HPRA
An tÚdarás Rialála Táirgí Sláinte
Health Products Regulatory Authority

Computerised System Validation

Considerations for the Validation Lifecycle

Paul Moody

GMP Conference
12th November 2014

Regulatory References

- EU GMP Annex 11 (2011)
  - http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf
- EMA Questions and Answers on Annex 11
  - http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/general/gmp_q_a.jsp&mid=WC0b01ac058006e06c#section8
- PIC/S PI 011/3 (2007)
  - http://www.picscheme.org/pdf/27_pi-011-3-recommendation-on-computerised-systems.pdf

HPRA
An tÚdarás Rialála Táirgí Sláinte
Health Products Regulatory Authority

Contents of this Presentation

- Introduction and "Pre-Validation"
- Validation Considerations
- Post Validation Considerations
- Sample Deficiencies

What is a Computerised System?

- ...a set of software and hardware components which together fulfill certain functionalities. [Annex 11 Principle].
  - Software....TrackWise, Empower, PAS X etc
  - Hardware....PC, Network, Server...etc.

- Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.

- Sounds Easy!

Validation Approach

- Infrastructure should be qualified….
  - The hardware and software such as networking software and operation systems, which makes it possible for the application to function.
    - PC and Operating System
    - Network

- Applications should be validated…..
  - Software installed on a defined platform/hardware providing specific functionality

What is Qualification?

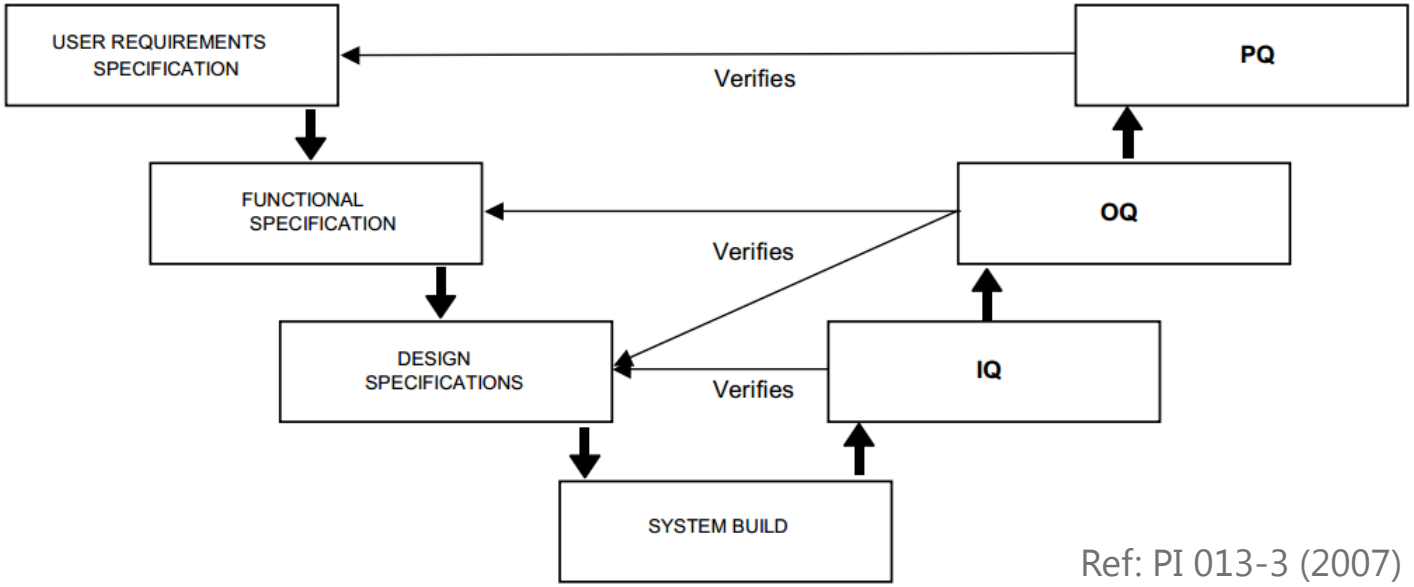
- Qualification (Glossary, EudraLex Vol. 4)
  - Action of proving, in accordance with the principles of Good Manufacturing Practice, that any procedure, process, equipment, material, activity or system actually leads to the expected results.
  - Action of proving that any equipment works correctly and actually leads to the expected results.
  - The word validation is sometimes widened to incorporate the concept of qualification.

What is Validation?

- Validation (Glossary, EudraLex Vol. 4)
  - Action of proving, in accordance with the principles of Good Manufacturing Practice, that any procedure, process, equipment, material, activity or system actually leads to the **expected results**.

