

# Computer validation - Starting on the right track

Author: Ian Lucas, Director, SeerPharma, Melbourne

May 2010

There is no silver bullet to ensure that your validation projects will be successful, but using a structured methodology and a science based risk assessment process, the chances of determining the correct ordering of activities will be greatly enhanced.



SeerPharma®  
CONFIDENCE IN COMPLIANCE

Most of us follow a professional sporting team. Each year we start the season with hope and enthusiasm that 'this year' will be 'our year'. Have our recruiters and management assembled the right mix of youth and experience and will they be coached to their strengths? Is the framework in place to raise our odds of success ?

In professional sport there is no guarantee of success as there are many opponents, all with the same focus on winning. There is one certainty however. If all the key factors aren't addressed (right mix of players, good leadership and a framework for success), then failure is certain. These factors are outside the influence of the average supporter.

Unfortunately, some companies approach the implementation of computerized systems with a similar attitude, hope and enthusiasm, but without addressing the other elements within their control; right team members, good project manager and a sound computer validation framework.

Obviously, having experienced and trained team members and project managers need to be assessed per project (and supplemented with external resources as required), but this paper describes a framework for getting started on the right track.

Firstly, there must be an easily understood and agreed definition on what computer validation means. This should be based around 'Assuring that the system works consistently and reliably to all defined requirements'. This, in itself, raises many questions that we will address in a separate paper.

'Assuring that the system works consistently and reliably to all defined requirements'.

## Change Control

Secondly, there must be a system of change control across all systems; both directly and indirectly affected. Once change control has been implemented and adhered to, an inventory of systems can be collected and reviewed.

Although there are automated tools that can probe networks and report on software implemented, these are not foolproof. The only certain way of establishing this inventory is via a full system audit.

This audit needs to assess all servers, PCs, laptops and other devices that are used across the company. An up to date network diagram can assist with this exercise. The output of this audit will be a preliminary inventory of systems. This needs to detail each functional system rather than just the software tools used (e.g. inventory reconciliation spreadsheet rather than Excel).

Initially, this will just be a list of all systems, but it can be used to provide and report on key attributes that are needed for ongoing validation and auditability of systems.

These attributes can contain:

- System name and ID – used for identification
- System family – type of system used to define a standard approach and recommended set of validation activities and documents to produce
- Business owner – named individual or position responsible for the functional requirements and continued operation of the system
- System owner – named individual or position responsible for the technical requirements and continued operation of the system
- Risk assessment number and priority – established through a checklist of questions that objectively assess and rank the system relative to other systems (see below for more details)
- Next key activity date – this is either the next review date for the system (for validated systems) or the proposed date that the system will be validated by. For a review, the business owner and system owner should meet with other key stakeholders and assess the system against defined criteria. The output should be, minimally, a formal report and an updating of the next review date.
- Other attributes, such as the network directory where the system documentation can be found can be added to the inventory.

## Objective Risk Assessment

As mentioned above, the approach to assessing the overall inherent risk of each system must be based on objective methodology. Questions regarding all key aspects of the system should be determined, assigning weightings (assuming different questions can have different importance to the overall risk assessment) and multi-choice answers and scores agreed. Relevant system user groups should be highlighted per question and these asked to answer and give justification for each answer per system.

“the approach to assessing the overall inherent risk of each system must be based on objective methodology.”

Areas such as: GAMP system category, complexity of system, size of system, number of users, number of changes per annum, ease of use, number of issues, training provision, support provision as well as business financial risk should be assessed.

Each question should be answered by the relevant user group e.g. operations, IT, management multiplied by the weighting factor associated with that question, usually 1-4, and then summed together to give an overall system score.

By performing this assessment on many systems using the same checklist, risk ranges can be determined e.g. 1-80 = very low, 81-120=low, 121-170=moderate, 171-210=high, 211-300=very high.

Risk priorities can then be set per system and an overall remediation plan developed.

Risk priorities can then be set per system and an overall remediation plan developed.

By reviewing each system's risk assessment, some immediate actions can be performed to reduce risks prior to any project actions.

The remediation plan may not be just as simple as performing validation activities on the highest ranked systems.

Factors such as the expected life of each system, upgrade strategies and business direction need to be considered along with the risk ranking to determine the order of validation activities and the amount of effort per system.

The order of systems should be justified in the remediation plan and the amount of effort should be justified in each system's validation plan.

There is no silver bullet to ensure that your validation projects will be successful, but using a structured methodology and a science based risk assessment process, the chances of determining the correct ordering of activities will be greatly enhanced.

---

### About the author:

Ian Lucas, Director SeerPharma

Ian has over 20 years experience in the pharmaceutical industry developing and implementing software solutions. He has designed and developed company wide MES (Manufacturing Execution Systems) and batch document management systems. As manager of the iQA (Integrated Quality Assurance) software business unit he gets involved with project management and technical development of dealing with third party software companies and delivery to clients.

Ian also provides Computer Validation consulting advice, and develops and delivers computer validation training courses. He has been a regular presenter at international conferences on practical approaches to computer validation.

AUSTRALIA

SeerPharma Pty Ltd

Melbourne (Head Office)

Level 1, 38 – 40 Prospect St.,  
Box Hill, Victoria, Australia 3128

Phone: + 61 3 9897 1990

Fax: + 61 3 9897 1984

Sydney

Level 1, 564 Princess Hwy,  
Rockdale, NSW, Australia 2216

Phone: + 61 2 9597 9947

Fax: + 61 2 9597 9943

SINGAPORE

SeerPharma (Singapore) Pte Ltd

10 Anson Road,  
#35 – 09 International Plaza  
Singapore 079903

Phone: + 65 6774 5800

Fax: + 65 6774 6800

UNITED KINGDOM

SeerPharma (UK) Ltd

P.O. Box63  
York YO1 1WY,  
United Kingdom

Phone: + 44 1347 833 101

Fax: + 44 1347 838 011

[www.seerpharma.com](http://www.seerpharma.com)