Computerised Systems

– Seeing the Wood from the Trees

Scope

WHAT IS A COMPUTERISED SYSTEM?

WHY DO WE NEED VALIDATED SYSTEMS?

WHAT NEEDS VALIDATING?

HOW DO WE PERFORM CSV?

WHO DOES WHAT?
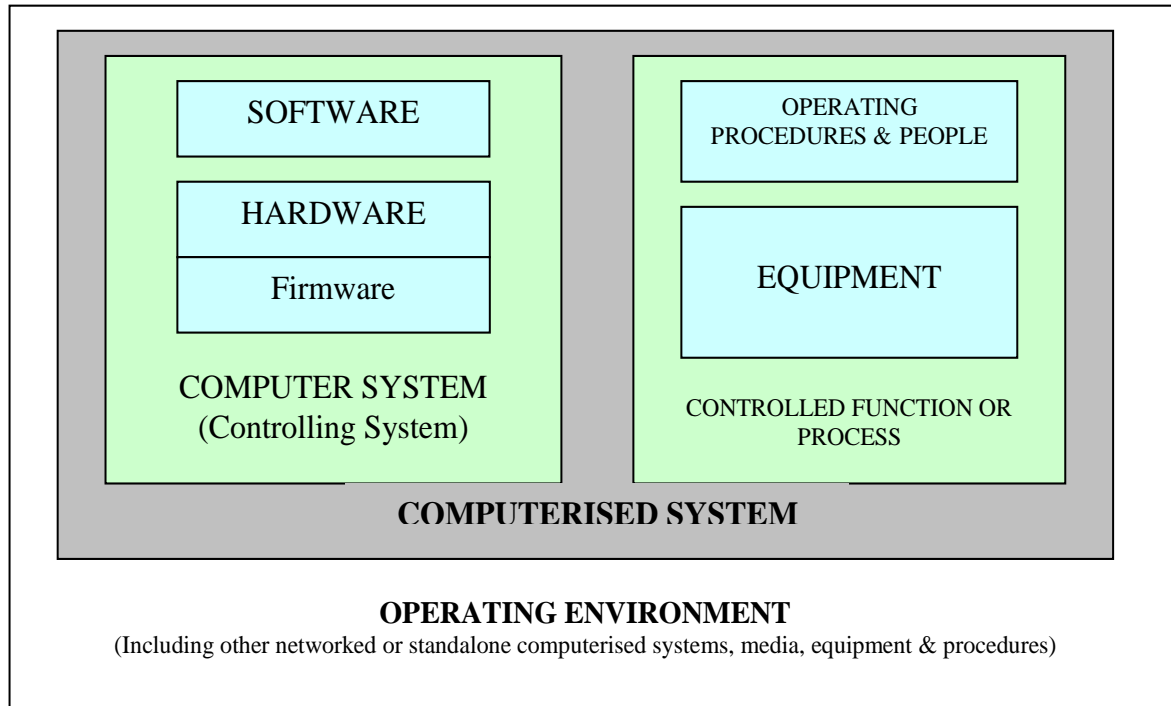
IT'S VALIDATED - WHAT NEXT?

IN SUMMARY

REFERENCES

ACKNOWLEDGEMENTS

What is a computerised system?

A COMPUTERISED SYSTEM INCLUDES:

Why do we need validated systems?

TO DEMONSTRATE THAT THE SYSTEM AND ITS USE ARE 'FIT FOR PURPOSE'

– Oxford English Dictionary definition of 'Fit for Purpose':
(of an institution, facility, etc.) well equipped or well suited for its **designated role or purpose**.