- The Quality of Validation depends on how the "expected results" are defined.

The Validation Lifecycle



Ref: PI 013-3 (2007)

Pre-Validation Activities

- Decisions on the extent of validation and data integrity controls should be justified and documented through risk assessment of the computerised system.

- When third parties are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.

Pre-Validation Activities

- Up to date listing of all relevant systems and GMP functionality
- For Critical Systems, a detail of the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures.
- "Expected Results" defined ultimately by the User Requirement Specification
  - should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle. [Annex 11, 4.4]
- Defining User Requirements is a key activity of a validation and time should be taken.

Pre-Validation Activties: Functional Spec

- Develops the functional specifications (bespoke)
- Clearly identifies the functional specifications for selection and purchase of off-the-shelf systems.
- Should define a system to meet the URS, i.e. the customer's needs.
- precise and detailed description of each of the essential requirements for the computer system and external interfaces.
- This means descriptions of functions, performances and where applicable, design constraints and attributes.

- Defining the URS, reviewing & understanding the FS is key
  - Comes from risk assessment
  - Assessing the current system against the proposed system

Computerised System Validation

- Generally follow the lifecycle of equipment validation: IQ, OQ, PQ with quality gates at the appropriate points.
- Level of validation depends on the criticality of the system and must be justified
- Typical validation includes:

Typical Validation Parameters		
Process Values	Data Integrity	Error Handling
Process Logic	Data Limits	Electronic Signatures
	Data Transfer	Configuration
	Audit Trails	Security

Data Integrity

- More detailed discussion on this in Parallel Session 1B

- **Maintaining** and **assuring** the **accuracy** and **consistency** of **data** over its entire **life-cycle** and is a critical aspect to the design, implementation and usage of any system which stores, processes or retrieves data

- Primary data is the data of interest, "Metadata" is the data about data and provides context and relationship to the primary data thus preserving the accuracy, completeness, content, and meaning.

Validation of Data Elements

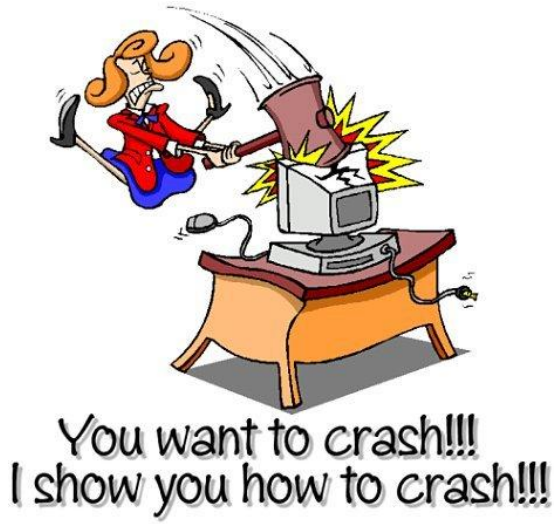
- Data limits
  - Include negative testing (from risk assessment)
- Data Transfer
  - Checks that data are not altered in value and/or meaning (primary and meta data)
  - Level of checking should be statistically sound

Data Integrity and Security

- How does the system transfer data to other systems?
  - Native to the software, Middleware, Custom code?
  - E.g. EBR with Balances, CDS data migration to LIMS
- Data security includes, Integrity, Reliability, and Availability of data.
- During validation of a database-based or inclusive system consider:
  - procedures and mechanisms to ensure data security, the meaning and logical arrangement of data
  - load-testing, incorporating future database growth
  - precautions for end of life-cycle data migration

Validation of Error Recovery

- Error handling
  - If the system crashes, what happens?
  - System recovery mid transaction?
  - Database corruption
  - Data flow and bandwidths?



Data Accuracy and Storage

- How accurate is the data?
  - Electronic Verification e.g. against a database or other system
  - Manual verification of entries e.g. manually on to a calculation spreadsheet
  - The consequence of bad data should be known and assessed.
- How, where is Data Stored?
  - Who has access?
  - Is integrity maintained?
- Ensure that clear printouts of data can be obtained.
- Records supporting batch release should indicate if any data has been corrected….all GMP records

Audit Trails

- Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions [Annex 11, 9].

