PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 011-3
25 September 2007

PIC/S GUIDANCE

GOOD PRACTICES FOR COMPUTERISED SYSTEMS IN REGULATED "GXP" ENVIRONMENTS

Editor: PIC/S Secretariat

e-mail: info@picscheme.org
web site: http://www.picscheme.org

TABLE OF CONTENTS

Page

1. DOCUMENT HISTORY

Adoption by PIC/S Committee	2-3 June 2003
Entry into force	1 September 2003

PART ONE - PREAMBLE

2. PURPOSE

2.1 The PIC/S Guide to Good Manufacturing Practices is the basis for GMP inspections. In particular its Annex 11, 'Computerised Systems' is used when inspecting such systems.

2.2 The purpose of this document is to provide recommendations and background information concerning computerised systems that will be of assistance to inspectors for training purposes and during the inspection of computerised systems. The document will be of assistance to all 'Good Practice' Inspectors responsible for inspecting applications in the regulated pharmaceutical sector[1]; hence the use of the acronym 'GxP' in the title. It is recognised that not all companies subjected to GLP inspections are linked to the regulated pharmaceutical sector. However, it is considered that the guidance contained within this PIC/S document may also be beneficial to companies subjected to other regulatory frameworks and GLP inspection.

2.3 GDP defines the scope of compliance requirements for wholesaling and distribution practice. Where automated systems and electronic records are used for such applications then inspectors will expect such regulated users to have in place the sorts of controls and disciplines outlined in this document, or a best practice alternative. Vertically integrated companies (R&D, manufacturing and distribution) will already apply such controls and compliance measures.

2.4 International regulatory agencies have collaborated to produce this harmonised guidance for the implementation, management and operation of computerised systems. It is intended as a reference for regulated users, including their suppliers, in addition to regulatory inspectors and investigators.

2.5 This guidance document is intended to provide a logical explanation of the basic requirements for the implementation, validation and operation of computerised systems. Additionally, the document may be adapted to identify the criteria that would be expected to be considered if a regulated user, or a regulatory agency, were to conduct an inspection of the implemented computerised system(s), against GxP compliance requirements and/or perceived risks.

2.6 This guidance document provides details of good practices, which should support new technology and technical innovations.

---

[1] Throughout this document the 'users' (owners of the good practice computerised systems being inspected) are collectively referred to as 'regulated users' for clarity.

2.7 It should be noted that it is important for national legislation to be referred to when determining the extent to which the provisions laid down in this document may be applicable.

2.8 An auditor or an inspector may wish to consider *evidence for compliance* as indicated in *italicised text* throughout this document.

2.9 It is to be hoped that the PIC/S Expert Circle on Computerised Systems will build on this consensus reference document, to deliver simplified training and aide memoires for the inspection of common GxP systems, as well as sector specific applications. As technology continues its relentless advance the Expert Circle could also provide interpretation of GxP and recommend changes, if appropriate. Such materials could provide further sub-set appendices to Section 24 ('Inspection tabulated checklists and aide memoires').

2.10 Some repetition is inevitable in a document that has evolved over many years and through various working party multinational iterations. It is not intended that this document is read from cover to cover, but should be 'dipped into' as a reference source when needed and for that reason some sections have to stand-alone.

3. SCOPE

3.1 It is acknowledged that the field of computer technology continues to develop at a considerable speed and the regulated user has to ensure that the software and systems have been developed to best engineering practices in a quality assured manner. It will be for regulated users to define relevant applications, impacted business units and corresponding deliverables for such applications. This document sheds some light on the techniques and controls required for this.

3.2 At the time of issue this document reflected the current state of the art. It is not intended to be a barrier to technical innovation or the pursuit of excellence. The advice in this Guidance is not mandatory for industry. However, industry should consider these recommendations as appropriate.

3.3 For hardware, peripherals, integrated process links and system functionality in general, the controls and testing arrangements are by comparison to software, fairly mature, logically more visible and the failure modes more predictable.

3.4 As a result, we have tried to keep the contents of this document practical and principle-oriented, to ensure that it retains relevance for as long as possible. However, value judgements and consensus between parties can be difficult to achieve at times in this complicated field.

3.5 The scope of the document is broad, covering necessary steps and the documentation needed for the implementation and validation of a computerised system. Management of such projects requires the linking[2] of important aspects of management policies, documentation and record systems embracing the

[2] For successful project management these links should be established between the supplier(s) [developer(s) and producer(s) of individual components or complete computerised system] and the regulated user [purchaser and user of the computerised system].

respective professional disciplines involved in the development and use of the computerised system.

3.6 Of necessity this guidance contains some 'how to' achieve GxP compliance advice for suppliers and developers of software and automated systems, in addition to guidance for the regulated users. This is because of the iterative nature of software development and the requirement for quality and functionality to be built into the software in a disciplined manner, to ensure structural integrity, consistency, robustness and reliability. This will often be outside of the direct control of the regulated user (as purchaser/customer). There will normally be a need to manage and control the split responsibilities of contracted suppliers (whether in-house or external party) and regulated user businesses (customers), for project management, product specifications, quality assurance standards and performance.

3.7 This document also identifies the important aspects of validation of computerised systems. Descriptions of strategies that may be used for different categories of computer systems are described as well as identifying the approach that might be taken for the retrospective validation of legacy (old) systems. (see in particular Sections 4.5 and 6.2 (Figure:1) and 16 of this document).

3.8 PIC/S considers that adoption of the principles, guidance, reporting and life cycle documentation best practices, outlined in this document, will enable users of computerised systems to establish quality assurance systems and records capable of demonstrating compliance with current GxP requirements and related guidance.

4. INTRODUCTION

4.1 The structure of the document is designed to identify discrete subsections and their interrelationship within the principal topics concerning the implementation, validation and operation of computerised systems. A reference section, together with a glossary of terms commonly used in this industry sector will be found at the end of this document. Section 26 'Further Reading' suggests a number of textbooks, technical reports and guidelines that amplify the science, technology and practices underpinning this guideline. The 1994 publication by Stokes et al (Further Reading Ref: 1) provides insight into the requirements for computerised systems in GCP, GLP and GMP, together with a historical perspective on validation and international regulatory requirements.

4.2 In recent years there has been an increasing trend to integrate electronic record and business management systems across all operational areas. In the future it is expected that our reliance on computer systems will continue to grow, rather than diminish. The use of validated, effective, GxP controlled computerised systems should provide enhancements in the quality assurance of regulated materials/products and associated data/information management. The extent of the validation effort and control arrangements should not be underestimated and a harmonised approach by industry and regulators is beneficial.

4.3 Commercial 'off the shelf', 'standard', or proprietary systems can be particularly difficult to assess from a quality and performance point of view. For GxP

regulated applications it is essential for the regulated user to *define a requirement specification* prior to selection and to carry out a properly *documented supplier assessment and risk analysis* for the various system options. Information for such exercises may come from *supplier audits* and research into the supplier's product versions in the user community and literature. This risk-based approach is one way for a firm to demonstrate that they have applied a controlled methodology, to determine the degree of assurance that a computerised system is fit for purpose. It will certainly be useful *evidence for consideration by an inspector.* (Note: What constitutes a 'critical application' may vary considerably, depending on the situation – perhaps more so in GLP than in other disciplines).

4.4 Whilst much of the detailed industry guidance relates to 'bespoke' and configured applications there are a number of tools and assessment techniques recommended for commercial packages and standard automated equipment. Complex automated state of the art processing equipment (such as high output tabletting machinery with in-process monitoring and feedback control functionality), or complex analytical instrumentation, for example, is difficult to assess without the supplier's help. The co-operation of the supplier is essential and it is important for suppliers to anticipate the needs of regulated user's for relevant product development life cycle quality and validation information. Such an approach also provides added value for the automated products. The QA and validation aspects for large automation aspects will inevitably be complex and may be subsumed in major engineering projects activated by the potential regulated user. *Inspectors will be interested in the evidence relating to the firm's assessment of the supplier's critical automated features as well as the traditional engineering, qualification and process performance aspects. Much of the guidance given in the GAMP Guide (Ref: 4), for example, is scaleable to complex projects and equipment with sub-contracted features. (Note: The risk assessment described in '4.3' above should identify critical features and functions for both the project team and the inspector).*

4.5 When a GxP inspector has to assess an installed computerised system at a regulated user's site, s/he may consider some, or all, of the elements shown in Figure 1: "Computerised system", (viz.: the ***controlling system*** and the ***controlled process*** in an ***operating environment***). *The inspector will consider the potential risks, from the automated system to product/material quality or data integrity, **as identified and documented by the regulated user**, in order to assess the fitness for purpose of the particular system(s). The company's risk assessment records may also be referred to as part of this process. The inspector's assessment may also involve a consideration of system life cycle, quality assurance measures, validation and operational control evidence for the controlling system, as well as validation and operational experience with the controlled process.*

4.6 *The validation documentation should cover all the steps of the life-cycle with appropriate methods for measurement and reporting, (e.g. assessment reports and details of quality and test measures), as required. Regulated users should be able to justify and defend their standards, protocols, acceptance criteria, procedures and records in the light of their own documented risk and complexity assessments, aimed at ensuring fitness for purpose and regulatory compliance.*

4.7 The Pharmaceutical Industry Systems Validation Forum in the UK developed the Good Automated Manufacturing Practice (GAMP) Supplier Guide to assist software suppliers in implementing an appropriate quality management system. *The GAMP Guide (and appendices) has evolved largely to define best practices in specifying, designing, building, testing, qualifying and documenting these systems to a rigorous validation management scheme, largely for the* ***controlling system****.* GAMP Forum is now sponsored by ISPE and has international membership and participation, including 'GAMP Americas'. (Websites: www.gamp.org and www.ispe.org)

4.8 Apart from user acceptance testing (OQ) versus the functional specification, which may include 'Factory Acceptance Testing' (FAT), for example, at the supplier, the regulated user also has responsibility for the (PQ) performance qualification of the system. In this context the PQ *user acceptance test of the system is in its operating environment*[3]*, and will again be against a User Requirements Specification (URS) that will include protocols and criteria for the performance and quality acceptance, not only for the* ***controlling system*** *but also for the* ***controlled*** *(pharmaceutical related)* ***process*** *application. Cross-references to any related, relevant process validation documentation should be clearly stated in respect of the latter. The GAMP Guide and PDA technical report No 18 (Further Reading Ref: 6) provide good practice guidance to drafting and using a URS, whereas pharmaceutical process validation guidance is given elsewhere (see PIC/S PI 006 and related EU/USFDA documents).*

4.9 Computerised systems may simplistically be considered to exist as three main application types, i.e.: process control systems, data processing systems, (including data collection/capture) and data record/ storage systems. There may be links between these three types of system, described as 'interfaces'. For critical systems, the inspector should study the user's specifications, reports, data, acceptance criteria and other documentation for various phases of the project. The regulated user should be able to demonstrate through the *validation evidence* that they have a high level of confidence in the integrity of both the processes executed within the ***controlling*** computer ***system*** and in those ***processes controlled*** by the computer system within the prescribed ***operating environment***.

4.10 The simplification of application system types may at first sight seem to be misleading for some readers. For GCP, examples of specific clinical systems have been described in 'Computer Systems Validation in Clinical Research' Section 9 (Further Reading Ref: 12). It can be seen that many of these systems have much in common with requirements for other GxP sectors, (e.g. Electronic transfer of data and/or software systems, (clinical) database management systems, statistical systems, derived data systems, electronic document management systems, electronic records and electronic signatures).

4.11 The regulated users of the system have the ultimate responsibility for ensuring that *documented validation evidence is available to GxP inspectors for review*.

---

[3] Large enterprise or MRP-II systems may be tested in a pilot mode environment initially, followed by controlled 'roll-out' to the user environment.

4.12 In addition to the validation considerations, the inspector will also be concerned with assessing the basic *operational controls, quality system and security features* for these systems, as indicated in the PIC/S GMP Annex 11 and amplified in the APV Guidance, q.v. For a copy of the APV Guidance, see GAMP 4 Appendix 09 (Further Reading Ref: 15).

