Advisory Notes for Quality Management Systems

Computer Systems Validation (CSV)

Clinical Research Facilities (CRFs) must provide evidence of validation for computer systems used in clinical trials. Computer Systems Validation (CSV) is a regulatory requirement and is important to demonstrate your systems are fit for purpose.

This guidance document aims to demystify computer systems validation and inform CRF Quality Managers and other colleagues responsible for maintaining QA across the UKCRF network on how to carry out the process. Often CSV can be seen as incredibly complicated and technical, or something which can only be completed by qualified IT personnel. However by following a series of simple steps CSV is not nearly as complex as it first appears. In its simplest terms, it involves checking that your computer system does what you expect it to do. You should always keep in mind the following: Is my computer system fit for purpose? CSV provides the evidence to prove that it is.

Who is responsible for carrying out CSV?

The owner of the computerised system should ensure that it is validated if required. Validation tests should ideally be performed by users of the system. Familiarity with the system requirements and functionality is more important than an extensive technical knowledge of software and IT systems. However the involvement of, or review by, IT personnel may be beneficial if available. A QA representative may also provide a level of independent review and approval.

CSV Stages

If you are carrying out CSV for the first time, it can be difficult to know where to start. Resources and guidance available on the topic can include an overwhelming level of detail and technical jargon, which is far beyond the scope of what would normally be required of CRF staff. However, the following key stages provide a straightforward, consistent and logical approach, and should be considered as part of any CSV programme.

Stage 1: Computer Systems Risk Assessment:

Any CSV should commence with a risk assessment. This will help determine whether CSV is required and if so, how much. The most important question to begin with is “Does the system impact participant safety, the validity, integrity and security of the research data, or on any other GCP requirement. An example of a risk assessment template is provided in appendix 1.

Do I need to validate?

The risk assessment will determine if CSV is necessary, as not all software will require validation. A commercially available, non-configurable application that is used for non-critical data may require very little or no validation at all. However, even if no validation is required, this should still be documented in a risk assessment.

How much validation should I do?

If validation is necessary, the risk assessment is also important in determining the level of validation required. This will depend on the function of the system and the nature of the software. Bespoke or customised applications, or applications critical to the safety of participants or the integrity of trial data, will require more extensive validation. The following examples are taken from the MHRA GCP Guide 2012, section 14.5:

Example 1 (off-the-shelf package)

An investigator may use MS Excel to manage the trial data and undertake some simple analysis. There would be an expectation that there is a documented check on formatting of the cells (for example, numeric, dates) and any formulae that have been put into the system. This could simply be recording that the ranges of the cells have been checked, writing down formulae or confirming that the spreadsheet is consistent with the written 'specification' prior to use of the system.

Example 2 (trial-specific configuration)

For the creation of a trial-specific application using a commercial off-the-shelf package (for example, set-up of a trial in an IRT system or an eCRF system), the following validation documentation would be the minimum expected:

- approved specification
- testing documentation for developers and users
- signed validation report
- production of user instructions and training of users
- documented release

Example 3 (bespoke system)

For bespoke application development, more comprehensive validation documentation would be required to demonstrate that the system was fit for purpose.

Stage 2: Computer Systems Validation Master Plan (VMP)

Before commencing the validation process, a CSV Master Plan (VMP) should be written. One key section included in this is the 'User Requirements Specification' (URS). It is important to make a list of all of the requirements you have for the computer system software or hardware in the validation plan. Ideally, this would be done prior to purchasing the software, but this should also be documented retrospectively for all software that has already been purchased. If there is a comprehensive URS associated with the software, then this may be completed in a separate document. The URS should include IT requirements, system scope, security features, audit trail, operational requirements, backup and restore procedures, maintenance requirements, and interface and data migration requirements. Further guidance on these can be found in the example VMP template in appendix 2.

The VMP should list the system functions that will be tested during the validation. You must ensure you cover at a minimum the key functionality you use in the system. It is NOT necessary to validate operations you will never use.

The criteria for Pass/Fail should also be defined as part of the plan, as well as the frequency of repeat testing. The VMP should be reviewed and signed off by an appropriate reviewer (e.g. the CRF Manager or QA Manager).