- Concept best understood in terms a paper record versus electronic record

Audit Trails: Paper vs Electronic

Change
001
002
003
004
005

Test ID 123 Test System ID: ~~HPLC-01~~ HPLC-02 AP 1/10/14
Test Objective: HPLC ASSAY
Specification: SPEC-001 (≥98%)

Step	Test Procedure	Expected Result	Actual Result	Required documents	Pass/fail
1	PROC01	98%	~~99~~ 97 AP 1/10/14	RESULT FILE	~~PASS~~ FAIL AP 1/10/14
2	~~PROC02~~ PROC01 AP 1/10/14	98%	97	RESULT FILE	FAIL

Tester: I confirm that I have all tests executed as described
Name: A. PERSON Signature A. Person Date 1/10/14
Tests passed: yes (no) Comment: DEVIATION 001

Reviewer: I confirm that I have reviewed test documentation
Name: S. ELSE Signature S. ELSE Date ~~1/10/14~~ S.E 3/10/14. 3/10/14

Reason
Entry Error
Calculation Error
Sequential to 002
Correct Procedure Referenced
Signature reapplied

Audit Trails

- Must be
  - convertible to a 'generally intelligible form'
  - regularly reviewed

- If system has no functionality showing changes to data since original entry
  - printout of the related audit trail report must be generated and linked manually to the record supporting batch release or certification as appropriate.

Audit Trail Validation: Consideration

- URS: States that you must an audit trail is required….
  - FS: Application Audit Trail function = on
  - IOQ: Test that an audit trail record is generated
  - All Done…?

  - Consider the following…

Consider Chromatography Data Systems…

- It's got "Audit Trail" functionality
  - System Audit Trail lists communication errors, account activity…
  - Each Method, Sample Set, Result, Integration has a 'Revision History'.
    - an audit trail by another name?
- What about Infrastructure audit trails, File History Revisions, Application System Transfer actions?
- Consider all areas of Computerised System which may be updated.
  - System Risk Assessment
  - User Requirements and Functional Specification should consider all GMP areas of Computerised System which may be updated

Multisite Systems

- Some examples:
  - EBR System
  - Deviation Management System
- Validation plan/overview for the approach taken
- Typical 'Corporate' core validation
  - Plan, URS, FDS, IQ, OQ etc
- Site should assess the corporate validation
  - include Site Infrastructure
  - Meets requirements of Annex 11

Multisite Systems

- Typically 'Site' performs activities to mitigate the risks identified
  - Some Infrastructure Qualification
  - Some software elements:
    - Mini URS, Mini FDS/Config Spec, Mini IQ, Mini OQ, PQ etc.
- All documentation may be subject to inspection
  - Includes 'Corporate' core validation and associated assessments, agreements etc

- 'Corporate' HQ typically not involved in manufacturing and are therefore not usually regulated
- Validation is the responsibility of the regulated user...

Using a "Third Party"

- Qualification/Validation performed by a 'Vendor'...
  - Subject to Chapter 7: Outsourced Activities
  - Must ensure Site not Vendor user requirements achieved.

- Where certain activities are outsourced by a manufacturer and computerised systems are used. The validation of such hardware and software should be maintained.
  - e.g. Kaye Validators etc

- Validation is the responsibility of the regulated user...

System Security and Electronic Signatures

- Security of the system
  - User Access Levels should be defined with management of access control including both Front End and Back End (if applicable).
  - Record of access within software
  - Extent depends on criticality of system
- Electronic Signatures should have the same impact as a hand written signature within the boundaries of the company and permanently linked to the record and time and date stamped.
  - Does your system rebuild the signed document or is the signature embedded within the document?
  - Embedded in database or file network location referenced within database? Who has back end access?

Back Up and Archiving

- Back Up and Archival are not the same thing.
- Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.
  - Is data verified – not just by a CheckSum?
  - What is media used and what is its expiration criteria?
  - Storage requirements of electronic data and documents the same as paper documents.
- Archived data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.
  - How is this achieved? Virtual Solutions to rebuild the system?

Change and Configuration Management

- Remember, the system is validated!
- Changes to a part of the system may pose a risk due to interdependencies.
- Change management system must be used.
  - Record, assess, approve and document change
  - Separate electronic system used for IT issues/changes?
    - …is it a GMP system in its own right?

Periodic Evaluation

- Consider it like other periodic evaluations (Water, Env Monitoring)
- Justify frequency of evaluation based on system criticality and complexity

Considerations for Periodic Evaluation			
Current Functionality	Problems	Performance	Deviations/Incidents
Validation Status Reports	Security	Reliability	Upgrade History

- Incident Management process can be key source of information

Incident Management

- All incidents should be reported and assessed.
- What is an incident?
  - System Failures
  - Data Errors
  - Any unplanned issue affecting product quality or data integrity.
- Root cause of a critical incident should be identified and CAPAs implemented.
- Useful to map incident reporting data "chain of custody" to ensure appropriate controls are in place.