PART TWO - IMPLEMENTATION OF SYSTEM

5. IMPLEMENTATION OF COMPUTERISED SYSTEMS

5.1 The assurance of the reliability of a Supplier's software products is attributable to the quality of the software engineering processes followed during development. This should include design, coding, verification testing, integration, and change control features of the development life cycle, (including after sales support). In order for customers to have confidence in the reliability of the products, they should evaluate the quality methodology of the supplier for the design, construction, supply and maintenance of the software[4]. A formal, extensive review of the history of the Supply Company and the software package may be an option to consider where an additional degree of assurance of the reliability of the software is needed. This should be documented in a *Supplier Audit Report*[5]. Prospective purchasers should consider any known limitations and problems for particular software packages or versions and the adequacy of any corrective actions by the Supplier. Appropriate, comprehensive *documented customer acceptance testing* should support the final selection of the software package. Errors often come to light after implementation and it is important for the Supplier to advise/assist the Customer concerning any problems and modifications to resolve errors. For so called 'standard software packages' and COTS (as referenced in the GAMP guide and commercial literature), it is important that purchasers are vigilant in maintaining reliable systems. This may include *documented reviews of their own experiences, (e.g. log books and error reporting and resolution),* from reading relevant literature or from interacting with application 'User Groups' to identify and resolve any serious problems. *Conclusions and recommendations from such activities should be recorded.*

5.2 Where the reliability and structural integrity of complex software products cannot be directly assessed, or completely evaluated, then it is even more important to assure that a good construction process has been used and has been properly documented. It is recognised that complex commercial proprietary applications can be extremely difficult to assess due to commercial secrecy and rivalry between suppliers, competing for market share[6]. Market

---

4 Refer also to ISO15504 (1998) 'Information Technology Software Process Assessment' and see GAMP 4 Appendix M2 'Guideline for Supplier Audit'.

5 A minority of suppliers are not responsive to requests for an audit. The need to perform a supplier audit should be linked to the regulated user's risk assessment and quality assurance standards.

6 The UK Government's Interdepartmental Committee on Software Engineering (ICSE) and the Real Time Engineering Group, have referred to such software as SOUP ('Software of Uncertain Pedigree') (1999).

research plus focused quality system and product specific audits[7] of the suppliers by the regulated user (or by an accredited third party auditor) may be beneficial here. The business/GxP criticality and risks relating to the application will determine the nature and extent of any assessment of suppliers and software products. GAMP Forum and PDA have provided advice and guidance in the GxP field on these matters.

5.3 *At all times there is a need for complete and accurate documentation and records to cover all aspects of the design phase, implementation & validation of the computerised system(s). Operating and reporting requirements for the important phases of the Software development Life Cycle related qualifications and testing exercises and commissioning should be covered by comprehensive Standard Operating Procedures or quality plans. The need for control and documentation of the development, implementation and operation of computer systems is extremely important for the validation of the system. There needs to be a strong emphasis on quality assurance in the development stages. It is fundamental for system life cycle documents to be controlled and maintained (version, audit trails as appropriate), within a quality assured document management system and available for inspection, if necessary.* Regulated users may choose to implement these requirements using either robust paper, electronic or hybrid systems.

6. THE STRUCTURE AND FUNCTIONS OF THE COMPUTER SYSTEM(S)

6.1 A recent USFDA document[8] identifies three premises that constitute the basic principles of quality assurance, which apply to software engineering:

- Quality, safety and effectiveness must be designed and built into the software.
- Quality cannot be inspected or tested into the finished software.
- Each phase of the development process must be controlled to maximise the probability that the finished software meets all quality and design specifications.

6.2 A computerised system is composed of the computer system and the controlled function or process. The computer system is composed of all computer hardware, firmware, installed devices, and software controlling the operation of the computer. The controlled function may be composed of equipment[9] to be controlled and operating procedures that define the function of such equipment, or it may be an operation, which does not require equipment other than the hardware in the computer system. Interfaces and networked functions through LAN and WAN are aspects of the computerised system and operating environment potentially linking a multitude of computers and applications. A firm's GxP system environment, functionality and interactions with other system(s) needs to be clearly defined and controlled in respect of GMP Annex

---

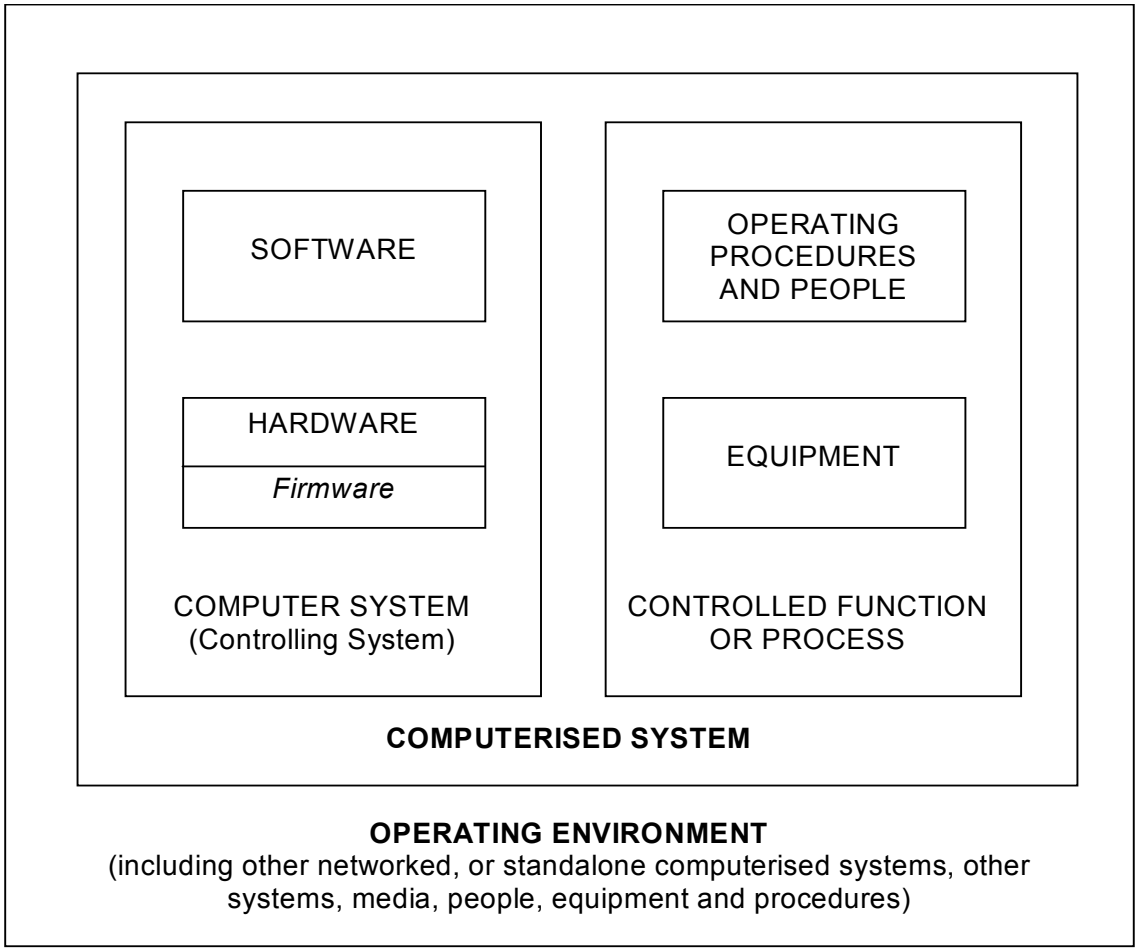
7 Audits are not mandatory but are considered 'good practice', and it is for the regulated user to determine any auditing needs, scope and standards.

8 'Final Guidance for Industry and FDA Staff: General Principles of Software Validation', CDRH, January 2002 (Further Reading Ref. 5).

9 e.g. automated equipment and laboratory or process related instrumentation.

11 (4). It may be necessary to equip personal PC applications and Internet/ e-mail/ personal data filing/ etc., with appropriate security and design measures to protect GxP systems whilst permitting authorised users to control the personal applications on their desktop PCs.

Figure 1 Schematic (below) identifies the relationship of the various components of a computerised system in its operating environment.



6.3 A large variety of computer systems are used in regulated user organisations. These range from the simple standalone to large integrated and complex systems. For example, a significant proportion of programmable electronic systems and proprietary automated equipment for manufacturing, laboratory or clinical use, contains 'firmware' with embedded software in place (for further details on firmware and embedded software refer to the glossary. Also, see Section 15.1 of this document for approaches to be taken with different systems. Firmware and operating systems are usually qualified for the intended use (including version, release or related criteria) as part of performance qualification / process validation. *Regulated users should have an inventory of all their computerised systems, ownership, supplier/developer, functionality, links and validation status. A policy and validation master plan for computerised systems should also be available for inspection.*

7. PLANNING AND LIFE-CYCLE MANAGEMENT

7.1 A high level of assurance of quality and reliability cannot be attributed to a computerised system based simply on a series of tests solely designed to confirm the correct function of the software and its interaction with hardware. There needs to be a *formal planned approach by the developer* to assure that quality is built into the product. ISO 9001 provides a quality system model for quality assurance in design, development, production, installation and servicing. The objective of testing during software development at the supplier should be to try to break the structural integrity of the software and find any weaknesses through a rigorous testing regime. Audits of suppliers conducted by or on behalf of regulated users should cover these issues when project related risk analyses deem it to be necessary.

7.2 ISO/IEC 12207:1995 provides guidance on acceptable practices for Information Technology - Software life cycle processes and ISO 9004, ISO 10005 and ISO 10007 provide guidance on Quality Management and system elements, including quality plans and configuration management. IEEE 1298 is specific and prescriptive on what should be addressed in planning. ISO 9126 concerns software quality and defines the quality attributes for critical applications. The GAMP Guide also provides relevant guidance for the pharmaceutical sector.

7.3 *It would be expected that the regulated user's Validation Policy or Validation Master Plan (VMP)*[10] *should identify the company's approach to validation and its overall philosophy with respect to computerised systems. The VMP*[11] *should:*

- *Identify which computerised systems are subject to validation.*
- *Provide brief descriptions of the validation strategies for different categories of computerised systems as well as other validation activities.*
- *Outline protocols and related test procedures for all validation activities including computer systems.*
- *Define reporting requirements to document validation exercises and related results.*
- *Identify key personnel and their responsibilities as part of the Validation Program*.

8. MANAGEMENT AND RESPONSIBILITIES

8.1 *It is important for a regulated user to have in place a comprehensive policy and procedures for the specification, purchase, development and implementation of computerised systems. Ideally these procedures would cover all computerised systems;* this PIC/S document will only concern itself with those systems that have an impact on GxP requirements.

---

[10] Refer to GMP Annex 15 for more details concerning the VMP requirements.

[11] It may be appropriate to refer to established policies, SOPs or individual validation plans to meet these requirements.

8.2 The organisation should regard disciplines related to the introduction of a computerised system as in accord with the basic principles of project management. Achieving the quality, performance and reliability objectives for any project requires competence in engineering and design. Where regulated users do not have the resources for engineering and design within their own organisation, there is a heavy reliance on the supplying company's resources.

8.3 To satisfy the quality, performance and reliability objectives, the regulated user needs to assure that the supplier's management policies; systems and related procedures will achieve the desired objectives. Enlightened suppliers should provide such evidence and added value to all customers, whether large or small, through the recognition of industry standards from GAMP Forum, Supplier Forum, PDA, ISPE, etc., and also through shared audits, user groups, and product certification arrangements.

8.4 *It is important to acknowledge that the scope and level of documentation and records needed to formalise and satisfy basic project management requirements for critical systems will be dependent upon:*

- *the complexity of the system and variables relating to quality and performance;*
- *the need to ensure data integrity;*
- *the level of risk associated with its operation;*
- *the GxP impact areas involved.*

8.5 Within the regulated user organisation there should be clearly defined responsibilities for the management of all ICT[12] products, computerised systems and projects. Management should cover the full spectrum, from simple input/output devices and programmable logic controllers (PLCs) through to integrated supervisory or information systems and business management levels. These responsibilities should involve development and administration of policies on purchase of IT products, as well as the introduction, commissioning and maintenance of IT products. The responsibilities should extend to development and implementation of formal monitoring, auditing and servicing of each system and designate the related documentation and records for such activities.

8.6 *BS 7799: 1999, (13), is issued in two parts (Part 1: Code of practice for information security management, and Part 2: Specification for information security management systems) and provides recommended guidance on a comprehensive set of controls comprising best practices in information security[13]. These controls and measures (or the equivalent) are recommended for adoption within this PIC/S guidance. They will assist in drafting the internal control standards and procedures to be implemented by IT management and administration departments.*

---

12 ICT = Information and Communications Technology

13 Relevant recent guidance is also provided in ISO/IEC17799:2000 on Information Technology – "Code of practice for information security management" and also in the pre-amble to FDA's 21 CFR Part 11.

