COMPUTER SYSTEMS VALIDATION

2nd Edition

November 2015

Contributors:

John Horncastle	Lead Production Pharmacist, Pharmacy Production Unit, Royal Victoria Infirmary, Newcastle upon Tyne Hospitals NHS Foundation Trust
Alison Beaney	Regional Quality Assurance Specialist, North-East

on behalf of the
NHS Pharmaceutical Quality Assurance Committee

For feedback contact Alison Beaney: alison.beaney@nuth.nhs.uk

Computer Systems Validation

Introduction

The increasing use of electronic systems for patient care has huge potential for streamlining and improving patient care. However these same electronic systems have potential for significant patient harm if they do not function as expected.

This risk can be mitigated or at least controlled via a robust program of system validation starting from the initial procurement stages of a new system and continuing throughout the system's lifecycle.

While the need for bespoke validation may seem onerous, the high level of variability in a modern system means that no two systems are identical. For this reason, although system manufacturers may provide validation packages, such material can only ever provide a basis for validation and should be supplemented with local testing on the actual system in place in the department.

This document is intended to act as a guidance framework on system validation which can be applied to any computerised system. While the contents of the document have their origins in Good Automated Manufacturing Practice (GAMP)[1], the processes can, and indeed should, be applied widely across patient-centred electronic systems such as electronic prescribing systems. Additional guidance is available for all potential areas of use; units making medicines should comply with Annex 11 of EU GMP[2], whilst other guidance is available for electronic prescribing sites (e.g. ISB0160[3]).

This document is written from the perspective of a potential purchaser of a computerised system and follows this pathway. Users who already have a system in place may of course join the pathway at an appropriate point.

What am I trying to achieve?

To confirm that computer hardware and software (collectively termed a computerised system) perform to the standard required delivering an output that meets the user requirements, is accurate and free of errors.

A holistic approach is required for validation of computerised and automated systems. The "System" is not just the software which produces the prescription, label, worksheet etc., but also:

- Computer hardware running the software
- Printers connected to that computer
- Network connecting the system to the wider hospital infrastructure
- People using the system
- SOPs on how to use the system
- Process being performed with / by the system

It is essential that all of these components work as expected otherwise the desired outcome (for example a clear, accurate, legible label to put on a product) cannot be achieved.

Key Considerations

- Where a computerised system replaces a manual operation, there should be no resultant decrease in quality, process control or patient safety. There should be no increase in the overall risk of the process.
- Where a computerised system is part of a wider network, the validation of the system should take into account the effect of the network on the operation of the system, especially with respect to the resilience of the network and any potential for data loss. When changes to the network are made consideration should be given as to the degree of revalidation required. Arrangements should be made to ensure that the accountable person is informed of any relevant problems with, or changes to, the network.
- Wherever possible the support of the organisation's IT department should be sought, with IT staff being seen as external contractors and a suitable written agreement put in place to ensure appropriate continuity of service. Depending on complexity of system and level of support needed, this may take the form of a detailed Technical (Quality) Agreement, or a service level agreement detailing basic quality requirements. At the very least responsibility for notifying key users of proposed changes to systems, software upgrades etc., before the change is made. All changes should be appropriately documented and their impact assessed **before** implementation.
- A standardised approach to validating all computerised systems should be used and documented, for example in a Validation Master Plan.
- The level of resource put into validating a system should be commensurate with the risk posed by system failure. For example, a system which calculates potential drug interactions carries a higher risk of failure than a system for printing delivery labels for ward boxes and hence would need a much greater level of validation effort.
- If the computerised system is replacing a manual process, operation of the two systems in parallel for an appropriate period with comparison of the output of the two systems should constitute part of the validation process.

Example 1 – A cautionary tale

The following example occurred in an American Hospital but is wholly applicable to the UK.