Installation Testing

Installation testing tests the integrity of the software by installing it on more than one computer and testing that, at a minimum, the main functional tests produce the same expected results.

Some larger and more complex software packages may have their own automated installation validation. This can be run against the software in place of users having to manually carry out the validation test scripts themselves, which can save a lot of time and effort.

Stage 3: Computer Systems Validation Tests

The next stage of the CSV process is to perform the validation tests on the key system functions identified in the VMP. Each step required to perform the function should be tested to ensure the outcome is as expected. All tests must be documented and signed off. This could be on a checklist or an excel spreadsheet (see appendix 4 for example), but someone who is performing the tests should sign and date after each test has been completed. The following could be included:

- date performed
- name and version of software
- name of person performing test
- test description
- expected outcomes
- actual outcomes
- actions taken in the case of failure of validation including the timescale within which they must be resolved

Stage 4: Computer Systems Validation Summary Report

It is important to document the validation process and summarise the outcomes in a Validation Summary Report. The key area for discussion refers to any discrepant results, which must be identified and investigated to determine the cause and the corrective action to be taken. The system owner must ensure that corrective actions are monitored and reviewed to ensure discrepancies have been addressed and changes have been implemented. An example of a CSV Summary Report template is provided in appendix 3.

Re-Testing

CSV is not a one-off event. Re-testing of the system should occur regularly and in particular when there is an update to the software version, or a bug fix. In addition, if the application is to be used in a different setting, e.g. on a different PC, additional CSV may be required.

Records of Validation

All activities related to CSV should be documented appropriately. All records should be retained and should be easily accessible and updated regularly so that they are available for audit and inspection.

Resources

Good Clinical Practice Guide, MHRA (2012)

GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems, ISPE. www.ispe.org

Computer Systems Validation in Clinical Research – A Practical Guide (Edition 2) ACDM. www.acdm.org.uk

IC/S publication/recommendation: 'Good Practices for Computerised Systems in Regulated GxP Environments' (PI 011-3) Sept 2007. Secretariat of the Pharmaceutical Inspection Convention, c/o EFTA Secretariat 9–11, rue de Varembé, CH – 1211 Geneva 20, Switzerland. www.picscheme.org

INS-GCP-3 Annex III to Procedure for conducting GCP inspection requested by the EMEA – Computerised Systems. www.emea.europa.eu

Appendices

Appendix 1: Computer Systems Risk Assessment TEMPLATE

Appendix 2: Validation Master Plan TEMPLATE

Appendix 3: Computer Systems Validation Summary Report TEMPLATE

Appendix 4: Computer Systems Validation Test Sheet TEMPLATE

UKCRF QA Workstream Members

These advisory notes were developed, based on documentation provided by the Edinburgh CRF, by the following members of the QA Workstream group:

- Paul Cross, BRC QA Manager, NIHR Guy's and St Thomas' (*chair*)
- James Gibson, Quality Assurance Lead, Edinburgh CRF (*deputy chair*)
- Sharon Cameron, CRF Deputy Director, Edinburgh CRF (*SMT Link)*
- Emma Deenihan, Quality and Regulatory Affairs Manager, NUI Galway
- Lara Edwards, NIHR Research Programme Manager at University Hospitals Bristol Foundation NHS Trust
- Manju Luckson, Quality Lead, NIHR/Wellcome Trust Manchester CRF
- Alex MacLellan, Quality Assurance Manager, Edinburgh ECMC
- Terese Hale, CRF Nurse Manager, Cardiff CRF
- Ann Ward, Head of Operations and Quality Systems, Surrey CRC

Acknowledgements

The QA Workstream would like to acknowledge the contribution and assistance of the following:

- UKCRF Network Strategic Management Team
- National Institute for Health Research (NIHR)

Appendix 1: Computer Systems Risk Assessment TEMPLATE
(blank copy for local adaptation)

Computer Systems Validation

Risk Assessment

[Insert System Name]

Validation Statement *Complete sections 1 - 3 of the Risk Assessment before you complete the statement below.*			
Sections 1 - 2 of this Risk Assessment have been completed as required, and this system has been assessed as: **HIGH** risk ☐ Full validation of all functions is required. **LOW** risk ☐ Validation of key functions is required. **NO** risk ☐ No further action is required.			
	Printed Name	Signature	Date
System Validator			
System Owner			
IT Representative			
QA Representative			

Note:
Software categories 1 and 2 (operating system and instruments with read-only firmware) are excluded from this assessment. This assessment is only applicable to software in categories 3 - 5, i.e. commercially available, configurable or custom-built software applications.

