td>• Distribution and recall</td>
<td>Complaints Records</td>
</tr>
<tr>
<td></td>
<td>• Regulated Financial Reporting</td>
<td>Financial Records</td>
</tr>
<tr>
<td></td>
<td>• Confidential Healthcare records</td>
<td></td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td>Records that indirectly affect either:</td>
<td>Training Records</td>
</tr>
<tr>
<td></td>
<td>• Patient safety</td>
<td>Validation Documentation</td>
</tr>
<tr>
<td></td>
<td>• Product quality, safety, identity, or efficacy</td>
<td>SOPs</td>
</tr>
<tr>
<td></td>
<td>• Data integrity for regulatory submission</td>
<td>Audit and Investigation Records</td>
</tr>
<tr>
<td></td>
<td>• Distribution and recall</td>
<td></td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>Records that have no impact on:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Patient safety</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Product quality, safety, identity, or efficacy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Data integrity for regulatory submission</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Distribution and recall</td>
<td></td>
</tr>
</tbody>
</table>

### Required Controls

<table>
<thead>
<tr>
<th>Impact</th>
<th>Required Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Unique user accounts</td>
</tr>
<tr>
<td></td>
<td>2 component or biometric security code / e-signatures</td>
</tr>
<tr>
<td></td>
<td>Electronic Audit trail</td>
</tr>
<tr>
<td></td>
<td>Password Ageing</td>
</tr>
<tr>
<td></td>
<td>Automatic user session timeout following inactivity</td>
</tr>
<tr>
<td></td>
<td>Manual user session lockout</td>
</tr>
<tr>
<td>Medium</td>
<td>Unique user accounts</td>
</tr>
<tr>
<td></td>
<td>2 component or biometric security code / e-signatures</td>
</tr>
<tr>
<td></td>
<td>Manual user session lockout</td>
</tr>
<tr>
<td></td>
<td>Audit trail of system changes (e.g. change control records)</td>
</tr>
<tr>
<td>Low</td>
<td>Password or Network Security</td>
</tr>
<tr>
<td></td>
<td>Audit trail of system changes (e.g. change control records)</td>
</tr>
</tbody>
</table>

### Recommended Controls

<table>
<thead>
<tr>
<th>Impact</th>
<th>Required Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Electronic Audit trail</td>
</tr>
<tr>
<td></td>
<td>Password Ageing</td>
</tr>
<tr>
<td></td>
<td>Automatic user session timeout following inactivity</td>
</tr>
<tr>
<td>Medium</td>
<td>Unique user accounts</td>
</tr>
<tr>
<td></td>
<td>Automatic user session timeout following inactivity</td>
</tr>
<tr>
<td>Low</td>
<td>Unique user accounts</td>
</tr>
<tr>
<td></td>
<td>Automatic user session timeout following inactivity</td>
</tr>
</tbody>
</table>
Configuration Management

- **Identify configuration item**
  - Hardware
  - Software
  - Documentation, SOPs

- **Configuration item control**
  - Effective change control
  - Change traceability
  - Backup, Version control

- **Status accounting**
  - Status of all configuration items is known

- **Configuration verification**
  - Build Controls, Installation and Operational Qualification

**Configuration Item**
(Software, Hardware, Documentation, SOPs)

Configuration Management is required in support of:
- Change management
- Problem investigation
- Disaster recovery in the event of system failure

Configuration management shall ensure:
- Business decisions leading to configuration settings are recorded
- Changes are recorded
- All configuration parameters can be recovered from a secure record (electronic backup or paper)
Configuration Management

- A configuration baseline shall be established at system go live in order to support problem investigation
- Configuration Specifications, log books or other suitable form shall record configuration changes post go live
- All configuration changes shall be traceable to the system release in which the change was made
- Electronic configuration files shall be subject to version control (where possible) and controlled backup. Security controls shall minimize the risk of unauthorized or inadvertent change

Software Coding Standards and Review

<table>
<thead>
<tr>
<th>Standards</th>
<th>Availability of, and conformance to coding standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structure</td>
<td>Modular, Module Size, Control Blocks</td>
</tr>
<tr>
<td>Readability</td>
<td>Layout, Naming Conventions, Annotation/Comments</td>
</tr>
<tr>
<td>Data</td>
<td>Local vs Global, Parameter Passing (mechanism)</td>
</tr>
<tr>
<td>Scope</td>
<td>Functions stated in design implemented</td>
</tr>
<tr>
<td>Logic</td>
<td>Critical functions e.g. calculations</td>
</tr>
<tr>
<td>Integrity</td>
<td>Deadcode, redundant code</td>
</tr>
<tr>
<td>Control</td>
<td>Configuration Management, Versioning, Change Control traceability</td>
</tr>
</tbody>
</table>
Principles of Risk-based Qualification

‘Supplier’s standard inspection and test documentation may be used and no other documents be produced that duplicate this information, provided that documentation clearly shows the items of interest have been verified or tested in an appropriate manner. This is subject to the supplier being of adequate quality.’

