EU GMP - Annex 11 Computerised systems	
Versione corrente	**Nuova versione per commenti (emessa 8 aprile 2008)**

Principle	**Principle**
	This annex applies to all forms of computerisation used in connection with regulated activities, including process control, documentation and data-processing systems. It also covers development, selection, validation and use of systems. For documentation, the requirements of GMP Chapter 4 shall also be considered.
The introduction of computerised systems into systems of manufacturing, including storage, distribution and quality control does not alter the need to observe the relevant principles given elsewhere in the Guide. Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality or quality assurance. Consideration should be given to the risk of losing aspects of the previous system which could result from reducing the involvement of operators.	The introduction of computerised systems into systems of manufacturing, (including storage, distribution, quality control) and other regulated GMP activities, does not alter the need to observe the relevant principles given elsewhere in the Guide. Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of product failure.
	The validation of computerised systems should enable both the manufacturing authorisation holder, 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 system(s).
	For proprietary systems, where the supplier will have completed the development lifecycle independently then, depending on the nature of the intended application, the manufacturing authorisation holder/ purchaser may need to assess the development/ validation evidence for the product at the supplier. (See also clauses 1, 2 and 6 below.)
	1. Risk Management
	1.1 Decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system in respect to its impact on product quality and safety as well as data security and integrity.

Personnel	**2. Personnel**
1. It is essential that there is the closest co-operation between key personnel and those involved with computer systems. Persons in responsible positions should have the appropriate training for the management and use of systems within their field of responsibility which utilises computers. This should include ensuring that appropriate expertise is available and used to provide advice on aspects of design, validation, installation and operation of computerised system.	2.1 It is essential that there is the closest co-operation between key personnel, such as users, system administrators, quality assurance and technical staff (both in-house and outsourced) involved with the development, validation, management and use of computerised systems. Persons performing such roles should have appropriate and documented qualifications, training, technical expertise, responsibilities and experience to carry out their assigned duties.
Validation	**3. Validation**
2. The extent of validation necessary will depend on a number of factors including the use to which the system is to be put, whether the validation is to be prospective or retrospective and whether or not novel elements are incorporated. Validation should be considered as part of the complete life cycle of a computer system. This cycle includes the stages of planning, specification, programming, testing, commissioning, documentation, operation, monitoring and modifying.	3.1 The manufacturing authorisation holder's quality management system will need to include policies and plans for the validation of computerised systems, together with up to date listings of systems and their GxP functionality. The validation status of each system should be clear from the Validation Schedule. The extent of validation necessary will depend on the type and complexity of the computerised systems and the manufacturing authorisation holder's documented risk assessments.[i] [ii]
	3.2 For the validation of bespoke or significantly customised computerised systems there should be a process 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, on-going support and retirement. (With regards to customised systems, the above described controls are required for customisation aspects and their impacts on the whole system)
	3.3 The validation documentation should cover all the relevant steps of the specific project life cycle with appropriate methods for measurement and reporting, (e.g. assessment reports and details of quality and test measures), as required. User requirements should be traceable throughout the validation process/ life cycle. Manufacturing authorisation holders 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.
	3.4 Validation documentation should include change control and error log records generated during the validation process.

	3.5 With regard to the testing phase of the validation process: ▪ Automated testing tools used for validation purposes should be assessed for their adequacy. ▪ Evidence of challenge testing should be included, particularly system parameter limits, data limits and error handling.
	3.6 In fitting with best practices for risk assessment and change management, the manufacturing authorisation holder should carry out periodic reviews of computerised systems to determine whether incremental change, system performance issues, or regulatory developments prompt further work to reconfirm validation or data integrity. Such reviews should include the current range of functionality, error logs, upgrade history, performance, reliability, security and validation status reports.
	3.7 Validation of database based/inclusive systems should include the following: ▪ Mechanisms for ensuring data integrity in terms of accuracy and reliability (e.g. macros for check of data logic; table field design etc) ▪ Provisions for data security (access control, views, and internal encryption mechanisms) ▪ Transaction control/protocols (particularly important with regard to distributed databases) ▪ Linkages between different databases (the software developed for linking different propriety databases) ▪ Recovery Mechanisms (recovery of a database to its consistent state after a failure) ▪ Load testing (to include the current needs and future growth of the database) ▪ Provisions for post-implementation monitoring of system's performance and growth of the database ▪ On line archiving of data where applicable

