Information Technology (IT)

IT team is responsible for ensuring that the validation studies accurately reflect the operation of the system, is practical, logical and achievable. IT is also responsible for supplying resources to assist with computer validation studies where required. IT also provide technical expertise and support for systems reliant on infrastructure and software development and testing and are responsible for ensuring that all GMP networks are validated and that all existing networks are maintained in a validated state.

Quality Assurance

Quality Assurance is responsible for ensuring that the GMP aspects of the computer validation program are in accordance with relevant procedures and that critical parameters and report conclusions are supported.

5.0 HARDWARE AND SOFTWARE CATEGORIES

The depth and scope of validation activities required for a particular system will depend on the type of hardware and software installed and on the quality of the software development and testing and will be detailed in the impact (risk) assessment. Hardware and software is divided into the following categories:

5.1 Hardware

Hardware is divided into 2 categories:

5.1.1 Category 1 Standard Hardware Components

Standard hardware components should be documented including manufacturer or supplier details, and version number. Hardware Acceptance or IQ should verify installation and connection of components. The model, version number and where applicable serial number, of pre-assembled hardware should be recorded. Pre assembled hardware that is sealed does not have to be disassembled if this breaks warranty. In such cases the hardware details can be taken from the hardware data sheet or other specification material.

5.1.2 Category 2 – Custom Built Hardware Components

These requirements are in addition to those of category 1 components. Bespoke (custom built) items of hardware should have a design specification and be subject to acceptance testing. A supplier audit should be performed for bespoke hardware development. Assembled system using bespoke hardware from different sources require verification confirming compatibility of interconnected hardware components. Any hardware configuration should be defined in the design documentation and verified in the IQ.

5.2 Software

Software is divided into 5 categories. The validation approach and minimum requirements are dependant on the category and GMP impact of the system.

information such as bug reports or reviews shall be documented and approved by the Site Validation Committee.

An evaluation shall be performed and documented that addresses the support and recovery of each system to ensure business continuity in the event that the developer is no longer able to provide support services.

6.3.4 Validation Project Plan (VPP)

A Validation Project Plan (VPP) shall be prepared for computer validation projects. The VPP shall reference the design documents and shall define as a minimum the intended use, principle hardware and software components, validation scope and approach, system boundaries, responsibilities (including Vendor/Contractor/Consultants), the validation documentation to be prepared and the deliverables.

The validation approach will depend on the software/hardware category, complexity and GxP criticality of the computerized application, which is determined by the impact assessment. The result from the assessment will provide the basis for the validation work effort and can be documented in the VPP or for a small system, or minor change in the validation protocol.

6.4 Design Phase of Lifecycle

6.4.1 Functional Specification (FS)

The FS shall be prepared by the system developers and shall describe how the system will function. The FS shall identify the process and functions to be provided by the computerized system in order to meet the requirements defined in the URS. The FS must be maintained current and reflect the system as implemented. The FS for configurable software packages shall be derived from the FS obtained from the system supplier. Where the system developer FS is not available, the FS shall be derived from the vendor-supplied manuals. The FS links to Operational Qualification which tests all the functions specified. The FRS should be approved at minimum by the system owner and the Quality Authority and maintained as a controlled document.

6.4.2 Design Specification (DS)

Design Specifications shall be prepared by the developers and IT/Engineering as required. Design Specifications shall specify minimum requirements for system hardware and system software, or ancillary software tools and the baseline configuration. This stage identifies how the System will meet the FS. The DS must be maintained current and reflect the system as implemented. The DS shall be approved at minimum by the system owner and the Quality Authority. Design specifications for operating systems, standard and configurable software packages shall consist of the documentation of the system configuration.

6.4.3 Design Qualification

6.7.2 Installation Qualification (IQ)

The purpose of the Installation Qualification is to verify and document that all the key aspects of the hardware and software installation, including operating system details adhere to approved Design Specifications (including Hardware and Software Design Specifications if applicable), manufacturer's recommendations and environmental conditions. An IQ protocol shall be prepared and will define the level of validation required. The IQ protocol may be separate for hardware and software. IQ must be performed in the production environment. If a validation environment is used for OQ, then IQ must also be performed in the validation environment, to demonstrate the equivalence of the validation environment with the production environment.

6.7.3 Operational Qualification (OQ)

The purpose of the OQ is to verify and document that the individual and integrated components of the System performs reliably and consistently within specified operating ranges as stated in the Functional Specification. OQ testing will be based on the Impact Assessment. OQ testing shall be conducted in a production environment or a validation environment that has been demonstrated to be equivalent to the production environment. An OQ protocol shall be prepared for each of the Systems and will define the level of verification required.

Operating software will be indirectly tested during OQ. Therefore OQ should include at minimum, security, time, date and network conductivity to qualify the Operating Software. Changes to Operating Software shall be assessed for qualification requirements.

There may be overlap between the testing performed at the System Integration Testing or Site Acceptance Testing stages. At the OQ stage it is not necessary to repeat tests that were performed as part of the Integration or Site Acceptance Tests. These documents may be referenced and reviewed as part of the Operational Qualification provided that the vendor audit demonstrates that the software is produced to a quality system and that the level and quality of testing and documentation of testing is acceptable to the Validation and Quality group.

6.7.4 Performance Qualification (PQ)

The purpose of the PQ is to challenge the fully configured release of the System in its normal integrated environment. A protocol shall be prepared which will verify the performance of the System in accordance with the approved URS, Standard Operating Procedures and related documentation. Testing will be developed to challenge the System as it is used and operated under routine conditions and environmental parameters. This includes the review of each procedure that interfaces with the System and provides evidence that the procedures are in existence, current, applicable and being followed. Sections of the PQ can be incorporated into the OQ for some Systems. PQ testing shall be performed in the production environment.

- Computerized System Operation, Start up and Shutdown
- Computerized System Administration, Access Control and Security
- Backup, Archiving and Restoration
- Change Control and Configuration Management
- Error Handling
- Disaster and Recovery Planning

8.4 Periodic Evaluation

Periodic reviews should focus on system reliability, repeatability, performance and diagnostic data, the satisfactory provision of critical data to support the batch record (if relevant), and the accuracy and use of SOPs. Periodic review should be performed at least every two years by IT. The validated status will be verified as a minimum via preventative maintenance, review of software and hardware change control logs, access logs, error logs and current documentation supporting the System.

8.5 Service Level Agreement (SLA)

An SLA shall be established with developers of custom of configurable software packages to ensure on-going support.

8.6 Maintaining the Validated State

All systems once validated will be maintained in a validated state through the life cycle of the process/ system. Maintaining the validated state will be achieved by change control, re-qualification, training, SOPs, calibration and engineering maintenance programs.

8.7 Training

Training on the computer system will be performed as part of the Qualification. All system operators will be trained prior to using the system. Training should also be provided following system changes.

All personnel (including external resources) with responsibility for the development, maintenance, validation testing and use of computerized systems or review and approval of computerized systems validation documentation shall be trained and qualified. All training shall be documented. Training includes SOP training, job function training and training in GMP regulations

8.8 Security

System security including physical security where necessary will be applied to all computer systems. System security will be defined in relevant SOPs and validated in the qualification documentation. Security should be such that the computer hardware and software is protected from accidental or malicious access, use, modification, destruction or disclosure.

A hierarchy of permitted access shall be established according to user need and software ability. Suitable methods of preventing unauthorized entry shall be available, such as pass cards or