Test Planning

- A Test Plan shall be created for all computerized systems. The Test Plan shall define:
  - List of tests to be conducted (positive and challenge tests)
  - Test Objective
  - Expected Result against Test Objective
  - Relationships / dependencies between tests
  - Equipment required to conduct tests
  - Data required to conduct tests
  - Test resources
  - Test failure management procedures

SOPs Supporting Testing

- SOPs / Work Instructions should be used in support of testing
  - Ensures consistency of testing
  - Verifies SOPs / Work instructions

- SOPs / Work Instructions used in support of testing must be managed:
  - Ensure current issue of SOP / Work Instruction being used
  - Ensure SOPs / Work Instructions used in testing are written before testing
  - Ensure that errors in SOPs / Work Instructions are addressed
Development Testing

- Development testing shall be conducted for any custom developed software by the system developer prior to qualification. Development testing shall challenge the structure and logic of the developed code.

- Development testing shall be conducted in accordance with the same controls as qualification testing however development testing does not need to be independently reviewed by Site Quality Assurance.

- Development test records should be retained and made available for periodic Site Quality Assurance audit.

Installation Qualification

- Documented verification of the installation and configuration of test and production environment hardware and software.
- Installation shall be controlled by written procedures and / or protocols.
- Installation verification shall confirm correct installation of:
  - Hardware
  - Operating system and other infrastructure software
  - Application software
  - System configuration
  - Security setup
- IQ of IT Infrastructure addressed by CSC.POL.0003, Risk Based Approach to Implementation, Qualification, Support and Retirement of IT Infrastructure.
Operational Qualification

- The Operational Qualification Protocol shall cover:
  - Functional/Operational tests vs. design
  - Challenge testing against operating ranges (e.g. data entry, performance)
  - Communication interfaces
  - Start-up & shutdown
  - Security and access
  - Data storage and recovery
  - Alarm, event status handling

Performance Qualification

- PQ comprises product performance and/or process performance qualification (vs URS)
- Performance related functionality/processes
- System Interface Performance
- Management controls
  - Monitoring of user enquiries
  - Data changes
  - System availability
  - System stability
  - Problem resolution to Incident Logging
  - System changes

Delivering sustainable risk based solutions
Acceptance Criteria

- Related to critical process parameters
- Predefined
- “Worst case”

SMART
- Sensible
- Maintainable
- Accurate
- Range
- Traceable

Results Recording

- Results must clearly demonstrate that acceptance criteria has been met
- Be positive / specific
  - For values record actual value
    - 20.3 deg C NOT > 20 deg C
  - For other items e.g. messages
    - As acceptance criteria
- No tick boxes, ok, etc
Expect the Unexpected!

- It is inevitable that changes will be required during testing
- Changes must be managed
  - No quick fixes
  - Don't pressure developers
  - Consider need for regression testing
  - Use run number to identify repeat tests
  - Changes must be managed

Objective Evidence

- Whenever possible generate objective evidence in support of test results
  - printouts
  - screen dumps
  - logs
  - photographs
  - certificates
  - charts
Test Summary Report

- Test Summary Report shall:
  - Provide a status of all testing conducted
  - Provide a list of test incidents
  - Provide a summary of actions taken to address test incidents
  - Identify the number of test runs conducted for each test

- Depending on the phasing and scope of testing, a test summary report may be created after each test phase, at the end of testing or in the overall project Validation summary Report.