	3.8 Spreadsheets should be suitably checked for accuracy and reliability and stored in a manner which ensures the appropriate version control. The calculations should be secured in such a way that formulations are not intentionally or accidentally overwritten. The calculations should be executed with precision displayed on the screen or in reports. Formulations should also be protected from accidental input of in appropriate data type (e.g. text in a numeric field and or a decimal format into integer field).
System	**4. System**
	4.1 An **inventory**, or listing, of all computerised systems is essential. The inventory should mention the site and purpose of the computerised system. This list should indicate the risk assessed category of each system. Systems that have an influence on regulated activities need to be identified... Manufacturing authorisation holders will need to maintain records detailing the physical and logical arrangements and the infrastructure for controlled, secure environments, together with up to date written detailed descriptions of each system, data flows and interactions with other systems or processes. These should be treated as controlled documents.
4. A written detailed description of the system should be produced (including diagrams as appropriate) and kept up to date. It should describe the principles, objectives, security measures and scope of the system and the main features of the way in which the computer is used and how it interacts with other systems and procedures. 3. Attention should be paid to the siting of equipment in suitable conditions where extraneous factors cannot interfere with the system.	4.2 Current specifications should be available (including diagrams as appropriate). They should describe the required functions of the system, any modularity and their relationships, its interfaces and external connections, system boundaries, main inputs and outputs, main data types stored, handled or processed, any hardware and software pre-requisites, and security measures. Attention should be paid to the siting of computer hardware in suitable conditions where extraneous factors cannot interfere with the system operation.
	5. Software
5. The software is a critical component of a computerised system. The user of such software should take all reasonable steps to ensure that it has been produced in accordance with a system of Quality Assurance.	5.1 The software is a critical component of a computerised system. The user of such software should take all reasonable steps, to ensure that it has been produced in accordance with an appropriate system of Quality Assurance. The supplier of software should be qualified appropriately; this may include assessment and/ or audit.

	5.2 Computerised systems should be designed and developed in accordance with an appropriate quality management system. Documentation supplied with Commercial Off-The-Shelf products should be reviewed by manufacturing authorisation holders to check that user requirements are fulfilled.
	5.3 Quality system and audit information relating to suppliers or developers of software and systems implemented by the manufacturing authorisation holder should be made available to inspectors on request, as supporting material intended to demonstrate the quality of the development processes.
	6. Data
6. The system should include, where appropriate, built-in checks of the correct entry and processing of data.	6.1 The system should include, where appropriate, built-in checks for the correct, secure entry and processing of data, including data transcribed manually from other media, or systems e.g. laboratory notebooks, or reports from other systems or instruments, that are not directly interfaced with the computerised system. Data and document management control systems should be designed to ensure the integrity of data and irrefutable recording of the identity of operators (i.e. shared passwords are disallowed) entering or confirming data as well as the routing and source of data captured or received automatically. Critical systems should be designed and protected to ensure that data and files cannot be changed without appropriate authorisations and with immutable electronic logs recording changes made even at the highest level of access, such as System Administrator.
	7. User testing and the system's fitness for purpose
7. Before a system using a computer is brought into use, it should be thoroughly tested and confirmed as being capable of achieving the desired results. If a manual system is being replaced, the two should be run in parallel for a time, as a part of this testing and validation.	7.1 Before a new, replacement or upgraded computerised system is brought into use, it should have been thoroughly specified, documented, validated, tested and approved as per the foregoing sections of this annex. User staff should also have received documented effective training in the use of such systems (Annex 15 also provides some advice on user acceptance testing). When manual or pre-existing computerised systems are being replaced, it may be appropriate to undertake comparative 'parallel', or 'in-series' testing.