Section 1: System Details

Hardware Name (if applicable):	
Software Name:	
Version Number: (if this RA applies to more than one version, enter all versions covered)	
Manufacturer / Vendor:	
Department Manager:	
Department:	
Locations (Site & Building):	
Outline of software use:	
Number of installations required:	

Section 2: Do I Need to Validate?

Is the system used to support any of the following activities?	Check Box
1. Non-clinical laboratory studies intended for submission to or review by a regulatory authority?	☐Y ☐N
2. Clinical investigations or studies?	☐Y ☐N
3. Generation of, submissions to, or withdrawal of an application for a clinical trial authorisation?	☐Y ☐N
4. Generation of, submissions to, or withdrawal of an application for marketing authorisation?	☐Y ☐N
5. Training records of personnel involved in the manufacture of drug product or API, or in the conduct of non-clinical, pre-clinical or clinical studies?	☐Y ☐N
6. Backup or storage of records supporting any of the above, in electronic format?	☐Y ☐N
7. Transfer of electronic records supporting any of the above from one GxP system to another?	☐Y ☐N
Complete the appropriate box below according to the responses above: If any response is YES, validation is required - complete Section 3. If all responses are NO, validation is not required - complete and sign off Validation Statement.	
Validation is NOT required: ☐	**Validation IS required:** ☐

Section 3: How Much Validation Should I Do?

Part A: Software Category		Check all that apply
5	Custom software application or custom extensions (e.g. macro, custom modules) to an existing commercial application.	☐
4	Commercially available software configurable using predefined software modules.	☐
3	Commercially available standard non-configurable software package providing an off the shelf solution to a business or regulatory process.	☐

Part B: Regulatory Risk	System Function / Regulatory impact	Check Box
High Impact Data	Data submitted directly to a regulatory authority	☐Y ☐N
	Support to pre- and/or non-clinical laboratory studies	☐Y ☐N
	Clinical trial data from participant or supporting work	☐Y ☐N
Medium & Low Impact Data	In-process monitoring of drug product and APIs	☐Y ☐N
	Supporting data not directly submitted to regulators	☐Y ☐N
Regulatory risk is high if ANY high impact options are YES.		

	Medium & Low Impact Data	High Impact Data
Software Category 4/5	Reduced Validation	**FULL VALIDATION**
Software Category 3	Reduced Validation	Reduced Validation

Full Validation is required where the software is Category 4/5 **AND** the data is High Impact. For all other combinations, reduced validation or testing of key functions only is required.

Appendix 2: Validation Master Plan TEMPLATE
(blank copy for local adaptation)

Computer Systems Validation

Validation Master Plan

[Insert System Name]

Statement: *(delete as applicable)*
This software, as determined in the Risk Assessment document is considered **high / low** risk and therefore requires **full / reduced** validation. This software **requires / does not require** to be installed on multiple PCs.

	Printed Name	Signature	Date
System Validator			
System Owner			
IT Representative			
QA Representative			

1. System Requirements

The purpose of this section is to define the system requirements to enable validation of the system to proceed efficiently.

Requirement Number	Feature	Present Y/N
IT Requirements *(server requirements, printing requirements, etc.)*		
System Scope (*number of users, availability of the application, acceptable downtime, installation on multiple PCs, etc.)*		
Security Features (*login requirements (such as forced unique usernames), password expiry*, *limited password retries, etc.)*		
Audit Trail (*any audit trail requirements. State details such as when and by whom modifications are made to the data/system.)*		
Operational Requirements (*document the functions you require or desire the application to have. You can add multiple tables/sections, potentially breaking the system into key functions required. If you already have the system, this section will help form your test plan.)*		
Backup and Restore (*what are your backup and restore requirements for the data. Specify archive features required.)*		
Operation and Maintenance (*specify how updates are applied and who will maintain the system.)*		
Interface Requirements (*Any links to other systems.)*		
Data Migration Requirements (*Any requirements to import or export data from the system.)*		

2. Validation Plan

This validation plan is written to summarise the validation of the *[insert system name]* system used for *[insert description here]*.