Chain of events

1. The new E-prescribing system was set up with option of ordering in "mg" or "mg/kg" to allow flexibility
2. Doctor original order in mg/kg for 38.6kg patient

"Rx Co-trimoxazole 5mg/kg"
Dose = 193mg

3. Order arrives in Pharmacy for screening, Pharmacist notes that the closest tablet = 160mg – Pharmacist asks doctor to alter prescription to "160mg".
4. Doctor opens original order and types "160" but forgets to change dosing mode to "mg"

- The system had no warning of which prescribing mode was selected
- There were no hard-stops or dose checking routines put in place

Patient received a massive overdose

We need to ask ourselves could this have been foreseen and prevented by:

- Validation of the system – finding the problem before it can cause harm
- Different system design
- User training

Validation Process – For a new system

1. Defining the System

As the computerised system consists of software, hardware and a process which is to be performed using the software, the first step is to decide what the process is that you wish to "computerise" and how this will broadly be achieved. For example, "The department wishes to produce patient-specific labels using a standardised template".

2. Documentation of requirements

Once the overall objective of a new system is defined, the exact requirements of what the system will need to achieve in its operating environment is documented in detail via the creation of a "User Requirement Specification" (URS). This document should take a stepwise approach through the processes which will be performed while using the system in order to identify all possible functionality the end user would like the system to provide.

Particular attention should be given to ensuring the new system can exactly mirror any existing complex manual processes to give the same end result. Areas where electronic systems have been seen to fall short are;

- Multiple dilutions of a starting material to arrive at patient doses (E.g. preparation of paediatric antibiotics which require a lower concentration than provided for by manufacturer instructions)
- Product expiry times shorter than the system allows (E.g. Melphalan with a 90 minute expiry when the system expects expiry in whole-hour increments)
- Allowing staff to split doses for subcutaneous administration for the purposes of patient comfort.

However the URS should not overlook the most basic of functionality as it is has been known for even fundamental points to be lacking in a system as shown by the following example;

Example 2 – Separated by a common language.

A hospital wide electronic prescribing, records and documentation system was being put in use in a large teaching hospital. The entire system was supplied by an American provider and was widely used in the US. When the system was being investigated for suitability by the hospital Pharmacy Department a number of problems were identified.

- Labelling with the direction "***Take half a tablet***" was not possible as standard practice in the US is to write "***Take 0.5 tablets***" – The consequences of poor quality labels in this instance don't even bear thinking about.
- Labelling with the direction "***Take Two Tablets ONCE a day***" was also not possible.

When questioned, the system provider explained that there had been a large number of errors among Spanish speakers with limited command of English who read "ONCE" and interpreted it as the Spanish number 11. Requests to change this functionality for UK systems were refused.

The URS fulfils a number of functions:

- Gives potential system suppliers a means of understanding what the system must do
- Forms the basis for all of the validation which follows

It can be useful to include a scoring system in the URS to rank functionality by level of importance, as unless a completely bespoke system is being produced it is unlikely that any supplier will be able to meet all of the requirements. Potential scoring systems include:

- The Acronym "MoSCoW" – which defines requirements as:
  - **M**ust Have (Essential Function)
  - **S**hould have (High Priority but not essential)
  - **C**ould have (Desirable but not necessary)
  - **W**ould Like (Would like to see functionality offered in the future)
- A simple assessment of each feature of a system as:
  - Essential
  - Desirable
  - Indifferent

3. Assessment of available solutions and suppliers / manufacturers (Sometimes called Design Qualification)

The URS should then be sent out to potential suppliers to invite them to submit a proposed system, which will meet the requirements stated. On receipt of the manufacturer's functional specification or description of the software (where existing software packages are supplied) an assessment should be made to compare how well the features offered by a system meet the requirements laid out in the URS, making use of the scoring systems defined above to aid decision making and allow a robust choice of supplier.

Once a shortlist of suppliers has been identified it is essential to assess the competency of the suppliers via ***Supplier assessment or audit*** depending on:

- Ability of supplier to demonstrate their quality systems (evidence of a robust quality system (e.g. ISO9001 accreditation) may negate the need for full supplier audit)
- Evidence of strong involvement in an NHS environment (suppliers with evidence of successful installations in a comparable environment are likely to need less rigorous assessment of competence to meet standards).