9. USER REQUIREMENT SPECIFICATIONS (URS)

9.1 When utilising a computerised system within a regulated environment it is appropriate to establish *system control documentation or a system description,* [e.g. as required by GMP Annex 11(4)],[14] giving a written detailed description of the system, also covering development and maintenance.[15] This system control document may include a record of, or a reference to, the documented 'User Requirement Specifications' (URS), or other life-cycle documents. It should also be the definitive statement of what the system must or must not do. This document is also important for legacy systems and those systems under development.[16]

9.2 *When properly documented, the URS should be complete, realistic, definitive and testable. Establishment and agreement to the requirements for the software is of paramount importance. Requirements also need to define non-software (e.g. SOPs) and hardware.*

9.3 "*User Requirement Specifications", (URS), requirements should satisfy the following criteria:*

- *Each requirement document should be reviewed, authorised and uniquely catalogued.*
- *There should be no conflict between requirements.*
- *Each requirement, particularly those to be met to satisfy GxP expectations, should be* specified in a manner such that compliance with the requirements is capable of being verified objectively by an authorised method, e.g. inspection, analysis or test.
- *The URS, although independent of the supplier should be understood and agreed by both user and supplier*[17]*. There should be a clear distinction between mandatory regulatory requirements and optional features.*
- *The URS should contain functional and non-functional requirements: functionality, effectiveness, maintainability, usability, etc. Requirements should be objectively verifiable.*[18]

---

14 Linked, approved system life-cycle records may very well meet the requirements for the system control documentation/system description.

15 Development and maintenance information may often be held in separate (referenced) documents for large complex systems.

16 Risk assessment in the URS phase also needs to be addressed.

17 Note: This is straightforward for a bespoke system. However, for marketed proprietary systems or configurable packages then it is for prospective users, integrators and suppliers to discuss and review proposed user requirements, versus package functionality. It is essential to determine the 'degree of fit' and then control any necessary configuration work, modification, coding, testing and validation requirements in line with this guidance.

18 When choosing a 'standard product' or component, the URS may be developed compiling required features from the supplier's specifications.

9.4 Evaluation of the URS and the functional specifications should allow identification of the GxP requirements covered by the system. Additionally the URS will provide information as to where there are important interfaces between the system and manual operations. *The URS should also form the basis for a risk assessment of the system for GxP compliance requirements, in addition to other risks such as safety. The risk analysis may be based on the FS, which is related to the URS, (e.g. for bespoke systems). The risk assessment and the results including the reasons for the ranking as either: 'critical' or 'not critical' should be documented.*[19] *The nature of any GxP risks should be clearly stated.*

9.5 All computerised systems should have been subjected to documented prospective validation or qualification. Readers should refer to Section 15 of this document for validation strategies for different categories of software and systems. However, as user's systems evolve through modification, enhancement or integration and in response to additional regulatory requirements, it may be necessary to conduct additional re-qualification and revalidation work on the existing systems. The URS and 'System Description' document should be correspondingly updated as validation life cycle evidence.

Figure 2 (see Section 11 below) shows the relationship between URS and performance qualification (PQ).

10. FUNCTIONAL SPECIFICATIONS (FS)

10.1 From the URS, the supplier (this would include in-house developer) of the software would be able to develop the functional specifications (in the case of bespoke programs) or clearly identify the functional specifications for selection and purchase of off-the-shelf systems. The functional specifications should define a system to meet the URS, i.e. the customer's needs.

10.2 The functional specifications should provide a precise and detailed description of each of the essential requirements for the computer system and external interfaces. This means descriptions of functions, performances and where applicable, design constraints and attributes.

10.3 *For particular types and levels of systems it may be appropriate to have a combined URS and FS. Section 14 of this document gives further details of validation strategies for the five different categories for computer software as identified in the GAMP Guide.*

10.4 *The regulated user should be able to provide documentation describing the computer system(s) to include logic flow or block diagrams where practical, also giving an indication of hardware layout, networks and interaction. These basic schematics should align with the functional specification and be traceable to the URS. Within the EU it is logical for this information to be held within the controlled 'System Description' document, required by GMP Annex 11 (4).*

---

[19] Risk assessments and analyses can be useful at various stages during the entire system life-cycle and not just for the FS or URS, (see also GAMP 4 'M3').

11. SUPPLIERS, SOFTWARE DEVELOPERS AND QUALITY MANAGEMENT

Figure 2 below maps the relationships between the key specification and qualification elements as the system is specified, designed, built and tested.

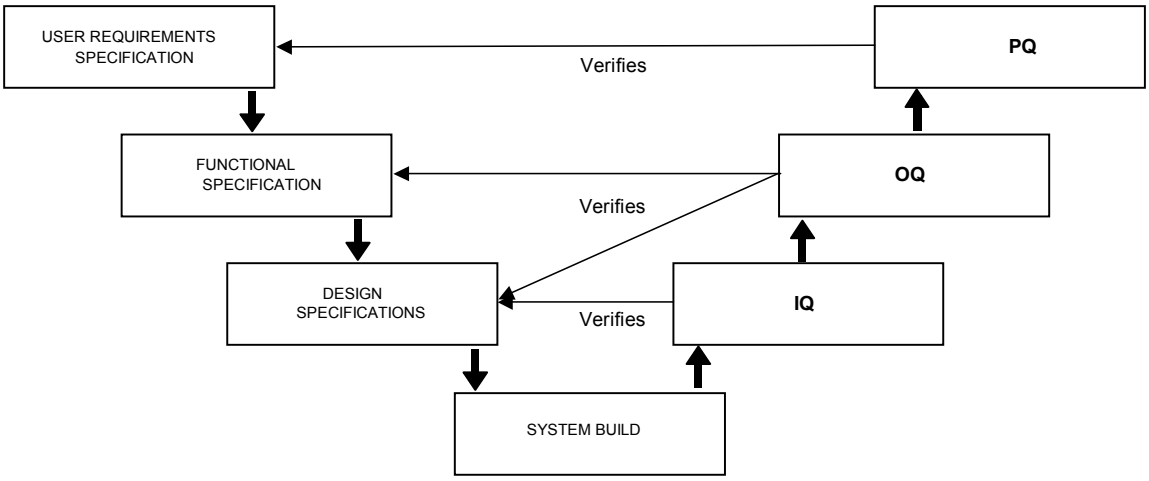


Figure 2. Basic framework for specification and qualification (based on Figure 6.2 of GAMP-4)[20]

11.1 The quality controls and quality assurance procedures, documentation and records related to the development and production of the software and hardware for computer systems are of critical importance. There are a number of accepted models for software development, e.g. the spiral model of development, the waterfall model and the life cycle model. All models have their own special attributes. As an example the GAMP guide adopts, but does not mandate a "V" framework (see figure 2 above). (Note: The URS and FS may be combined for smaller projects. These are related to the OQ.)

11.2 Supplier and developer reputations and trading histories for the software product provide some guidance to the level of reliability that may be assigned to the product supplied. *The pharmaceutical regulated user therefore should have in place procedures and records that indicated how and on what basis suppliers were selected.*

11.3 Compliance with a recognised Quality Management System (QMS) may provide the regulated user and regulatory agencies with the desired confidence in the structural integrity, operational reliability and on-going support for software and hardware products utilised in the system. The accreditation assessment schedule and scope of certification needs to be relevant to the nature of the proposed application. Structural integrity and the application of good software and hardware engineering practices are important for critical systems.

---

[20] This is an example only. Regulated users would be expected to comment on their own particular model. They should also interpret and define the relationships between various life-cycle elements as appropriate.

11.4 Confidence in the structural integrity may be based to some extent on the recognition of relevant certification of a company's software and hardware development methodology and QMS to ISO 9001 standard, such as (for example) TickIT certification and utilisation of ISO 9000 related guidance. However, it is essential that the assessment scope and schedules applied by the certifying auditors for these schemes should cover the engineering quality standards, actual practices, controls and records in place including non-conforming product (error feedback from the market), corrective actions, change management and so forth for particular products and versions. These can be very useful benchmarks for the design engineering, replication and maintenance standards in place at suppliers of large proprietary packages and can assist pharmaceutical clients with short listing and selection criteria.

11.5 However, an assessment of the supplier's QMS and recognised certification alone is unlikely to be the final arbiter for critical systems. The certification may very well be inadequate, or inappropriate. *In such cases, the regulated user may wish to consider additional means of assessing fitness for purpose against predetermined requirements, specifications and anticipated risks. Techniques such as supplier questionnaires, (shared) supplier audits and interaction with user and sector focus groups can be helpful.* This may also include the specific conformity assessment of existing, as well as bespoke software and hardware products. GAMP and PDA guideline documents identify a need to audit suppliers for systems carrying a high risk and have detailed guidance on supplier auditing procedures/ options.

11.6 Appendix O9 of the GAMP 4 Guide incorporates an independent commentary on PIC/S GMP Annex 11 and provides specific advice on quality and operational matters to help ensure compliance with the PIC/S and EU GMP. Users and suppliers need to ensure that software, hardware and systems are:

- quality assured;
- fit for their intended purpose; and
- *supported by appropriate documentation for quality and validation traceability*.

12. IMPORTANT QMS AND SOFTWARE STANDARDS ATTRIBUTES

12.1 The Standards ISO 9001, ISO 9126 & IEEE 1298 have a number of important features that can be summarised in the following points:

- They are structured around a QMS approach to the development, testing and documentation for software design, production and installation.
- Compliance with the standard requires formal systems for control, traceability and accountability of product(s) and personnel.
- The standard outlines the features and requirements of a life cycle approach to software production ("manufacture"), with emphasis on the importance of a change control procedure.
- The need for, and importance of, testing of software product/s is identified by the standard as it requires a tiered approach to testing and identifies three levels of testing for software:

- Unit code testing;
- Integrated module testing; and
- Customer acceptance testing.
- The GAMP Guide is also widely used as an industry standard of relevance here.

12.2 There are a number of advantages in organisations utilising a QMS approach for development and changes to software product. It would be expected that this approach if utilised by developers and producers of software should ensure (within the limitations of the quality management system approach) the following:

- Management commitment to quality and design control by instituting systems for quality control, documentation and quality assurance.
- Development, production and installation based on quality plans, verified by quality records. The QMS requires development, testing and programming standards.
- Adherence to quality assurance disciplines such as internal audits of the processes, corrective & preventative action procedures and control of non-conforming product.
- QMS methodology to establish requirements for purchased (subcontracted) software product.

13. TESTING

13.1 Assurance of reliability of software is achieved by execution of quality plans and testing during the software development process. This involves unit code testing and integration testing in accordance with the principles of ISO 12207, IEEE 1298 and IEEE 829 'Software Test Documentation'[21]. See also the corresponding sections in the GAMP Guide. *The development and testing of hardware and software should be done under a quality assurance system, documented and formally agreed between the various parties. This can ultimately provide evidence in support of GxP quality compliance (e.g. Annex 11(5)). Locations and responsibilities for testing (depending on the category of the software and system) are outlined in the GAMP Guide, qv.*

13.2 One of the most critical aspects of development of software is the integration testing phase where individual elements of software code (and hardware, where applicable), are combined and tested during or prior to this stage until the entire system has been integrated. Extra benefits may be achieved by code walk-throughs including evaluation of critical algorithms and/or routines, prior to testing. Errors found at the integration testing phase are much cheaper to correct than errors found at a later stage of testing. Code review (walk-through) is best done as early in the process as possible, preferably before submitting a module to test. Code reviews are best performed before formal unit code testing (i.e. before a unit or module is frozen and enters formal testing).

---

[21] This testing is defined as verification of the software element. Verification is defined as the process of determining whether or not the products of a given phase of the software development cycle fulfil the requirements established during the previous phase.

13.3 For some simpler GxP systems, for example certain PLCs and systems based on basic algorithms or logic sets, the functional testing may provide adequate assurance of reliability of the computerised system. For critical and/or more complex systems the verification testing that is conducted at the IQ, OQ & PQ stages provides only a limited level of assurance that the system does what it purports to do, reliably. This level of testing provides only limited assurance of the operation and reliability of hidden functions and code. For complex systems there should also be a high level of assurance that the development of the software has ensured delivery and operation of a quality product that is structurally sound, clearly defined and controlled.

13.4 *Test scripts should be developed, formally documented and used to demonstrate that the system has been installed, and is operating and performing satisfactorily. These test scripts should be related to the User Requirements Specifications and the Functional specifications for the system*. This schedule of testing should be specifically aimed at demonstrating the validation of the system[22]. In software engineering terms satisfactory results obtained from the testing should confirm design validation.

13.5 Any processing equipment and activities related to or controlled by the computer system would require additional IQ, OQ and PQ testing regimes. It may be appropriate to combine test phases and test scopes for a group of equipment or activities, and this should be defined in a test plan or strategy.

13.6 Regulated Users should be able to demonstrate formal acceptance of systems after testing and controlled transfer into the live operational environment.

14. VALIDATION STRATEGIES AND PRIORITIES

14.1 Regulated users need to be able to provide evidence for their computerised systems to demonstrate their range, complexity, functionality, control and validation status.