Business Continuity

- What happens if the system breaks down?
- Manual or Alternative system?
- Risk Assessment for bringing them up
- Manual/Alternative systems should be tested in their own right

In Summary….

- There should be no resultant decrease in product quality, process control or quality assurance

- Understand the system and its interactions
- Risk Assess the system
- Software should be validated and maintained
- Infrastructure should be qualified and maintained
- Data Integrity should be assured
- E-Signatures should be permanently linked
- Issues should be appropriately investigated and resolved

Sample Deficiencies: General

- A listing of GMP computerised systems was not maintained.
- The software utilised to control [equipment] had not been categorised.
- Not all critical GxP systems were present. For example the [Equipment] Program and Review software.
- While a statement of GxP or non-GxP was documented for Global Systems, there was no associated documentation justifying the statement.
- Computerised System Risk Assessments for critical systems were not in place.
- There was no system description/boundary despite the critical system being 'live'.

Sample Deficiencies: General

- The [business continuity process] was not available for use as documented in [a deviation]. The associated investigation did not assess why the contingency procedure and process had failed.
- The third party audit performed of the software supplier was considered deficient in that the memo describing the qualification or impartiality of those persons performing the audit was not signed by those individuals.

Sample Deficiencies: User Accounts

- It was possible for administrators to verify their own test result recording in ERP. There were no procedural restrictions around this and was hence considered to increase the overall risk of the associated testing processes.
- The 'system owner access level' was not described.
- The removal of test accounts had not been considered by the company prior to the system going 'live'.
- [ERP] access configurations for the job roles within the site was not adequately defined in that there was no documented correlation of roles to the user access elements defined by the Global [ERP] group.
- System authorization concepts were not always considered in that Users could be administrators with full system access and also have batch manufacturing responsibilities.

Sample Deficiencies: Audit Trails

- Audit trail comments on [the CDS] were not always sufficiently detailed. For example, a number of changes were observed to have been made to the integration method utilised on [a test] on [a date] and these had a comment of 'save' documented.
- Operating System User Accounts were utilised to access the <system>. There was no periodic review of Operating system audit trails (logs) as appropriate and this was not justified.

Sample Deficiencies: Validation

- The qualification of the ERP system was considered deficient in that:
  - The independent code review was not available for review during the inspection.
  - The actual observed results were not always documented within the qualification records
  - The procedure for electronic signatures data transfer to the ERP system was not described in a procedure and was not qualified.
  - There was no assessment of ERP database integrity.
- The decision not to test requirement [Electronic Signatures] documented in [Rationale] was not considered to be justified in that the referenced documents disclaimer stated that the information should not be relied upon.

Sample Deficiencies: Validation

- The Virtual Private Network software had not been subject to GxP assessment or qualification as appropriate.
- In relation to the back up and restoration of data
  - There was no process for logging of media used to back up the server systems.
  - The maximum number of uses for the magnetic tapes was not defined or the number of uses controlled.
  - All backup activities on the site were not procedurised. For example back up of the [Program] data from [Equipment] and back up of certain [Equipment] PLC code was performed on an ad-hoc basis using HDDs which were not stored in an appropriate location.

Sample Deficiencies: Periodic Evaluation

- The periodic assessment of computerised systems had not been completed for all equipment. For example, [computerised system] was installed [a long time ago] and at the time of the inspection had not been reassessed.
- Periodic review of global applications was not performed and there was no procedure in place for periodic review.
- The periodic system review of the <system> was <documented>. The review stated that there was no requirement for audit trail review as they were "displayed on the screen". This was not considered to justified. Further to this, there was no procedure in place for periodic audit trail review.

Sample Deficiencies: Change Management

- In relation to the testing associated with <IT Change Control System>, the evidence for the appropriate test scenario was not available for review. The system permitted only the most recent test scenario for the process to be viewed. There was no evidence that the system level risk assessment had been critically assessed prior to this change in order to determine the appropriate test scenarios. Further to this, the change to this production parameter had been assigned as a non regulatory change i.e. not subject to GxPs.
- Change logs for <ERP> user access sub-role profiles were maintained in an uncontrolled manner. E.g Z_XXX_XXX_XX_DATA, the associated text box change log had three entries post implementation of <IT Change Control System> whereas <IT Change Control System> listed four valid changes for this profile

HPRA
An tÚdarás Rialála Táirgí Sláinte
Health Products Regulatory Authority

Thank You for Listening