ALL COMPUTERISED SYSTEMS USED FOR THE CAPTURE, PROCESSING, MANIPULATION, REPORTING AND STORAGE OF DATA SHOULD BE DEVELOPED, VALIDATED AND MAINTAINED IN WAYS WHICH ENSURE THE VALIDITY, INTEGRITY AND SECURITY OF THE DATA

– Guidance document GCP for Laboratories, Issue 1, 2009

Why do we need validated systems? (2) - Further Regulatory Guidance

'ALL COMPUTER SYSTEMS USED IN CLINICAL TRIALS, IN PARTICULAR THOSE THAT IMPACT ON THE QUALITY OF THE TRIAL DATA (AND SUBJECT SAFETY), SHOULD BE VALIDATED'

- GCP Guide, MHRA, 2012 (Grey Guide)

WHEN USING ELECTRONIC TRIAL DATA HANDLING AND/OR REMOTE ELECTRONIC TRIAL DATA SYSTEMS, THE SPONSOR SHOULD:

ENSURE AND DOCUMENT THAT THE ELECTRONIC DATA PROCESSING SYSTEM(S) CONFORMS TO THE SPONSORS ESTABLISHED REQUIREMENTS FOR COMPLETENESS, ACCURACY, RELIABILITY, AND CONSISTENT INTENDED PERFORMANCE (i.e. VALIDATION)

- ICH E6 (R1) Guideline for Good Clinical Practice

Why do we need validated systems? (2) - UK Regulations

STATUTORY INSTRUMENT 2004/1031 (AS AMENDED)

– Regulation 31A (4)

- The essential documents relating to a clinical trial are those which –

- (a) enable both the conduct of the clinical trial and the quality of the data produced to be evaluated; and

- (b) show whether the trial is, or has been, conducted in accordance with the applicable requirements of Directive 2001/83/EC, the Directive, the GCP Directive and Commission Directive 2003/94/EC

– Schedule 1, Part 2 (9)

- All clinical information shall be recorded, handled and stored in a way that it can be accurately reported, interpreted and verified, while the confidentiality of records of the trial subjects remain protected.

What needs validating?

WHEN IS COMPUTERISED SYSTEM VALIDATION (CSV) REQUIRED?

- Identify what the system is to be used for.
  - Does or will it directly control, record for use, or monitor laboratory testing or clinical data?
  - Is it or will it be the official, auditable, archive or record of a regulated activity?
  - Does or will it create, update or store data prior to transferring to an existing validated system?
- If the answer to any of these is **YES** then validation will be needed.
  - Is it a non configurable product which will or has been subject to testing as part of documented equipment or method qualification processes?
- If the answer to this is **YES** then further validation will **NOT** always be needed*

  *as long as the qualification processes fully cover the intended use of the computer system

What needs validating? (2)

SCOPE AND EXTENT OF VALIDATION

– Should be linked to the level of regulatory risk, the category of software to be used and the level of functionality that will be used.

– To do this each has to be defined separately.

LEVELS OF REGULATORY RISK

Level of Regulatory Risk	Type of record utilised (examples of)
High Impact	Data submitted to a regulatory agency Clinical trial data from patients or supporting networks Supporting non-clinical laboratory studies
Medium Impact	Calibration and validation records Supporting data not directly submitted to a regulatory agency
Low Impact	Planning and scheduling of regulated work Monitoring records

What needs validating? (3)

CATEGORIES OF SOFTWARE TO BE USED

Software Categories	Description	Types of software (examples of)
Custom Applications (GAMP 5)	Software custom designed and coded to suit the business process.	Spreadsheets (with Macros).
Configured Products (GAMP 4)	Software that can be configured by the user to meet the user's specific process needs. Software code is not altered.	Laboratory Information Management Systems (LIMS), Manufacturing Resource Planning (MRPII), Chromatographic Data Systems (CDS), Electronic Document Management Systems (EDMS), Spreadsheets (developed).
Non-Configured Products (GAMP 3)	Run time parameters may be entered and stored but the software cannot be configured to meet the business process.	Firmware based applications Commercial Off The Shelf (COTS) software Laboratory Instruments
Infrastructure Software (GAMP 1)	Layered software (upon which applications are built) or software used to manage the operating environment.	Operating Systems, database managers, programming languages, middleware, statistical programming tools, spreadsheet packages*, network monitoring software, batch job scheduling tools, security software, antivirus software and configuration management tools. *but not applications developed using these packages.