14.2 For the validation of computerised systems there should be a system in place that assures the ***formal assessment and reporting*** of quality and performance measures for all the life-cycle stages of software and system development, its implementation, qualification and acceptance, operation, modification, re-qualification, maintenance and retirement[23]. This should enable both the regulated user, and competent authority, to have a high level of confidence in the integrity of both the processes executed within the controlling computer system(s) and in those processes controlled by and/or linked to the computer

---

22 The supplier/developer should draft test scripts according to the project quality plan to verify performance to the functional specifications. The scripts should stress test the structural integrity, critical algorithms and 'boundary value' aspects of the integrated software. The test scripts related to the user requirements specification are the responsibility of the regulated users.

23 Tools and controls within the QMS, such as audits, change controls, configuration management and continuous improvement programmes may feature here.

system(s), within the prescribed operating environment(s).[24] (See also Section '4.6')

14.3 ***The regulated user's range of computerised systems needs to be formally listed in an inventory*** *and the scope/extent of validation for each detailed in a consolidated written Validation programme[25]. Validation scope should include GxP compliance criteria, ranked for product/process quality and data integrity risk criticality, should the system fail or malfunction.* This process represents one of the most important pre-requisites of Validation Master Planning (*see PIC/S doc. PI 006*), in that it is essential to assign priorities and attention to those systems (and features within systems) that represent the highest potential for disaster, should they malfunction or become inoperative. The risk analyses and the results, together with reasoning for ***critical*** or ***non-critical*** classifications, should be documented. Risks potentially impacting on GxP compliance should be clearly identified. There are a number of techniques to help identify and analyse risks and to select risk reduction and control measures. For further information refer to the GAMP Guide appendix and the GAMP Forum special interest group paper on 'Functional Risk Assessment'.

14.4 GxP compliance evidence is essential for the following aspects and activities[26] related to computerised systems:

- data input (capture and integrity), data filing, data-processing, networks, process control and monitoring, electronic records, archiving, retrieval, printing, access, change management, audit trails and decisions associated with any automated GxP related activity;
- in this context, examples of GxP related activities might include: regulatory submissions, R&D, clinical trials, procurement, dispensing/weighing, manufacturing, assembly, testing, quality control, quality assurance, inventory control, storage and distribution, training, calibration, maintenance, contracts/technical agreements and associated records and reports.

14.5 Historically, these systems have relied on manual systems, some electro-mechanical controls and paper based documentation. The introduction of computerised systems does not diminish the need for compliance with GxP requirements and guidelines.

---

[24] The italicised-bold part of this definition should be interpreted as requiring controlled documented methodology and records based on best compliance practices. This is to ensure that firms have generated documented evidence (electronic and/ or paper based), that gives a high level of assurance that both the computer system and the computerised system, will consistently perform as specified, designed, implemented and validated. Related validation dossiers for complex integrated projects should be clearly cross-linked for audit purposes.

[25] The scope or extent of validation for each system can be detailed in individual validation plans. A hierarchy of linked validation plans may be appropriate as outlined in GAMP 4 guidance Appendix M1: 'Guideline for validation planning'.

[26] These examples are intended to be illustrative, not exhaustive.

14.6 The current Good Automated Manufacturing Practice (GAMP) Supplier Guide provides essential guidance to suppliers of software to the Industry. The guide also provides a concise explanation of the interrelationship between various stages of software development and the requirements for Installation, Operational & Performance Qualification. The **GAMP Guide** identifies five different categories of software.

15. GAMP VALIDATION APPROACH BASED ON DIFFERENT CATEGORIES OF SOFTWARE PRODUCTS

15.1 The GAMP Guide may be referred to as appropriate for detailed guidance both in the core project management section, the quality narrative and the specific appendices. The following are category summaries from GAMP 4:

Reproduced from the GAMP 4 Guide (with permission) Appendix M4

Table 2.1: Summary of Software Categories

Category	Software Type	Validation Approach
1	**Operating System**	Record version (including service pack). The Operating System will be challenged indirectly by the functional testing of the application.
2	**Firmware**	For non-configurable firmware record version. Calibrate instruments as necessary. Verify operation against user requirements.
		For configurable firmware record version and configuration. Calibrate instruments as necessary and verify operation against user requirements.
		Manage custom (bespoke) firmware as Category 5 software.
3	**Standard Software Packages**	Record version (and configuration of environment) and verify operation against user requirements. Consider auditing the supplier for critical and complex applications.
4	**Configurable Software Packages**	Record version and configuration, and verify operation against user requirements. Normally audit the supplier for critical and complex applications.
		Manage any custom (bespoke) programming as Category 5.
5	**Custom (Bespoke) Software**	Audit supplier and validate complete system.

15.2 However, this pre-defined category approach may be difficult to apply to complex integrated computerised systems where different GAMP category 'levels' are effectively combined. Many systems span the category levels. For all critical systems a holistic risk-based approach is necessary. This should consider the risks from the entire pharmaceutical application. Quality assurance controls, qualification work and risk reduction measures can cascade from this to consider each of the elements comprising the computerised system. GAMP guidance is considered to be scaleable for large, medium and small, complex and simple systems. Where software and systems do not appear to fit readily into this category system then it is for users to apply judgement in determining particular quality measures, validation strategies and acceptance criteria. For instance, under particular circumstances the operating system configuration may contribute to the overall risk of the system and the level of validation should reflect this. *Inspectors will be interested in the company's approach to identifying GxP risks and the criteria for assessing the fitness for purpose of the system application*.

15.3 There are a number of additional important aspects that would be required in the documentation and records necessary to support a validation exercise. These aspects relate to on-going evaluation and system maintenance. As a result the documentation and records for validation of a computer system would also require information and records for the following aspects of system control:

- *Evaluation records to demonstrate that the system works as described in the URS (verification stage and on-going monitoring).*
- *Records of operator training (introduction and on-going training).*
- *Procedure for on-going monitoring, this procedure would interlink the error report system and the deviation reports system with the change control procedure.*
- *Maintenance of user manuals and SOPs for all systems*.

16. RETROSPECTIVE VALIDATION

16.1 Retrospective validation is not equivalent to prospective validation and is not an option for new systems. Firms will be required to justify the continued use of existing computerised systems that have been inadequately documented for validation purposes. Some of this may be based on historical evidence but much will be concerned with re-defining, documenting, re-qualifying, prospectively validating applications and introducing GxP related life-cycle controls. Reference should also be made to GAMP Forum's forthcoming guidance on 'Legacy Systems'. *Inspectors may be interested in seeing whether 'system descriptions' are available and that documented evidence exists that the system has been checked/tested against URS and other specifications. Risk and criticality analysis and assessment of supplier may also be relevant. A documented evaluation of system history i.e. error logs, changes made, evaluation of user manuals and SOPs would also be expected to provide some of the documentation relating to the 'controlled system' in place of formal validation evidence.*

16.2 A significant number of legacy systems may operate satisfactorily and reliably, however, this does not preclude them from a requirement for validation. The approach to be taken is to provide data and information to support the retrospective documentation of the system to provide validation and re-qualification evidence. GxPs have required the validation of computerised systems for many years. *It should therefore be noted that a lack of prospective validation evidence for computerised systems would increasingly be seen as a serious deviation from GxPs by a number of regulatory authorities*[27]*. However retrospective validation might be justified if a non-GxP system is newly classified as a GxP system.*

16.3 The principles identified above for computer systems validation should be addressed where a retrospective validation approach has been undertaken for a legacy system. For legacy systems, because of their age and unique characteristics, the system development documentation and records appropriate for validation may not be available. As a result the approach taken to establish and document system reliability and on-going assurance based on the "build-in-quality" concept for software development would, of necessity, be different to a current system.

16.4 Nevertheless, the validation strategy would be consistent with the principles established for classic retrospective validation where the assurances are established, based on compilation and formal review of the history of use, maintenance, error report and change control system records and risk assessment of the system and its functions. These activities should be based on documented URS's[28]. If historical data do not encompass the current range of operating parameters, or if there have been significant changes between past and current practices, then retrospective data would not of itself support validation of the current system.

16.5 *The validation exercise for on-going evaluation of legacy systems should entail inclusion of the systems under all the documentation, records and procedural requirements associated with a current system. For example, change control, audit trail(s), (where appropriate), data & system security, additional development or modification of software under a QMS,*[29] *maintenance of data integrity, system back up requirements, operator (user) training and on-going evaluation of the system operations.*

---

[27] Compared with 10 to 20 years ago, when GxP related applications were often rudimentary and 'standalone', there are now many more integrated, 'infrastructure' computer systems to consider, especially when regulated users are striving to achieve 'so-called' paperless systems. Some specific national GxP compliance regulations, such as the US FDA's 21 CFR Part 11: 'Electronic Records and Electronic Signatures' have set specific requirements in this field. For legacy systems, firms often have to consider retrospective validation, upgrading or replacement.

[28] 'Experience reports' supported by additional testing have reportedly been used to retrospectively derive a URS.

[29] QMS = Quality Management System

16.6 *Ultimately, regulated users have to be able to demonstrate:*

- *Defined requirements*
- *System description, or equivalent*
- *Verification evidence that the system has been qualified and accepted and that GxP requirements are met*

16.7 *In the absence of adequate 'retrospective qualification or validation' evidence this could be a reason to suspend, discontinue or turn-off any legacy system(s).*

PART THREE - SYSTEM OPERATION / INSPECTION / REFERENCES

17. CHANGE MANAGEMENT

17.1 It is important for proper control that a comprehensive change management system is instituted. This may take two forms in that during the Design phase it may only be necessary to keep records pertaining to the project up-to-date without formal "sign-off" approvals for all changes. However, once the project reaches a point where specifications are under development and conceptual aspects have been finalised, then a formal change control procedure should be established which will require clear, prescriptive and accurate documentation and records. It is important for the responsibilities of participants in the change control procedure to be carefully defined.

17.2 As discussed previously, it is appropriate for regulated users to have a *system control document* or some other record system to achieve a documented baseline record for the description of the computerised system. The system control documentation should be the definitive statement of what the system must do. The control document should also provide a record of the User Requirement Specifications. The change control procedure for the computerised system "project" should be integrated with the Master change control procedure for the regulated user organisation[30]. *The change control procedure will need to take account of the corresponding procedures and records used by suppliers, integrators and other parties contracted to support the particular system and applications.* Validated decentralised arrangements for change control may be a feature in large complex regulated user companies.

17.3 Common IT infrastructure features may need to be controlled centrally by IT systems and security management. Key roles, responsibilities and procedures need to be clearly documented in relevant internal and external *Service Level Agreements,* (SLAs), or equivalent documents.

---

[30] It is important for regulated users to ensure that change control management is in place during all system life cycle phases, i.e. from design and development through operation, maintenance, modification and retirement. The arrangements should be described in the validation plans for the project. Records should be kept with the project files.

18. CHANGE CONTROL AND ERROR REPORT SYSTEM

18.1 The formal *change control procedure* should outline the necessary information and records for the following areas:

- *Records of details of proposed change(s) with reasoning.*
- *System status and controls impact prior to implementing change(s).*
- *Review and change authorisation methods (also see 12.5).*
- *Records of change reviews and sentencing (approval or rejection).*
- *Method of indicating 'change' status of documentation.*
- *Method(s) of assessing the full impact of change(s), including regression analysis and regression testing, as appropriate (IEEE).*
- *Interface of change control procedure with configuration management system.*

18.2 *The procedure should accommodate any changes that may come from enhancement of the system, i.e. a change to the user requirements specifications not identified at the start of the project. Or alternatively a change may be made in response to an error, deviation or problem identified during use of the system. The procedure should define the circumstances and the documentation requirements for emergency changes ("hot-fixes"). Each error and the authorised actions taken should be fully documented. The records should be either paper based or electronically filed.*

18.3 Computer systems seldom remain static in their development and use. For documentation and computer system control it should be recognised that there are several areas that would initiate change or a review for change. These are:

- a deviation report;
- an error report; or
- a request for enhancement of the computer system;
- hardware and software updates.

18.4 The results of periodic reviews may be helpful, e.g. in indicating process drifts and the need for change. *Quality systems procedures should ensure that the changes are clearly documented and closed out after actions have been completed. The change control procedure should complement and link with the deviation and errors report system. Various GAMP 4 'Operation' appendices include guidance in these areas.*

18.5 *The supplier of the software should have its own change control system in place and there should be clear and agreed procedures covering the interrelationship of the suppliers and users change control system. Where changes are made then the modifications of software should be undertaken following formal QMS documentation, records and procedural requirements*.