As with all processes, supplier assessment should follow a risk-based approach with levels of scrutiny being dictated by the criticality of the system being offered. For a bespoke critical system, assessment may take the form of a formal audit of quality systems at a supplier's premises. While for a system with a proven history of use in a comparable environment, assessment via a questionnaire sent to the supplier (postal audit), or visits to appropriate reference sites may be sufficient.

Implementation of a system from a limited pool of suppliers (or a single vendor)

Where the system is chosen from a limited pool of options (or indeed is the only option available), and has evidence of successful use in a similar NHS environment, the URS is still a key document, however it may be possible to draw much of its content from documentation provided by the system vendor, with requirements being based largely on the functionality of the available system.

4. Installation Qualification (IQ) – Does it switch on?

Once the software is installed the first step of validation is to ensure:

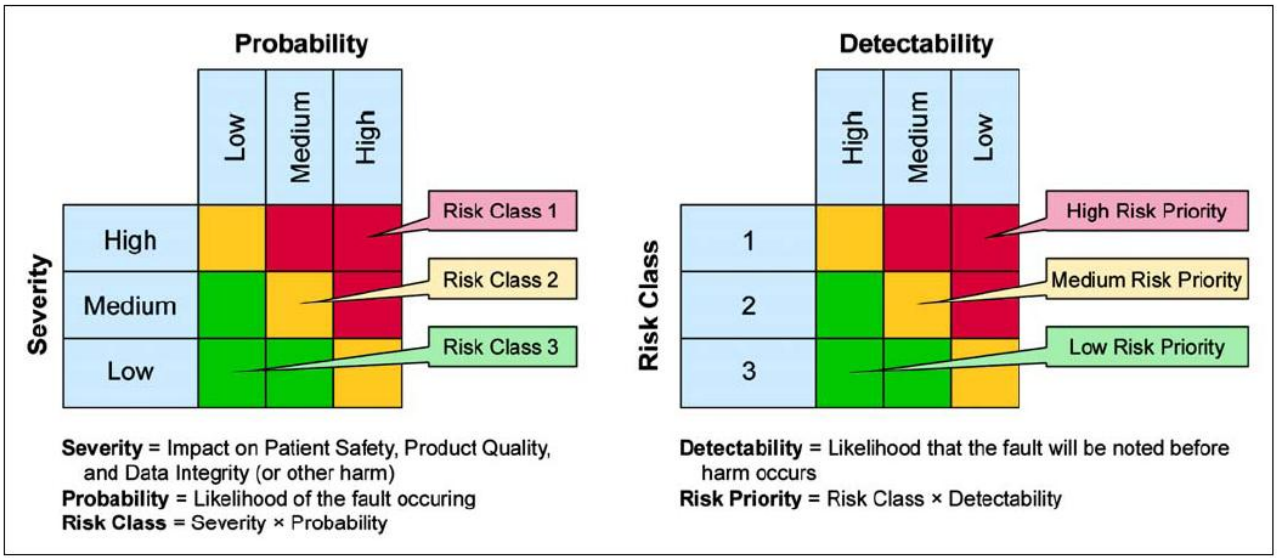
- The correct version of application software is available on all appropriate computers
- Correct version of Server software (where applicable) is installed and accessible by the local client machines
- Users are able to gain access to the software throughout the facility (according to software licence arrangements)
- It is possible to create security accounts for users with access privileges appropriate to their role
- Creation of labels, worksheets, reports, prescriptions, and similar system outputs to match currently approved hard-copy or electronic versions and the standard departmental document format.
- Creation / alteration of system descriptors to match existing ward and department identifiers as appropriate.

5. Operational Qualification (OQ) – Do all functions work correctly on your site?

The key functional requirements of the system identified in the URS should undergo a risk assessment process to evaluate which of these functions have the potential to cause a failure and therefore potential patient harm.