What needs validating? (3)

THE EXTENT OF VALIDATION TO BE CARRIED OUT

– Using the level of risk and software category:

		Level of Regulatory Risk		
		Low	*Medium*	*High*
Software Category	*GAMP 5*	Full Validation	Full Validation	Full Validation
	GAMP 4	Reduced Validation	Full Validation	Full Validation
	GAMP 3	Reduced Validation	Reduced Validation	Reduced Validation
	GAMP 1	No Validation	No Validation	No Validation

– 'Full Validation' requires consideration of the full system validation life cycle (due to the higher levels of risk identified)

– 'Reduced Validation' requires a more simplified system validation life cycle based on risk and software complexity.

– 'No Validation' requires no computer system validation at all due to the minimal nature of risk or impact the system is considered to pose to patients or quality.

How do we perform CSV?

WHERE TO START?

– Planning: Parallels with analytical method validation

Analytical Method Validation	Computerised System Validation
Establish outline strategy	Validation Master Plan
Establish method requirements	Establish system requirements (URS)
Identify, develop and finalise method	Identify, develop and finalise system functionality (FS/DS)
Validation plan of testing	Validation plan or individual qualification test protocols (IQ, OQ, PQ, UAT)
Execute validation testing	Execute qualification or user acceptance testing
Validation report	Validation (summary) report
Routine Use: Controls & Monitoring e.g. on-going QC monitoring, trending, etc.	Routine Use: System Controls and Monitoring e.g. on-going PQ testing, Change Control, Fault resolution mechanisms, etc.

CANCER RESEARCH UK | MANCHESTER INSTITUTE

CANCER RESEARCH UK

How do we perform CSV? (2)

WHERE TO START? (CONTINUED)

– Planning: The Validation Master Plan

- Its purpose is to define, describe and document the overall strategy and responsibilities for the CSV activities to be performed.
- This should include (but not be limited to):

  – **Purpose and Scope**   **(What is being validated)**

  – **Objectives**   **(What is to be achieved)**

  – **Roles & Responsibilities**   **(Who is involved and what do they do)**

  – **Methodology to be used**   **(e.g. URS, IQ, OQ, UAT, PQ, etc.)**

  – **System Risk Assessment**   **(What vulnerabilities there are)**

  – **System Life Cycle**   **(Including Operation and Maintenance)**

  – **Approvals and Authorisation**   **(e.g. Who reviews/accepts for use)**

How do we perform CSV? (3)

WHERE TO START? (CONTINUED)

– Planning: The User Requirements Specification (URS)

- Must define clearly and precisely what the end user wants the computerised system to do.
  - **Including ensuring the validity, integrity and security of the data.**
- All end users of the computerised system must be consulted to capture requirements.
- Each requirement should be SMART.
  - **S**pecific**, M**easurable**, A**chievable**, R**ealistic and **T**estable**.
- Each requirement should also be unambiguous, clear, precise and self contained.
- Each requirement should be numbered to enable traceability to test documentation.

How do we perform CSV? (4)

AN EXAMPLE OF USER REQUIREMENTS

URS #	Description
3.0	**Compliance Requirements**
3.1	21 CFR Part 11 Requirements – Security
3.1.1	The system must expire the current password 90 days after password creation/modification, and not allow the user to control or change this period of time.
3.1.2	The system must not allow the user to log on with the old password if the password has expired.
3.1.3	If the user enters the wrong password, the system must prompt a message "Invalid user ID/Password" or equivalent.
3.1.4	If the user enters the wrong password 3 times, the system must not allow the user to log on.
3.1.5	The system must not allow the password and the user name to be the same.
3.1.6	The system must require passwords to be a minimum of 7 characters in length.

How do we perform CSV? (5)

SCOPE AND EXTENT OF VALIDATION (AGAIN)

- Each of the user requirements should be individually risk assessed (to identify the level of functionality to be tested).

- The rationale and methodology of the risk assessment must be clearly defined and documented.

- Two examples from a document management system:

URS #	Description	Mandatory or Desirable?	GCP Critical or Non Critical?
3.1.1	The system must expire the current password 90 days after password creation or modification, and not allow the user to control or change this period of time.	Mandatory	Critical
4.5.1	The SOPs folder is to contain a list of effective GCP SOPs.	Desirable	Non Critical

How do we perform CSV? (6)

WHERE TO DOCUMENT TESTING?