Hardware and Software Categories

Example text:

For standard, centrally managed PC set ups, the Operating System is Category 1 software and the anti-virus is Category 3 (standard software package). Both the hardware and firmware which controls this hardware are also Category 1.

Validation details

Major functions: List major functions to be tested

Function	Test	Frequency*	Timeframe**	Multiple PCs?
				Y/N
				Y/N
				Y/N
				Y/N
				Y/N

* Include triggers for re-testing, for example, major updates or as part of disaster recovery.

** Date by which the testing must be completed, in relation to the date of this document.

Documentation

Validation Plan: This document – this has been developed to specify the validation documentation, requirements and responsibilities.

Test methods and results: Each function of the application will be tested, with results and output being recorded in the **CSV Test Sheet** for the system.

Validation Report: Summarises the retrospective validation of *[insert system name]*.

SOPs: List relevant SOPs

Title	Date	Version

Additional Documents: List documents such as User Requirements and User Manuals.

Title	Date	Version

Appendix 3: Computer Systems Validation Summary Report TEMPLATE
(blank copy for local adaptation)

Computer Systems Validation

Report

[Insert System Name]

	Printed Name	Signature	Date
System Validator			
System Owner			
IT Representative			
QA Representative			

Introduction

This report summarises the retrospective validation of the *[insert system name]*.

Validation Activities

Configuration of Host PC

Name of Feature	Workstation Configuration
Managed desktop?	Y/N
Operating System *(e.g. Windows XP / Vista / 7 / 10, OS X 10.6, Ubuntu)*	
Do you need a username and password to login?	Y/N
Network connection required?	Y/N
Software was installed before validation? *(was the software you're validating already installed)*	Y/N
Computer meets minimum hardware specification as stated in the user manual?	Y/N

Configuration of *[insert system name]*

Users / Access Privileges	*Example text:* *Although initial access to the system has been tested, Software X does not require any form of authentication, nor does it use varying levels of system access.* *Software X requires a login / code / valid license key as authentication. Separate logins / codes / licenses are required to activate different modules in the software.*
Application Configuration	*Example text:* *No changes to the configuration of Software X have been made since installation.* *The default values set at the time Software X was installed can be reconfigured to suit the template requirements.*
Custom Calculations	*Example text:* *No custom calculations / macros are used with Software X.*
Reports	*Example text:* *No reports are produced by Software X.* *Software X generates reports based on input during measurements. Fields to be extrapolated from the data set can be customised and reports can be transferred into an Excel document.*

Execution of Test Scripts

Tests of major functions listed in the Validation Plan were carried out and are recorded in the CSV Test Sheet.

A summary of the tests conducted for each installation can be seen below.

Summary of Test Results

If any test fails this should be noted, along with whether or not the problem needs to be fixed, plans on how it will be fixed and time scales.

Test Script – PC Name	Test Coverage	Results (include any comments)
Test 1	Description	PASS / FAIL
Test 2	Description	PASS / FAIL
Etc.	Etc.	Etc.
Overall Result: **PASS / FAIL**	Date:	

Test Script – PC Name	Test Coverage	Results (include any comments)
Test 1	Description	PASS / FAIL
Test 2	Description	PASS / FAIL
Etc.	Etc.	Etc.
Overall Result: **PASS / FAIL**	Date:	

Appendix 4: Computer Systems Validation Test Sheet TEMPLATE
(blank copy for local adaptation)

Computer Systems Validation Test Sheet						
Test Date:						
Tested By:						
Software Tested:						
Software Version:						
Function Tested:						
Test No.	Test Date	Test Description	Expected Behaviour / Outcome	Actual Behaviour / Outcome	Pass / Fail	Comment
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						