18.6 Any changes to the validated computerised system should not be undertaken without *review and authorisation* on behalf of all stakeholders responsible for the current user requirements. It may be appropriate for this to be undertaken by the system owner and QA representative. *Test scripts, determined by the project plan, q.v., (of defined test type and extent of tests),* should be used to verify the acceptability of the software element developed in response to a change request. *Integration testing may also be necessary before release of the new software version*[31]*.*

19. SYSTEM SECURITY, INCLUDING BACK-UP

19.1 The security of the system and security of the data is very important and the procedures and records pertaining to these aspects should be based on the IT policies of the regulated user and in conformance with the relevant regulatory requirements. The use of a computerised system does not reduce the requirements that would be expected for a manual system of data control and security. 'System owner's' responsibilities will include the management of access to their systems and for important systems the controls will be implemented through an Information Security Management System (ISMS).

19.2 It is very important for the regulated user to maintain the *procedures and records related to the access to the system(s). There should be clearly defined responsibilities for system security management, suitable for both small and complex systems, including:*

- *The implementation of the security strategy and delegation*
- *The management and assignment of privileges*
- *Levels of access for users*
- *Levels of access for infrastructure (firewall, backup, re-booter, etc.).*

19.3 *The examination of the procedures and records should assure that the following basic requirements are satisfied:*

- *Access rights for all operators are clearly defined and controlled, including physical and logical access.*
- *Basic rules exist and are documented to ensure security related to personal passwords or pass cards and related system/data security requirements are not reduced or negated.*
- *Correct authority and responsibilities are assigned to the correct organisational level.*
- *Procedures are in place to ensure that identification code and password issuance are periodically checked, recalled or revised.*
- *Loss management procedures exist to electronically invalidate lost, stolen or potentially compromised passwords. The system should be capable of enforcing regular changes of passwords. Precise change rates to be justified within the ISMS.*

---

[31] It may be necessary to regard proposed changes to infrastructure as a special case and define a set of stakeholders.

- *Procedures identify prohibited passwords.*
- *An audit log of breaches of password security should be kept and measures should be in place to address breaches of password security.*
- *The system should enforce revoking of access after a specified number of unsuccessful logon attempts.*
- *Measures are needed to ensure the validated recovery of original information and data following back up, media transfer, transcription, archiving, or system failure.*
- *Attempted breaches of security safeguards should be recorded and investigated.*
- *Some equipment, such as standalone computerised systems and dedicated operator equipment interfaces and instruments may lack logical (password etc.) capabilities. These should be listed, justified and subjected to other procedural controls.*

19.4 It should be realised that when absolutely necessary Inspectorates of the national competent authorities may need to be able to access a firm's encrypted GxP data. In such circumstances, either keys for decryption would need to be made readily available to the Inspectors working for the competent authorities, or decryption would have to take place under the inspector's supervision.

19.5 The *validated back-up procedure* including storage facilities and media should assure data integrity. The frequency of back up is dependent on the computer system functions and the risk assessment of a loss of data. In order to guarantee the availability of stored data, back-up copies should be made of such data that are required to re-construct all GxP-relevant documentation (including audit trail records).

19.6 There should be *written procedures for recovery of the system* following a breakdown; these procedures should include documentation and record requirements to assure retrieval and maintenance of GxP information. *The examination of the procedures and records should assure that the following basic back up and disaster recovery requirements are satisfied:*

- *There should be procedures to assure routine back-up of data to a safe storage location, adequately separated from the primary storage location, and at a frequency based on an analysis of risk to GxP data.*
- *The back-up procedure including storage facilities and media used should assure data integrity. There should be a log of backed up data with references to the media used for storage. Media used should be documented and justified for reliability.*
- *All GxP related data, including audit trails should be backed-up.*
- *Procedure for regular testing, including a test plan, for back up and disaster recovery procedures should be in place.*
- *A log of back up testing including date of testing and results should be kept. A record of rectification of any errors should be kept.*

19.7 The *physical security* of the system should also be adequate to minimise the possibility of unauthorised access, wilful or accidental damage by personnel or loss of data.

20. DATA CHANGES - AUDIT TRAIL/CRITICAL DATA ENTRY

20.1 Where applicable, the audit trail for the data integrity may need to include functions such as authorised user, creations, links, embedded comments, deletions, modifications/corrections, authorities, privileges, time and date, inter-alia. *All linked components are to be immutably[32] linked in an IT system security controlled audit trail. All original data records and masters and any subsequent alterations, additions, deletions or modifications are to be retained accurately and comprehensively within the retrievable audit trail. The nature and context of transactions logged in the audit trail to be deducible from and in agreement with, the firm's approved Standard Operating Procedures for information security management for the particular computerised applications and user's authorities[33]. Firms will need clearly documented policies, standard operating procedures, validation reports and training records covering such system controls. Information Security Management standards such as ISO/IEC 17799:2000[34] may be of assistance with the design, implementation and control of such systems.*

20.2 Where applicable, there should be *special procedures for critical data entry* requiring a second check, for example the data entry and check for a manufacturing formula or the keying in of laboratory data and results from paper records[35]. A second authorised person with logged name and identification, with time and date, may verify data entry via the keyboard. For other automated systems featuring direct data capture linked to other databases and intelligent peripherals then the second check may be part of validated system functionality (e.g. in a dispensary). Special access, system control features and/or special devices such as identification code bars, and the inclusion and use of an audit trail to capture the diversity of changes possibly impacting the data may facilitate this check.

20.3 The *records pertaining to the audit trail* events should be documented, ideally as features of the operating system, database management system (DBMS), document management system (DMS) and other major applications. Time-linked audit trail records should be available, if required, in a human readable form as required by the inspector[36]. *GxP Inspectors may see evidence for different forms of audit trail depending on the regulations prevailing in the intended regulated markets for the products or data.*

---

32 Penguin English Dictionary: 'Immutable [imewtab'l] adj unchangeable; without variation - immutably adv.

33 The systematic contextual 'labelling' of transactions in the electronic audit trail log is recommended as it can have automated functional feedback control links with security validation features.

34 Information Technology - – "Code of practice for information security management" BSI/DISC and national standards bodies. Other guidance will be found in the guidelines supporting FDA's 21 CFR Part 11.

35 This is an established compliance requirement in the GMP discipline.

36 It should be noted that for the USA market it may be a requirement in for audit trails to be available in electronic form, not just paper, but the implementation and enforcement of compliance with 21 CFR Part 11 is under review by FDA in 2003, (see Ref. 11).

20.4 It is expected that appropriate controls will exist such as the maintenance of a *register of authorised users, identification codes, scope of authorised actions*, in support of GxP electronic records and electronic signatures.

20.5 There should be *records of checks* that the data/control/monitoring interface(s) between the system and equipment ensure correct input and output transmission.

21. ELECTRONIC RECORDS AND ELECTRONIC SIGNATURES

21.1 EC Directive 91/356 sets out the legal requirements for EU GMP. The GMP obligations include a requirement to maintain a system of documentation, (Article 9)[37]. The main requirements here being that the regulated user has validated the system by proving that the system is able to store the data for the required time, that the data is made readily available in legible form and that the data is protected against loss or damage.

21.2 The guidelines relating to documentation in the GMP Guide are in Chapter 4 and there is no requirement here that documents be in writing. Indeed in paragraph 4.9 the section amplifies Article 9.2 (see above). It references electronic data processing (EDP) systems and implies a number of good practice measures that should be in place to protect the data:

- access by authorised personnel only
- use of passwords
- creation of backup copies
- independent checking of critical data
- safe storage of data for the required time

Such systems also require evidence to demonstrate:

- (fundamental) the use of validated, secure computerised systems
- the systematic use of an accurate, secure, audit trail, (where appropriate)

21.3 The central consideration here as in Directive 91/356, is that *records are accurately made and protected against loss or damage or unauthorised alteration so that there is a clear and accurate audit trail throughout the manufacturing process available to the licensing authority for the appropriate time.*

---

[37] The main requirements in Article 9.1 are that documents are clear, legible and up to date, that the system of documentation makes it possible to trace the history of manufacture (and testing) of each batch and that the records are retained for the required time. Article 9.2 envisages that this documentation may be electronic, photographic or in the form of another data processing system, rather than written.

21.4 The situation for an authorised wholesale distributor is similar for records covering purchases/sales invoices, (on paper or on computer, or any other form)[38]. The requirements for records are clear: "*Records should be made… in such a way that all significant activities or events are traceable… and are clear and readily available".*

21.5 *Regulated user companies generally have a choice as to whether to use electronic records or electronic signatures instead of paper based records. When regulated users elect to use electronic records for GxP applications then it will be necessary for the companies to identify the particular regulations being applied and whether they are to be considered legally binding and equivalent to their paper-based counterparts. Regulations applicable to particular GxP disciplines may impose specific rules e.g. when electronic records and electronic signatures are used as a primary source of data, records and/or evidence.*
It is for the regulated user to explain and justify the technologies and controls in place.
An appropriate form of Electronic signature[39] or authentication / identification[40] should be applied where

- *external access can be made to a computerised GxP system*
- *the system electronically generates GxP regulatory records, or*
- *key decisions and actions are able to be undertaken through an electronic interface.*

21.6 Generally there is no requirement for records and documents created and maintained, as part of GxP, to be in 'writing',[41] and validated, secure electronic versions are permitted. In the absence of provisions to the contrary this will arguably extend to "electronic signatures". Certainly, **where regulated users have elected to use electronic records in place of paper-based media,** then it can be argued, (from the forgoing requirements) that for accurate, authorised, secure electronic record systems these systems would logically require *an attached immutable audit trail identifying person, time and date and linking to particular transactions. However, some systems may utilise a combination of human actions together with other automated functions and a variety of media for GxP data processing, records and information. Such systems may be described as 'hybrid' and in such cases documented procedural controls with*

---

38 The relevant EC directive being 92/25, Article 6(e), as amplified in the GDP guidelines (94/C 63/03). Article 8 of 92/25 requires that the documentation system makes it possible to trace the distribution path for every product.

39 It has been proposed via industry comments that a signature should be unique to the owner of that signature but not necessarily unique to the system. It has also been argued that it may be desirable to issue and maintain only one signature across a multitude of systems. Regulated users may need to explain and justify such arrangements, controls and logic.

40 The regulated user is expected to justify the choice of methods to be used to ensure compliance with regulations and GxP, (see glossary 'Advanced Electronic Signature', 'Electronic Signature (3)' etc.

41 In this context 'writing' meaning 'written by hand and/or signed by hand' on paper media.

recorded links, by reference and signatures may have to be used to complete the audit trail across, for example, a mixture of paper based records[42] *and electronic files.*

21.7 Whilst EC Directive 2001/83[43] requires a Qualified Person to "certify" in a 'register' that batches for release meet the required condition we are not aware of any provisions that would restrict this activity to paper based media and a handwritten certifying signature. Validated and secure electronic data processing systems may therefore be used in this context.

21.8 *The key aspects of infrastructure, system and specific application to be controlled and managed are:*

- *the authorised user log-on for a specific application*
- *a unique combination of user ID and password called for by the computerised system and linked to the user's authorised account for the use of a specific application*
- *permitted task functionality for that user*
- *the system to have defined time zone(s) and date standard referencing with relative transaction linking, (complex systems may span several time zones)*
- *the audit trail*[44]
- *other physical and logical system information security infrastructure control features.*

21.9 Issues to consider when assessing GxP compliance in the use of electronic signatures include that:

- *Documentary evidence of compliance exists* for all aspects of infrastructure, system and specific application.
- *Where risk assessment concludes that the use of a digital signature may be necessary (e.g. Certification to a third party or in GCP field data collection and transmission) that adequate security measures* exist to protect the key to a digital signature. The level of security that is appropriate depends on the sensitivity of the transaction and the possible impact of the unauthorised use of the key. Public Key Infrastructure (PKI) may be appropriate where risk assessment indicates that a high level of security is required.
- *A register of entities* that are authorised is being maintained.
- There are *procedures* that ensure that entities authorised to use electronic signatures are aware of their responsibilities for actions initiated under their electronic signatures.
- Personnel administering the systems have *appropriate security clearances, training, skills and knowledge.*

---

42 Including printouts from computerised systems.

43 Superseding 75/319 Article 22 following codification.

44 See previous Section ('20.1').

- *Procedures* are in place to record the printed name, or 'identity', of the signer, the date and time when the signature was executed and the meaning associated with the signature.
- *Procedures* exist to try to detect the unauthorised use of an electronic signature or compromised ID password combinations.

21.10 *Issues to consider where electronic records are used to retain GxP data*:

- Documentary *evidence of compliance exists*
- *Archiving procedures* are provided and records of use exist
- *Procedures exist* to ensure accuracy, reliability and consistency in accordance with the validation exercise reported for the electronic record system
- *System controls and detection measures (supported by procedures) exist* to enable the identification, quarantining and reporting of invalid or altered records
- *Procedures exist* to enable the retrieval of records throughout the retention period
- *The ability exists* to generate accurate and complete copies of records in both human readable and electronic form
- Access to records is limited to authorised individuals
- *Secure, computer-generated, time-stamped audit trails to independently record GxP related actions following access to the system are used*[45].