Leveraging the Supplier’s Documentation

- Supplier’s documentation
  - Should be assessed for suitability, accuracy and completeness
  - Allowed flexibility regarding acceptable format, structure and documentation practices
- Consider
  - Style
  - Level of Approvals (e.g., Site QA)
  - Management of Deviations
- Quality of supplier documentation
- Need for oversight of testing
- How supplier testing will be integrated with end user testing
### Test Case Header

<table>
<thead>
<tr>
<th>Test Case Number</th>
<th>Test Case Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>OQ-1.0</td>
<td></td>
</tr>
</tbody>
</table>

- **Test Case Objective**

- **Test Case Acceptance Criteria**
  - Pass Criteria: Actual result recorded is same as the expected result of the test
  - Fail Criteria: Actual result is not same as the expected result

- **Test Case Set-up (Equipment, Data, Related Tests)**

- **Test Case Comments**

<table>
<thead>
<tr>
<th>Test Case Start Date/Time (dd-mm-yyyy hh:mm)</th>
<th>Test Case Finish Date/Time (dd-mm-yyyy hh:mm)</th>
<th>Pass / Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test Case Executed By: Initial and Date</th>
<th>Test Case and Related Results Reviewed By: Initial and Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Delivering sustainable risk based solutions**

### Test Case Body

<table>
<thead>
<tr>
<th>OQ-1.1 SubTest</th>
<th>Step No.</th>
<th>Step Description</th>
<th>Expected Result</th>
<th>Actual Results</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Actual Result Evidence Reference</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pass / Fail Initial and Date</td>
</tr>
<tr>
<td>OQ-1.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OQ-1.1.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Delivering sustainable risk based solutions**
Test Incidents

Incident Number: IN.003
Test Reference (where relevant) Test OQ.002 BOM Printing, failed at step 5
System Name and Id Global ERP

Title: Test OQ.002 BOM Printing, failed at step 5

Person Reporting Incident: Chris Reid
Department: IT

Person Managing Incident: A.N. Other
Department: Development

Date Reported: 15th July 2009
Impact GxP

Test Incidents

Test Incidents

Description of Incident
Failed to meet acceptance criteria set forward in test OQ.002, step 5

Incident Impact
Test OQ.001 needs to be re-tested Data supporting test OQ.002 requires reset to original values

Investigation and Diagnosis
Error in software module "Print BOM"

Action Taken
Change control CC.0032 raised to address software error and test OQ.001 and OQ.002 re-executed successfully

Delivering sustainable risk based solutions
Go Live

- Ensures operations and support organizations are prepared to receive the validated system:
  - Documentation updated to as built status
  - Operation and support SOPs in place
  - Technical and support documentation available to support staff
  - Internal and external SLA are in place
  - Operations and support personnel trained in system use and SOPs
  - Residual risks from validation have been evaluated and actions defined.
  - Operations take ownership of risk mitigation
  - Support organizations trained
Post Implementation Monitoring

System stability and availability shall be monitored for a period, post go live:
- Extent of changes post go live
- Number of workarounds implemented
- Number of issues / incidents raised and their severity
- System failures
- System availability against Service Level Agreements
- System and Infrastructure performance

Focused monitoring and regular reporting shall continue until full business as usual status is achieved and statistics demonstrate stable and acceptable operation.

Report created to summarize the outcome.

Operational Controls

Delivering sustainable risk based solutions
Emergency Changes

Very occasionally it is necessary to implement changes quickly to minimise risk to patient safety or business operation.

1) Consult users to discuss and agree
2) Do change
3) CC completed usually within 24 hours
4) Consider “holds” based on impact e.g. product not released until CC reviewed and signed off.

Delivering sustainable risk based solutions

Incident Management

- System failures, bugs, anomalies, errors recorded on an Incident Report, System Logbooks or in an appropriate Error Log.
- Issues must be reviewed and appropriate action taken to rectify the problem.
- Incident Reports / Error Logs periodically reviewed to determine trends indicating inadequate system design, implementation or testing.

Delivering sustainable risk based solutions
Security Management

- Maintain integrity of data
- Maintain availability of Information Assets
- Maintain confidentiality and to restrict accessibility (physically and logically) of information and system functionality to authorized personnel only.
- Support business continuity processes.

User Access Controls
Password Reset

- If a user forgets their password they must request a System Administrator reset.
- Before implementing the reset, the System Administrator must positively identify the user.
  - System Administrator knows the person requiring reset and is able to identify them (e.g. by voice) when a reset is requested
  - User’s line manager / supervisor sends email to System Administrator confirming identity of requester
  - Person requesting reset presents themselves to System Administrator with picture ID
- System is implemented to allow use of characters from secret words
- User must change their password the first time they log onto the system following reset (providing system has the capability).