	8. Security
	8.1 Physical and/or logical controls should be in place to restrict access to computerised systems to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.
	8.2 Access to applications, folders, files and data should be controlled via the permissions detailed within the manufacturing authorisation holder's Information Security Management System (ISMS) (See Chapter 4 in the GMP Guide and also current PI011 from PIC/S).
8. Data should only be entered or amended by persons authorised to do so. Suitable methods of deterring unauthorised entry of data include the use of keys, pass cards, personal codes and restricted access to computer terminals. There should be a defined procedure for the issue, cancellation, and alteration of authorisation to enter and amend data, including the changing of personal passwords. Consideration should be given to systems allowing for recording of attempts to access by unauthorised persons.	8.3 Suitable methods, commensurate to the criticality of data, should be in place to deter and record unauthorised entry and/or or modifications of data. These methods may include time limiting logging, encryption, and re-entry of unique identifier for critical data.
	8.4 Within the ISMS there should be a defined procedure, that would enable tracking and where possible audit trailing for the issue/alteration, and cancellation of authorisation to system/application/data access.
	8.5 Mechanisms for the detection of attempts of unauthorised access, to the system, files and data should be considered based on a risk assessment so that appropriate action may be taken.
	9. Accuracy Checks
9. When critical data are being entered manually (for example the weight and batch number of an ingredient during dispensing), there should be an additional check on the accuracy of the record which is made. This check may be done by a second operator or by validated electronic means.	9.1 For critical data entered manually or transferred from another system (for example the weight and batch number of an ingredient during dispensing, or the keying in of laboratory data), there should be an additional check on the accuracy of the record which is made prior to further processing of these data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be evaluated in a risk assessment and as part of validation. (See also sections 7 to 9 above)
	9.2 If a computerised system controls a critical process (where criticality determination is based on the risk assessment, as documented by a manufacturing authorisation holder), an independent secondary check of critical parameters of such a process should be in place.

	10. Audit Trails
10. The system should record the identity of operators entering or confirming critical data. Authority to amend entered data should be restricted to nominated persons. Any alteration to an entry of critical data should be authorised and recorded with the reason for the change. Consideration should be given to building into the system the creation of a complete record of all entries and amendments (an "audit trail").	10.1 The system should enable the recording of the unique identity of operators entering or confirming critical data. Any entry or alteration of critical data should be authorised and recorded with the reason for the change. Consideration should be given to building into the system the creation of a complete record of all entries and amendments (a system generated "audit trail"). (See also sections 7 to 10 above and Chapter 4 (4.9)). Audit trails need to accurately reflect changes. (For example if a relevant electronic record is created using a number of data fields, all these data fields need to be linked within the audit trail. The aim is to know at any given time point what the information was.) Audit trails need to be available and convertible to human readable form.
	11. Signatures
	11.1 Electronic records may be signed electronically or by applying a hand-written signature to a printed copy of the record. This is only acceptable if all relevant meta-data is included in the printout. Electronic signatures and identification by biometric means are expected to: ▪ be legally equivalent to hand-written signatures, ▪ be linked to their respective record, ▪ include the time and date that they were applied.
12. For quality auditing purposes, it should be possible to obtain clear printed copies of electronically stored data.	11.2 Country specific national legislations may apply to the requirements and controls for electronic records and linked electronic signatures, or identities. Printed copies of electronically compiled and electronically signed documents should be traceable via printed links to the original electronic transaction. (See also section 20, below)
	12. Change control and configuration management
11. Alterations to a system or to a computer program should only be made in accordance with a defined procedure which should include provision for validating, checking, approving and implementing the change. Such an alteration should only be implemented with the agreement of the person responsible for the part of the system concerned, and the alteration should be recorded. Every significant modification should be validated.	12.1 Alterations to any component of a computerised system should only be made in accordance with a defined procedure within the manufacturing authorisation holder’s Change and Risk Management policies/procedures. These should include provision for the evaluation of the impact of the change on product quality and data and system integrity, scoping any necessary validation work, reporting, reviewing approving and implementing the change.