Each of the aspects of the system should be taken in turn and evaluated as to potential failure modes. To facilitate this process it is sometimes useful to employ tools such as FMEA (Failure Mode and Effect Analysis) or SWIFT (Structured What-IF Technique) to systematically identify potential routes of failure in a system.

Once identified the potential routes of failure should then undergo risk assessment as follows:



Those areas which have a medium - high risk of failure, or a significant impact in the event of failure, should be made the subject of a series of stepwise test cases written to stress the system in a simulation of "in-use" conditions in order to prove that the configuration of the system is such that the error/failure either cannot occur, or would be readily detected should it ever occur. All test cases should be carried out in triplicate, with a 100% pass rate expected. Any deviation from expected behaviour should be recorded in a deviation report, to ensure remedial action is taken before the system is put into active use.

A word on "Off the shelf" validation packages

Beware manufacturers' "Validation Packages". They prove that the system worked:

- In the manufacturer's office
- On their system
- With their particular setup and configuration
  But will it work like that in YOUR installation?

Example 3 – Making sure a system works in your location can be "One L of a difference"

An established US system was installed in a large UK hospital, and came pre-programmed with a rule to send electronic adverse drug reaction reports to the MHRA when a medication was discontinued or cancelled under certain specified conditions.

The rule came programmed as follows (N.B. system coding has been removed);

- **Trigger this event when order status is;**
  - **"Discontinued"**
  - **"Canceled"**

AND

- **Triggering request contains an order with status of Discontinued; Canceled and Cancel Reason, that is listed in Adverse Drug Reaction**

OR

- **Triggering request contains an order with status of Discontinued and a Discontinue Reason, that is listed in Adverse Drug Reaction**

The rule had been created by the American system designers and worked for all US sites using the system to send similar reports to the FDA.

However the UK hospital noticed that the reports only ever got sent due to "discontinued" medicines and not for those marked as "Cancelled"

Can you spot the problem?

- The American sites CANCE**L**ED the medication
- The UK site CANCE**LL**ED the medication.

The System worked when tested in the US….but in the UK we saw "one L" of a difference in testing!

OQ Example.

Functionality

A new interface for the electronic prescribing system is proposed. The system will take results from the Trust Pathology system and populate the patient record. It will also be possible for medical staff to enter biochemical result data manually.

Potential Failure Modes

- Manually entered data overwrites data from the interface

  Risk score – ***Probability*** = Medium ***Severity*** = High ***Detectability*** = Medium ≡ High Risk; Evaluate via Test case 1

- Manual entries are not saved

  Risk score – ***Probability*** = Medium ***Severity*** = High ***Detectability*** = Medium ≡ High Risk; Evaluate via Test case 1

- Data via either route is not "sense checked" leading to gross error which could affect treatment decisions

  Risk score – ***Probability*** = Medium ***Severity*** = Medium ***Detectability*** = Medium ≡ Medium Risk; Evaluate via Test case 2

Proposed Test Cases

1.

A. Set up a test system with links established between pathology and e-prescribing system, send sample results data through the interface.
B. Ensure results have populated correctly.
C. Manually annotate a patient record with a new result, ensure the manual entry is retained.
D. Make a manual result entry into a new patient record which has received no data from the interface. Send a result set for the same patient via the interface; ensure that the most recent result is visible.
E. Ensure that any changes to results are obvious and form part of a full audit trail.

2.

A. In the lab system enter a Sodium value of 12mmol/L for patient X – ensure system challenges entry with a suitable warning. Change value to 1450mmol/L, system should challenge entry with suitable warning. Acknowledge the warning and save the high result. Repeat for excessively high and low values for Creatinine, and Thyroid stimulating hormone. Finally enter correct values and ensure system accepts the entered value.
B. In the E-prescribing patient record screen repeat test A, ensure system challenges each erroneous entry with the option to accept entered value or make an alteration.
C. Check system audit logs, ensure that acceptance of high / low results is recorded in the audit trail and is attributable to the user accepting the warnings.