21.11 *Procedures exist* to ensure that change-control and revision (additions, modifications, deletions) transactions are documented in the audit trail.

21.12 *Issues to consider when the GxP system has a provision for external access*[46]:

- The system has a method of ensuring that external access and inputs come *only from authorised clients* and that they come *in the correct format*, for example as encrypted, digitally signed mail or data packets. *A mechanism must exist to quarantine external inputs where security conditions are not met*. The information security management arrangements need to cover the quarantine, notification and the final sentencing of such inputs.
- Mechanisms are in place to ensure that all external access can be tracked. *Each element of the processing stage should incorporate logging and monitoring facilities.* ***However, inspectors may expect to see less onerous tracking for 'read only' access to a suitably secure and protected system.***
- *The capacity should exist to keep copies of data and to re-send them from one stage to another if they get "lost" or corrupted at a later stage of processing.*

---

[45] A database management system (DBMS) will have this included as an optional feature, but for other systems it may be necessary to ensure that it is an added function. Regulated users will then need to ensure that it is left 'switched' on.

[46] Sometimes referred to as 'open' systems

21.13 *Additional security arrangements and controls will be needed for GxP computerised systems which electronically generate regulatory records, allow external access, or enable key decisions and actions to be undertaken through electronic interfaces*. These requirements are being determined largely by international initiatives to establish electronic commerce[47]. However, where firms are interfacing such open system (external access) functionality, in whole or in part, with their GxP systems, *then the security, control and validation information will need to be documented and available to GxP inspectors.*

22. PERSONNEL

Note: 22.1 to 22.7 is based largely on the APV Guideline[48], q.v., with judicious editing where necessary to fit the context of this document.

22.1 There should be *sufficient, qualified staff with the relevant experience* to carry out tasks for which the regulated user is responsible in connection with the planning, introduction, application (operation), application consultancy on, and regular monitoring of, computerised systems.

22.2 Ideally staff qualifications should be assessed on the basis of professional training, education and experience in handling and developing computerised systems. The field of work in which the staff will be operating should determine qualification requirements. *Staff should only be deployed in areas suited to their skills and training.*

22.3 The individual *areas of responsibility should be laid down in writing* and be clearly understandable to every member of staff. The fact that computerised systems may take over decision-making functions does not affect the legally prescribed responsibilities of the persons in key positions.

22.4 Prior to converting a process from manual to automated control (or the introduction of a new automated operation) it is important that project staff consider any quality assurance and safety issues as part of an *impact assessment of risks*. Risk reduction measures may need to be incorporated into the systems design and operation[49]. (Additional risks to the quality of GxP related products/materials should not be introduced as a result of reducing the manual involvement in the process).

---

47 Including 21 CFR Part 11. Title 21 Code of Federal Regulations Part 11 (21 CFR Part 11), which was issued by the US FDA in 1997 and provides criteria under which that agency considers electronic records and electronic signatures to be equivalent to paper records and hand-written signatures. In Europe EC Directive 1999/93/EC (December 1999) on a community framework for electronic signatures and EC Directive 2000/31/EC (May 2000) on electronic commerce in the internal market are important. These directives were implemented during 2001. It is not the purpose of GxP guides to reproduce such business and commerce requirements.

48 Section 22.4 has been substantially re-worded compared with the original (English language version) APV guidance, for clarity.

49 "Account should be taken of the risk of certain aspects of the previous procedures such as quality or safety being lost as a result of reduced operator involvement following the introduction of a computerised system."(to quote the APV document)

22.5 The regulated user is responsible for ensuring all staff who have to perform tasks in connection with computerised systems are given the *requisite training* and *relevant guidelines* on computerised systems. That should also apply to system developers, maintenance and repair staff and staff whose work could affect the documented operability of the systems.

22.6 Apart from a basic training in computerised systems, newly recruited staff should also be trained in the tasks assigned to them personally. Furthermore, ongoing/awareness training should also be undertaken according to *standard training programs* and the effectiveness of the training assessed periodically following implementation, (through testing).

22.7 In connection with training, the GxP and life-cycle concept and all measures to improve understanding and application of the concept should be explained. Training **measures and qualifications** should be *documented* and stored as part of the life cycle documentation. (Training records may be stored in accordance with regulated user procedures)

23. INSPECTION CONSIDERATIONS

23.1 The attention paid by inspectors to the assessment of the GxP implications of computerised systems on a site (and between sites), will be determined to some extent by the overall *site history and risk assessment* carried out by the inspector in preparing for the inspection. Information computer technology management arrangements for the procurement and validation of software and systems may be centralised at the regulated user's headquarter site rather than at the site of inspection. In such circumstances the controls, SOPs and records in place to ensure GxP compliance at inspection sites will need to be made available on site. In some circumstances it may also be necessary to consider an inspection at the HQ site.

23.2 Clearly where a site has a lot of automation and integrated computerised systems - and manufactures a range of sterile products - (for example), then the **potential** risks from a GxP failure, (whether computer related or otherwise) for the patient are high. However, where such automated systems are well designed, implemented, managed and controlled, then potential risks to product quality (and to patients) may be considerably reduced, compared with labour intensive operations, as the latter carry inherent risks from human variability and errors. Inspectors have to come to a judgement on this by *studying the firm's evidence not just in relation to the technology aspects (through the application of GAMP etc.) but also the GxP risks identified (through PQ*[50] *reports and such-like).*

23.3 Humans design, build, test, implement **and change** these complex systems and there is opportunity for critical error with automated systems at any stage in the life-cycle unless properly managed. The GAMP Guide provides relevant guidance on these aspects.

---

[50] PQ = Performance Qualification

23.4 It is not intended that this guidance should be used as a 'blunt instrument' for all on-site inspections but inspectors should use it selectively to build up a clear picture of a company's scale and complexity of on-site computerization (or automation) and investigate selectively the critical systems and risks. As stated in '2.7' of this PIC/S guidance, inspectors may wish to consider evidence for compliance with GxP as indicated by *italicised text* throughout the document. Table 1 (page 34) immediately following this section provides a suggested checklist for information to be considered prior to inspection[51].

23.5 Where little is known about computerization on a site, then it may be necessary to use a *pre-inspection questionnaire* to amplify the Site Master File details.

23.6 Inspectors should *select the GxP critical computerised systems* from the information provided and consider firstly the *validation evidence* for the selected system(s) and then the *routine operational controls* for maintaining a valid system that is accurate and reliable. Inspectors may find that different departments in pharmaceutical companies will have responsibility for GxP aspects of commercial, or business (IT systems) and lower level process control systems. *Look for evidence of inconsistency, or muddled standards*.

23.7 GxP critical computerised systems are those that can affect product quality and patient safety, either directly (e.g. control systems) or the integrity of product related information (e.g. data/information systems relating to coding, randomisation, distribution, product recalls, clinical measures, patient records, donation sources, laboratory data, etc.). This is not intended as an exhaustive list.

23.8 *It is essential that firms have a computerised systems validation policy together with linked SOPs and plans, including a listing, or inventory, of all their computerised systems - classified as to their use, criticality and validation status.* For long standing systems, validation may have been carried out retrospectively and for systems purchased or implemented in the last few years, the validation should have been carried out (and recorded) prospectively. Firms should have plans to complete any outstanding retrospective validation of GxP related computer systems within a reasonable time period depending on the risks and complexity of the systems. The continued use of critical systems that are unsupportable by suppliers and cannot be validated must be justified by regulated users, supported by alternative fail-safe arrangements and considered for urgent phased replacement.

23.9 The firm's validation approach should follow a life-cycle methodology, with management controls and documentation as outlined in this guidance, which contains consensus best practice guidelines.

---

[51] An electronic keyword search of GxP documents will reveal specific compliance requirements to assist in preparing for particular topic inspections. Keywords such as: 'document', 'specification', 'formula', 'procedure', 'record', 'data', 'log book', 'instruction', 'written', 'sign', 'approve', 'writing', 'signature' are particularly helpful for records, data, documentation, authorisation and signature issues.

23.10 Inspectors should review the firm's *Validation Summary Report*[52], (VSR) for the selected system and refer as necessary to the *System Acceptance Test Specification* and lower level documents. They should *look for evidence that the qualification testing has been linked with the relevant specification's acceptance criteria, viz:*

- PQ versus URS .
- OQ versus FS[53]
- IQ versus DS or DR[54]
- Supplier audit reports
- Validation and *quality plans. e.g. Validation Master Plan, (VMP) or Policy.

(*For big projects there should be a project quality plan and a QMS for the documentation. For smaller projects established SOPs may suffice)

23.11 *Inspectors should look for the traceability of actions, tests and the resolution of errors and deviations in selected documents. If the firm has* ***not*** *got proper change and version controls over its system life-cycle and validation documents, then the validation status is suspect.*

23.12 *Inspectors should consider all parts of PIC/S GMP Annex 11 for relevance* to particular ***validation projects*** and in particular, the 'Principle' and items 1, 2, 3, 4, 5 and 7.

23.13 ***The lack of a written detailed description of each system, (kept up-to-date with controls over changes), its functions, security and interactions (A11.4); a lack of evidence for the quality assurance of the software development process (A11.5), coupled with a lack of adequate validation evidence to support the use of GMP related automated systems may very well be either a critical or a major deficiency. The ranking will depend on the inspector's risk assessment judgement for particular cases***. ***(NB. Since 1983, the GMPs have called for validated electronic data-processing systems and since 1992 for the validation of all GMP related computer systems).***

23.14 *If satisfied with the validation evidence, inspectors should then study the system when it is being used and calling for printouts of reports from the system and archives as relevant. All points in Annex 11 (6, 8-19) may be relevant to this part of the assessment. Look for correlation with validation work, evidence of change control, configuration management, accuracy and reliability. Security, access controls and data integrity will be relevant to many of the systems particularly EDP (i.e.:* ***E****lectronic* ***D****ata* ***P****rocessing) systems.*

---

52 VSR=A best practice high level report, summarising the validation exercise, results and conclusions, linking via cross referencing to lower level project records, detailed reports and protocols. This is useful for briefing both senior managers, in regulated user organisations and for reference by auditors/ inspectors.

53 OQ = Operational Qualification; FS = Functional Specification

54 IQ = Installation Qualification; DS= Design Specification; DR = Design Review

23.15 *Consider also PIC/S GMP 4.9 and EC Directive 91/356/EEC Article 9(2) for EDP systems.* Guidance on the common industry interpretation of Annex 11 is given in the GAMP Guide, from the German APV.

23.16 ***Deficiency ratings applied by Inspectors will be based on the relative risk of the application and their judgement of risk criticality.***

24. CHECKLISTS AND AIDE MEMOIRES

Table 1

Table 13.5 in the publication 'Good Computer Validation Practices', (Suggested Further Reading Ref.1), provided a summary of typical information to be made available to an inspector as part of preparation work. As it is still largely relevant, it is reproduced in updated form below, with the author's permission, for information:

INSPECTORS - PREPARING FOR AN INSPECTION	
1.	Details of the organisation and management of IT/Computer Services and Project Engineering on Site.
2.	The regulated user's policies on procurement of hardware, software and systems for use in GxP areas.
3.	The regulated user's policy on the validation of GxP computerised systems
4.	A list of IT/Computer Services Standards and SOPs.
5.	The project management standards and procedures that have been applied to the development of the various applications.
6.	Identify work contracted out routinely for systems support and maintenance.
7.	A list, or inventory, of all Computerised Systems on site by name and application for business, management, information and automation levels. The list should also indicate validation status and risk ranking. (Include basic schematics of installed hardware and networks).
8.	Identify and list those systems, sub-systems, modules and/or programs that are relevant to GxP and product quality. Cross-refer to the lists provided for '6' above.
9.	For the GxP significant elements and systems identified in '7' please provide additional information as below:
10.	Details of disaster-recovery, back up, change-controls, information security, and configuration management.
11.	A summary of documentation that generally exists to provide up-to-date descriptions of the systems and to show physical arrangements, data flows, interactions with other systems and life cycle and validation records. The summary should indicate whether all of these systems have been fully documented and validated and confirm the existence of controlled system description documents as required by EU GMP A11 (4).
12.	A statement on the qualifications and training background of personnel engaged in design, coding, testing, validation, installation and operation of computerised systems, including consultants and sub-contractors, (specifications, job descriptions, training logs).
13.	State the firm's approach to assessing potential suppliers of hardware, software and systems.
14.	Specify how the firm determines whether purchased or "in-house" software has been produced in accordance with a system of QA and how validation work is undertaken.
15.	Document the approach that is taken to the validation and documentation of older systems where original records are inadequate.
16.	Summarise the significant computer system changes made since the last inspection and plans for future developments.
17.	Ensure that records relating to the various systems are readily available, well organised, and key staff are prepared to present, discuss and review the detail, as necessary.