Periodic Review

- Periodic Reviews of regulated computerized systems shall be conducted in order to ensure systems are maintained in a validated state. Periodic Review shall examine:
  - Maintenance of documentation and records in line with system changes
  - Reported issues / incidents
  - Evidence of unstable or unreliable operation
  - Changes in environment, process or business requirements, regulation or accepted best practice
  - Level and type of changes being made
  - Outstanding actions from Validation Report, Audit Reports and Previous Periodic Reviews
  - Change of system use
  - Security controls
  - Personnel (training of new users or persons changing roles)
- Periodic Review shall be conducted annually for critical systems (e.g. patient safety related) and every 3 years for non critical regulated systems (e.g. training systems).
- Periodic Review of regulated IT Infrastructure shall be conducted every 2 years.
Data Migration Planning

- Approaches
  - Re-keying of records into new system
  - Custom data migration programs
  - Inbuilt tools within application

- SOPs required for manual data migration operations

- Validation of custom Data Migration Programs

- Off-the-shelf data migration tools validation in accordance with risk

- Data Cleansing
Data Migration Verification

- Data migration verification tests shall be documented to describe the checking process. The sample of data verified shall be determined by:

  - Scope of data to be migrated
  - Criticality of data to be migrated
  - Degree of data translation between systems
  - Risk of data error arising from the data migration approach (e.g., upgrade to new version of same product, custom data migration tools, manual data entry)
Legacy Systems

- Legacy computerized systems are those systems that are in use and may not adequately comply with this policy, regardless of age.
- Documented Risk Assessments shall be conducted to determine the criticality of any identified shortfalls.
- Remediation plans shall be established to address unacceptable risks. Remediation shall be focused on demonstrating:
  - System specification to a level that supports understanding and acceptance of system processes and functions
  - Suitable platform for system use, change, maintenance and disaster recovery (e.g. configuration specifications, system specifications)
  - System processes and functions operate and perform in accordance with approved specifications (e.g. testing)
  - System performance, stability and free of known critical faults

GAMP categories and spreadsheets

- Category 1 - Product on which the spreadsheet is developed
- Category 2 – N/A
- Category 3 – Use of native spreadsheet functions with no configuration
- Category 4 – Initial input of data requires the application to automatically branch to different cells to perform the data manipulation
- Category 5 – Custom macros or nested logic/lookup functions
Disposable Spreadsheets

- Intended to be used only once
- Only for “simple” applications
- Print the spreadsheet showing:
  - Formula
  - Input data
  - Output results
- Calculations must be verified. Attach hardcopy verification evidence as to the printed spreadsheet

Internal Audit

- Internal functions audit other functions (or disciplines)
- Focus on a specific area of the QMS
- Keep scope sensible
- Observations more practical and value added
- Better ownership of observations
Common Pitfalls / Audit Observations – Docs / Plans / SOPs

- Documentation
  - Failure to follow templates
  - Templates too rigid
  - No justification for not addressing a template requirement
  - Documents not approved
  - Documents not under configuration management

- Plans and SOPs
  - Don’t follow the plan or SOP
  - Don’t raise deviations when plan or SOP not followed
  - SOP assigns roles to people who don’t have authority to execute role
  - Not prescriptive enough so difficult to follow
  - Too prescriptive so difficult to follow!!!
  - Not practical

Thank you

Questions?
Common Pitfalls / Audit Observations - Specifications

- Requirements not clear, concise, measurable
- Defined too early or too late
- Project team ignore URS
- Focus on product rather than business processes
- Not maintained during the implementation phase
- Not tested
- Not created
- Developed by wrong people
- Design not traceable to Requirements
- Deviations from requirements not managed
- Design evolves after issue of Requirements or Design Documentation
- Design issues are documented but not addressed

Common Pitfalls / Audit Observations - Testing

- Specifications
  - No test specifications
  - Lack of approvals (pre, test, post)

- Methods
  - Not repeatable
  - Lack of boundary challenges
  - Not traceable to design
  - Inadequate deviation management

- Acceptance criteria
  - Not defined
  - Ambiguous
  - Embedded in method

- Results
  - Inappropriate Records
  - Do not clearly demonstrate that acceptance criteria met
  - Not supported (where required) by raw data
  - Raw data not signed
  - Raw data not referenced to test