– Test Script Protocols and Proforma should be developed.

  • Each test should be traceable to the identified requirement(s).

– Ultimately you define where testing is documented
(in the validation plan).

  • For more complex systems

    – **It may be more appropriate to provide protocols and completed test scripts/reports for each part of the qualification performed (IQ, OQ, etc.)**

    – **Additionally this can apply to each functional area tested (e.g. Project management or sample management modules within a LIMS).**

  • For less complex systems

    – **It may be possible to create a single test script protocol/proforma**

How do we perform CSV? (7)

AN EXAMPLE OF A TEST SCRIPT PROFORMA

Log-in Security

URS #	Test steps required	Results/Comments (delete where applicable)	Result (delete where applicable)	User (Initials)	Witness (Initials)	Date
3.1.5	Access the change password menu in the My Account tab (sidebar), via the GCP Portal, and change the current password to be the same as the User ID. If this is successful, the **user** is to log-out of the portal and then log back in using the same User ID/Password combination. (User role: **Any** except System Administrator)	Could the password be changed to match the User ID? Yes/No If Yes, could the user log-out of the portal and then log back in again using the same User ID/Password combination? Yes/No	Pass/Fail			
3.1.3 (a)	Log into the GCP Portal using an incorrect password. (User role: **Any** except System Administrator)	Access to the Portal denied? Yes/No Warning message displayed? Yes/No If Yes, then describe message below or take screenshot:	Pass/Fail			

How do we perform CSV? (8)

EXECUTE TESTING

– The easiest part of the process.

– As usual, all recording should be contemporaneous.

– Should deviations from the protocol or test scripts occur these must be documented and the impact on the validation status considered and justified.

– Should test failures occur these must be investigated, documented and the impact on the validation status considered and justified.

- Is the system fit for purpose?

- Is reconfiguration and retesting required?

How do we perform CSV? (9)

REPORTING

– Each requirement identified for testing must be reported.

– Deviations from the test protocols or scripts must be recorded and justified.

– All test failures should be investigated and corrective actions implemented where necessary.

– Limitations should be described in the final (summary) report.

– There should be a statement of fitness for purpose in the final (summary) report.

How do we perform CSV? (10)

EXAMPLE FINAL REPORT TABLE

- Including a test that had originally failed.

URS #	Test steps required	Acceptance Criteria	Result	Comments
3.1.4	Log into the GCP Portal using an incorrect password on 3 consecutive occasions and then log into the GCP Portal using a correct password. (User role: **Any** except System Administrator)	Access to the GCP Portal /GCLP Drive must be denied on all 4 occasions.	**Pass**	None
3.1.5	Access the change password menu in the My Account tab (sidebar), via the GCP Portal, and change the current password to be the same as the User ID. If this is successful, the **user** is to log-out of the portal and then log back in using the same User ID/Password combination. (User role: **Any** except System Administrator)	The password cannot be changed to match the User ID. Alternatively, the same User ID/Password combination cannot be used to access the portal.	**Pass***	* Initially the test was found to Fail (See Appendix A for details). The GCP Portal had not been configured to prevent the password from matching the User ID or using the same User ID/Password combination to access the portal. The software was reconfigured to correct this issue. The test was then repeated and passed the original acceptance criteria.

Who does what?

ROLES & RESPONSIBILITIES

- – Management (a.k.a. the Process Owner)
  - Ultimately responsible for compliance and operation.
  - Provides adequate resources to support development and operation.
- – System Administrator (a.k.a. the System Owner)
  - Responsible for availability, support, maintenance, security and compliant operation.
- – Subject Matter Experts
  - Responsible for providing scientific input (Technical, Process or Product understanding).

Who does what? (2)

ROLES & RESPONSIBILITIES (CONTINUED)

- End Users
  - Responsible for using the system, reporting issues and identifying improvement opportunities .
  - May also be involved with providing input to the URS and CSV testing.

- IT Department
  - Responsible for providing a controlled (stable) platform or network for the computerised system to operate from.
  - Responsible for System (Network) Security & Maintenance, Disaster Recovery and Back-up processes.