Table 2
Software Related - Inspector's Aide Memoir[55]

Life Cycle Stage	Project Stage Activity	Evidence for Review
1. Development	Develop URS/FS/DS	URS/FS/DS Documents
1. Development	Plan Testing	Test plan and test scripts
1. Development	Plan documentation of Testing	Written document describing how testing should be documented.
2. Implementing	Select programming language and tools	Document recording programming choices
2. Implementing	Write/create software program.	Documented source code with comments; explanation of function; in-data and expected out-data for each structured module. How modules influence each other. If program is purchased, how is access to source code guaranteed?[56]
3. Testing (Modules)	Make sure each module only accepts allowed in-data and gives only allowed out-data. Testing should discover incorrect data and logic errors.	Sample reports from testing if possible. Has testing covered boundaries of limits and also the input of invalid data? Have all tests been documented? Have all errors/failures been followed up?
Testing (Integrated Modules).	Same type of tests but applied after integrating the modules.	Same kind of review of evidence. If the program is purchased, then validation proof needs to have been assessed by regulated user.
4. Maintenance	Correct errors, update versions when needed.	Formal routines and records for configuration management and change control. Regression testing and periodic evaluation (as a system goes through multiple changes over time)
5. Documentation	System documentation (including software) correct and updated.	User handbook, supporting SOPs, correct versions.
6. Re-validation.	Re-validate when changes are made to the program.	Changes are reviewed and decisions documented. Routines and records are in-place, scoped dependent on the size/complexity of the changes
7. Other matters	Alternative routines are put in place for system failure and training includes this.	The alternative routines are documented, including training records.

[55] Some of the details below are not relevant for COTS but it is necessary to have clearly defined the requirements for intended use and to have assessed the application's fitness for purpose.

[56] Under some circumstances, access to source code cannot be guaranteed. Regulated users are expected to have assessed the business risks and put in place contingency measures in the event of the business failure of the supplier.

Table 3
Computer System Validation Related – Inspector's Aide Memoir

Number	Element	Control Measure Checks
1.	Define	Is the system defined? What should it do? Is there a written validation plan? Are there full specifications? Are there written protocols? (Including acceptance criteria).
2.	Testing	Do the test records show that 'in' and 'out' data meets the specifications?
3.	Documented results	Are the results complete and documented?
4.	Verify correctness	Are data and documentation correct and complete? Have these been verified by the regulated user?
5.	Compare with Acceptance Criteria	Have competent responsible personnel carried out the validation and review work? Is this all documented?
6.	Conclusions	Are conclusions complete, meaningful and based on results? Are acceptance criteria fulfilled? Are there any conditional conclusions?
7.	Approval	Has approval been formally recorded? Was there any QA/QC involvement at the regulated user?
8.	On-going evaluation	What is the procedure to ensure on-going evaluation of the system? What are the change control procedures?

Table 4
Annex 11 – Inspector's Checklist

Point	Requirement	Inspector's Check/Comment
Personnel (1)	Key personnel/computer specialists co-operate.	
Personnel (1)	Project and user personnel are trained and any necessary experts are involved.	
Validation (2)	Life-cycle model; formal policy and procedures in place.	
System (3)	Influence of environment	
(4)	There is a written, up to date, detailed description of the system.	
(5)	Software has been produced according to a quality assured system.	
(6)	Checks of data and calculations built in.	
(7)	System tested and validated. Verified against previous/or manual system being replaced.	
(8)	Data entry and change only by authorised personnel. Password / security manage-ment.	
(9)	Critical data (GXP data) verified by a 2nd person, or by a validated electronic method.	
(10)	Audit trail for data entry and processing.	
(11)	Alterations to system and programs subjected to rigorous change controls, including re-validation and approvals.	
(12)	Printed copies of electronically stored data available if needed?	
(13) and GMP 4.9	Physical and logical protection of data. Information security management and change management.	
(14)	Data back up procedures; separate and secure media and locations.	
(15)	Alternative routine arrangements established in the event of system failure.	
(16)	Validated alternative arrangements (15) defined and documented. Records of failures and remediation exist.	
(17)	Records show the analysis of errors and corrective actions taken.	
(18)	Service level agreements or contracts in place for services provided by outside agencies for computerised systems at regulated user's sites.	
(19)	Responsibilities in chain of release of batches defined and linked to QP.	

Table 5
General Points for Inspectors To Consider On Inspection

Number	Area	Remember
1.	Personnel	Is there only one key person? (Dependence on only one person may be catastrophic).
2.	Organisation	Is management involved?
3.	Organisation	Is the Quality organisation involved?
4.	Data system	Early during the inspection, ask for a complete overview of the system(s) including flow of data.
5.	Data system	The use of 'parallel' systems may indicate 'grey' areas and potential system weaknesses.
6.	Validation	Has terminology actually been defined? Is it used correctly?
7.	Security	How is access controlled? Information Security Management?
8.	Maintenance	Is there a maintenance manual of each system detailing what to do on a periodic basis? (Daily, weekly, monthly etc). Are there corresponding records of compliance?
9.	Control of System	Routines for configuration management, and change control in place?
10.	Self-inspections	Are self-inspection routines in place?

Table 6
Overview of User Responsibilities (from GAMP 4 Table 7.1)[57]

Step	Task	Description
1.	Identify system	Each automated system should be assessed and GxP regulated systems identified.
2.	Produce URS	The URS should define clearly and precisely what the user wants the system to do, state any constraints, and define regulatory and documentation requirements.
3.	Determine validation strategy	
	• Risk Assessment	An initial Risk Assessment should be carried out during validation planning. Further assessments should be performed as specifications are developed.
	• Assessment of system components	System components should be assessed and categorized to determine the validation approach required. The output from this assessment will feed into the Validation Plan.
	• Supplier assessment	Suppliers should be formally assessed as part of the process of selecting a supplier and planning for validation. The decision whether to perform a Supplier Audit should be documented and based on a Risk Assessment and categorization of the system components.
4.	Produce Validation Plan	The Validation Plan should define the activities, procedures, and responsibilities for establishing the adequacy of the system. It typically defines what Risk Assessments are to be performed.
5.	Review and approve specifications, including the system description	The user should review and approve specifications produced by the supplier.
6.	Monitor development of system	The user should monitor development and configuration activities against an agreed plan.
7.	Review source code	The user should ensure that source code is adequately reviewed during system development.
8.	Review and approve test specifications	The user should review and approve test specifications prior to formal testing.
9.	Perform testing	The user may be involved in testing, as a witness during test execution, or as a reviewer of test results.
10.	Review and approve test reports	The user should approve the test reports and associated test results.
11.	Produce Validation Report	The Validation Report should summarize all deliverables and activities and provides evidence that the system is validated.
12.	Maintain System	Once the system has been accepted, the user should establish adequate system management and operational procedures.
13.	System Retirement	The user should manage the replacement or withdrawal of the automated system from use.

[57] Refer also to Section 15 for context (validation strategy for different systems).

25. REFERENCES FOR RELEVANT STANDARDS AND GMP GUIDES / CODES

(1) EU Annex 11 to the EU guidelines of Good Manufacturing Practice for Medicinal Products.

(2) Annex 11 to PIC/S Guide to Good Manufacturing Practice for Medicinal Products, Document PH 1/97 (Rev. 3), PIC/S Secretariat, 9-11 rue de Varembé, CH-1211 Geneva 20

(3) GAMP Guide for Validation of Automated Systems, GAMP4 (ISPE (GAMP Forum), 2001)

(4) Australian Code of GMP for Medicinal Products, August 2002.

(5) WHO Guideline for GMP for Manufacture of Pharmaceutical Products.

(6) Relevant CFR sections of the USFDA Register:

Hardware

21 CFR 211.63, 67, 68	
21 CFR Part 11	Electronic Records: Electronic Signatures

Software

21 CFR 211.68, 180, 188, 192	
21 CFR Part11	Electronic Records: Electronic Signatures

Quality System

21 CFR 820	Quality system regulation

GLP

21 CFR 58	Good laboratory practice for non-clinical laboratory studies

(7) ISO standards:

Quality management and quality assurance

ISO 9000-1	Part 1:	Guidelines for selection and use.
ISO 9000-3	Part 3:	Guidelines for the application of ISO9001:1994 to the development, supply, installation and maintenance of computer software. See also current Tick-IT Guide for construction, software engineering, assessment and certification (see ref. 12 re:BSI DISC London)

Quality Management and quality system elements

ISO 9004-1	Part 1:	Guidelines.
ISO 9004-2	Part 2:	Guidelines for Services .
ISO 9004-4	Part 4:	Guidelines for quality improvement.
ISO 10005:	1995	Quality management - Guidelines for quality plans.
ISO 10007:	1995	Quality management - Guidelines for Configuration Management

Life cycle management

ISO/IEC 12207:1995	Information Technology - Software Life Cycle processes
ISO/IEC 17799:2000	(BS 7799-1:2000) Information technology – Code of practice for information security management.

(8) IEEE Publications:

IEEE 729	Glossary of Software Engineering Terminology
IEEE 730	Quality Assurance Plan
IEEE 828	Software Configuration Management Plans
IEEE 829	Software Test Documentation
IEEE 830	Guide to Software Requirements Specification
IEEE 983	Guide to Software Quality Assurance Planning
IEEE 1012	Software Verification Plans
IEEE 1298	Software Quality Management System Part 1: Requirements

(9) British Standards:

BS 7799:	1999 “Information Security Management”, BSI DISC 389 Chiswick High Road, London W4 4AL (Tel:+44 181 995 7799 Fax:+44 181 996 6411 http://www.bsi.org.uk/disc)
BS 7799: 2000	Information technology – Code of practice for information management

(10) DISC BSI Guides

DISC PD 5000 series of ‘Codes for Electronic Documents and e-Commerce Transactions as Legally Admissible Evidence’ (including DISC PD 0008:1999 in Pt 1):

Pt 1	Information Stored Electronically
Pt 2	Electronic Communication and e-mail policy
Pt 3	Identity Signature and Copyright
Pt 4	Using Certification Authorities
Pt 5	Using trusted Third Party Archives

DISC PD 3002	Guide to BS 7799 Risk Assessment and Risk Management (ISBN 0 580 29551 6)
DISC PD 3005	Guide on the selection of BS 7799 controls (ISBN 0 580 33011 7)

(11) ‘Guidance for Industry, Part 11, Electronic Records; Electronic Signatures – Scope and Application’, US Dept. of Health and Human Services and all FDA Centers/ Offices, February 2003. (\\CDS029\CDERGUID\5505dft.doc) – draft guidance for comment.

26. SUGGESTED FURTHER READING

1. Good Computer Validation Practices – Common Sense Implementation [Stokes, Branning, Chapman, Hambloch & Trill. Interpharm Press, USA: ISBN: 0-935184-55-4]

2. Computer Systems Validation for the Pharmaceutical and Medical Device Industries [Chamberlain. ISBN 0-9631489-0-8].

3. Validating Automated Manufacturing and Laboratory Applications, [Wingate et al., Interpharm Press, USA: ISBN 1-57491-037-X]

4. Validation of Computerized Analytical Systems, Interpharm Press, L. Huber, ISBN: 0-935184-75-9, 1995

5. General Principles of Software Validation - Final Guidance for Industry and FDA Staff (FDA, CDRH, January 2002)

6. PDA Technical Report No 18, "Validation of Computer-Related Systems", PDA Journal of Pharmaceutical Science and Technology, 1995 Supplement, Vol. 49, No.S1

7. PDA Technical Report No. 32, "Report on the Auditing of Suppliers providing Computer Products and Services for Regulated Pharmaceutical Operations" (PDA, 1999)

8. 'Validation of Process Control Systems: a Guideline by GMA & NAMUR', in Section 5 of GAMP-3 (1998) Vol. 2, Best Practice for Users and Suppliers.

