Procedure

1. General Approach

Computerised System Validation is the process of:

"Establishing documented evidence which provides a high degree of assurance that a computerised system will consistently function in accordance with its pre-determined specifications and quality attributes throughout its lifecycle."

The inherent complexity of software presents major challenges when attempting to establish such assurance. It is usually impossible to test every potential combination of input, output and function of a system. Consequently, it is difficult to gain assurance by depending on post-development testing and qualification activities alone. The intention of this SOP is to build assurance by the management of:

Design – using a structured process to specify the intended outcomes of an activity

Quality – using a documented process to trace and approve the deliverables of each activity

Risk – taking an approach that focuses efforts on the areas that are most critical

Lifecycle – maintaining a system from its original concept to eventual retirement from use

Commonly used acronyms:

ER/ES	Electronic Records/Electronic Signatures
FAT	Factory Acceptance Test (i.e. Acceptance Testing at the supplier's premises)
FS	Functional Specification
GAMP	"Good Automated Manufacturing Practice" a guidance document by ISPE
GxP	The range of good practices i.e. • GMP (Good Manufacturing Practices), • GLP (Good Laboratory Practices), • GCP (Good Clinical Practices), • GDP (Good Distribution Practice).
PLC	Programmable Logic Controller
SAT	Site Acceptance Test (i.e. Acceptance Testing within the site environment)
SDS	Software Design Specification
SMDS	Software Module Design Specification
URS	User Requirements Specification

2. Validation Process

The Validation process envisaged by this SOP is prospective and encompasses the entire life of the Computerised System, from initiation onwards. It includes many activities in common with other Validation and Project activities. A typical lifecycle is made up of Planning, Specification, Design, Construction, Testing, Installation, Acceptance, Operation and De-commissioning. The activities in these phases are illustrated in Figure 1 and outlined below. Appendix 1 also summarises these activities and refers to related SOPs and guidance within the GAMP document. (Note: compliance with this SOP is the expected standard. GAMP is a useful reference, however other approaches may be acceptable).

should be written in a manner that allows requirements to be verified, (e.g. by inspection or testing).

Specifications should be subject to documented review processes prior to implementation. Ideally this will include approval by the site management. This review should address the completeness of design, (i.e. are all the **URS** functions addressed) and the integrity of design (i.e. what are risks of potential failures in this design). SOP **VAL 055** identifies a number of methods for Risk Assessment and Design Review that should be considered for use in this process. It is expected that site analysis will be to the Functional Specification level; the supplier may manage more detailed analysis.

Developers should establish suitable techniques to ensure that the developed or configured software meets the specified requirements. They should implement a Quality Management System to monitor the software development and configuration; maintain specifications throughout the development; and control the deployment of version changes. The supplier should also ensure that programming rules and conventions are followed.

A site representative should monitor progress of the development against an agreed timeline.

The Impact Assessment **(SOP VAL 045)** will identify where review of the actual code is appropriate. This is known as Structural Testing and utilises expertise in programming to assess the code for compliance with technical, (i.e. specified functionality) and quality (i.e. programming standards) requirements. The system programmer must not complete the Structural Testing.

Regulatory authorities may expect to be able to inspect a copy of the source code for application software. Availability may also be critical for long-term support, maintenance and enhancements. Arrangements should be made with the supplier regarding access to the source code. The access arrangement should be recorded in the IQ report.

2.4. Testing, Installation and Acceptance

This phase is a planned process of challenging and evaluating a system, and its components, throughout its development. The Impact Assessment, and any Risk Assessments, will guide the overall scope and depth of testing. **SOP VAL 050** describes the process for functional testing. Each test should be part of an overall strategy that is designed to make the whole process coordinated, efficient and effective. Since it is impossible to test every potential combination of input, output and function of a system, testing should be structured to:

- Consider those aspects that are of critical importance
- Specify what coverage can be achieved
- Find errors in the software (not merely confirm correct operation in normal conditions).

Test Protocols (sometimes called Test Plans, Test Specifications or Test Scripts) should define in detail the areas to be tested, the test data to be used, and the expected results. The **Test Protocols** must be reviewed and approved prior to commencing formal testing. Tests are conducted at various levels, corresponding to the hierarchy of details developed in the specification phase. Documented traceability should be provided between **Test Protocols** and their controlling documents, such as Functional and Design Specifications, to demonstrate complete coverage of specified requirements. This is illustrated in Figure 2.

Testing must be documented as it is performed and this raw data is to be referenced, dated and retained to demonstrate the testing was performed to an agreed standard. Each test result should contain a clear pass or fail statement. All results will be kept, as primary evidence of testing, and so should be filled out with care.

retain the original data as well as that associated with the change. Any 'audit-trail' produced is to form an integral part of the data record, (i.e. not a separate file). Ideally, measures should be provided to ensure the uniqueness, authenticity and appropriateness of a user-identity.

Some GxP data entry may only require the lowest level of control, (e.g. selecting a machine set-up); other data, the maximum, (e.g. entering a dispensed weight, batch number, batch release decision). The appropriate level of control must be determined as part of the system design and included in the development and testing program. To support this decision, a risk assessment of the criticality of the data is recommended.

Evidence of the review and authorisation of GxP data must be maintained with the master record. This may not require the generation of an associated electronic 'audit-trail' or authorisation. If a record is generated on a computer solely for use in its printed form, (e.g. a SOP produced on a Word processor), the hand-signed paper-record may be considered the 'master'. To be consistent with such a decision the distribution, access and use of any electronic image must be restricted. The Business System Owner should decide which format (i.e. paper or electronic) is to be treated as the 'master' and develop procedures that document and align with this decision.

The introduction of a Computerised System must not compromise the reliability of records that support the assurance of product quality. Record reliability should comprises four separate attributes:

- Accuracy: Data is factually correct; free from error, defect or misrepresentation
- Authenticity: Data is genuinely sourced from the reputed author, device or origin. May include the ability to uniquely trace the data to that entity.
- Availability: Data is suitable or ready for timely, future, authorised use. May include restriction of access to intended purposes / users.
- Integrity: Data is complete and entire; not altered in an unauthorised, unanticipated or unintentional manner.

SOP VAL 060 outlines the risk assessment process to verify these reliability attributes where computerised systems create, process, use or store data that has GMP impact. This process confirms the adequacy of control measures (management, technical and operational) employed by a system to support the record reliability.

3.4. Retrospective Validation / Legacy Systems

Validation of an existing system, whether it was purchased or internally developed, is called retrospective validation.
Retrospective validation is employed:

- When a system not previously validated is allocated to GxP duties.
- When a system that was validated has lapsed to a non-validated status (including when the standard of
- validation performed is no longer considered adequate).

In general, where retrospective validation is required it will be based (as much as possible) on recovering the equivalent documents for prospective validation,
(i.e. reverse engineering). The effort required to generate these documents depends on:

- The adequacy of existing documentation
- The degree of system customisation
- The intention for future changes

The process for identifying this work is illustrated in Figure 3.