	13. Printouts
	13.1 Printouts of records must indicate if any of the data has been changed since the original entry. For complex systems it may also be necessary for inspectors to be able to access and study electronic systems records on-line (e.g. databases, chromatography, process control, etc.).
	14. Data Storage
13. Data should be secured by physical or electronic means against wilful or accidental damage, in accordance with item 4.9 of the Guide. Stored data should be checked for accessibility, durability and accuracy. If changes are proposed to the computer equipment or its programs, the above mentioned checks should be performed at a frequency appropriate to the storage medium being used.	14.1 Data should be secured by both physical and electronic means against wilful or accidental damage, in accordance with item '4.9' of the Guide and the manufacturing authorisation holder's information security management requirements. The storage media used should have been subjected to evaluation for quality, reliability and durability by or on behalf of the manufacturing authorisation holder. Stored data should be checked for accessibility, durability, readability and accuracy. The mechanism of checking should not present a risk to the current data on the system. If changes are proposed to the computer equipment or its programs, the above mentioned checks should be performed at a frequency appropriate to the storage medium being used. Access to data must be ensured throughout the retention period.
	15. Back Up; Migration; Archiving; Retrieval
14. Data should be protected by backing-up at regular intervals. Back-up data should be stored as long as necessary at a separate and secure location.	15.1 Regular backups of all relevant data should be done. Back-up data should be stored at a separate and secure location. Integrity and accuracy of back-up data should be checked during or on completion of the back-up process.
	15.2 If the system does not have a capacity to retain records for the period specified in chapter 4, then the data must be suitably archived. The archived data should be secured by physical and/or electronic means against wilful and/or accidental damage. This data should be checked for accessibility, durability, readability and integrity. If changes are made to the computer equipment or its programs, then the ability to restore the data should be checked.
	15.3 Backup, archiving, retrieval and restoration (recovery) practices need to be defined, tested and established in accordance with the manufacturing authorisation holder's QMS, ISMS and risk management requirements.

	16. Business Continuity
15. There should be available adequate alternative arrangements for systems which need to be operated in the event of a breakdown. The time required to bring the alternative arrangements into use should be related to the possible urgency of the need to use them. For example, information required to effect a recall must be available at short notice.	16.1 For the availability of computerised systems supporting critical regulatory or lifesaving processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be minimal and appropriate for a particular system. These arrangements should be adequately documented and tested.
	17. Incident Management
16. The procedures to be followed if the system fails or breaks down should be defined and validated. Any failures and remedial action taken should be recorded. 17. A procedure should be established to record and analyse errors and to enable corrective action to be taken.	17.1 System failures and data errors should be tracked, recorded, analysed and corrective actions should be implemented as appropriate. Any procedures to be followed if the system fails or breaks down should be defined and verified.
	18. Suppliers
18. When outside agencies are used to provide a computer service, there should be a formal agreement including a clear statement of the responsibilities of that outside agency (see Chapter 7).	18.1 When outside agencies, suppliers, or other parties are used to provide, install, configure, integrate, validate, maintain or modify a computerised system or related service or for data processing, there should be a formal agreement including a clear statement of the responsibilities of that outside body.
	18.2 As the holder of the Manufacturing Authorisation must ensure that the medicinal product(s) is fit for its intended use, the competence and reliability of a supplier are key factors when selecting a product or service provider. The need for a supporting audit should be based on a risk assessment (in respect to the system's impact on product quality and safety, as well as data security and integrity) to determine whether the computerised system has been designed and developed, and is maintained, in accordance with an appropriate quality management system. Ongoing technical support from suppliers should be documented in a written contract.

	19. Batch Release
19. When the release of batches for sale or supply is carried out using a computerised system, the system should allow for only a Qualified Person to release the batches and it should clearly identify and record the person releasing the batches.	19.1 When the release of batches for sale or supply is carried out using a computerised system, the system should allow for only a Qualified Person to certify the release of the batches and it should clearly identify and record the person releasing the batches. Any certification produced by computerised systems should be clearly cross-linked to the identity of the certifying person. Names should be clearly stated and transactions traceable for verification or audit purposes from both the electronic records and paper printouts- to time, date, context and identities (human or electronic source) for all GMP related transactions.

Further guidance on security considerations and risk management in regulated applications will be found in PIC/S publication PI011-1 (August 2003) 'Good practices for computerised systems in 'GxP' regulated environments' and in ISO 17799 'A code of practice for information security management'.

Industry best practice publications are available from ISPE (International Society of Pharmaceutical Engineers), PDA (Parenteral Drug Association),and other sources. PIC/S guidance on the validation of these systems and other matters will be found in PI011-1 'Good Practices for Computerised Systems in Regulated 'GxP' Environments'

In the context or electronic records the term 'written' means 'recorded, or documented on media, paper, electronic or other substrate'.

Tabella comparativa curata da:

ing. Sandro De Caris
Consulenze in Informatica e Qualità
Chairman GAMP Italia

Via Giardino, 60
40065 Pianoro (BO)
Tel 051 6516945
Fax 051 6516945
e-mail: sandro@decaris.it

Prima versione: 24 aprile 2008
Ultima revisione: 04 dicembre 2008