- QA
  - Responsible for providing an independent role focusing on the quality critical aspects of the system.

It's Validated - What next?

During implementation or operation the following will be required:

- Supporting Documentation and Infrastructure (Support processes/ SOPs/ Forms/ Maintenance/ Change Control/ etc.).

- Training (for the roles required).

- Process for migration from any superceded system.

- Retirement and archiving of the superceded system, data and documentation.
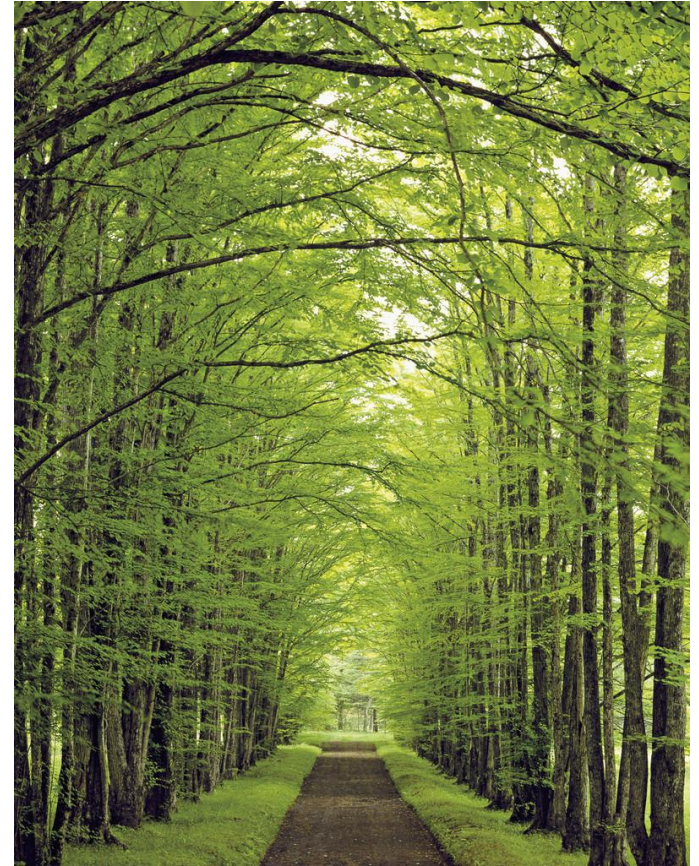
In Summary

DON'T FORGET

- A computerised system is a tool.
- Planning computerised system validation is key.
  - Especially the User Requirement Specification (Identifying what we want).
- Document Everything.
  - Including decision making, risk assessments, test failures and deviations.
- It is a team effort.
  - Many individuals have responsibilities within the process.
- Maintaining the validation status of a system is an on-going process.

References

- **GOOD CLINICAL PRACTICE GUIDE, MHRA, 2012**

- **MHRA GOOD CLINICAL PRACTICE: GUIDANCE ON THE MAINTENANCE OF REGULATORY COMPLIANCE IN LABORATORIES THAT PERFORM THE ANALYSIS OR EVALUATION OF CLINICAL TRIAL SAMPLES, ISSUE 1, JULY 2009**

- **INS-GCP-3 ANNEX III - TO PROCEDURE FOR CONDUCTING GCP INSPECTIONS REQUESTED BY THE EMEA: COMPUTER SYSTEMS**

- **ICH E6 (R1) GUIDELINE 'GUIDELINE FOR GOOD CLINICAL PRACTICE'**

- **ICH Q9 GUIDELINE 'QUALITY RISK MANAGEMENT'**

- **21 CFR PART 11 'ELECTRONIC RECORDS; ELECTRONIC SIGNATURES'**

- **GOOD AUTOMATED MANUFACTURING PRACTICE (GAMP) 5 'A RISK BASED APPROACH TO COMPLIANT GXP COMPUTERISED SYSTEMS'**

Acknowledgements

THANKS TO:

- Jeff Cummings
- CEP QA Team
- Paul Stewart
- Bill Greenhalf
- Rebecca Gallagher
- Richard Sugar
- Hannah Brown