6. Performance Qualification (PQ)

PQ is the final step in the initial validation effort and encompasses testing of the system once it is under actual "In-use" conditions to ensure that it continues to operate as expected. As a minimum testing should cover:

- Security – ensure users can only access functions appropriate to their role. Ideally an audit trail should be present recording all attempts at access to the system (successful or not).
- System accessibility – to ensure that the software remains responsive when in use by several concurrent users.
- Data integrity - ensure that information input by one operator can be retrieved by another operator at a later date. Also ensure that changes to data can only be made in appropriate circumstances, and that any such alteration leaves an audit trail which leads back to the user involved.

Choice and content of test cases should be guided by risk assessment of potential failure modes and likely to be a mixture of tests used during the OQ stage and specific PQ stepwise test cases created to verify functionality of software in an "in-use" state (e.g. load testing of the system with multiple operators using functions at the same time).

7. Change Control and Performance Requalification

Throughout the operational life of the system it is likely that updates to the software will be applied and alterations made to its configuration. Any such changes should be handled through a documented change control mechanism to ensure that changes over time do not cause the system to diverge from its validated state. In response to updates or to ensure maintenance of the validated state, periodic re-validation is required:

- Where alterations have been made to critical software components (as assessed through change control mechanisms)
- At regular intervals not exceeding every three years (using a subset of the original OQ / PQ test cases)

In circumstances where site-specific data is entered into a system (for example local treatment regimens), users should ensure that this data remains intact and has not been overwritten or corrupted following any system upgrades or maintenance.

8. Continuity Planning / Disaster Recovery

Failure of the hardware or software supporting a computerised system is a very real possibility, resulting in the system becoming unavailable for use. As function of the computerised system is potentially critical to ensuring continuity of care, there is a need for a plan to be in place for each computerised system to enable work to continue as promptly as possible following system failure. Therefore each system should have:

- A method of running the system from backup data which mirrors "normal" functionality.
- An approved written procedure of how to bring the backup system into use.
- Documentary evidence that this plan has been tested as effective.

Such capability should ideally be written into the URS so that the backup system is an integral part of the overall system and can be tested as such.

9. System Succession Planning

At a point in the future it is likely that current computerised systems will be superseded by newer software better able to support the processes of the business. At this time validation activities will be required to ensure:

- Records and data stored in the outgoing system continue to be accessible after retirement of the software

Or

- Records and data can be reliably transferred into the new system and continue to be interrogated.

10. Documentation

Once all validation activities are completed, each validated system will have a set of documentation comprising:

- User requirement specification
- Record of risk assessment carried out against requirements
- System Validation Report to include:
  - Detail of IQ test results
  - OQ protocol (comprising a full set of completed test cases)
  - Traceability matrix (tying together risk assessment outcomes with OQ test cases)
  - PQ Protocol (with results of “In-Use” testing performed)
- A system description detailing:
  - Principles, objectives, and scope of the computerised system
  - System topology (listing computers, and associated servers, networks etc.)
  - Security measures (including full listing of current user permissions)
  - Interfaces to other systems
- Record of requests for changes to the system
- Training records: User training is a key part of any system and records should be kept of all staff trained to use the system and the level of permissions assigned to that user following training. Delivery of training should make use of a range of trainers and not rely solely on the system expert to ensure information is presented in a form understood by all users.

The validation methods and activities for all computerised systems present in a unit should be detailed in an over-arching document (sometimes referred to as a “Computerised System Validation Master Plan” (CSVMP))

References

1. GAMP-5 A Risk-Based Approach to Compliant GxP Computerized Systems International Society for Pharmaceutical Engineering. http://www.ispe.org/gamp-good-practice-guides
2. EU GMP http://ec.europa.eu/health/documents/eudralex/vol-4/index_en.htm
3. ISB0160 Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems. http://www.hscic.gov.uk/isce/publication/isb0160

Document History	Issue date and reason for change
Version 1	Issued
Version 2	Issued November 2015 - updated to current practice and scope widened e.g. to electronic prescribing. Worked examples included
Version 3	
Version 4	