9. PDA Technical Report No. 31: "Validation and Qualification of Computerised Laboratory Data Acquisition Systems", PDA Journal of Pharmaceutical Science and Technology, 1999 Supplement, Vol. 53, No.4

10. Guidance for Industry - 'Computerized systems used in Clinical Trials', US FDA, April 1999

11. GLP Consensus Document 'The Application of the Principles of GLP to Computerised Systems', 1995, OECD/ OCDE/GD (95) 115 (Environment Monograph No.116)

12. Computer Systems Validation in Clinical Research, 1997, ACDM/ PSI Working Party. (ACDM, PO Box 129, Macclesfield, Cheshire SK11 8FG England)

13. ICH Topic E6: 'Guideline for Good Clinical Practice'. (ICH-GCP/CPMP/ICH/135/95)

14. EU GMP Guide Annex 15, 'Qualification and Validation', European Commission, July 2001, (based on PIC/S recommendations)

15. APV Guidance, Appendix 9 to GAMP4 'Guide for Validation of Automated Systems', ISPE (GAMP Forum), 2001

27. GLOSSARY OF TERMS

This glossary has been extracted predominantly from the (1) EU GMP Annex 15, Qualification and Validation document, [see 'Further Reading Ref:14]; (2) the GAMP Guide; and (3) the PDA Technical Report No 18. The list of definitions has been compiled to reflect the current terminology generally accepted internationally. Inspectors may have to correlate or adapt the terms in the light of internal policies, standards and guidelines used by regulated user's companies and relevant SDLC methodologies. The sources of each of the definitions have been identified in the following manner:

- EU GMP Annex 15 PIC/S document definitions are recorded as (1);
- GAMP definitions are recorded as (2);
- PDA technical report no. 18 definitions are recorded as (3);
- EC Directive 1999/93/EC on a Community framework for electronic signature, (Official Journal of the European Communities, 19.1.2000), (4);
- Definitions elaborated in this PIC/S document do not carry a suffix number.

Advanced Electronic Signature
(EU) means an electronic signature, which meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using means that the signatory can maintain under his control; and

(d) it is linked to the data to which it relates in such a manner that any change of the data is detectable. (4)

Application-Specific Software
A software program developed or adapted to the specific requirements of the application. (3)

Automated System
Term used to cover a broad range of systems, including automated manufacturing equipment, control systems, automated laboratory systems manufacturing execution systems and computers running laboratory or manufacturing database systems. The automated system consists of the hardware, software and network components, together with the controlled functions and associated documentation. Automated systems are sometimes referred to as computerised systems; in this Guide the two terms are synonymous. (2) (GAMP 4 (3) 'Scope' page 14)

Bespoke
A system produced for a customer, specifically to order, to meet a defined set of user requirements. (2)

Bug
A manifestation of an error in software (a fault). (2)

Change Control
A formal system by which qualified representatives of appropriate disciplines review proposed or actual changes that might affect a validated status of facilities, systems, equipment or processes. The intent is to determine the need for action that would ensure that the system is maintained in a validated state. (1)

[Authors note: FDA may specifically require evidence of pre and post implementation reviews of changes. The latter to detect any unauthorised changes that may have been made despite established procedures. These are quality assurance activities.]

Commercial off-the-shelf (COTS)
Configurable Programs- Stock programs that can be configured to specific user applications by "filling in the blanks", without (COTS) altering the basic program. (3)

Computer Hardware
Various pieces of equipment in the computer system, including the central processing unit, the printer, the modem, the cathode ray tube (CRT), and other related apparatus. (3) (See also Figure 1, page 8, of this document).

Computer System
Computer hardware components assembled to perform in conjunction with a set of software programs, which are collectively designed to perform a specific function or group of functions. (3) (See also Figure 1, page 8, of this document).

Computerised System
A computer system plus the controlled function that it operates. (3)

[Authors note: Today this may be considered to be rather a narrow definition, especially in the context of integrated computers. The definition should therefore include all outside influences that interface with the computer system in its operating environment. These may typically include monitoring and network links, (to/from other systems or instruments), manual (keypad inputs), links to different media, manual procedures and automation. The term also covers automated instruments and systems. See also the definition for 'automated systems' in this section and Section 26, Reference 11, the GLP OECD consensus document. PIC/S GMP Annex 11(4) is relevant here regarding documenting the scope and interaction of systems.]

Configuration
The documented physical and functional characteristics of a particular item, or system, e.g. software, computerised system, hardware, firmware and operating system. A change converts one configuration into a new one.

Configuration Management
The process of identifying and defining the configuration items in a system, controlling the release and change of these items throughout the system life cycle, recording and reporting the status of configuration items and change requests, and verifying the completeness and correctness of configuration items. (2)

Debugging (IEEE)
The process of locating, analysing, and correcting suspected faults. (2)

Electronic Signature
An electronic measure that can be substituted for a handwritten signature or initials for the purpose of signifying approval, authorisation or verification of specific data entries. See also definition for 'Advanced Electronic Signature', above.

Electronic Signature (FDA)
21 CFR Part11 defines this as: The computer data compilation of any symbol or series of symbols executed, adopted, or authorised by an individual to be the legally binding equivalent of the individual's hand-written signature.

Electronic Signature (EU)
1999/93/EC states: 'electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. (See also 'Advanced Electronic Signature') (4)

Embedded System
A system, usually microprocessor or PLC based, whose sole purpose is to control a particular piece of automated equipment. This is contrasted with a standalone computer system. (2)

Executive Program (ANSI/IEEE/ASO)
A computer program, usually part of the operating system, that controls the execution of other computer programs and regulates the flow of work in a data processing system. (2)

Firmware
A software program permanently recorded in a hardware device, such as an EPROM. (3) (Note: EPROM stands for 'Erasable Programmable Read Only Memory')

Functional Requirements (ANSI/IEEE)
Statements that describe functions a computer-related system must be capable of performing. (3)

Functional Specifications
Statements of how the computerised system will satisfy functional requirements of the computer-related system. (3)

Functional Testing
A process for verifying that software, a system, or a system component performs its intended functions. (3)

Hardware Acceptance Test Specification
Statements for the testing of all key aspects of hardware installation to assure adherence to appropriate codes and approved design intentions and that the recommendations of the regulated user have been suitably considered. (2)

Hardware Design Specification (APV)
Description of the hardware on which the software resides and how it is to be connected to any system or equipment. (2)

Hybrid Systems
Refer to Section '21.6' of this document

Integration testing (IEEE)
An orderly progression of testing in which software elements, hardware elements, or both are combined and tested until the entire system has been integrated. (2)

Interface (ANSI/IEEE)
A shared boundary. To interact or communicate with another system component. (2)

Legacy Computerised Systems
These are regarded as systems that have been established and in use for some considerable time. For a variety of reasons, they may be generally characterised by lack of adequate GMP compliance related documentation and records pertaining to the development and commissioning stage of the system. Additionally, because of their age there may be no records of a formal approach to validation of the system.

Life Cycle Concept
An approach to computer system development that begins with (PMA CSVC) identification of the user's requirements, continues through design, integration, qualification, user validation, control and maintenance, and ends only when commercial use of the system is discontinued. (2)

Loop Testing
Checking the installed combination of elements characterising each type of input/output loop. (2)

Network (ANSI/IEEE & GAMP)
(a) An interconnected, or interrelated group of nodes.
(b) An interconnected communications facility. A Local Area Network (LAN) is a high bandwidth (allowing a high data transfer rate) computer network operating over a small area such as an office or group of offices. (2)

Operating Environment
Those conditions and activities interfacing directly or indirectly with the system of concern, control of which can affect the system's validated state. (3)

Operating System
A set of software programs provided with a computer that function as the interface between the hardware and the applications program. (3)

Public Key Infrastructure
Public Key Infrastructure (PKI) provides a framework for secure communication, using a combination of public-key cryptography and Digital Certificates.
PKIs can exist within many different domains but essentially there are two types:
A Private PKI is deployed by a corporation for the benefit of its business and any related parties (e.g. customers, suppliers).
Public PKIs (using 'Trusted Third Parties') are deployed on open systems, such as the Internet and facilitate security between previously unrelated parties.

Raw Data[58]
Any work-sheets, records, memoranda, notes, or exact copies thereof, that are the result of original observations and activities and which are necessary for the reconstruction and evaluation of a work project, process or study report, etc. Raw data may be hard/paper copy or electronic but must be known and defined in system procedures. (2)

Regulated User
The regulated Good Practice entity, that is responsible for the operation of a computerised system and the applications, files and data held thereon. (See also 'User')

Revalidation
Repetition of the validation process or a specific portion of it. (2)

Security (IEEE)
The protection of computer hardware and software from accidental or malicious access, use, modification, destruction or disclosure. Security also pertains to personnel, data, communications and the physical protection of computer installations. (2)

Source Code (PMA CSVC)
An original computer program expressed in human-readable form (programming language), which must be translated into machine-readable form before it can be executed by the computer. (2)

Standalone System
A self-contained computer system, which provides data processing, monitoring or control functions but which is not embedded within automated equipment. This is contrasted with an embedded system, the sole purpose of which is to control a particular piece of automated equipment. (2)

Structural Integrity (Software)
Software attributes reflecting the degree to which source code satisfies specified software requirements and conforms to contemporary software development practices and standards. (3)

Structural Testing
Examining the internal structure of the source code. Includes low-level and high-level code review, path analysis, auditing of programming procedures and standards actually used, inspection for extraneous "dead code", boundary analysis and other techniques. Requires specific computer science and programming expertise. (2)

Structural Verification
An activity intended to produce documented assurance that software has appropriate structural integrity. (3)

---

[58] PIC/S Author's Note on 'Raw Data'- For information: FDA's 21 CFR Part 11 requires the retention of electronic records in electronic form (thus including raw data electronically captured or recorded). Also, for all good practice disciplines regulated by competent authorities it must be possible to reconstruct studies and reports from raw data and the electronic records may be needed to support any paper printouts.

System Acceptance Test Specification (2)
The system acceptance test specification is a description of those tests to be carried out to permit acceptance of the system by the user. Typically it should address the following:

- System functionality
- System performance
- Critical parameters
- Operating procedures

The tests should ensure that the product operates as indicated in the functional specification and meets the user requirements as defined in the URS. The tests typically include limit, alarms and boundary testing.

The System Acceptance Test Specification is a contractual document and, as such, should be approved by both the supplier/ developer/ integrator and the end user.
An example procedure for producing a System Acceptance Test Specification is given in a GAMP Guide Appendix.

System Software
Software designed to facilitate the operation and maintenance of a computer system and its associated programs, such as operating systems, assemblers, utilities, network software and executive programs. System software is generally independent of the specific application. (3)

System Specifications (PMA CSVC)
Describe how the system will meet the functional requirements. (2)

Unplanned (Emergency) Change (PMA CSVC)[59]
An unanticipated necessary change to a validated system requiring rapid implementation, also known as a "hot-fix". (2)

User
The company or group responsible for the operation of a system. (3) (see also 'Regulated User'). The GxP customer, or user organisation, contracting a supplier to provide a product. In the context of this document it is, therefore, not intended to apply only to individuals who use the system, and is synonymous with 'Customer'. (2)

Utility Software (ANSI/IEEE)
Computer programs or routines designed to perform some general support function required by other application software, by the operating system, or by system users. (2)

Validation of Computerised Systems
See text Section '14.2' for definition.

---

[59] This can be very risky. 'Fix' testing/ implementation work should ideally not be carried out initially in the live environment. All changes to the live validated system(s) must be subjected to the firm's change control, configuration management and validation procedural controls, to ensure compliance with GMP and the maintenance of a validated state.

28. ABBREVIATIONS USED IN THE DOCUMENT

ANSI: American National Standards Institute

APV: Arbeitsgemeinschaft für Pharmazeutische Verfahrenstechnik E.V.

BSI: British Standards Institute

DCS: Distributed Control System

DR: Design Review

DS: Design Specification

DQ: Design Qualification

EDP: Electronic Data Processing

EU: European Union

FDA: US Food and Drug Administration

FS: Functional Specification

GAMP: Good Automated Manufacturing Practice

GCP: Good Clinical Practice

GDP Good Distribution Practice

GLP: Good Laboratory Practice

GMP: Good Manufacturing Practice

GxP: Compliance requirements for all good practice disciplines in the regulated pharmaceutical sector supply chain from discovery to post marketing.

IEC: International Electrical Commission

IEEE; Institute of Electrical and Electronics Engineers, Inc.

IQ: Installation Qualification

ISMS Information Security Management System

ISO: International Standards Organisation

ISPE International Society for Pharmaceutical Engineering

LIMS: Laboratory Information Management System

LAN: Local Area Network

MRP: Materials Requirements Planning

MRP-II: Manufacturing Resource Planning

OQ: Operational Qualification

PDA: Parenteral Drug Association

PIC/S: Pharmaceutical Inspection Co-operation Scheme

PKI Public Key Infrastructure

PLC: Programmable Logic Controller

PQ: Performance Qualification

QMS: Quality Management System

R&D: Research and Development

SCADA: Supervisory Control And Data Acquisition

SLA: Service Level Agreement

SOPs: Standard Operating Procedures

URS: User Requirements Specification

VSR: Validation Summary Report (see footnote to Section '23.10')

WAN: Wide Area Network

29. REVISION HISTORY

Date	Version Number	Reasons for revision
1 July 2004	PI 011-2	➢ Added Revision History ➢ Changed Editor's co-ordinates
25 September 2007	PI 011-3	➢ Changed Editor's co-ordinates